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
Operations and Maintenance - Passive Infrastructure

Reference ID: **TEL/Q4105,** Version **4.0**
NSQF Level **4.0**

Wireless Technician

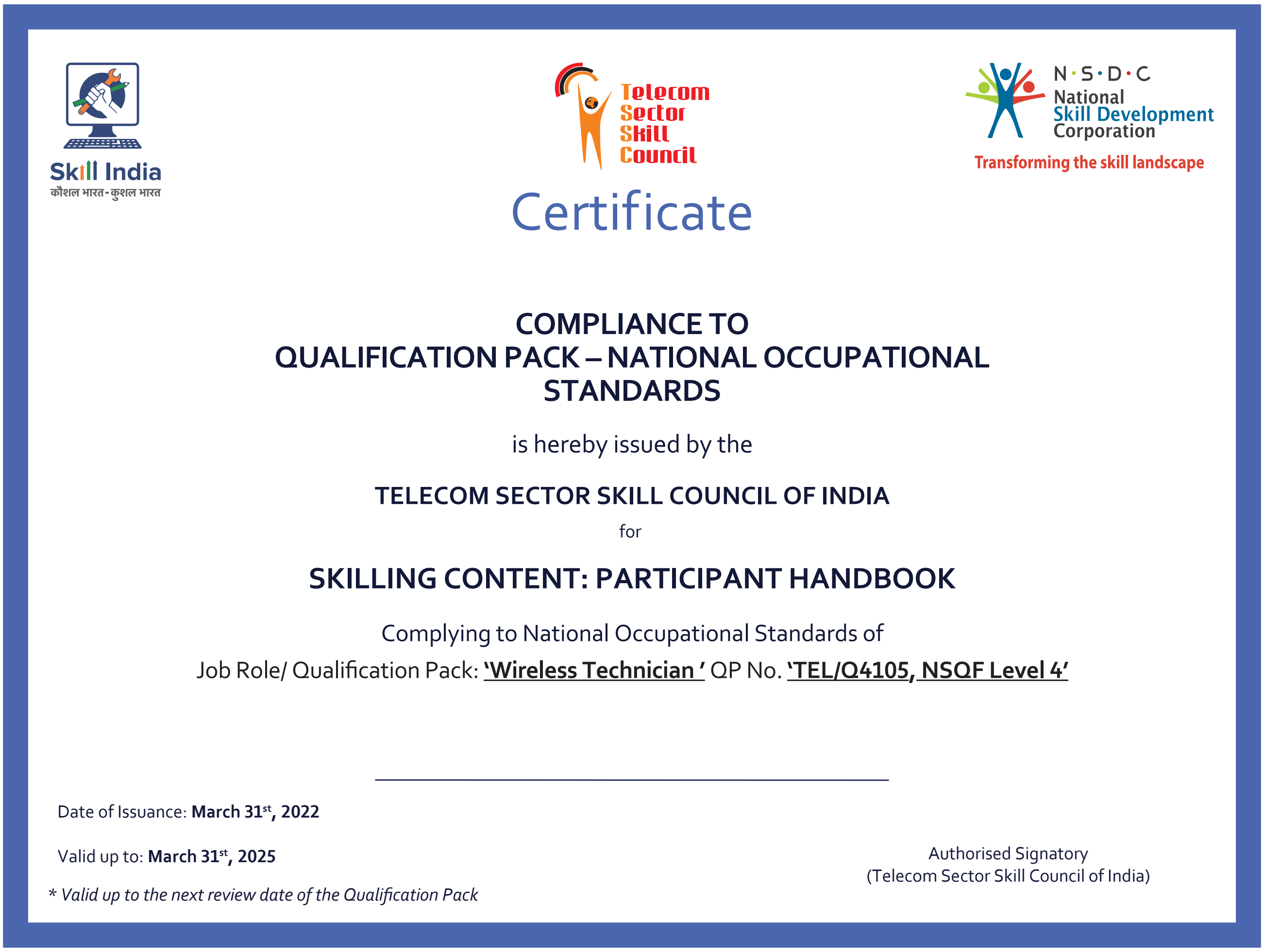
This book is sponsored by
Telecom Sector Skill Council
Estel House,3rd Floor, Plot No: - 126, Sector-44
Gurgaon, Haryana 122003
Phone: 0124-2222222
Email: tssc@tsscindia.com
Website: www.tsscindia.com

Disclaimer

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

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

Shri Narendra Modi
Prime Minister of India



Skill India
कौशल भारत-कुशल भारत

Telecom
Sector
Skill
Council

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

Certificate

COMPLIANCE TO QUALIFICATION PACK – NATIONAL OCCUPATIONAL STANDARDS

is hereby issued by the

TELECOM SECTOR SKILL COUNCIL OF INDIA

for

SKILLING CONTENT: PARTICIPANT HANDBOOK

Complying to National Occupational Standards of
Job Role/ Qualification Pack: **'Wireless Technician '** QP No. **'TEL/Q4105, NSQF Level 4'**

Date of Issuance: **March 31st, 2022**

Valid up to: **March 31st, 2025**

** Valid up to the next review date of the Qualification Pack*

Authorised Signatory
(Telecom Sector Skill Council of India)

Acknowledgments

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

The preparation of this handbook would not have been possible without the Telecom Industry's support. Industry feedback 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 that will be a lifelong asset for their future endeavours.

About this book

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

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

This Participant handbook is designed to impart theoretical and practical skill training to students for becoming Wireless Technician in the Telecom Sector.

Wireless Technician or the DT engineer is the person who is responsible for maintaining the networks functionality and efficiency

This Participant Handbook is based on Wireless Technician Qualification Pack (TEL/Q4109) and includes the following National Occupational Standards (NOSs):

1. TEL/N4122: Carry out installation and wiring of wireless communication equipment
2. TEL/N4123: Configure equipment and establish wireless network connectivity
3. TEL/N4124: Diagnose and rectify wireless network faults
4. TEL/N4125: Install, test, and maintain UPS and domestic power supply
5. TEL/N9105: Follow sustainable practices in telecom infrastructure installation
6. DGT/VSQ/N0102: Employability Skills (60 Hours)

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

Post this training, the participant will be able to manage the counter, promote and sell the products and respond to queries on products and services.

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

Symbols Used

Key Learning Outcomes

Unit Objectives

Exercise

Tips

Notes

Activity

Summary

Table of Contents

It is recommended that all trainings include the appropriate Employability skills Module. Content for the same is available here:
https://www.skillindiadigital.gov.in/content/list

सत्यमेव जयते
GOVERNMENT OF INDIA
MINISTRY OF SKILL DEVELOPMENT
& ENTREPRENEURSHIP

1. Introduction to the sector and the job role of a Wireless Technician

Telecom Sector Skill Council

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

TEL/N4122

Key Learning Outcomes

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

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

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

Unit Objectives

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

1. Discuss the Wireless Technician's responsibilities in deploying, maintaining, and troubleshooting wireless communication equipment.
2. Describe the key components of wireless network infrastructure, including antennas, access points, and backhaul equipment.
3. Identify different wireless technologies used in broadband connectivity, such as Wi-Fi, 5GHz backhaul, and fixed wireless access (FWA).
4. Elucidate the importance of wireless network performance metrics, such as signal strength, throughput, and interference, in service quality.
5. Explain the importance of communication skills in assisting with wireless equipment configuration, troubleshooting, and resolving connectivity issues.
6. Discuss safety protocols, grounding techniques, and PPE required for wireless equipment installation and maintenance tasks, including working at heights.
7. Describe the career advancement opportunities available for a Wireless Technician in the telecommunications industry.

1.1.1 Telecom Sector in India

The telecommunications sector in India is one of the most rapidly growing industries in the country. It has seen significant progress in the past two decades due to the implementation of various government policies and regulatory frameworks aimed at boosting the growth of the sector. The sector has played a critical role in shaping India's economy, driving innovation, and bringing people closer.

India's telecom sector is the second-largest in the world, with over 1.2 billion subscribers, second only to China. It comprises a wide range of services, including mobile, fixed-line, broadband, and satellite-based services. The sector is primarily dominated by private players, with a few state-owned companies operating in the market.

The telecom industry in India started in the 1850s with the establishment of the first telegraph line between Calcutta and Diamond Harbour. However, it was only after the liberalization of the Indian economy in the early 1990s that the sector started experiencing rapid growth. In 1994, the National Telecom Policy was introduced, which aimed to increase the availability of telecom services in the country, promote competition, and attract foreign investment.

The sector saw significant growth after the introduction of mobile services in 1995. With the entry of private players such as Bharti Airtel, Vodafone, and Idea Cellular, competition intensified, leading to a drop in prices and an increase in the number of subscribers. The government also implemented several policies to promote the growth of the sector, such as the New Telecom Policy in 1999, which aimed to create a level playing field for all players in the market.

The telecom sector in India has also been at the forefront of technological innovation. With the introduction of 3G and 4G services, mobile internet usage increased exponentially, leading to the development of various applications and services such as mobile wallets, e-commerce, and digital payments. The government has also launched various initiatives, such as Digital India, aimed at promoting the use of technology to deliver services to citizens.

With a 1.20 billion customer count (wireless + wireline users) as of June 2025, India's telecom sector is the second largest in the world. India has an overall teledensity of 86.09%, of which the rural market has a teledensity of 59.43%, and the urban market has a teledensity of 133.56%. The total gross revenue of the telecom sector in FY 2024–25 was approximately USD 46 billion, with adjusted gross revenue (AGR) of about USD 37 billion.

With 6.24% of all FDI inflows, the telecom sector ranks third in terms of FDI inflows and directly supports 2.2 million jobs while indirectly supporting 1.8 million jobs. In the telecom industry, 100% Foreign Direct Investment (FDI) is now permitted via the automatic route.

However, the sector has also faced several challenges, such as regulatory issues, spectrum availability, and the high cost of infrastructure development. The sector was also affected by the COVID-19 pandemic, which led to a decrease in revenue due to the economic slowdown and reduced mobility of people. Recently, the industry has experienced a plateau in wireless subscriber growth, although Average Revenue Per User (ARPU) has risen to ₹174.46 in FY 2024–25 due to tariff hikes.

Despite these challenges, the telecom sector in India is expected to continue growing in the coming years. The government has announced several initiatives, such as the National Broadband Mission, which aims to provide broadband access to all citizens, and the Production-Linked Incentive (PLI) scheme, which aims to boost domestic manufacturing of telecom equipment. With the growth of the sector, it is expected to play an even more significant role in shaping India's economy and society in the years to come.

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.

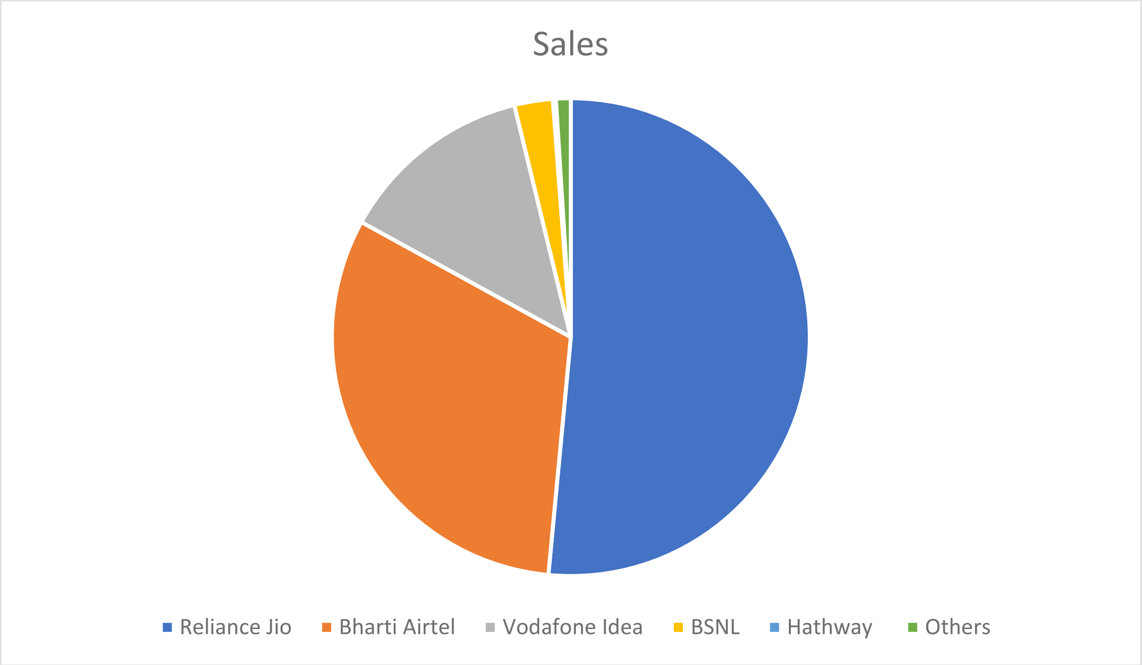


Fig 1.1.1: Market share of Wi-Fi broadband players in India

Source: https://pib.gov.in/

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 Role and Responsibilities of a Wireless Technician

A wireless technician is a professional responsible for installing, configuring, maintaining, and troubleshooting wireless networks and equipment. The roles and responsibilities of a wireless technician can vary depending on the organization they work for and the specific job requirements. However, some common responsibilities of a wireless technician may include the following:

- **Installing and configuring wireless networks:** Wireless technicians are responsible for installing and configuring wireless network equipment, including routers, access points, antennas, and other devices.
- **Conducting site surveys:** They may perform site surveys to determine the best location for wireless network equipment and to identify any potential issues that may affect network performance.
- **Troubleshooting network issues:** Wireless technicians must have strong problem-solving skills to troubleshoot network issues and resolve them quickly. They must be able to diagnose problems with network equipment, software, and network connectivity.
- **Testing and evaluating network performance:** Wireless technicians should test and evaluate network performance regularly to identify and resolve any issues that may impact network performance.
- **UPS Installation and Domestic Power Supply Checks:** Wireless technicians should also perform the installation of UPS and check the relevant electrical parameters at the site.
- **Providing technical support:** Wireless technicians may be responsible for providing technical support to end-users or other members of the organization.

1.1.4 Electrical and Electronic Components used for Wireless Installations

Wireless technicians use a variety of electrical and electronic components to install, configure, maintain, and troubleshoot wireless networks.

Antennas: An antenna is an electrical device designed to transmit or receive electromagnetic waves. It is usually a metallic structure or arrangement of conductors that converts electrical signals into electromagnetic waves (transmitting) or electromagnetic waves into electrical signals (receiving). Antennas are commonly used in communication systems such as radio, television, cellular telephony, and satellite communication. The shape, size, and design of an antenna depend on the frequency of the signal it is intended to send or receive and the specific application for which it is used.

Antennas are also used in scientific research, military applications, and other fields where the transmission and reception of electromagnetic waves are important. Antennas are used to transmit and receive wireless signals. Wireless technicians use different types of antennas, including omnidirectional antennas, directional antennas, and Yagi antennas, depending on the network requirements.

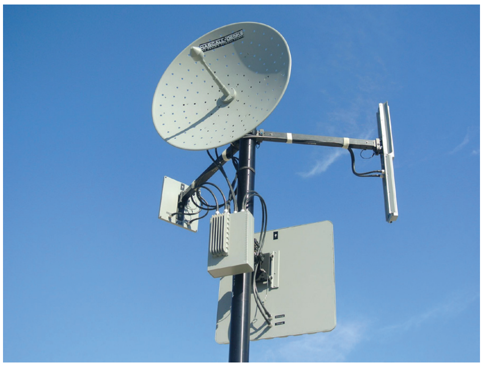


Fig 1.1.2: Directional Antenna

Transmitters and Receivers: Transmitters and receivers are used to send and receive wireless signals. They can be integrated into other devices or stand-alone components.

Amplifiers: Amplifiers are used to boost the signal strength of wireless transmissions. They can be used to increase the range of wireless networks or to improve signal quality.

Repeaters: Repeaters are used to extend the range of wireless networks by receiving and re-transmitting signals. They are often used in large buildings or outdoor areas to improve wireless coverage.

Fig 1.1.3: Fiber Optic Repeater

Power over Ethernet (PoE) Injectors: PoE injectors are used to power network devices such as wireless access points, IP cameras, and VoIP phones. They eliminate the need for separate power cables, making installation easier.

Fig 1.1.4: PoE Injectors

Routers and Switches: Routers and switches are network devices that are used to manage and direct data traffic on the wireless network. Routers connect multiple networks together and help to direct data packets to their intended destination. Switches are used to connect multiple devices together and to manage the flow of data between them.

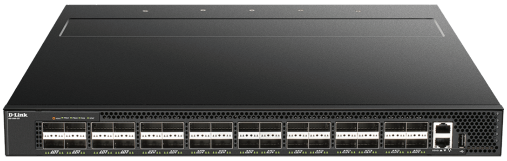


Fig 1.1.5: Network Switch

Surge Protectors: Surge protectors are used to protecting network equipment from power surges and lightning strikes. They can help prevent damage to network equipment and ensure that wireless networks remain operational.

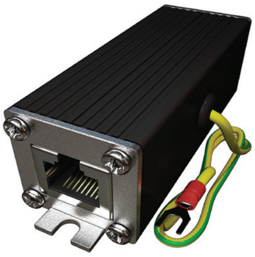


Fig 1.1.6: Ethernet Surge Protector

Cables: Coaxial and fibre-optic cables are used to transmit data and power to network devices. Coaxial cables are commonly used for short-distance connections, while fibre-optic cables are used for long-distance connections.

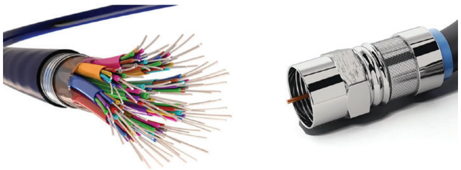


Fig 1.1.7: Fiber Optics Cable and Coaxial Cable

Ethernet Cables: Ethernet cables are used to connect network devices such as wireless access points, routers, and switches. They are available in different lengths and categories, such as Cat5e, Cat6, and Cat7.

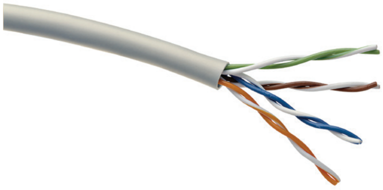
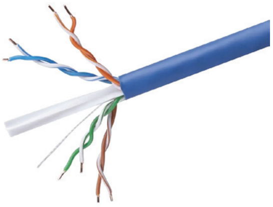
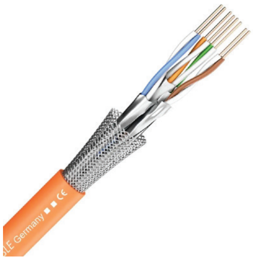
 **Cat5e**	 **Cat6**	 **Cat7**

Table 1.1.1: Categories of Ethernet cables

Power Supplies: Power supplies are used to provide power to network equipment. They can be integrated into devices or be stand-alone components.

Wireless Network Adapters: Wireless network adapters are used to connect devices to wireless networks. These adapters can be built-in or external and can connect to wireless networks using various standards, such as 802.11a/b/g/n/ac.

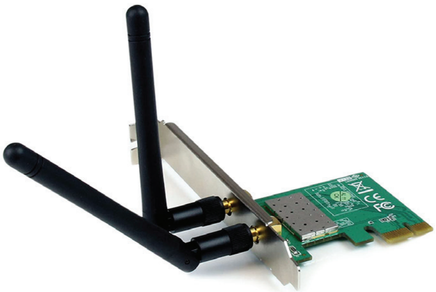


Fig 1.1.8: Wireless Network Adaptor (PCI)

1.1.5 Wi-Fi Broadband Technology

Wi-Fi broadband is a wireless networking technology that uses radio waves to provide high-speed internet connectivity to devices such as laptops, smartphones, and tablets. Wi-Fi broadband uses a set of technologies to ensure reliable and fast data transmission over wireless networks.

One example of Wi-Fi Broadband Technology is 802.11ac, also known as Wi-Fi 5. This is a wireless networking standard that operates in the 5 GHz frequency band and supports data transfer rates of up to 1.3 Gbps. It uses multiple antennas and advanced modulation techniques to provide faster and more reliable wireless connections than previous Wi-Fi standards.

An example of the installation process of Wi-Fi 5 is stated below

Pre-installation preparation

The technician will contact you to arrange a suitable installation date and time. They will also check the location and requirements for installation, including the type of router, modem, and any additional hardware needed.

Installing the modem

The technician will install the modem in a suitable location, such as near the telephone or cable outlet. They will then connect the modem to your internet service provider's network.

Installing the router

The technician will install the Wi-Fi 5 router in a central location within your home or office, ensuring that it is located away from any sources of interference, such as microwaves or other electronic devices.

Connecting devices

The technician will then connect any devices that you want to use with the Wi-Fi network, such as smartphones, laptops, or tablets, to the network.

Configuring the router

The technician will configure the router's settings, such as the Wi-Fi network name (SSID) and password, and ensure that the router is using the latest firmware version.

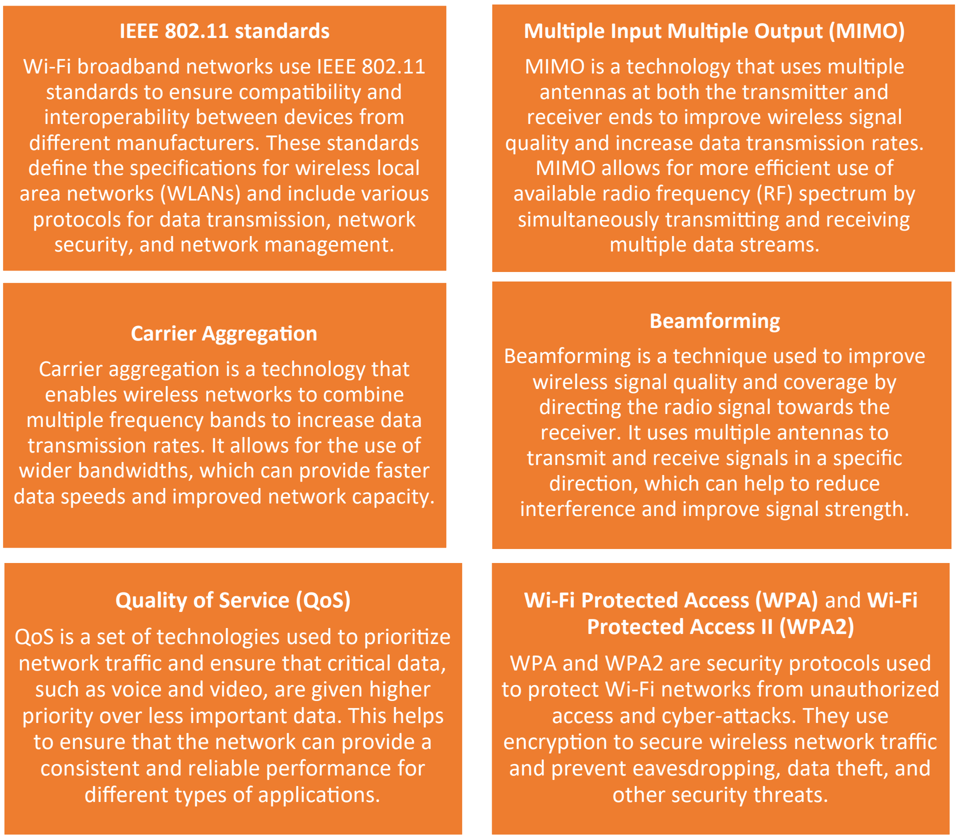
Testing the connection

Once the installation is complete, the technician will test the Wi-Fi network to ensure that it is working correctly and that all devices are able to connect to it.

Providing after-sales support

After the installation, the technician will provide you with any necessary information or documentation, such as the Wi-Fi network name and password, and provide you with contact information for after-sales support in case of any issues or concerns.

Some of the key technologies used in Wi-Fi broadband are:



IEEE 802.11 standards

Wi-Fi broadband networks use IEEE 802.11 standards to ensure compatibility and interoperability between devices from different manufacturers. These standards define the specifications for wireless local area networks (WLANs) and include various protocols for data transmission, network security, and network management.

Multiple Input Multiple Output (MIMO)

MIMO is a technology that uses multiple antennas at both the transmitter and receiver ends to improve wireless signal quality and increase data transmission rates. MIMO allows for more efficient use of available radio frequency (RF) spectrum by simultaneously transmitting and receiving multiple data streams.

Carrier Aggregation

Carrier aggregation is a technology that enables wireless networks to combine multiple frequency bands to increase data transmission rates. It allows for the use of wider bandwidths, which can provide faster data speeds and improved network capacity.

Beamforming

Beamforming is a technique used to improve wireless signal quality and coverage by directing the radio signal towards the receiver. It uses multiple antennas to transmit and receive signals in a specific direction, which can help to reduce interference and improve signal strength.

Quality of Service (QoS)

QoS is a set of technologies used to prioritize network traffic and ensure that critical data, such as voice and video, are given higher priority over less important data. This helps to ensure that the network can provide a consistent and reliable performance for different types of applications.

Wi-Fi Protected Access (WPA) and **Wi-Fi Protected Access II (WPA2)**

WPA and WPA2 are security protocols used to protect Wi-Fi networks from unauthorized access and cyber-attacks. They use encryption to secure wireless network traffic and prevent eavesdropping, data theft, and other security threats.

Fig 1.1.9: Technologies used in Wi-Fi Broadband

1.1.6 Importance of Communication Skills

Communication skills are crucial when assisting with wireless equipment configuration, troubleshooting, and resolving connectivity issues because they ensure technical solutions are delivered clearly, efficiently, and with minimal misunderstandings. Here's why they matter:

- Understanding User Needs – Good communication helps you actively listen to the user's description of the problem, ask clarifying questions, and gather the right details before starting troubleshooting.
- Explaining Technical Steps Clearly – Not all users are technically skilled. Strong communication allows you to explain complex configuration steps (e.g., SSID settings, encryption types, firmware updates) in simple, non-technical language.
- Efficient Troubleshooting Collaboration – When working in a team or with the end user remotely, clear and concise instructions help in performing real-time tests, checking signal strength, or resetting equipment without confusion.
- Preventing Misinterpretation – Poor communication can lead to incorrect configurations, wasted time, or even new technical issues. Using precise terms, confirming actions, and summarizing progress avoids such mistakes.
- Building Trust and Confidence – A calm, professional tone combined with empathy reassures the user, making them more cooperative during the troubleshooting process and improving customer satisfaction.
- Documenting and Reporting – Good written communication ensures that troubleshooting steps, findings, and resolutions are documented accurately for future reference or escalation to higher-level support.

1.1.7 Safety, Health and Environmental Regulations for Workplace

Safety, health, and environmental policies and regulations are crucial for the workplace and telecom sites to ensure the well-being of employees, customers, and the environment. Here are some examples of such policies and regulations:

- **Workplace Safety and Health:** Employers are required to provide a safe working environment for their employees. This includes ensuring that the workplace is free from hazards, providing appropriate safety equipment and training, and complying with local safety regulations. Employers are also required to have an emergency response plan in place in case of accidents or natural disasters.
- **Electrical Safety:** Telecom sites use high-voltage electrical equipment, and there are specific regulations in place to ensure the safety of employees who work with or near these devices. These regulations include requirements for electrical safety training, the use of personal protective equipment, and compliance with local and national electrical codes.
- **Environmental Regulations:** Telecom sites can have an impact on the environment, and there are regulations in place to ensure that these impacts are minimized.
    - **Environmental Impact Assessment (EIA):** Telecom sites must undergo an EIA to assess the potential environmental impact of their operations. The EIA report includes information on the site's location, the potential impact on local ecosystems, and measures to mitigate any adverse effects.
    - **Air Pollution Control:** Telecom sites must comply with local air pollution control regulations. This includes minimizing the release of pollutants such as dust, emissions from backup generators, and other sources that may contribute to air pollution.
    - **Noise Pollution Control:** Telecom sites must comply with local noise pollution control regulations. This includes minimizing the noise generated by backup generators, cooling systems, and other equipment.
    - **Hazardous Waste Management:** Telecom sites generate hazardous waste, such as batteries and electronic waste, and must comply with local regulations for their disposal. This includes the safe storage, transportation, and disposal of hazardous waste.
    - **Green Energy:** Telecom sites are encouraged to use renewable energy sources such as solar, wind, or hydropower to reduce their carbon footprint. The Indian government has introduced several schemes to promote the use of green energy in telecom sites.
    - **Biodiversity Conservation:** Telecom sites must take measures to protect local biodiversity, such as planting trees and maintaining green cover. They must also take care not to disturb local ecosystems, including wildlife and water bodies.

- **Radiofrequency (RF) Radiation:** Telecom sites use RF radiation to transmit wireless signals, and there are regulations in place to ensure that this radiation does not exceed safe limits. Employers are required to provide appropriate safety training and protective equipment to employees who work with RF radiation, and there are limits on the amount of RF radiation that can be emitted by telecom equipment.
- **Occupational Health:** Employers are required to provide a healthy working environment for their employees. This includes providing appropriate medical and first aid facilities, providing access to health and wellness programs, and complying with local health regulations.

1.1.8 Career Enhancement Opportunities for a Wireless Technician

Career advancement opportunities for a Wireless Technician in the telecommunications industry are diverse, as the role builds both technical expertise and problem-solving skills. Some key pathways include:

- Senior Wireless Technician / Lead Technician – Taking on more complex projects, mentoring junior staff, and overseeing large-scale wireless installations and maintenance.
- Network Engineer / Wireless Network Engineer – Specializing in designing, implementing, and optimizing wireless networks, including enterprise Wi-Fi, 4G/5G infrastructure, and IoT connectivity.
- Field Service Supervisor / Manager – Leading technical teams, managing field operations, ensuring compliance with safety and quality standards, and coordinating with clients.
- RF (Radio Frequency) Specialist – Focusing on frequency planning, interference management, and performance tuning for mobile and wireless systems.
- Technical Support or NOC (Network Operations Center) Specialist – Monitoring network performance, troubleshooting large-scale outages, and ensuring high uptime for telecom services.
- Project Manager – Telecom – Overseeing end-to-end deployment of wireless projects, from site surveys to commissioning, with responsibility for budgets, timelines, and stakeholder communication.
- Specialization in Emerging Technologies – Moving into areas like 5G deployment, satellite internet systems, private LTE networks, and smart city wireless infrastructure.

Summary

- The telecom sector in India has experienced significant growth in recent years, with the number of wireless subscribers surpassing 1 billion and the introduction of 4G technology.
- The future of Wi-Fi broadband in India is promising, with increasing demand for high-speed internet and government initiatives such as Digital India and BharatNet promoting the expansion of broadband infrastructure.
- A wireless technician is responsible for the installation, maintenance, and repair of wireless communication systems, including equipment such as antennas, transmitters, and receivers.
- Various electrical and electronic components are used in wireless installations, including cables, connectors, amplifiers, and power supplies.
- Wi-Fi broadband uses a variety of technologies, including 802.11 standards, frequency bands, and modulation techniques, to provide high-speed wireless internet access.
- Workplace safety, health, and environmental policies and regulations are important considerations for wireless technicians, as they may be exposed to hazards such as electromagnetic radiation and electrical shock. Proper training and protective equipment can help mitigate these risks.

Exercise

Multiple Choice Questions:

1. What are the responsibilities of a Wireless Technician?

   a. Installation of Wi-Fi broadband
   b. Troubleshooting connectivity issues
   c. Configuring network settings
   d. All of the above

2. Which of the following is an electronic component used in Wi-Fi broadband technology?

   a. Transistor
   b. Capacitor
   c. Inductor
   d. All of the above

3. What is the scope of Wi-Fi broadband technology?

   a. Limited to residential use only
   b. Used for internet connectivity in commercial and public spaces
   c. Limited to certain geographical regions only
   d. None of the above

4. What technology is used in the installation of Wi-Fi broadband?

   a. Fiber optics
   b. Microwave technology
   c. Wi-Fi routers
   d. All of the above

5. What is the future of Wi-Fi broadband technology?

   a. Decreasing demand due to advancements in 5G technology
   b. Increasing demand due to remote work and online education
   c. . Only applicable in developed countries
   d. . None of the above

Descriptive Questions:

1. What are the key responsibilities of a Wireless Technician in the telecommunications industry?
2. Describe the various electrical and electronic components used in Wi-Fi broadband technology and their specifications.
3. Discuss the scope and future of Wi-Fi broadband technology.
4. What safety, health, and environmental policies and regulations should be followed at telecom sites?
5. What are the pre installation preparations that are conducted during setting of broadband?

Notes

Scan the QR codes or click on the link to watch the related videos

https://www.youtube.com/watch?v=tha-DJhkih8

Telecom Sector in India

https://www.youtube.com/watch?v=x3c1ih2NJEg

How does the INTERNET work?

https://www.youtube.com/watch?v=cppHX2bMjEc

Technical Support Jobs

https://www.youtube.com/watch?v=6UTOTgbJ_8E

Basic Electronic components

https://www.youtube.com/watch?v=IZVxBlX18Dw

Environment, Health & Safety (EHS) Effectiveness

सत्यमेव जयते
GOVERNMENT OF INDIA
MINISTRY OF SKILL DEVELOPMENT
& ENTREPRENEURSHIP

2. Installation and Wiring of Wireless Communication Equipment

Unit 2.1 - Installation of Wi-Fi System

Unit 2.2 - Complete Documentation

TEL/N4122

Key Learning Outcomes

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

1. Describe the procedures for preparing, wiring, and installing a wireless communication system.
2. Explain the methods for conducting quality checks and performance testing on installed wireless equipment.
3. Discuss the steps involved in completing documentation and site cleanup after a wireless network installation.

UNIT 2.1: Installation of Wi-Fi System

Unit Objectives

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

1. Describe industry standards, policies, and best practices for wireless equipment installation and structured cabling.
2. Explain different cable types and their respective connectors.
3. Discuss safety procedures for working at heights, handling electrical installations, and preventing hazards.
4. Describe structured cabling guidelines, including PoP setup, cable routing, and cable management techniques.
5. Determine methods of obtaining and handling installation materials, tools, and equipment at various sites.
6. Explain transmission loss testing methods, power level verification, and troubleshooting techniques.
7. Discuss basic Wi-Fi network principles, including signal propagation, interference, and coverage optimization.
8. Describe firmware updates, basic configurations, and network connectivity checks for wireless devices.
9. Demonstrate how to review and interpret installation plans, site layouts, and job specifications.
10. Show how to coordinate with superiors and site personnel to confirm job requirements and site access.
11. Demonstrate how to select and collect appropriate tools, equipment, and materials as per installation plans.
12. Show how to identify and use suitable cables and connectors based on site requirements.
13. Demonstrate how to measure and verify cable lengths, ensuring continuity and optimal performance.
14. Show how to inspect cable routes for electrical hazards, environmental constraints, and obstructions.
15. Demonstrate how to liaise with local authorities and comply with regulatory requirements for outdoor installations.
16. Show how to determine optimal installation locations adhering to structured cabling norms and signal coverage guidelines.
17. Demonstrate how to ensure systematic and organized wiring from Point of Presence (PoP) to designated sites.
18. Show how to secure and route cables neatly using appropriate clips, trays, and conduits.
19. Demonstrate how to install, terminate, and test feeder cables and connectors, ensuring minimal transmission loss.
20. Show how to mount equipment securely following manufacturer guidelines and electrical safety standards.
21. Demonstrate how to implement proper grounding and earthing techniques for system safety and reliability.

22. Show how to conduct initial equipment setup, firmware updates, and basic configuration as required.
23. Demonstrate how to test cable connectivity, transmission loss, and signal strength using appropriate testing tools.
24. Show how to re-terminate cables if the transmission loss exceeds prescribed limits.
25. Demonstrate how to verify power supply, grounding, and voltage levels to prevent equipment damage.
26. Show how to configure and test Wi-Fi backhaul and access point connectivity for seamless operation.
27. Demonstrate how to troubleshoot and rectify basic connectivity issues and escalate unresolved issues.
28. Show how to dispose of installation waste materials as per environmental and workplace safety guidelines.

2.1.1 Analysing Work Orders and Job Sheets

A job-sheet provides detailed instructions on what needs to be done, including the type of equipment that needs to be installed, the cabling and wiring required, and any other specifications that need to be followed.

Technicians and other workers typically use the job sheet to complete the job correctly and efficiently. It may also include information about the materials and tools needed to complete the job and any safety precautions that need to be taken. Once the job is completed, the job sheet is usually used to document the work done and any issues that were encountered.

As an Wireless Technician, my primary responsibility is to support the installation and maintenance of wireless communication equipment. Analyzing work orders and job sheets is important because it provides the necessary information to complete the assigned tasks correctly and efficiently.

Here are the steps an Wireless Technician may take to analyze work orders and job sheets:

- **Review the Work Order:** The first step is to review the work order to understand the scope of work, the location of the site, and the type of equipment that needs to be installed or serviced. This helps the technician to plan the work and gather the necessary equipment and tools.
- **Identify the Job Requirements:** Once the technician has reviewed the work order, they will then analyze the job sheet to identify the job's specific requirements. This includes the type of equipment that must be installed, the cabling and wiring required, and any other specifications that must be followed.
- **Plan the Work:** Based on the information gathered from the work order and job sheet, the technician will then plan the work to be done. This includes identifying the required tools and equipment, scheduling the work, and estimating the time required to complete the job.
- **Prepare the Site:** Before beginning any work, the technician will prepare the site by ensuring that it is safe to work on. This includes checking for any potential hazards, such as electrical wiring, and ensuring that the area is clear of debris.
- **Perform the Work:** With the site prepared, the technician will then begin the work, following the instructions provided in the job sheet. This may include installing or repairing equipment, testing the system, and ensuring that everything is working correctly.
- **Document the Work:** Finally, the technician will document the work done by completing the job sheet with all the necessary information, including any problems encountered, any additional work required, and any parts used.

2.1.2 Wi-Fi Backhaul

Wi-Fi backhaul is a term used to describe the process of using wireless networking technology to connect one or more access points to a wired network, usually the internet. Backhaul refers to the connection that carries data between the access points and the network infrastructure in a Wi-Fi network.

For example, in a Wi-Fi network that provides internet access in a public space, such as a park or shopping center, multiple access points may be deployed to provide coverage across the entire area. These access points are connected to the internet via a wired connection, usually provided by an internet service provider (ISP).

The connection between the access points and the ISP is the backhaul connection, and it can be achieved using various wireless technologies, such as Wi-Fi, microwave, or satellite. The backhaul connection must be fast and reliable to ensure that the network can handle high volumes of data traffic and provide a seamless user experience.

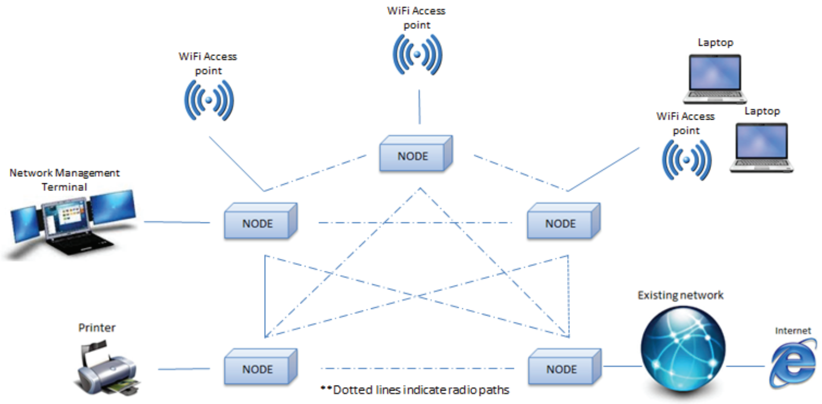


Fig. 2.1.1: Wi-Fi Backhaul

In summary, Wi-Fi backhaul refers to the process of using wireless networking technology to connect Wi-Fi access points to a wired network, such as the internet. It is an essential component of modern Wi-Fi networks, allowing users to access the internet from any location within range of the network.

2.1.3 Cables, Connectors, Tools and Equipment Required for Installation

Cables

Several types of cables, connectors, tools, and equipment are required to install, configure, and test Wi-Fi backhaul equipment (5 GHz) and Wi-Fi access points (2.4 GHz) for broadband access. Here are some of the most commonly used items:

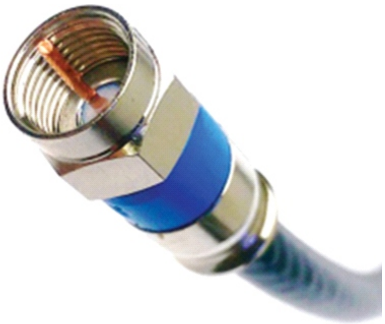


Fig. 2.1.2: Coaxial Cable

1. **Coaxial Cables:**
    - Purpose: Carry high-frequency RF signals between antennas, access points, and radio equipment.
    - Common Types: RG-6, RG-58, LMR-400.
    - Connectors: N-type connectors (common for outdoor antennas), SMA and RP-SMA connectors (used for access points and wireless cards), BNC connectors (in some specialized setups).

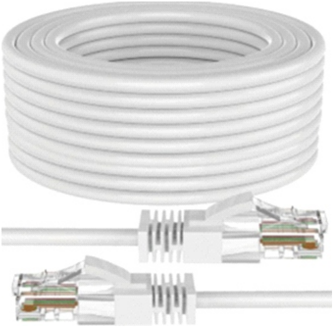


Fig. 2.1.3: Ethernet Cable

2. **Ethernet (Twisted Pair) Cables:**
    - Purpose: Connect Wi-Fi access points, routers, and switches to the network; also used for Power over Ethernet (PoE).
    - Common Types: Cat5e, Cat6, Cat6a (shielded or unshielded).
    - Connectors: RJ-45 connectors (standard for Ethernet cabling).

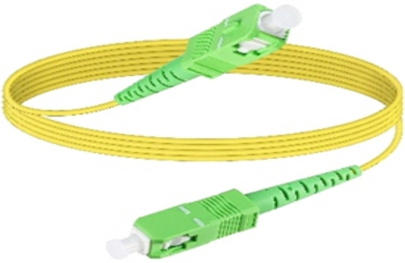


Fig. 2.1.4: Fiber Optic Cable

3. **Fiber Optic Cables:**
    - Purpose: Used in backbone connections where high bandwidth and long-distance transmission are required, such as between network distribution points feeding Wi-Fi access points.
    - Common Types: Single-mode (SMF) and multi-mode (MMF).
    - Connectors: SC, LC, ST connectors (depending on equipment).

Fig. 2.1.5: USB Cable

4. **USB Cables**
    - Purpose: Connect certain Wi-Fi adapters or test instruments to computers.
    - Common Types: USB 2.0, USB 3.0 cables.
    - Connectors: USB-A, USB-B, USB-C, Micro-USB depending on device.

Connectors

1. **SMA Connector:** SMA connectors are commonly used to connect the antennas to the Wi-Fi backhaul equipment. These connectors are designed to maintain a constant impedance across the connection, which is essential for transferring high-frequency signals.

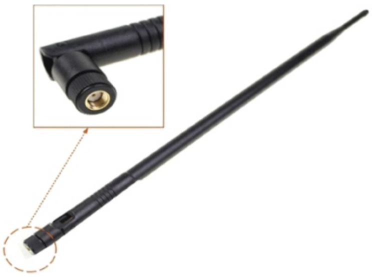
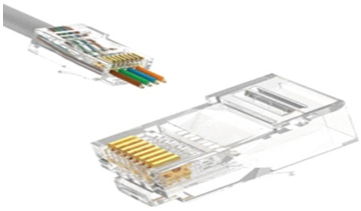


Fig. 2.1.6: SMA Connector

2. **RJ45 Connector:** RJ45 connectors are used to terminate Ethernet cables. These connectors are designed to maintain a secure and reliable connection between the cable and the network device.



Fia. 2.1.7: RJ45 Connector

3. **N-Type Connector:** A large, threaded RF connector designed for outdoor use; weather-resistant and supports high-frequency signals.

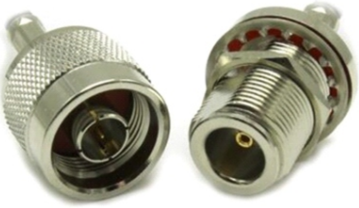


Fig. 2.1.8: N-Type Connector

Tools

1. **Cable Crimper:** A cable crimper is used to attach the connectors to the cables. This tool helps ensure a secure and reliable connection between the cable and the connector.

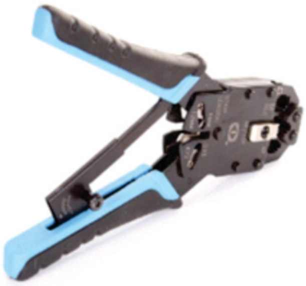


Fig. 2.1.9: Cable crimper

2. **Mounting hardware:** Depending on the installation location, mounting hardware may be required to secure the antennas and radio units in place
3. **Cable Tester:** A cable tester is used to check the connectivity of the cables. This tool helps ensure that the cables are properly terminated and are transmitting data correctly.

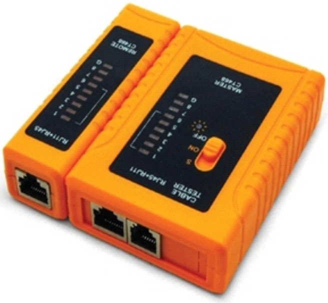


Fig. 2.1.10: Cable tester

4. **Power Meter:** A power meter is used to measure the power output of the Wi-Fi backhaul equipment. This tool helps ensure that the equipment is operating within the desired power range.

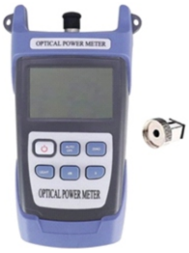


Fig. 2.1.11: Power Meter

Equipment

1. **Wi-Fi Backhaul Equipment: This includes:**
   - **Wi-Fi access points:** These are the devices that provide wireless connectivity to the network. They can be standalone devices or built into routers or modems.

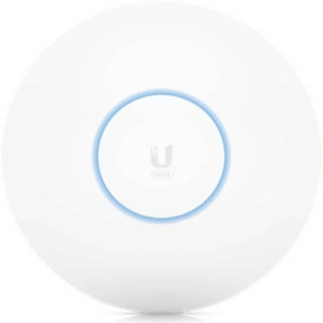


Fig. 2.1.12: Wireless Access Point

2. **Power over Ethernet (PoE) injectors or switches:** These are devices that can power the access points over the same Ethernet cable that is used for data transmission.

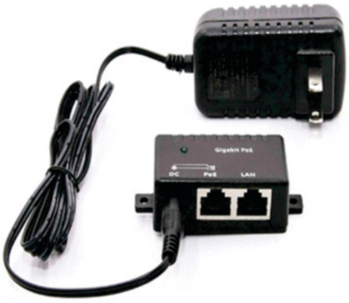


Fig. 2.1.13: POE Injector

3. **Network switch or router:** This is the device that connects all of the access points and provides connectivity to the internet.

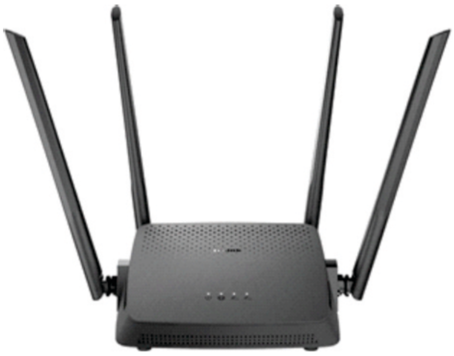


Fig. 2.1.14: Router

4. **Broadband Modem:** The broadband modem is required to connect the Wi-Fi backhaul equipment to the internet.

Fig. 2.1.15: Modem

5. **Antennas:** Antennas are used to boost the signal strength of the Wi-Fi backhaul equipment. They come in different types, such as omni-directional and directional, and can be used to provide coverage to different areas.

Fig. 2.1.16: Antenna

2.1.4 Steps to Obtain Cables/Equipment from the Company

Step 1: Determine what cables and equipment you need: Before you can request cables and equipment from the company, you should first determine what specific items you need. Make a list of the cables and equipment required to complete your project or task.

Step 2: Contact the company: Once you have determined the specific cables and equipment needed, contact the company responsible for providing these items. This could be your employer, an IT department, or a third-party supplier. You can typically reach out to the company via phone, email, or online contact form.

Step 3: Provide detailed information: When you contact the company, provide them with detailed information about the cables and equipment you need. Be specific about the type, quantity, and any other relevant information. If you are unsure about the specific items you need, the company may be able to provide guidance or recommendations.

Step 4: Verify availability and pricing: Once you have provided the company with the specific items you need, they will likely check their inventory to determine availability. They may also provide you with pricing information for the cables and equipment. If the items are not immediately available, they may be able to provide an estimated delivery date.

Step 5: Place the order: If the cables and equipment are available and you are satisfied with the pricing, you can place the order. You will likely need to provide payment information and a shipping address.

Step 6: Receive the cables and equipment: After the order is placed and processed, you will receive the cables and equipment. Depending on the company's policies and shipping methods, this could take anywhere from a few days to a few weeks.

Step 7: Test the cables and equipment: Before using the cables and equipment, it is important to test them to ensure they are functioning correctly. This can help identify any defects or issues early on, which can prevent delays or other problems down the line.

2.1.5 Feeder Cable Laying

Feeder cable laying refers specifically to the installation of cables for telecommunications and networking systems, such as Wi-Fi systems or cellular networks. Feeder cables are typically used to connect the core network infrastructure, such as switches or base stations, to the access points or end-user devices. Feeder cable laying may involve specialized techniques and equipment, such as fiber-optic splicing equipment or specialized cable trays, to ensure that the cable is installed and protected properly.

The following steps describe a general process of cable laying:

- **Planning:** The planning stage is critical to the success of the cable laying process. A detailed plan should be created that considers factors such as the type of cables to be laid, the distance they need to cover, the terrain they will pass through, the equipment needed, and any permits or permissions that may be required. The plan should also consider potential obstacles, such as existing infrastructure, water bodies, or other physical barriers, and identify solutions to overcome them.
- **Site Preparation:** Once the plan is in place, the site where the cables will be laid must be prepared. This involves clearing the ground of debris or obstacles, marking out the route for the cable, and excavating trenches or channels for the cable to be laid in. The width and depth of the trench or channel will depend on the cable's type and size.
- **Laying the Cable:** The next step is to lay the cable in the trenches or channels. This may involve feeding the cable through conduits or ducts, pulling it along a path, or using specialized equipment such as cable plows or trenchers. The cable should be laid straight and secured in place, avoiding any sharp bends or kinks that could damage the cable or affect its performance. Care must be taken to avoid damaging the cable or interfering with any existing utility lines or infrastructure.
  - **Cable Feeding:** The first step in cable laying is feeding the cable through any conduits or other obstacles that are present in the cable route. This may involve attaching the cable to a pulling rope or cable, then using a winch or other pulling equipment to draw it through the conduit or other obstacle.
  - **Cable Pulling:** Once the cable is fed through the conduit, the pulling process can begin. This may involve using a specialized cable pulling equipment such as a cable puller or winch to pull the cable along the prepared route. This equipment is typically operated by trained personnel who are familiar with the cable pulling process.
  - **Cable Plowing:** In some cases, cable plowing equipment may be used to install the feeder cable. Cable plows are specialized machines that create a channel in the ground and simultaneously lay the cable into the channel. This method can be faster and more efficient than traditional cable pulling techniques, especially in areas with soft soil or where trenching is not feasible.

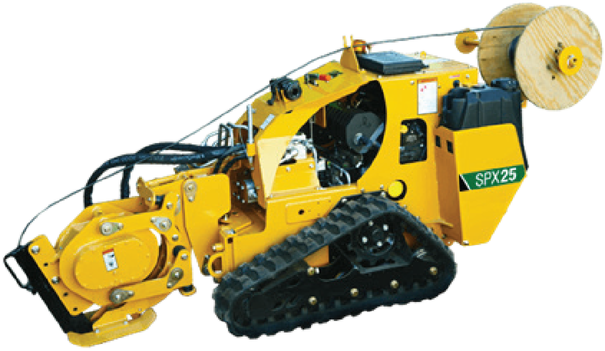


Fig. 2.1.17: Cable Plowing Machine

  - **Cable Protection:** During cable laying, it is important to take steps to protect the cable from damage. This may involve placing warning tape over the cable to indicate its location, or using cable markers to indicate its depth below the surface. Additionally, in areas where the cable may be exposed to hazards such as water or sharp objects, protective sheaths or sleeves may be used to minimize the risk of damage.
  - **Cable Splicing:** In some cases, it may be necessary to splice two or more sections of cable together during the laying process. This may be done in the field by trained personnel using specialized splicing equipment. Splicing must be done carefully to ensure that the connection is strong and reliable and does not affect the cable's signal transmission properties.

- **Cable Tension:** The feeder cable must be properly tensioned during installation to prevent sagging or damage to the cable due to excessive tension. The appropriate tension level will depend on the type of cable being installed, as well as the distance and elevation changes that the cable must span.

After the feeder cable is laid, the connectors and accessories are installed to prepare the cable for connection to the wireless network equipment. The connectors and accessories include connectors, weatherproofing boots, grounding kits, and other equipment needed to make sure the cable is properly secured and protected against the weather and other environmental conditions.

- **Terminating and Splicing:** Once the cable has been laid, it must be terminated at each end and spliced as needed. This may involve attaching connectors, crimping or soldering wires, or using specialized equipment to join fiber-optic cables. These processes must be performed carefully to ensure the cable is properly connected and the signal or power can flow uninterrupted. Proper labeling and documentation of the cable termination points and splices is essential for future maintenance or troubleshooting.

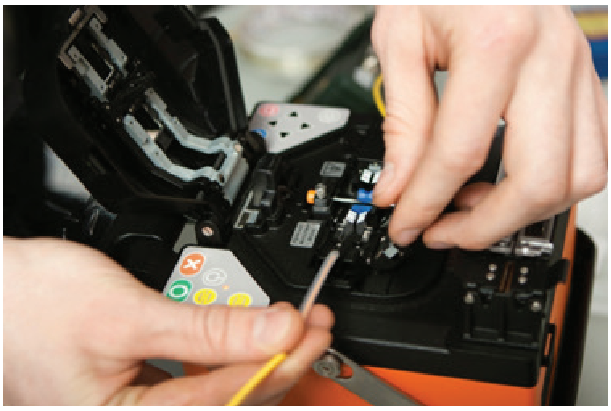


Fig. 2.1.18: Optical Fiber Splicer Machine

- **Testing and Commissioning:** After the cables are laid and terminated, they must be tested to ensure they are functioning correctly. This may involve testing for continuity, resistance, and signal strength, among other factors. Specialized test equipment such as TDRs, Optical Time-Domain Reflectometers (OTDR), and power meters are used to verify proper signal transmission, power levels and fiber attenuation. The test results should be documented and reviewed to ensure the cable meets the design specifications. Once testing is complete, the cables can be commissioned and put into service.
- **Restoration:** Finally, the site must be restored to its previous state or better. This may involve backfilling trenches or channels, landscaping, and cleaning up any debris or equipment. Restoration is an important part of the cable laying process as it ensures that the site is safe and functional for future use.

2.1.6 Wi-Fi System Installation

Here are the general steps involved in Wi-Fi system installation:

Site survey

- This involves visiting the site where the Wi-Fi system is to be installed and conducting a survey to assess the area's size, shape, and other environmental factors that could affect the system's performance.

Network design

- Based on the site survey, a network design is created that outlines the number of access points required, their placement, and other components needed to ensure adequate coverage.

Equipment selection

- Once the network design is finalized, the appropriate Wi-Fi equipment is selected, including access points, switches, routers, and cabling.

Installation of network components

- The network components are then installed, which may involve running cables, mounting access points, and configuring routers and switches.

Configuration and testing

- The Wi-Fi system is then configured and tested to ensure that it is working correctly and providing the desired coverage.

Fig. 2.1.19: Steps of Wi-Fi Installation

2.1.7 Match Connectors to the Correct Type of Cable for Installation

Matching connectors to the correct type of cable is an important step in the installation process, as it ensures that the cable and connector are compatible and can transmit data effectively. Here are the steps to match connectors to the correct type of cable for installation:

The first step in matching connectors to the correct cable type is to identify the cable being used. Cables can vary in terms of their materials, diameter, and other properties, so it is important to know the exact type of cable being used.

Once the cable type is identified, the next step is to determine the type of connector that will be required for the installation. There are many different types of connectors, each with different physical characteristics and compatibility with different types of cables.

There are several types of connectors used in Wi-Fi backhaul installations. Some of the most common types include:

- **N-Type Connectors:** These connectors are commonly used in Wi-Fi backhaul systems as they offer good performance and low loss. N-type connectors are available in both male and female versions and are typically used with coaxial cables.

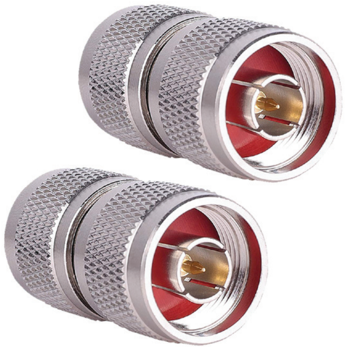


Fig. 2.1.20: N-Type Connectors

- **SMA Connectors:** SMA (SubMiniature version A) connectors are small-sized, high-frequency connectors that are commonly used in Wi-Fi backhaul installations. SMA connectors are typically used with smaller diameter coaxial cables.
- **RP-SMA Connectors:** RP-SMA (Reverse Polarity SMA) connectors are similar to SMA connectors, but with the polarity reversed. RP-SMA connectors are typically used in Wi-Fi access points and routers.

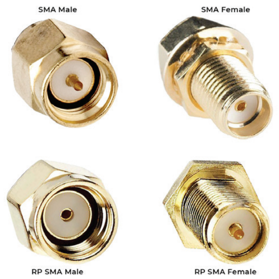


Fig. 2.1.21: SMA and RP SMA Connectors

- **TNC Connectors:** TNC (Threaded Neill-Concelman) connectors are similar to BNC connectors, but offer a threaded connection for added security. TNC connectors are commonly used in Wi-Fi backhaul systems as they offer good performance and low loss.
- **RP-TNC Connectors:** RP-TNC (Reverse Polarity TNC) connectors are similar to TNC connectors, but with the polarity reversed. RP-TNC connectors are commonly used in Wi-Fi access points and routers.

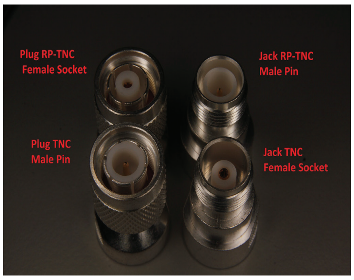


Fig. 2.1.22: TNC and RP TNC Connectors

- **MCX Connectors:** MCX (Micro Coaxial) connectors are smaller than SMA connectors and are commonly used in Wi-Fi access points and routers.

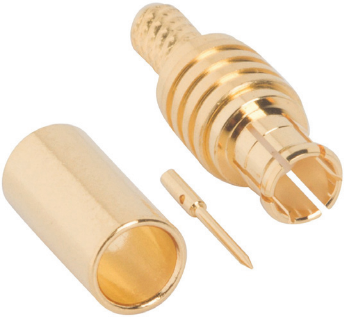


Fig. 2.1.23: MCX Connector

After identifying the required connector type, it is important to check the connector specifications to ensure that it is compatible with the specific type of cable being used. The specifications will indicate the cable diameter, conductor size, and other parameters that must match the cable being used.

Before connecting the connector to the cable, the end of the cable should be prepared by stripping the outer jacket and exposing the inner conductor wires. This may involve using specialized tools such as wire strippers or scissors.

After preparing the cable end, the connector can be installed onto the cable. This may involve using crimping tools or other specialized equipment to securely attach the connector to the cable.

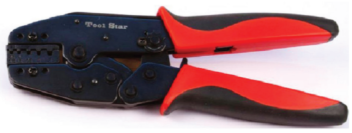


Fig. 2.1.24: Crimping Tool

Once the connector is installed, it is important to test the connection to ensure that the cable and connector are transmitting data effectively. This may involve using specialized testing equipment to measure the signal strength and quality of the connection.

2.1.8 Firmware Updates, Basic Configurations, and Network Connectivity Checks for Wireless Devices

1. Firmware Updates

Firmware is the embedded software that enables a wireless device to function according to its design. Periodic firmware updates are essential to improve device performance, fix software bugs, enhance security, and introduce new features.

Procedure for Firmware Updates:

1. Identify the device model and version number.
2. Download the latest firmware from the manufacturer's official website.
3. Create a backup of the existing configuration to prevent data loss in case of update failure.
4. Access the device's management interface (usually via a web browser or dedicated application).
5. Upload the downloaded firmware file and initiate the update process.
6. Allow the device to reboot and apply the changes.

2. Basic Configurations

After installation, wireless devices require basic configuration to ensure correct operation and secure network access. These settings are usually applied through a web-based interface, mobile application, or command-line configuration.

Key Configuration Steps:

- **SSID Configuration:** Assign a unique network name (SSID) to identify the wireless network.
- **Security Settings:** Enable encryption protocols such as WPA2 or WPA3 to prevent unauthorized access.
- **IP Address Assignment:** Configure devices to obtain an IP address via DHCP or set a static IP address.
- **Frequency and Channel Selection:** Select an appropriate frequency band (2.4 GHz or 5 GHz) and channel to minimize interference.
- **Additional Features:** Activate optional functions such as guest networks, MAC address filtering, and Quality of Service (QoS).

3. Network Connectivity Checks

Once the device has been updated and configured, network connectivity checks must be performed to verify proper operation and troubleshoot potential issues.

Common Connectivity Verification Methods:

- **Ping Test:** Sends data packets to a target IP address (such as the default gateway) to confirm connectivity.
- **Signal Strength Analysis:** Uses network analyzer tools to measure wireless signal strength and coverage.
- **Speed Testing:** Measures data transfer speeds to ensure they meet expected performance levels.
- **Status Indicator Monitoring:** Observes the device's LED indicators for power, network, and wireless activity status.
- **Traceroute Analysis:** Identifies network path delays or failures by tracing the route taken by data packets.

Regular firmware updates, accurate basic configurations, and systematic network connectivity checks are critical to ensuring the reliability, security, and performance of wireless communication systems. Technicians must follow proper procedures and safety guidelines while performing these tasks to maintain optimal network functionality.

2.1.9 Installation and Usage of Cable Termination between Equipment and Antenna

Cable termination refers to the process of connecting cables from equipment to an antenna, which is an important step in the installation of a wireless communication system. Here are the steps to install and use cable termination between equipment and antenna:

- Determine the required termination type: The first step in the installation of cable termination is to determine the type of termination that is required. This may involve selecting the appropriate connector type based on the equipment and antenna being used.
- Prepare the cable end: After determining the required termination type, the next step is to prepare the end of the cable that will be connected to the equipment or antenna. This may involve stripping the outer jacket and exposing the inner conductor wires.
- Install the connector: Once the cable end is prepared, the next step is to install the connector onto the cable. This may involve using specialized crimping tools or other equipment to securely attach the connector to the cable.
- Connect the termination to the equipment: After the connector is installed, the cable can be connected to the equipment using the appropriate port or interface. This may involve screwing the connector onto the port or plugging it into the interface.
- Connect the termination to the antenna: After connecting the cable termination to the equipment, the other end of the cable can be connected to the antenna. This may involve screwing the connector onto the antenna port or using other specialized equipment to securely attach the connector to the antenna.
- Test the connection: Once the cable termination is installed, it is important to test the connection to ensure that it is transmitting data effectively. This may involve using specialized testing equipment to measure the signal strength and quality of the connection.

- To use cable termination between equipment and antenna, it is important to ensure that the termination is installed correctly and that the connection is secure. This will help to ensure that the wireless communication system is functioning effectively and that data is being transmitted accurately between the equipment and antenna. It is also important to regularly check the termination and connection for any signs of damage or wear, and to replace any damaged components as needed.

2.1.10 Basic Wi-Fi Network Principles: Signal Propagation, Interference, and Coverage Optimization

Introduction:

Wi-Fi networks operate using radio waves to provide wireless connectivity between devices and access points. Understanding how signals travel, what factors affect their quality, and how to optimize coverage is essential for designing and maintaining efficient wireless networks.

1. Signal Propagation

Signal propagation refers to the way radio waves travel from the Wi-Fi access point to connected devices. Wi-Fi commonly uses the 2.4 GHz and 5 GHz frequency bands.

- Line-of-Sight (LOS): A clear path between the transmitter and receiver results in the strongest signal.
- Obstructions: Walls, furniture, and metal structures weaken the signal due to absorption, reflection, and scattering.
- Distance: The farther the signal travels, the weaker it becomes due to natural attenuation.

2. Interference

Interference occurs when unwanted signals disrupt normal Wi-Fi communication, causing slow speeds, packet loss, or disconnections.

- Co-Channel Interference: When multiple devices share the same channel, they compete for bandwidth.
- Adjacent Channel Interference: Overlapping channels create noise and reduce performance.
- Non-Wi-Fi Interference: Devices such as microwave ovens, cordless phones, and Bluetooth devices can cause disruption in the 2.4 GHz band.

3. Coverage Optimization

Coverage optimization ensures that the Wi-Fi signal is strong and reliable throughout the intended area.

- Access Point Placement: Install APs at central, elevated locations with minimal physical obstructions.
- Channel Planning: Use non-overlapping channels to reduce interference (e.g., channels 1, 6, and 11 in the 2.4 GHz band).
- Power Adjustment: Set transmit power to balance coverage and avoid excessive overlap between APs.
- Use of Repeaters or Mesh Networks: Extend coverage in large or complex areas without degrading performance.

A well-designed Wi-Fi network depends on a solid understanding of signal behavior, effective interference management, and careful planning of coverage. Applying these principles ensures high performance, reliability, and user satisfaction.

2.1.11 Electrical Principles to be Considered while Turning on the Wi-Fi System

When turning on a Wi-Fi system, there are several electrical principles that should be considered to ensure that the system functions properly and safely. Here are some key electrical principles to consider:

- **Voltage:** The voltage of the power supply must be appropriate for the Wi-Fi system being used. Voltage is the electrical potential difference between two points, and the system may be designed to operate at a specific voltage range. Using a power supply with a voltage outside of this range can damage the system or cause it to malfunction.
- **Current:** The current draw of the Wi-Fi system should also be considered when turning it on. Current is the flow of electrical charge through a circuit, and the system may be designed to draw a specific amount of current. Using a power supply that cannot deliver enough current can cause the system to malfunction or fail to operate.
- **Power:** Power is the rate at which electrical energy is transferred, and it is determined by the voltage and current being used. The power rating of the Wi-Fi system and its components should be considered when turning it on, to ensure that the power supply can provide enough power to operate the system effectively.
- **Circuit protection:** It is important to ensure that the Wi-Fi system and its components are protected from overvoltage, overcurrent, and other electrical faults. This can be accomplished through the use of fuses, circuit breakers, or other protection devices, which can prevent damage to the system in the event of an electrical fault.
- **Grounding:** Grounding is an important electrical principle to consider when turning on a Wi-Fi system. Grounding provides a low-resistance path for electrical current to flow to the earth, and can help to prevent electrical shock and other hazards. The system and its components should be properly grounded to ensure safe operation.

By considering these electrical principles when turning on a Wi-Fi system, it is possible to ensure that the system functions properly and safely, and that the risk of electrical hazards is minimized. It is also important to follow any manufacturer recommendations and safety guidelines for the specific Wi-Fi system being used, and to seek professional assistance if necessary.

2.1.12 Test the Cable and Joints for Transmission Loss and Strength

To test a cable and its joints for transmission loss and strength, there are several methods that can be used. Here are some common techniques:

Cable Testing

Cable testing is a crucial step in ensuring the quality and reliability of a cable installation. One common method of cable testing is to use a cable tester. A cable tester is a specialized device that can measure various characteristics of the cable, such as the continuity of the conductors, the impedance, and the capacitance.

A cable tester typically consists of two units, a transmitter and a receiver. The transmitter is connected to one end of the cable being tested, and it sends a signal through the cable. The receiver is connected to the other end of the cable, and it receives the signal and analyzes it.

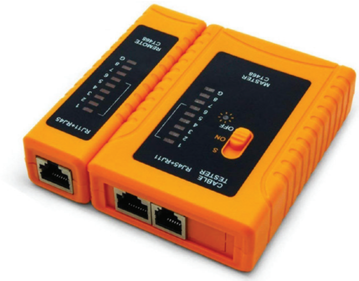


Fig. 2.1.25: Cable Tester

By using a cable tester, it is possible to identify any breaks or faults in the cable that could cause transmission loss. For example, if there is a break in one of the conductors, the cable tester will detect it and indicate that there is a fault. Similarly, if there is an issue with the impedance or capacitance of the cable, the cable tester will be able to identify it.

Some cable testers also have additional features, such as the ability to measure the length of the cable and the location of any faults or breaks. This can be useful for identifying the specific location of any issues in the cable.

Time Domain Reflectometry (TDR)

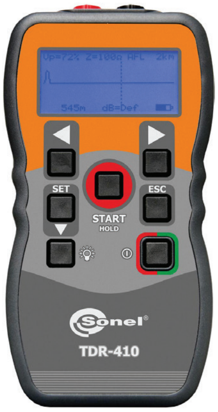


Fig. 2.1.26: Time Domain Reflectometry (TDR)

Time Domain Reflectometry (TDR) is a highly advanced technique for testing and analyzing the quality of a cable. TDR works by sending a high-frequency signal down the cable being tested, and measuring the reflections that occur at any discontinuities or faults in the cable.

The TDR tester consists of a pulse generator that sends a signal through the cable, and a receiver that detects and measures the reflections. The pulse generator sends a short electrical pulse down the cable, which then travels down the cable until it reaches the end or encounters any discontinuity or fault in the cable.

At any discontinuity or fault in the cable, a portion of the electrical signal is reflected back towards the TDR tester. The TDR tester then detects and measures the time it takes for the signal to travel to the fault and back, which corresponds to the distance between the TDR tester and the fault. The amplitude of the reflection is also measured, which indicates the severity of the fault.

By analyzing the reflections, it is possible to determine the location and severity of any faults or damage in the cable. The TDR tester can provide a graphical display of the signal reflections, known as a Time Domain Reflectogram (TDR), which provides a visual representation of the cable's quality.

TDR testing is a highly advanced technique and is used in more complex cable installations. It can be used to measure a wide range of cable characteristics, such as cable length, impedance, and capacitance. TDR is often used in applications that require precise measurement and analysis of cable quality, such as in telecommunications, data centers, and power transmission systems.

VSWR Testing

VSWR (Voltage Standing Wave Ratio) testing is an important method of measuring the reflection of radio frequency (RF) energy at the joints between two cables. It is used to identify any impedance mismatches or other issues that could cause transmission loss. VSWR is a measure of the efficiency of a radio frequency transmission system, and it is an indication of how well the system is matched to the antenna and cable.

In a transmission system, it is essential to match the impedance of the cable and the antenna to minimize the reflection of the radio frequency energy. Any mismatch in the impedance can result in a reflection of the energy that is not transferred to the antenna, causing transmission loss. VSWR is a measure of the ratio of the maximum voltage to the minimum voltage in a transmission line.

A VSWR meter is a specialized device that is used to measure the VSWR at the joints between two cables. The VSWR meter sends a signal down the cable and measures the ratio of the maximum voltage to the minimum voltage in the signal that is reflected back from the joint. The VSWR meter then compares the measured VSWR to the acceptable range for the specific cable type and application.

If the VSWR measurement is outside the acceptable range, it indicates that there is an impedance mismatch or other issue that could cause transmission loss. The VSWR meter can help identify the location of the impedance mismatch or issue, allowing for targeted troubleshooting and repair.

VSWR testing is an essential part of any cable installation process, especially in radio frequency transmission systems such as those used in telecommunications, broadcasting, and satellite communications. It helps to ensure that the transmission system is properly matched to the cable and antenna, and that the system is operating at its maximum efficiency.

Pull Testing

Pull testing is a critical method of testing the strength and durability of the cable and its joints. This method involves applying a controlled amount of force to the cable and measuring the amount of force required to cause it to fail. Pull testing is used to ensure that the cable and its joints can withstand the expected loads and stresses of the installation process and the environment in which it will operate.

During pull testing, a specific amount of tension is applied to the cable and is then gradually increased until the cable or its joints fail. The amount of force required to cause the failure is then recorded, and this information is used to determine whether the cable and its joints meet the required strength specifications.

Pull testing can be conducted using specialized equipment that applies tension to the cable and records the force applied. The equipment can also be programmed to apply a specific amount of tension for a specified period to simulate the effects of long-term use.

The results of the pull test are compared against the specifications of the cable and its joints to determine if they are suitable for use in the installation. If the cable or its joints fail to meet the required strength specifications, they must be replaced or repaired before installation can proceed.

Pull testing is an essential part of the cable installation process, particularly in applications where the cable will be subjected to high loads and stresses, such as telecommunications and power transmission. It helps to ensure that the cable and its joints are strong enough to withstand the expected loads and stresses, reducing the risk of failure or damage to the installation.

Notes

UNIT 2.2: Complete Documentation

Unit Objectives

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

1. Explain documentation processes, including technical reports, installation logs, and compliance records.
2. Describe customer handling protocols, payment procedures, and conflict resolution strategies.
3. Show how to maintain accurate records of installation, testing results, and equipment details.
4. Demonstrate how to complete all required installation documents and reports in the prescribed format.
5. Show how to collect customer acknowledgment and necessary payments, if applicable.

2.2.1 Importance of Satisfactory Customer Service

Providing satisfactory customer service is an essential aspect of any service-oriented job, and it is particularly important for an Wireless Technician who works directly with customers on a regular basis. There are several reasons why providing good customer service is important for an Wireless Technician:

- **Customer satisfaction:** The primary reason for providing good customer service is to ensure customer satisfaction. When customers are happy with the service they receive, they are more likely to return for future services and to recommend the technician to others.
- **Positive reputation:** Satisfactory customer service can also help build a positive reputation for the technician and the company they work for. This can lead to increased business through positive word-of-mouth referrals and repeat customers.
- **Increased revenue:** Happy customers are more likely to spend money on additional services or upgrades, which can increase revenue for the technician and the company they work for.
- **Better job performance:** Providing good customer service can also improve job performance by increasing productivity, reducing errors, and improving morale.

There are several specific steps an Wireless Technician can take to provide satisfactory customer service, including:

- **Clear communication:** The technician should communicate clearly and effectively with the customer, using language that the customer can understand. They should also listen carefully to the customer's needs and concerns.
- **Prompt response:** The technician should respond promptly to customer inquiries and concerns, demonstrating a sense of urgency and attentiveness.
- **Professional demeanor:** The technician should maintain a professional demeanor at all times, demonstrating respect and courtesy to the customer.
- **Knowledge and expertise:** The technician should have a deep understanding of the technology they are working with and be able to answer any technical questions the customer may have.
- **Problem-solving skills:** The technician should be able to identify and solve any problems the customer may be experiencing, using a combination of technical expertise and communication skills.

Taking Customer Feedback

Taking customer feedback is a vital practice for a Wireless Technician, as it enables them to understand the customer's needs, preferences, and expectations more effectively. Feedback offers valuable insights that can be used to improve service quality, resolve concerns promptly, and enhance the overall customer experience.

By actively listening to feedback, a Wireless Technician can pinpoint areas that require improvement and take corrective actions to address them. This not only improves service delivery but also helps build trust and stronger relationships with customers.

Customer feedback also provides the opportunity to identify trends and recurring issues, allowing the technician to anticipate and address potential problems before they escalate. Proactive problem-solving leads to higher customer satisfaction and loyalty, as clients are more inclined to return to service providers who value their input and act upon it.

Furthermore, feedback highlights both strengths and weaknesses in a technician's performance. Recognizing these aspects allows for targeted skill development and knowledge enhancement, contributing to personal growth, professional competence, and increased job satisfaction.

2.2.2 Documentation Required for Installation

The documentation required for the installation of Wi-Fi backhaul may vary depending on the specific project and location, but generally, the following documents are important:

- **Site survey report:** A report containing the details of the site survey, including the type of equipment needed, the layout of the area, and any potential obstacles or challenges that may affect the installation process.
- **Bill of Materials (BOM):** A list of all the materials, components, and equipment required for the installation, including their specifications, quantities, and costs.
- **Network diagram:** A diagram that shows the layout of the network and how all the devices will be connected, including access points, routers, switches, and other network components.
- **Installation manual:** A document that outlines the step-by-step procedures for installing and configuring the Wi-Fi backhaul equipment.
- **User manual:** A document that provides instructions and information on how to use the Wi-Fi backhaul system, including how to connect to the network, configure settings, and troubleshoot issues.
- **Testing and commissioning report:** A report that outlines the results of the testing and commissioning process, including any issues or problems that were encountered and how they were resolved.
- **As-built drawings:** A set of drawings that show the actual layout and installation of the equipment, including the location of devices, cabling, and other components.
- **Maintenance manual:** A document that provides guidelines and instructions for maintaining the Wi-Fi backhaul system, including routine maintenance procedures, troubleshooting, and repair instructions.

2.2.3 Different Payment Modes

The payment modes in which an Wireless Technician can collect payment from the customer post installation includes:

- **Cash:** The customer can pay the Assistant Technician in cash for the services provided.
- **Credit or Debit Cards:** The Assistant Technician can accept payment from the customer using a credit or debit card. They may use a mobile card reader to process the payment or may manually enter the customer's payment information into a payment terminal.
- **Unified Payments Interface (UPI):** Unified Payments Interface (UPI) services such as PhonePe, GooglePay, PayPal, etc. may be used to accept payment from the customer.

2.2.4 Write and Record Appropriate Technical Forms, Activity Logs

Writing and recording appropriate technical forms and activity logs is an important part of the job of an Wireless Technician. The purpose of these forms and logs is to document the work that has been done, provide information to other technicians who may need to work on the system in the future, and to create a record of the work that has been done for the customer. Here are the steps to write and record appropriate technical forms and activity logs:

- **Identify the type of form or log needed:** There are different types of technical forms and activity logs used for different purposes, such as work orders, inspection forms, installation reports, and maintenance logs. Choose the appropriate form or log based on the specific work being done.
- **Fill in all necessary information:** Technical forms and activity logs should contain all relevant information about the work being done, including the date, time, location, equipment used, materials used, and any issues or challenges encountered. Make sure to fill in all necessary fields accurately and completely.
- **Use clear and concise language:** When filling out forms and logs, use clear and concise language that is easy to understand. Avoid technical jargon or abbreviations that may not be familiar to others who need to read the forms.
- **Be detailed:** Provide as much detail as possible about the work that has been done, including any tests performed, measurements taken, and any adjustments made to equipment. This information can be helpful to other technicians who may need to work on the system in the future.
- **Include any necessary attachments:** If there are any diagrams, photos, or other attachments that are relevant to the work being done, include them with the form or log.
- **Review and check for accuracy:** Before submitting the form or log, review it to ensure that all information is accurate and complete. Make any necessary corrections or additions.
- **Store and organize forms and logs:** Keep technical forms and activity logs in a safe and organized location where they can be easily accessed when needed. Make sure to label and date the forms so that they can be easily identified.

2.2.5 General Safety Norms to be Followed at Workplace

Safety is an essential consideration in any installation or maintenance work, including wireless technology installations. Here are some safety norms that an Wireless Technician should follow:

- **Use proper Personal Protective Equipment (PPE):** When working with wireless equipment, it is essential to use PPE to protect against potential hazards. This may include gloves, safety glasses, hard hats, earplugs, and high-visibility clothing.

- **Turn off the equipment before working on it:** Before working on any wireless equipment, make sure it is turned off to avoid electric shock.
- **Use insulated tools:** Insulated tools should be used when working on any electrical equipment to avoid the risk of electric shock.

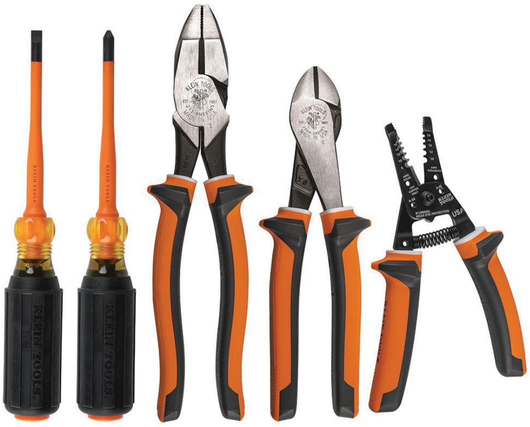


Fig. 2.2.1: Insulated Tools

- **Follow the manufacturer's instructions:** Always follow the manufacturer's instructions when working with wireless equipment to ensure that you are following the recommended safety procedures.
- **Secure the equipment:** Make sure that the equipment is properly secured before starting any installation work to avoid any accidents.
- **Be aware of your surroundings:** Always be aware of your surroundings when working with wireless equipment to avoid potential hazards, such as tripping or falling.
- **Use caution when working at heights:** If working at heights, use proper safety equipment such as harnesses, lanyards, and safety nets.
- **Use caution when lifting heavy objects:** Use proper lifting techniques and equipment to avoid injury when lifting heavy objects.
- **Keep the work area clean and organized:** A clean and organized work area helps to reduce the risk of accidents and injuries.
- **Follow proper electrical safety procedures:** Follow proper electrical safety procedures, such as grounding and locking out equipment, to avoid electric shock and other hazards.

2.2.6 Escalation Matrix for Reporting Incidents

An escalation matrix is a set of procedures and protocols that define the steps that need to be taken in the event of an incident or emergency. In the context of a Wi-Fi Backhaul installation, an escalation matrix helps to ensure that any issues or problems are reported, escalated and resolved in a timely and efficient manner. The matrix defines the hierarchy of contacts that need to be notified in case of incidents, troubles, and emergencies.

The escalation matrix typically starts with the first level of contact, which is usually the Wireless Technician who is responsible for the installation. If an issue or problem is identified, the Assistant Technician should follow the appropriate procedures for reporting and escalating the issue. This could involve contacting the second level of support, which could be a more experienced technician or supervisor, who can provide further assistance and guidance.

If the issue is not resolved at the second level, it may need to be escalated to the third level, which could be the network operations center or the customer support team. At this level, a more experienced and specialized team can help to diagnose and troubleshoot the issue, and provide more advanced support.

If the issue still cannot be resolved, it may need to be escalated to the fourth level, which could involve senior management or executives who can provide additional resources, funding, or other forms of support. At this level, the incident is typically treated as a high priority, and urgent action is taken to resolve the issue as quickly as possible.

The escalation matrix should also define the appropriate communication channels and protocols for reporting and escalating incidents. This could involve using a dedicated phone line or email address, or following a specific reporting format or template. The matrix should also define the response times and targets for each level of support, as well as the procedures for tracking and closing out incidents once they have been resolved.

Summary

- Analysing Work Orders and Job Sheets
- Wi-Fi Backhaul
- Cables, Connectors, Tools and Equipment Required for Installation
- Steps to Obtain Cables/Equipment from the Company
- Feeder Cable Laying
- Wi-Fi System Installation
- Installation and Usage of Cable Termination between Equipment and Antenna
- Electrical Principles to be considered while turning on the Wi-Fi System
- Test the Cable and Joints for Transmission Loss and Strength
- Importance of Satisfactory Customer Service
- Documentation Required for Installation
- Different Payment Modes
- Write and Record Appropriate Technical Forms, Activity Logs
- Safety Norms to be followed
- Escalation Matrix for reporting Incidents

Exercise

Multiple-choice Question

1. A ________ provides detailed instructions on what needs to be done

   a. work-sheet b. job-sheet

   c. blank-sheet d. None of the above

2. __________ is a term used to describe the process of using wireless networking technology to connect one or more access points to a wired network

   a. Wi-Fi backhaul b. Wi-Fi overhaul

   c. Hi-Fi backhaul d. None of the above

3. __________ cable laying refers specifically to the installation of cables for telecommunications and networking systems

   a. Reader b. Weedier

   c. Feeder d. None of the above

4. __________ is a report containing the details of the site survey

   a. Site Survey Report b. Night Survey Report

   c. Light Survey Report d. None of the above

5. An _________ is a set of procedures and protocols that define the steps that need to be taken in the event of an incident or emergency

   a. calculation matrix b. escalation matrix

   c. wireless matrix d. None of the above

Descriptive Questions:

1. Describe the process to conduct installation of Wi-Fi system
2. Discuss the safety norms to be follow at the workplace
3. Explain the significance of taking customer feedback
4. Explain the escalation matrix for reporting identified incidents
5. What are the electrical principles to be considered while turning on the Wi-Fi System?

Notes

Scan the QR codes or click on the link to watch the related videos

https://www.youtube.com/watch?v=P8j2H5J4fU4

How to Set Up a Wi-Fi Network

https://www.youtube.com/watch?v=-DIbLZ3hL9M

Wireless OR Wired Backhaul Benefits

https://www.youtube.com/watch?v=P8j2H5J4fU4

How to Set Up a Wi-Fi Network

https://www.youtube.com/watch?v=WnQ7L4WFrcQ

Why is customer service important?

https://www.youtube.com/watch?v=GUurzvS3DlY

What is a payment gateway and how does it work?

सत्यमेव जयते
GOVERNMENT OF INDIA
MINISTRY OF SKILL DEVELOPMENT
& ENTREPRENEURSHIP

3. Configuring Equipment and Establishing Wireless Network Connectivity

Unit 3.1 - Setting up Wi-Fi Network

Unit 3.2 - Establishing Connectivity

TEL/N4123

Key Learning Outcomes

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

1. Describe the process of configuring wireless network equipment.
2. Explain the steps involved in establishing and verifying wireless network connectivity.
3. Determine the methods for recording configuration settings and test results for wireless network deployments.

UNIT 3.1: Setting up Wi-Fi Network

Unit Objectives

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

1. Describe the fundamental concepts of wireless networking, including IEEE 802.11 standards, frequency bands, and channel interference.
2. Explain network topologies, broadband network elements, gateways, TCP/IP, DHCP, and subnetting.
3. Discuss key performance parameters such as signal strength, VSWR, return loss, and link budget calculations.
4. Describe industry best practices for securing wireless networks, including encryption standards, firewall configurations, and intrusion prevention measures.
5. Determine tools and software used for configuring, testing, and monitoring network performance.
6. Elucidate the importance of firmware updates and software patches in maintaining network security and reliability.
7. Describe guidelines for proper cable management, grounding techniques, and protection against environmental damage.
8. Discuss basic electrical safety measures and first aid procedures for handling installation-related hazards.
9. Demonstrate how to install and securely mount Wi-Fi backhaul equipment and access points as per site specifications.
10. Show how to connect feeder cables with antennas and measure VSWR/return loss to ensure optimal signal transmission.
11. Demonstrate how to align antennas based on surveyed signal strength and adjust orientation for optimal connectivity.
12. Show how to establish physical connections between Wi-Fi backhaul equipment, Wi-Fi access points, and network switches.
13. Demonstrate how to configure equipment settings, including IP addresses, subnet masks, and default gateways, according to base configurations.
14. Show how to access network settings using default login credentials and update them with secure passwords.
15. Demonstrate how to apply encryption and authentication settings (WPA2/WPA3) to secure network access.
16. Show how to update firmware and software patches to ensure compliance with industry standards and security best practices.
17. Demonstrate how to ensure all cables and connectors are properly secured and free from damage.

3.1.1 Concept of Wireless Technology

Wireless technology is a type of communication technology that uses radio waves or microwaves to transmit data or signals without the need for physical wires or cables. Wireless technology has become an essential part of modern life, and it is used in a variety of applications, including mobile phones, Wi-Fi, Bluetooth, GPS, and many more.

Wireless technology is a means of communication that uses electromagnetic waves to transmit information over the air. The technology uses radio frequency signals to connect devices, allowing them to communicate without the need for physical cables or wires.

Wireless technology operates on the principle of electromagnetic radiation. When an electrical charge oscillates or vibrates, it produces an electromagnetic wave that radiates outwards. In wireless communication, information is modulated onto these electromagnetic waves and transmitted from one device to another.

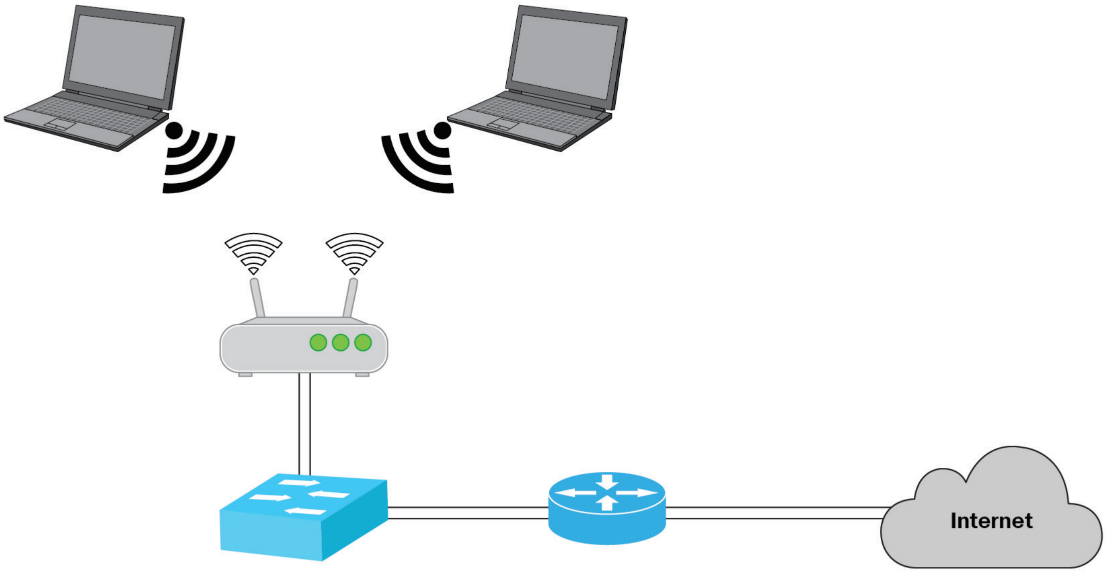


Fig. 3.1.1: Wireless Connectivity

Wireless networks use radio waves to transmit data between devices. The wireless network consists of two main components: the wireless router and the wireless adapter. The wireless router receives data from the wired network and converts it into radio signals. The wireless adapter receives the radio signals and converts them back into data.

The wireless router and the wireless adapter communicate with each other using a standard set of protocols known as the IEEE 802.11 standards. These standards define the method of transmitting and receiving data over the wireless network.

When a device connects to a wireless network, it first needs to authenticate itself to the network. This is typically done using a password or a security key. Once authenticated, the device is assigned an IP address by the router, which allows it to communicate with other devices on the network.

Wireless technology has enabled a wide range of applications, including mobile phones, laptops, tablets, smart homes, and the Internet of Things (IoT).

Evolution of wireless Technology

Wireless technology has evolved significantly since the first wireless telegraph system was developed by Guglielmo Marconi in the late 19th century. The evolution of wireless technology can be broadly classified into five generations, with each generation bringing significant improvements over the previous one.

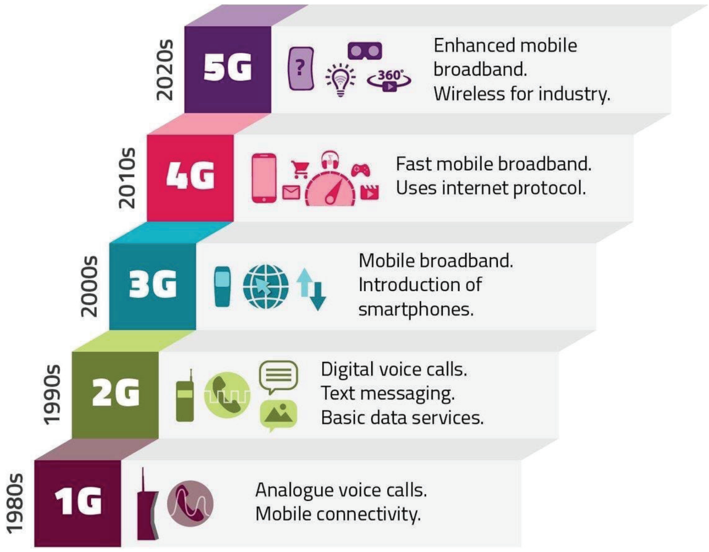
1G (First Generation): The first generation of wireless technology was based on analog signals and was primarily used for voice communications. The first commercially available 1G network was launched in Japan in 1979.

2G (Second Generation): The second generation of wireless technology was based on digital signals and introduced the ability to send short text messages. The first commercially available 2G network was launched in Finland in 1991.

3G (Third Generation): The third generation of wireless technology brought significant improvements in data transfer speeds, allowing for the transmission of multimedia content. The first commercially available 3G network was launched in Japan in 2001.

4G (Fourth Generation): The fourth generation of wireless technology was a significant leap forward in terms of data transfer speeds and enabled the widespread adoption of mobile broadband. The first commercially available 4G network was launched in Sweden in 2009.

5G (Fifth Generation): The fifth generation of wireless technology represents a major leap forward in terms of data transfer speeds, latency, and network capacity. 5G networks are designed to support the Internet of Things (IoT), virtual reality, and other emerging technologies. The first commercially available 5G network was launched in South Korea in 2019.



`Fig. 3.1.2: Evolution of Wireless Communication

The evolution of wireless technology has brought significant improvements in data transfer speeds, network capacity, and reliability, enabling the development of new and innovative applications and services. With the advent of 5G, we can expect to see further advancements in wireless technology, enabling new use cases and applications that were previously not possible.

3.1.2 Network Topologies

A network topology refers to the layout or structure of a network, including its nodes and connecting lines. Different types of network topologies are used depending on the specific needs of a system. Some of the common network topologies are:

Bus topology

Bus topology is a type of network topology in which all the devices are connected to a single communication line or a bus. It is also called a linear bus topology.

In a bus topology, each device is connected to a single cable, also known as a trunk, which serves as the main communication line. The devices on the network communicate by sending signals on this single cable. The signals travel in both directions on the cable and are picked up by all the devices connected to it.

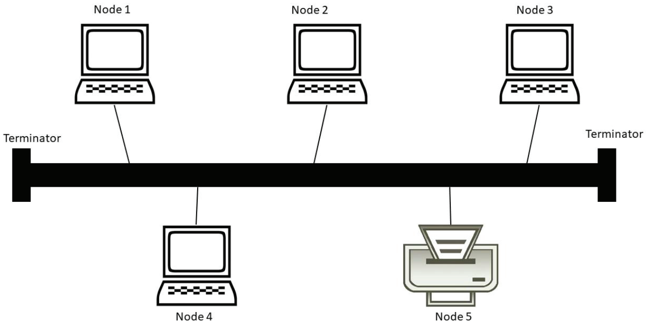


Fig. 3.1.3: Bus Topology

One advantage of a bus topology is that it is relatively simple and easy to set up. It requires less cabling than other topologies, which makes it less expensive. Also, adding or removing a device from the network is relatively easy, as it simply involves plugging or unplugging the device from the bus.

However, one major disadvantage of a bus topology is that the entire network can be affected if the communication line is damaged or breaks. Also, the bandwidth of the network is shared among all the devices on the bus, which can lead to network congestion and slower data transfer rates as the number of devices on the network increases.

Another limitation of a bus topology is that it does not provide any redundancy or backup in case of a cable failure. If the main cable is damaged, the entire network will be affected until the cable is repaired.

Bus topology is mostly used in small networks, such as in homes and small offices. It is not suitable for larger networks where redundancy and high bandwidth are required.

Star topology

Star topology is a type of network topology in which all devices are connected to a central hub or switch. The hub or switch acts as a central point for communication and data transmission between devices.

In a star topology, all devices are connected to the hub or switch using point-to-point links, typically Ethernet cables. Each device has its own dedicated link to the hub or switch, which ensures that there is no interference between devices. The hub or switch is responsible for managing and directing traffic between the devices.

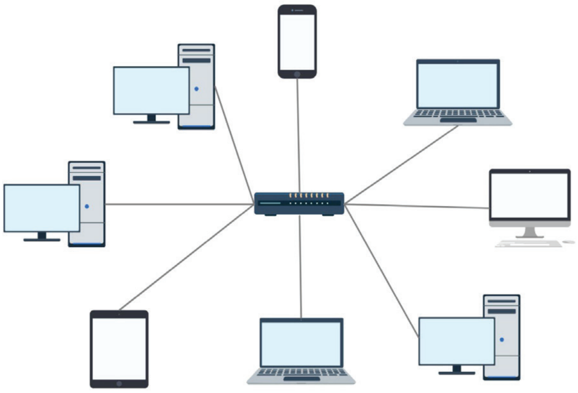


Fig. 3.1.4: Star Topology

One of the key advantages of a star topology is that it is easy to manage and maintain. Since all devices are connected to the central hub or switch, it is easy to add or remove devices without disrupting the entire network. In addition, the hub or switch can be easily replaced if it fails, without affecting the devices on the network.

Another advantage of the star topology is that it provides good performance, particularly for large networks. Since each device has its own dedicated link to the hub or switch, the bandwidth available to each device is not shared with other devices. This means that devices can transmit and receive data at high speeds, without being affected by other devices on the network.

However, one of the disadvantages of a star topology is that it is more expensive to implement than other topologies, particularly if a large number of devices need to be connected. In addition, if the hub or switch fails, the entire network can be affected.

Ring topology

In a ring topology, the network nodes are arranged in a circular configuration, with each node connected to the two adjacent nodes. In this topology, the data travels around the ring in a unidirectional manner, with each node receiving and transmitting data packets in turn.

To prevent the data from circulating indefinitely, a mechanism is implemented to detect and remove packets that have traveled around the ring without being delivered to their destination. One common mechanism is the use of a token, which is a special packet that is passed around the ring. The node that has the token is allowed to transmit data, and when it has finished transmitting, it passes the token to the next node on the ring.

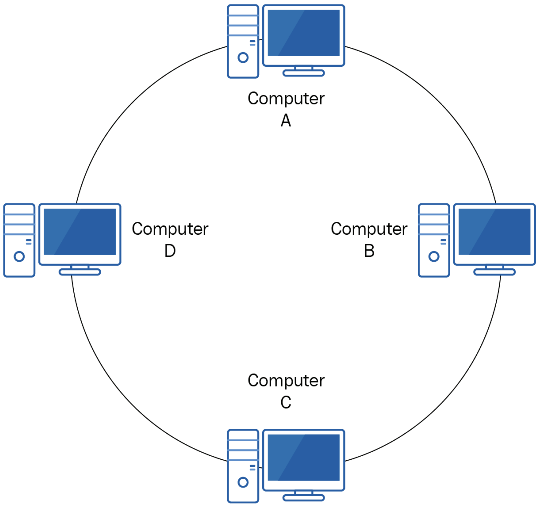


Fig. 3.1.5: Ring Topology

Ring topology is simple to implement and can be used for both small and large networks. It also provides consistent performance as each node has equal access to the network. Additionally, it is easy to add or remove nodes from the network without affecting other nodes.

However, ring topology also has some disadvantages. The failure of a single node can cause the entire network to go down. Additionally, adding or removing nodes from the ring can disrupt the network's operation until the changes are fully propagated. Finally, the maximum distance between nodes in the ring is limited, which can be a constraint for large networks.

Mesh topology

Mesh topology is a type of network topology in which all devices or nodes are connected to every other node in the network. In other words, it is a fully connected network where each node is connected to all the other nodes in the network. This makes mesh topology a highly reliable and fault-tolerant network, as there are multiple paths for data to flow in the network.

In a mesh topology, the devices are typically connected in a point-to-point fashion. Each device in the network acts as a repeater, helping to propagate the signals to the other devices. This means that a mesh network can be extended without the need for additional infrastructure, as each device can act as a relay point.

There are two types of mesh topologies: Full mesh and Partial mesh.

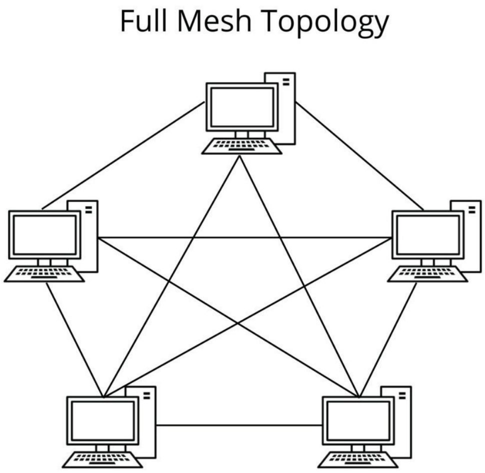


Fig. 3.1.6: Full Mesh Topology

In a full mesh topology, every device is connected to every other device in the network. This provides the highest level of redundancy and fault tolerance, but it can also be expensive to implement, as it requires a large number of connections.

In a partial mesh topology, some devices are only connected to a subset of the other devices in the network. This reduces the number of connections required and can lower the cost of the network, but it also reduces the fault tolerance.

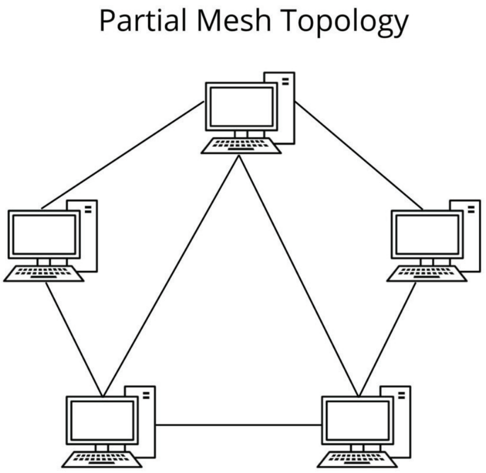


Fig. 3.1.7: Partial Mesh Topology

Mesh topology is commonly used in wireless networks, where the wireless nodes can act as repeaters to extend the network range. It is also used in wired networks, such as in the case of the internet backbone, where there are multiple paths for data to flow in the network, providing redundancy and fault tolerance.

One of the main advantages of mesh topology is its high level of reliability and fault tolerance. Since each node in the network is connected to every other node, there are multiple paths for data to flow in the network. This means that if one node or connection fails, the network can still function, as data can be rerouted through other nodes. Another advantage of mesh topology is its scalability, as new nodes can be easily added to the network without the need for additional infrastructure. However, mesh topology can also be expensive to implement, as it requires a large number of connections and devices.

Hybrid topology

A hybrid topology is a type of network topology that combines two or more different types of topologies to form a single network. This approach is often used in larger networks to take advantage of the strengths of different topologies while minimizing their weaknesses.

For example, a network may use a bus topology for the main network, but use a star topology for a sub-network. Hybrid topology provides the benefits of multiple topologies, but can be complex to design and implement.

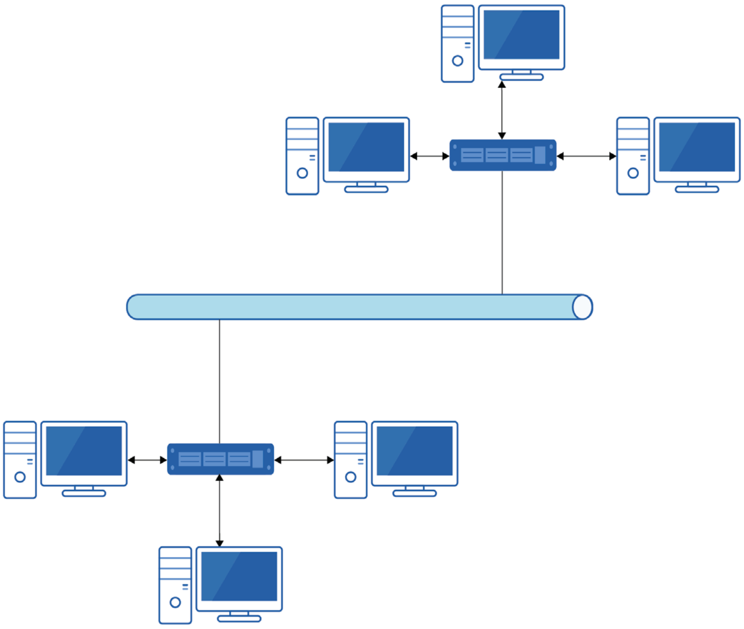


Fig. 3.1.8: Hybrid Topology

The advantages of a hybrid topology include:

- **Scalability:** A hybrid topology can be scaled easily by adding or removing nodes or by adjusting the network configuration.
- **Redundancy:** By combining different topologies, a hybrid network can provide redundancy and fault tolerance, reducing the risk of network downtime.
- **Flexibility:** A hybrid topology allows for greater flexibility in network design, allowing administrators to tailor the network to the specific needs of the organization.
- **Efficiency:** By combining different topologies, a hybrid network can achieve greater efficiency and performance than a single topology alone.

The disadvantages of a hybrid topology include:

- **Complexity:** The combination of different topologies can make the network more complex and difficult to manage.
- **Cost:** A hybrid topology may require additional hardware and software, increasing the cost of the network.
- **Maintenance:** A hybrid topology may require more frequent maintenance and updates to ensure that all components are working together properly.

3.1.3 Broadband Network Elements

Broadband networks consist of various elements that work together to enable high-speed internet connectivity. Here are some of the key elements of a broadband network:

- **Modem:** A modem is a device that connects to the internet service provider (ISP) network to provide internet connectivity to the user's device. It converts the analog signal from the ISP to a digital signal that can be understood by the user's device.
- **Router:** A router is a device that connects multiple devices to the same network and manages the traffic between them. It acts as a gateway between the user's devices and the ISP's network.
- **Switch:** A switch is a device that connects multiple devices on the same network and forwards data between them. It is often used to connect multiple computers, printers, and servers in an office environment.

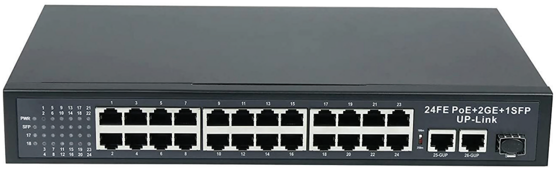


Fig. 3.1.9: Network Switch

- **Access Point:** An access point is a device that connects wireless devices to a wired network. It enables wireless devices to connect to the network and access the internet.

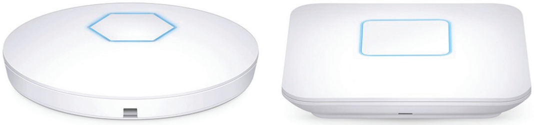


Fig. 3.1.10: Access Point

- **Network Interface Card (NIC):** A network interface card is a hardware component that enables a device to connect to a network. It provides the physical connection between the device and the network.

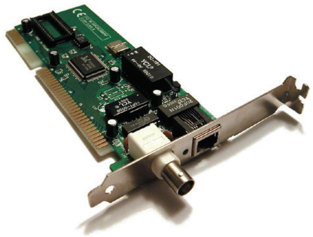


Fig. 3.1.11: Network Interface Card

- **Firewall:** A firewall is a device that monitors and controls the traffic between different networks. It is often used to protect a network from unauthorized access and to prevent malicious attacks.
- **Server:** A server is a computer system that provides network services to other devices on the network. It can provide services such as file sharing, email, and web hosting.

All of these broadband network elements work together to provide users with high-speed internet connectivity and the ability to connect multiple devices on the same network.

3.1.4 Gateways

A gateway is a device that connects two different networks or network segments together. It acts as a bridge between networks that use different protocols or communication methods. The main function of a gateway is to translate data from one format to another, making it possible for different networks to communicate with each other.

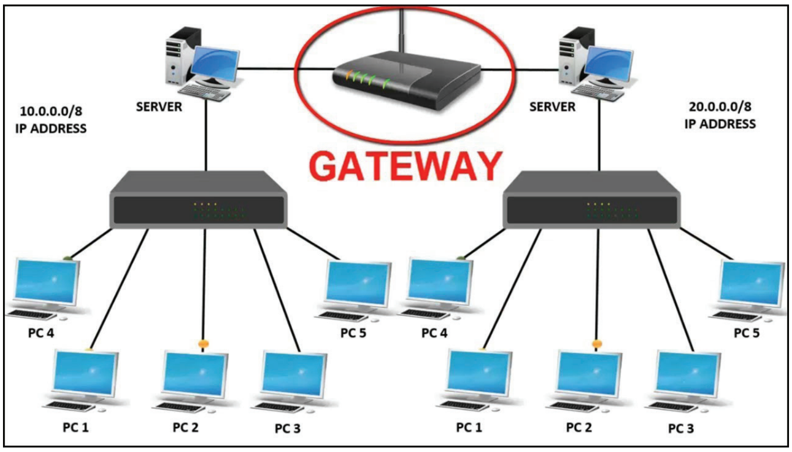


Fig. 3.1.12: Gateway

In broadband networks, gateways are used to connect local area networks (LANs) to the wider internet or other external networks. They act as an interface between the LAN and the external network, allowing data to be transmitted between the two. Gateways are usually equipped with security features such as firewalls to protect the LAN from unauthorized access or attacks from the internet.

Gateways can also perform other functions, such as protocol conversion, traffic management, and network monitoring. For example, a gateway can convert data from one protocol to another, such as translating IP traffic to ATM traffic for transmission over an ATM network. It can also prioritize traffic based on the type of data or application, ensuring that important traffic such as voice or video is given higher priority than less critical data.

3.1.5 TCP/IP

TCP/IP (Transmission Control Protocol/Internet Protocol) is a set of protocols that defines how data is transmitted across a network. It is the most widely used protocol in the world for connecting devices and systems to the internet.

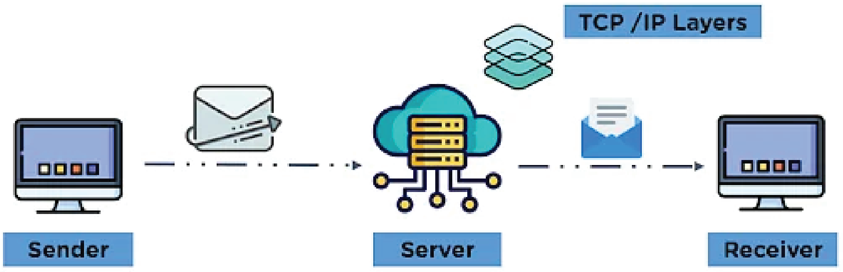


Fig. 3.1.13: TCP/IP Model

TCP/IP has two main components:

- Transmission Control Protocol (TCP)
- Internet Protocol (IP)

The IP part of the protocol is responsible for addressing and routing packets of data across a network. The TCP part of the protocol is responsible for ensuring that the data is transmitted correctly, without errors, and in the correct order.

When data is sent across a network using TCP/IP, it is divided into small packets of data. Each packet is sent separately across the network to the destination device, where they are reassembled into the original data. The IP part of the protocol is responsible for ensuring that each packet is sent to the correct destination address and that the packets are routed through the network in the most efficient way.

The TCP part of the protocol ensures that the packets are sent in the correct order and that there are no errors or data loss during transmission. It does this by using a three-way handshake process to establish a connection between the sending and receiving devices. This process includes establishing a session, acknowledging the session, and then closing the session when the data transmission is complete.

TCP/IP is used in a wide range of applications and devices, including web browsing, email, file sharing, and many other internet-based services. It is an essential part of modern networking and enables devices and systems to communicate with each other across the world.

3.1.6 IP Address

An IP (Internet Protocol) address is a unique identifier assigned to devices connected to a network that uses the Internet Protocol for communication. It is a 32-bit number (IPv4) or a 128-bit number (IPv6) that is used to identify a device on the network.

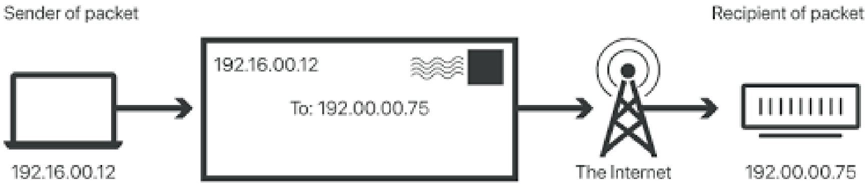


Fig. 3.1.14: Internet Protocol (IP) Address

In IPv4, an IP address is represented as four groups of numbers separated by dots, such as 192.168.0.1. The IP address is divided into two parts: the network address and the host address. The network address is used to identify the network, while the host address is used to identify the specific device on the network.

In IPv6, an IP address is represented as eight groups of four hexadecimal digits separated by colons, such as 2001:0db8:85a3:0000:0000:8a2e:0370:7334. IPv6 addresses are designed to provide a large number of unique addresses and to improve the efficiency of packet routing.

IP addresses are necessary for devices to communicate with each other on a network. When a device wants to send data to another device, it needs to know the IP address of the destination device. IP addresses can be assigned manually or dynamically using protocols such as DHCP (Dynamic Host Configuration Protocol).

It is important to note that IP addresses are not permanent and can be changed, especially in cases where a device is moved to a different network or a new network is added. Additionally, IP addresses can be private or public, and the distinction is important for security and routing purposes.

3.1.7 Subnet Masks

A subnet mask is a numerical code used in Internet Protocol (IP) address configuration to identify the network and the nodes within that network. In essence, the subnet mask provides a way for a computer to distinguish between the network and the host portions of an IP address.

An IP address consists of four 8-bit numbers separated by periods. For example, 192.168.0.1 is a typical IP address. The subnet mask also consists of four 8-bit numbers separated by periods, such as 255.255.255.0.

The subnet mask works by indicating which bits of an IP address identify the network and which bits identify the host. The 1s in the subnet mask indicate the network portion of the IP address, while the 0s indicate the host portion.

For example, if the subnet mask is 255.255.255.0, the first three numbers of the IP address (192.168.0) identify the network, and the final number (1) identifies the host. This means that there can be up to 254 devices (2^8-2, since some IP addresses are reserved for special purposes) on the network, with each device having a unique host ID.

Subnet masks can be adjusted to create smaller networks within a larger network, which can improve network performance and security. By dividing a larger network into smaller subnets, it is possible to reduce the number of devices on each network segment, which can reduce traffic and improve performance. Additionally, by creating separate subnets, it is possible to limit the broadcast traffic on each subnet, which can improve security and reduce network congestion.

3.1.8 IPv4 and IPv6

IPv4 and IPv6 are two versions of the Internet Protocol (IP) used to identify and communicate with devices on a network. IPv4 is the older version and has been in use since the early days of the internet, while IPv6 is the newer version and was developed to address the limitations of IPv4.

IPv4 uses a 32-bit address space, which allows for approximately 4.3 billion unique addresses. However, with the growth of the internet and the increasing number of connected devices, this address space has become exhausted, and it is becoming more difficult to allocate new addresses.

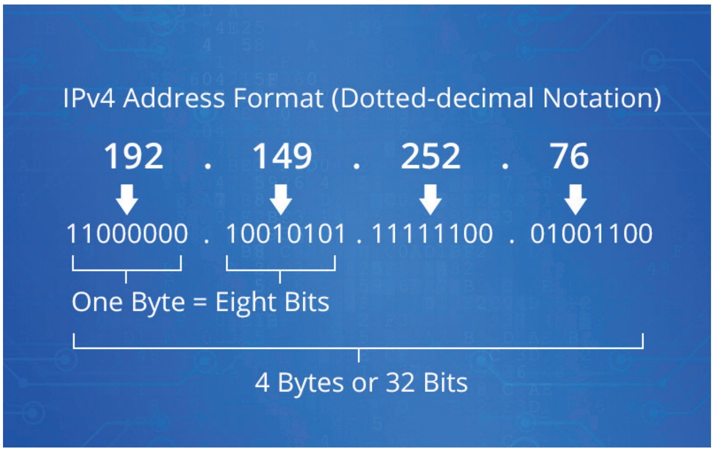


Fig. 3.1.15: IPv4 Address Format

IPv6 uses a 128-bit address space, which allows for a virtually unlimited number of unique addresses (approximately 3.4 x 10^38 addresses). In addition to the larger address space, IPv6 includes other improvements over IPv4, such as built-in security features, simplified header format, and better support for multicast communication.

One of the main differences between IPv4 and IPv6 is the way they represent IP addresses. IPv4 addresses are represented as a series of four decimal numbers separated by periods, with each number ranging from 0 to 255. For example, 192.168.0.1 is a typical IPv4 address.

In contrast, IPv6 addresses are represented as eight groups of four hexadecimal digits separated by colons. For example, 2001:0db8:85a3:0000:0000:8a2e:0370:7334 is a typical IPv6 address. IPv6 addresses can also be shortened by removing leading zeroes and consecutive groups of zeroes can be replaced with two colons.

Both IPv4 and IPv6 are used today, but IPv6 adoption is gradually increasing as the number of devices connected to the internet continues to grow.

3.1.9 Ethernet address / MAC Address

An Ethernet address, also known as a Media Access Control (MAC) address, is a unique identifier assigned to a network interface controller (NIC) for use as a network address in communications within a network segment. It is a 48-bit address that is usually represented as a series of 12 hexadecimal digits, such as "00:11:22:33:44:55".

MAC addresses are typically displayed in hexadecimal notation, which consists of the numbers 0-9 and letters A-F. The first three sets of two characters (separated by colons or dashes) represent the vendor or manufacturer of the network interface card, while the last three sets of two characters represent a unique identifier for that particular device.

For example, the MAC address 00-1B-63-84-45-E6 could be decoded as follows:

The first set of characters (00-1B-63) represents the vendor or manufacturer, in this case, Apple Inc.

The last three sets of characters (84-45-E6) represent a unique identifier for a particular device, such as a MacBook or iPhone.

The Ethernet address is used to identify devices on a Local Area Network (LAN). When data is transmitted over a network, it is sent to a destination address. The destination address is the Ethernet address of the device to which the data is being sent. The source address is the Ethernet address of the device that is sending the data.

MAC address/Ethernet addresses are assigned by the manufacturer of the NIC and are stored in the hardware of the device. They are used by the data link layer of the OSI model to control access to the network media and to ensure that data is delivered to the intended recipient.

There are several ways to find the MAC address of a device, depending on the operating system and device type. Here are some common methods:

Using the Command Prompt/Terminal:

For Windows: Open the Command Prompt and type "ipconfig /all". Look for the "Physical Address" which is the MAC address.

For Mac: Open the Terminal and type "ifconfig -a". Look for the "ether" section which is the MAC address.

Using the Settings:

For Windows: Go to the Settings and select "Network & Internet". Click on "Ethernet" or "Wi-Fi" and then click on "Hardware properties". The MAC address will be listed under "Physical address".

For Mac: Go to the Apple menu and select "System Preferences". Click on "Network" and then select the network connection. Click on "Advanced" and then select the "Hardware" tab. The MAC address will be listed as "Wi-Fi Address" or "Ethernet Address".

On a Mobile Device:

For iOS: Go to the Settings and select "General". Tap on "About" and then scroll down to find the "Wi-Fi Address".

For Android: Go to the Settings and select "About phone". Tap on "Status" and then scroll down to find the "Wi-Fi MAC address" or "Bluetooth address".

It is important to note that the Ethernet address/MAC Address is not the same as the IP address, which is used at the network layer of the OSI model for routing data between networks. While the Ethernet address is used for communication within a local network segment, the IP address is used for communication between different network segments.

3.1.10 Connecting Laptop/PC with Wi-Fi

1. **Installation**

   Acquire a wireless router

   There are a variety of factors that will determine which router is best for you. These include distance, interference, transfer speed, and security.

   - One of the most important factors to consider when purchasing a router is the distance between the router and the devices that you are wirelessly connecting. More expensive routers generally have more antennae, which can lead to a more stable connection at further distances.
   - Another factor to consider is the amount of signal interference. If you have multiple devices that operate on the 2.4 GHz band, such as microwaves and cordless phones, these can interfere with the Wi-Fi signal. Newer routers can operate on the 5 GHz band, which is much less crowded and thus less prone to interference. The drawback is that 5 GHz signals do not travel as far as 2.4 GHz signals.
   - Transfer speed is a feature to consider. Newer routers claim to be able to transfer data up to 450 Mbps. While this may be helpful when moving data between two computers over a network, it will not increase your general Internet speed, as this is set by your ISP. There are three main router speeds available: 802.11g (54 Mbps) 802.11n (300 Mbps), and 802.11ac (450 Mbps). It is important to note that these speeds are virtually impossible to attain in any environment other than a clean room free of signal interference.
   - Finally, make sure that the router you are purchasing has the latest form of wireless encryption, WPA2. This is pretty much standard in all new routers, but is something to consider if purchasing an older, second-hand router. Older encryption algorithms are much less secure; a WEP key can be cracked in just a few minutes.

   Connect the router to your modem.

   Once you've purchased your router, you will need to connect it to your modem. The router will have a port in the back labeled WAN/WLAN/Internet. Connect this port to the modem using a standard Ethernet cable.

   Make sure that the router is properly powered and turned on.

Connect a computer via Ethernet cable.

This step is not always necessary, but can be very useful if you want to set up the wireless router before connecting any wireless devices to it. Connecting a computer through a physical cable will allow you to tinker with the wireless settings without losing your connection to the router.

For optimum efficiency while setting up the router, plug it in next to your computer while you adjust the settings. After you are finished configuring the router, you can move it to where it will normally stay.

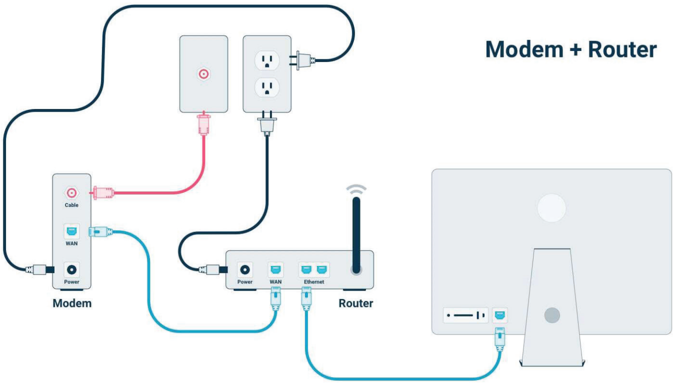


Fig. 3.1.16: Connect Wireless Router with Modem and Computer via Ethernet Cable

2. **Configuration**

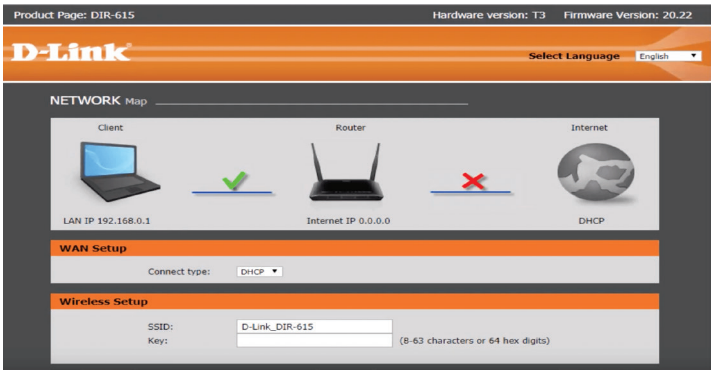
Install the router software.

Not every router comes with software to install, but if yours did, then install it on a computer that is connected to the router via an Ethernet cable. Using the bundled software makes setting up a router much more convenient than going in to the configuration menus.

- Using the software, designate the name of your wireless network, and the type of security that you want to use. Choose WPA2 for the most secure network. Choose a password and continue.
- Most router software will automatically detect your internet settings. This is the information that the router needs to translate your internet connection and transfer it to all of your wirelessly connected devices.

Open the router's configuration page.

If your router did not come with any installation software, you will need to connect to the router's configuration page through your web browser. Open your browser of choice and enter the web address for the router. This is typically 192.168.1.1 or 192.168.0.1. Consult the documentation that came with the router to find the exact address.



Product Page: DIR-615 Hardware version: T3 Firmware Version: 20.22

LAN IP 192.168.0.1

Internet IP 0.0.0.0

DHCP

WAN Setup

Connect type: DHCP

Wireless Setup

SSID: D-Link_DIR-615

Key: (8-63 characters or 64 hex digits)

Fig. 3.1.17: Router Configuration page

You will be asked for a username and password to continue into the router configuration. These are also provided in the documentation that came with your router. Typical defaults are username: admin and Password: password or admin.

Enter your Internet connection information.

This includes the IP address and DNS information from your internet service provider. Most routers will fill this section in automatically. If it does not, contact your ISP for the information that you need to enter.

Set your wireless settings.

Most routers will have a Wireless Settings section towards the top of the router's menu. From this section you can enable or disable the wireless signal, change the network name, and set the encryption.

- To set the name of the network, select the SSID field. This is the name that will be displayed on any device that detects your network. If you are living in an area with a lot of public traffic, avoid putting any identifiable information in the SSID, as anyone with a wireless device can see it.
- Make sure to set the encryption to the latest version allowed by your router. In most cases, this will be WPA2. WPA2 operates with a single password. You can enter whatever you'd like, but a strong password is recommended. Stronger passwords contain upper and lowercase letters, numbers, and symbols.

Apply your settings.

Make sure you click the Apply or Save Changes button in your router's configuration when you are done changing the settings. The router will process for a moment, and your new settings will take effect.

Place your router.

In order to get the best possible signal, try to place your router in a central location. Keep in mind that any obstacles such as walls and doors will degrade the signal. If you have multiple floors, you may want to consider multiple routers to ensure that you have the coverage you need.

- Remember that it must be physically connected to your modem, so this may limit your options when placing the router.

3. **Connection**

Connect a device to the network.

Once the router is broadcasting a wireless signal, you can test the connection by scanning for wireless networks using a Wi-Fi device such as another computer, a smartphone, a tablet, etc.

Scan for new networks. In Windows, click the network icon in the system tray in the lower-right corner of the desktop. Select Connect to a Network and look for your SSID. On a Mac, click the AirPort icon in the menu bar, which looks like 3 curved lines. Select your SSID from the list of available networks.

Enter the password.

If you enabled WPA2 encryption, you will need to enter your password to connect to the network. If you are using a private computer, you can disable the hidden characters on some systems to let you see the password you are typing easier.

Test your connection.

Once you are connected to the network, wait a moment for your IP address to be assigned. Open a web browser and try to connect to a website you don't normally visit, as this will ensure that you aren't loading the website from memory.

3.1.11 Command Line Access / Command Prompts

Command line access or Command Prompt provides a text-based interface to execute basic commands on a computer system. This interface allows the user to interact with the operating system and execute various commands without using a graphical user interface (GUI).

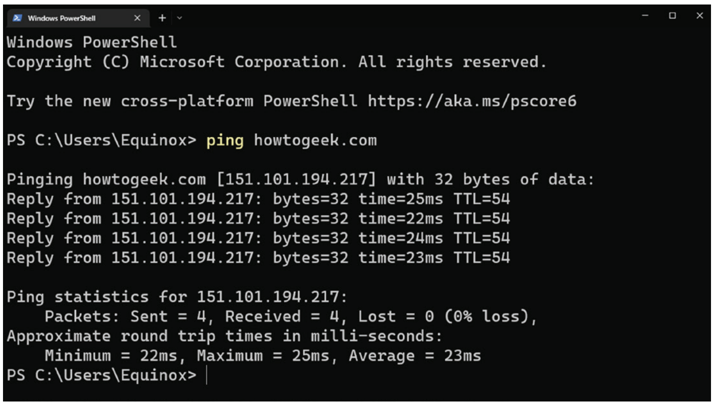
It allows users to execute a wide range of commands, perform system tasks, and automate processes. Here are the basic steps for using the command prompt:

- **Open the command prompt:** To open the command prompt, click on the Start menu, type "cmd" in the search box, and hit Enter. Alternatively, you can press the Windows key + R, type "cmd" in the Run box, and press Enter. On a Mac, open the Terminal application by navigating to Applications > Utilities > Terminal. Once you have opened the command line, you can start typing commands.
- **Navigate to a directory:** To change the current directory, use the "cd" command. For example, to change to the "Documents" directory, type "cd Documents" and press Enter.
- **View the contents of a directory:** To view the contents of a directory, use the "dir" command. For example, to view the contents of the "Documents" directory, type "dir" and press Enter.
- **Run a program or file:** To run a program or file, type the name of the program or file, followed by any required parameters. For example, to run the "notepad" program, type "notepad" and press Enter.
- **Execute a command:** To execute a command, type the command and any required parameters, and press Enter. For example, to check the IP configuration of the computer, type "ipconfig" and press Enter.
- **Use flags and switches:** Many commands have optional flags and switches that can be used to modify their behavior. For example, the "dir" command has a "/w" switch that displays the contents of a directory in a wide format. To use the "/w" switch, type "dir /w" and press Enter.

Basic Commands

When troubleshooting network connectivity issues, there are several basic commands that can be used in the command prompt to help identify and diagnose problems. Some of the most common commands include:

- **ipconfig -** This command displays information about the network configuration on the local computer, including the IP address, subnet mask, and default gateway.
- **ping -** This command sends a series of packets to a specified network address or hostname to test connectivity. It can help determine whether a network connection is working or not, and can be used to diagnose problems with DNS or routing.



```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\Users\Equinox> ping howtogeek.com

Pinging howtogeek.com [151.101.194.217] with 32 bytes of data:
Reply from 151.101.194.217: bytes=32 time=25ms TTL=54
Reply from 151.101.194.217: bytes=32 time=22ms TTL=54
Reply from 151.101.194.217: bytes=32 time=24ms TTL=54
Reply from 151.101.194.217: bytes=32 time=23ms TTL=54

Ping statistics for 151.101.194.217:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 22ms, Maximum = 25ms, Average = 23ms
PS C:\Users\Equinox>
```

Fig. 3.1.18: Ping Test

- **tracert -** This command traces the path that packets take from the local computer to a specified network address or hostname. It can be used to identify network problems such as routing loops, network congestion, or unreachable hosts.
- **netstat -** This command displays statistics about network connections, including the current state of each connection, the local and remote IP addresses, and the protocol being used. It can be used to identify problems with open network connections or to monitor network traffic.
- **nslookup -** This command queries DNS servers to look up the IP address associated with a specified hostname. It can be used to diagnose problems with DNS resolution, such as when a website is not resolving correctly.

3.1.12 Configuration Settings at Wi-Fi Equipment and Wi-Fi Access Points

Configuration settings are used to set up and manage Wi-Fi equipment and access points. They include a range of parameters that define the behavior of the device, such as network information, security settings, and radio frequency settings.

Here are some of the key configuration settings for Wi-Fi equipment and access points:

- **Network name (SSID):** This is the name that is broadcast by the access point and identifies the wireless network. It must be unique and recognizable, and should not contain any personal or sensitive information.
- **Network mode:** The network mode defines the protocol and frequency band used by the access point. Common modes include 802.11a, 802.11b, 802.11g, 802.11n, and 802.11ac.
- **Channel:** This setting determines the specific radio frequency channel used by the access point. In the 2.4 GHz band, there are 11 channels, while the 5 GHz band has many more channels to choose from.
- **Security mode:** This setting defines the type of security used to protect the Wi-Fi network. Common security modes include WEP, WPA, and WPA2. It is important to choose a strong security mode and set a strong password to prevent unauthorized access.
- **Encryption:** Encryption is used to secure the wireless data transmitted between the access point and client devices. Common encryption types include WEP, TKIP, and AES.
- **Transmit power:** This setting controls the strength of the wireless signal transmitted by the access point. Higher transmit power can improve coverage, but can also cause interference with other nearby networks.

- **Quality of Service (QoS):** QoS settings allow you to prioritize network traffic and ensure that important applications receive adequate bandwidth.
- **Access control:** Access control settings allow you to restrict access to the wireless network based on MAC address, IP address, or other criteria.

To configure these settings, you will need to access the management interface of the Wi-Fi equipment or access point. This is typically done through a web browser, using a specific IP address assigned to the access point. Once you have accessed the management interface, you can modify the configuration settings as needed. It is important to carefully review and test the settings before deploying the access point to ensure that the network is secure and functioning correctly.

3.1.13 Recording Configuration Setting

Recording configuration settings is an important step in documenting the setup of a Wi-Fi network. This can be useful for troubleshooting, reconfiguration, and maintenance of the network.

Here are the steps to record configuration settings for a Wi-Fi network:

- **Identify the device and location:** Record the name of the device, its model number, and its location in the network.
- **List the configuration settings:** Record the various settings configured on the device. These may include the SSID (network name), security settings (encryption type and password), DHCP settings, IP address and subnet mask, DNS settings, port forwarding settings, and other settings that may have been changed from the default configuration.

  To list the configuration settings of a device, you can use various methods depending on the type of device and the operating system it is running. Here are some common ways to list the configuration settings:

  - **On a Windows computer:** Open the Command Prompt and type "ipconfig /all" to see the IP address, subnet mask, default gateway, and other network configuration settings. You can also use the "netsh wlan show settings" command to see the Wi-Fi adapter configuration settings.
  - On a Mac computer: Open the Terminal and type "ifconfig" to see the IP address, subnet mask, and other network configuration settings. You can also use the "networksetup -getinfo Wi-Fi" command to see the Wi-Fi adapter configuration settings.
  - **On an iOS device:** Go to Settings > Wi-Fi and tap the (i) icon next to the network you are connected to. You will see the IP address, subnet mask, router, and DNS server information.
  - **On an Android device:** Go to Settings > Network & internet > Wi-Fi and tap the (i) icon next to the network you are connected to. You will see the IP address, gateway, DNS server, and other network configuration settings.
- **Record the date and time:** Note the date and time when the configuration settings were recorded. This can be useful in tracking changes to the network over time.
- **Include any relevant notes:** Record any other notes that may be relevant to the configuration, such as any changes made to the default settings, any issues encountered during configuration, or any special configurations required for specific devices or applications.
- **Store the configuration settings:** Store the recorded configuration settings in a safe and easily accessible location, such as a secure file storage system or a network documentation system.

Notes

UNIT 3.2: Establishing Connectivity

Unit Objectives

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

1. Explain standard troubleshooting methodologies for network failures, slow speeds, and intermittent connectivity issues.
2. Explain best practices for maintaining customer satisfaction, including clear communication of service expectations and troubleshooting guidance.
3. Show how to conduct a ping test to the service provider gateway and analyze latency, packet loss, and jitter parameters.
4. Demonstrate how to validate throughput performance using network testing tools and document results.
5. Show how to configure end-user devices with appropriate SSIDs, security credentials, and DNS settings.
6. Demonstrate how to verify end-user connectivity by executing network diagnostic commands and troubleshooting connectivity issues.
7. Show how to perform a security compliance check by testing firewall settings, encryption status, and unauthorized access points.
8. Demonstrate how to maintain accurate records of network configurations, including IP assignments, security protocols, and firmware versions.
9. Show how to document testing procedures, expected results, and any deviations observed during connectivity tests.
10. Demonstrate how to create a troubleshooting log with identified issues, root causes, and corrective actions taken.
11. Show how to educate customers on basic troubleshooting techniques and network optimization tips.

3.2.1 Establishing Connectivity with Service Provider Gateway

Establishing connectivity with the service provider gateway involves configuring the network settings of the Wi-Fi equipment to connect to the gateway provided by the service provider. The following steps outline the basic process:

- Connect the Wi-Fi equipment to the service provider gateway using an Ethernet cable.
- Access the configuration settings of the Wi-Fi equipment through a web browser using the default IP address provided in the user manual.
- Enter the login credentials provided by the service provider or create a new account with a username and password.
- Navigate to the network settings and select the appropriate connection type, such as DHCP or static IP, as required by the service provider.

- Enter the network details provided by the service provider, including the IP address, subnet mask, default gateway, and DNS servers.
- Save the configuration settings and restart the Wi-Fi equipment to apply the changes.
- Test the connectivity to the service provider gateway by pinging the default gateway IP address or accessing the internet through the Wi-Fi equipment.

Establish Connectivity between Wi-Fi Backhaul Equipment, Wi-Fi Access Points and End user Devices

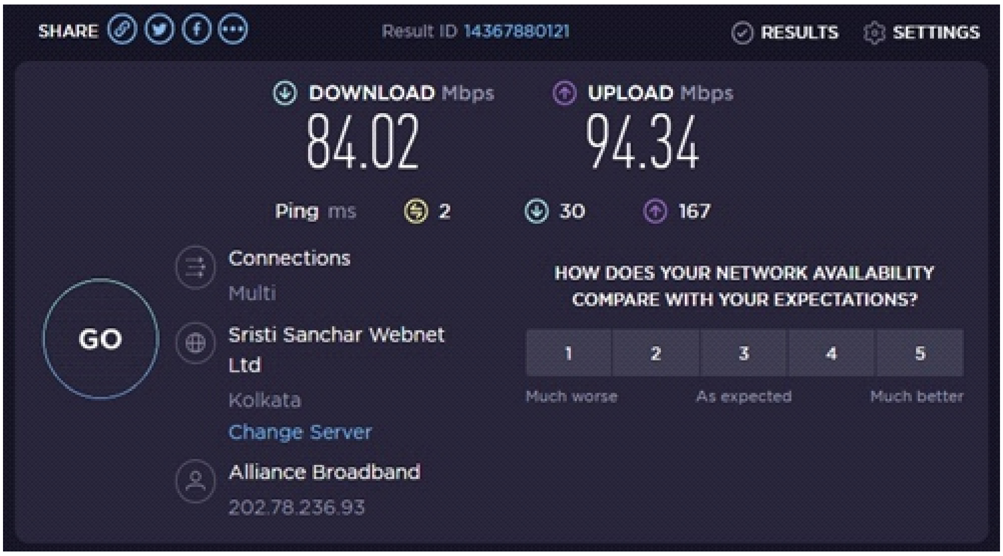
The steps to establish connectivity between Wi-Fi backhaul equipment, Wi-Fi access points, and end-user devices may vary depending on the specific equipment and network configuration. However, here are some general steps that may be involved:

- Install the Wi-Fi backhaul equipment: Install and configure the Wi-Fi backhaul equipment, such as wireless bridges or access points, according to the manufacturer's instructions. This may include mounting the equipment, connecting it to power, and configuring its network settings, such as IP address, subnet mask, and default gateway.
- Connect the Wi-Fi backhaul equipment: Connect the Wi-Fi backhaul equipment to the existing network infrastructure, such as switches or routers, using Ethernet cables. Make sure the cables are securely connected and that any necessary VLAN or QoS settings are configured.
- Configure the Wi-Fi access points: Install and configure the Wi-Fi access points, such as routers or wireless access points, according to the manufacturer's instructions. This may include configuring their network settings, such as SSID, security settings, and DHCP server.
- Connect the Wi-Fi access points: Connect the Wi-Fi access points to the Wi-Fi backhaul equipment using Ethernet cables or wireless links. Make sure the access points are securely connected and that their configuration settings are properly configured.
- Configure the end-user devices: Configure the end-user devices, such as laptops or smartphones, to connect to the Wi-Fi network. This may involve selecting the appropriate network name (SSID), entering any necessary security settings, such as a password or passphrase, and configuring the device's IP settings if necessary.
- Test the connectivity: Once the devices are connected, test the connectivity by accessing various resources on the network, such as a website or a file share. Verify that the devices are able to communicate with each other and that the network is performing as expected.
- Troubleshoot as needed: If any issues arise during the connectivity testing, troubleshoot the network to identify and resolve the problems. This may involve checking the network configuration settings, reviewing logs and error messages, and testing different components of the network to isolate the source of the issue.

3.2.2 Conduct Speed Test of the Connection

To conduct a speed test of the connection and demonstrate its functioning to the customer, you can follow these steps:

- Choose a reliable and reputable speed testing website or application, such as Ookla's Speedtest.net, Google's speed test, or Fast.com.
- Make sure that there is no other network activity going on, such as downloads or streaming, which could interfere with the accuracy of the test.
- Connect your device to the Wi-Fi network and access the speed test website or application.



Result ID 14367880121

DOWNLOAD Mbps 84.02

UPLOAD Mbps 94.34

Ping ms 2 30 167

Connections Multi

Sristi Sanchar Webnet Ltd Kolkata

Alliance Broadband 202.78.236.93

HOW DOES YOUR NETWORK AVAILABILITY COMPARE WITH YOUR EXPECTATIONS?

Fig. 3.2.1: Ookla's Speedtest.net

- Run the speed test and record the results. The speed test should measure the download and upload speeds as well as the ping time.
- Share the results with the customer and explain what the results mean in terms of network performance.
- If the results are not up to the expected standards, troubleshoot the network to identify and address any issues that may be causing the slow speeds.
- Re-run the speed test after troubleshooting and ensure that the results meet the expected standards.
- Confirm with the customer that the Wi-Fi network is working as expected, and ask if they have any further questions or concerns.
- Provide the customer with a summary of the speed test results and any troubleshooting steps that were taken to address any issues.

3.2.3 Ping Test

A **ping test** is like sending a "Hello, are you there?" message to another computer or server on the network and measuring how quickly it replies.

- **Latency** = How long the reply takes.
- **Packet Loss** = How many "Hello" messages never came back.
- **Jitter** = How much the reply times vary.

2. Steps to Do a Ping Test

Windows

1. Press **Windows Key + R**, type cmd, and press **Enter**.
2. Type:

css

CopyEdit

```
ping [Gateway_IP] -n 10
```

Example:

nginx

CopyEdit

```
ping 192.168.1.1 -n 10
```

(-n 10 means send 10 pings.)

Mac / Linux

1. Open **Terminal**.
2. Type:

css

CopyEdit

```
ping -c 10 [Gateway_IP]
```

3. Understanding the Results

- **Latency (ms)** → Look for the **time=XXms** in each line. Lower is better (under 50 ms is good for most networks).
- **Packet Loss (%)** → At the end of the ping, it will say something like Lost = 0 (0% loss) — you want **0%**.
- **Jitter (variation)** → Look at the difference between fastest and slowest ping times. If one ping is **10 ms** and another is **50 ms**, you have high jitter (bad for video calls/gaming).

4. Example Output (Windows)

python

CopyEdit

```
Reply from 192.168.1.1: bytes=32 time=12ms TTL=64
Reply from 192.168.1.1: bytes=32 time=13ms TTL=64
Reply from 192.168.1.1: bytes=32 time=15ms TTL=64
```

```
Ping statistics for 192.168.1.1:
Packets: Sent = 10, Received = 10, Lost = 0 (0% loss)
Approximate round trip times in milli-seconds:
Minimum = 12ms, Maximum = 15ms, Average = 13ms
```

- **Latency**: Average = 13 ms
- **Packet Loss**: 0% (good)
- **Jitter**: Max (15 ms) – Min (12 ms) = 3 ms (very low, good)

Minimum = 12ms, Maximum = 15ms, Average = 13ms

- **Latency**: Average = 13 ms
- **Packet Loss**: 0% (good)
- **Jitter**: Max (15 ms) – Min (12 ms) = 3 ms (very low, good)

3.2.4 Documenting Testing Procedure

Steps to Document Connectivity Test Results

Step 1 – Record Basic Test Information

- Date and time of the test
- Location/site details
- Equipment details (model, firmware, serial number)
- Name of the tester
- Purpose of the test

Step 2 – Describe the Testing Procedure

- Test method used (e.g., ping test, throughput test, signal strength check)
- Tools or software used
- Test parameters (number of pings, frequency band, SSID, test duration)

Step 3 – Define Expected Results

- Set clear pass/fail criteria before testing
- Examples:
  - Latency ≤ 50 ms
  - Packet loss = 0%
  - Signal strength ≥ −65 dBm

Step 4 – Record Actual Results

- Document exactly what happened during the test
- Use numbers, screenshots, or tables for clarity

Step 5 – Identify Deviations

- Note any differences between expected and actual results
- Describe possible causes
- State the impact on network performance

Step 6 – Document Corrective Actions

- Write down steps taken to fix issues
- Include whether the fix was successful or if escalation was needed

Step 7 – Final Sign-Off

- Tester's name and signature
- Supervisor verification (if required)
- Reference any related job tickets or reports

Summary

- Concept of Wireless Technology
- Network Topologies
- Broadband Network Elements
- Gateways
- TCP/IP
- IP address
- Subnet Masks
- IPv4 and IPv6
- Ethernet address / MAC Address
- Connecting Laptop/PC with Wi-Fi
- Command Line Access / Command Prompts
- Configuration Settings at Wi-Fi Equipment and Wi-Fi Access Points
- Explain the Process to Record Configuration Setting
- Establishing Connectivity with Service Provider Gateway
- Conduct Speed Test of the Connection
- Conducting Ping Test
- Documenting Testing Procedure

Exercise

Multiple-choice Question

1. _________ is a type of communication technology that uses radio waves or microwaves to transmit data or signals without the need for physical wires or cables

   a. Cordless technology   b. Wireless technology

   c. Fireless technology   d. None of the above

2. A network __________ refers to the layout or structure of a network

   a. geology   b. physiology

   c. topology   d. None of the above

3. A __________ is a device that connects to the internet service provider (ISP) network to provide internet connectivity to the user's device

   a. modem   b. router

   c. switch   d. None of the above

4. A ___________ is a device that connects two different networks or network segments together

   a. passage   b. corridor

   c. gateway   d. None of the above

5. __________ is the immediate assistance or treatment given to someone who is injured or suddenly becomes ill before the arrival of a medical professional.

   a. Local Anesthesia   b. First aid

   c. ayurveda   d. None of the above

Descriptive Questions:

1. Explain the evolution of wireless technology
2. Explain the advantages and disadvantages of Hybrid topology
3. What is Network Interface Card?
4. How to access command prompt on windows system?
5. What is the significance of first aid box at workplace?

Notes

Scan the QR codes or click on the link to watch the related videos

https://www.youtube.com/watch?v=I2PKJslPObM

Wireless Technology

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

Wireless OR Wired Backhaul Benefits

https://www.youtube.com/watch?v=CsektxtqA8c

TCP/IP Protocol Explained

https://www.youtube.com/watch?v=TIiQiw7fpsU

MAC Address Explained

https://www.youtube.com/watch?v=8assGpZvwG4

What Should be in a First Aid Kit?

सत्यमेव जयते
GOVERNMENT OF INDIA
MINISTRY OF SKILL DEVELOPMENT
& ENTREPRENEURSHIP

4. Diagnosing and Rectifying Wireless Network Faults

Unit 4.1 - Prepare for Troubleshooting Wi-Fi Backhaul Equipment

Unit 4.2 - Troubleshoot Wi-Fi Network Setup

TEL/N4124

Key Learning Outcomes

At the end of this module, you 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: Prepare for Troubleshooting Wi-Fi Backhaul Equipment

Unit Objectives

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

1. Describe the types, specifications, and limitations of network cables, connectors, and feeder cables.
2. Explain industry standards and best practices for cable crimping, soldering, and termination.
3. Discuss the functionality and usage of test equipment such as network testers, spectrum analyzers, and cable testers.
4. Determine the impact of Electromagnetic Interference (EMI) and Electromagnetic Compatibility (EMC) on network performance.
5. Discuss safety procedures for handling electrical equipment, including grounding and surge protection.
6. Describe risk assessment techniques and incident response protocols for network failures.
7. Explain escalation processes for unresolved faults and emergency incidents, such as power failures and system crashes.
8. Demonstrate how to conduct continuity tests using appropriate tools and localize fault distance.
9. Show how to perform re-connectorization/crimping of cable pairs with connectors or replace faulty cables.
10. Demonstrate how to replace feeder cables or antennas as per network specifications.
11. Show how to conduct signal and interference tests to validate cable performance.
12. Demonstrate how to reconfigure network devices, if necessary, after cable replacement.
13. Show how to interpret status and error indicators on the Wi-Fi backhaul equipment.
14. Demonstrate how to connect and operate a handheld network tester for fault diagnosis.
15. Show how to use cable and antenna testers to check connectivity and performance.
16. Demonstrate how to verify and adjust antenna alignment for optimal signal strength.
17. Show how to analyze diagnostic results to localize and rectify faults in backhaul connectivity.

4.1.1 EMI/EMC Concepts

EMI stands for Electromagnetic Interference, while EMC stands for Electromagnetic Compatibility. These are related concepts in the field of electronics and refer to the ability of electronic devices to function properly in the presence of electromagnetic interference.

EMI is the unwanted disturbance or noise that is induced in an electronic circuit or device due to the presence of electromagnetic radiation from other sources, such as radio waves, electrical motors, or other electronic devices. EMI can cause errors or malfunctions in electronic systems, and can be particularly problematic in wireless communications, where the received signal can be swamped by interference from other sources.

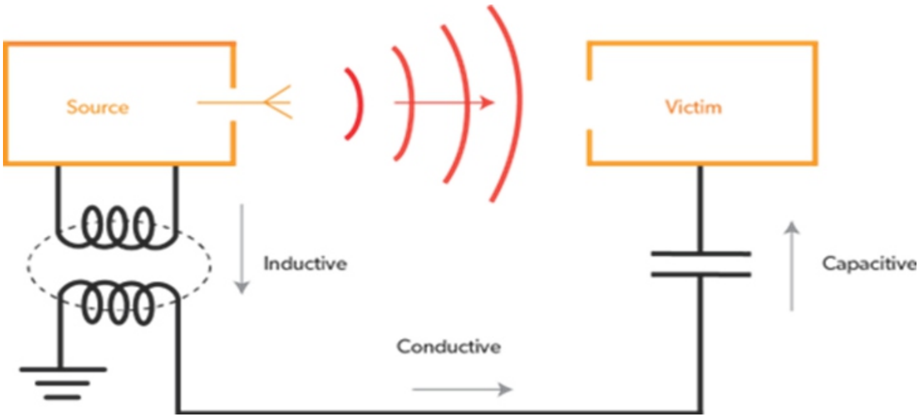


Fig. 4.1.1: Electromagnetic Interference (EMI)

EMC, on the other hand, is the ability of electronic devices to operate properly in the presence of EMI. When electronic devices are in operation, they generate electromagnetic fields that can affect other electronic devices in the vicinity. Conversely, other electronic devices in the environment can also generate electromagnetic fields that can interfere with the operation of the device in question.

EMC is an important consideration in the design, manufacture, and operation of electronic devices. In order to ensure that electronic devices can operate reliably in their intended environment, they must be designed to comply with established standards for EMC.

To prevent EMI/EMC issues, modem manufacturers and installers can take several approaches:

- Shielding: Modems can be shielded with conductive materials, such as metal casings or coatings, to prevent EMI from escaping the device.
- Grounding: Proper grounding of the modem and other electronic devices in the installation can reduce the buildup of electrical charges that can lead to EMI.
- Filtering: Filters can be installed to attenuate the frequencies that are causing EMI.
- Layout: The layout of the installation can also be optimized to reduce EMI, such as by separating sensitive electronic devices from sources of EMI.
- Compliance: Modem manufacturers can ensure their devices comply with industry standards for EMI/EMC.

4.1.2 Re-Configuring the Wi-Fi Backhaul Equipment

Re-configuring the Wi-Fi backhaul equipment at the end user devices may be necessary to address issues with the wireless network, such as poor signal strength or interference from other devices. In some cases, the end user devices may need to be reconfigured to work with the Wi-Fi network or to troubleshoot connectivity problems. This process can involve adjusting various settings such as the IP address, subnet mask, gateway address, DNS server address, and Wi-Fi channel.

The process for re-configuring the Wi-Fi backhaul equipment can vary depending on the specific equipment being used and the nature of the changes that need to be made. However, some general steps that may be involved in the re-configuration process are:

- **Identify the need for re-configuration:** Determine the specific reason why the Wi-Fi backhaul equipment needs to be re-configured, such as a change in network topology, a need to update security settings, or performance issues.
- **Gather the necessary information:** When re-configuring Wi-Fi backhaul equipment at the service provider gateway or end user devices, it is important to gather all the necessary information before making any changes. This can help ensure that the new configuration is accurate and that the network functions properly.

  Identify the specific device that needs to be reconfigured, such as the service provider gateway, Wi-Fi access point, or end user device. Log in to the device's web-based management interface using a web browser and enter the device's IP address. This will allow access to the current configuration settings of the device.

  - **Current IP address:** This is the address currently assigned to the device. It may be a static IP address or a dynamic IP address assigned by a DHCP server. To check the IP address of a device, you can use the following steps:
    - Open the Command Prompt on Windows or Terminal on macOS.
    - Type the command "ipconfig" on Windows or "ifconfig" on macOS and press Enter.
    - Look for the section labeled "IPv4 Address" or "inet" to see the IP address of the device.
    - Alternatively, you can go to the network settings of the device to find the IP address. On Windows, go to "Network and Sharing Center" and click on the connection for which you want to check the IP address. Then click on "Details" to see the IP address. On macOS, go to "System Preferences" and click on "Network." Then select the connection for which you want to check the IP address and click on "Advanced" and then "TCP/IP" to see the IP address.

- **Subnet mask:** This is a number that defines the size of the network the device is on. It is used to determine the network portion and the host portion of an IP address. Checking the subnet mask of a device depends on the operating system of the device. Here are the steps to check the subnet mask for some commonly used operating systems:

  Windows:

  - Click on the Start menu and type "cmd" into the search box.
  - Press Enter to open the Command Prompt.
  - Type "ipconfig" and press Enter.
  - Look for the IPv4 Address and Subnet Mask under the appropriate network adapter.

  Mac:

  - Click on the Apple menu and select System Preferences.
  - Click on Network.
  - Select the appropriate network adapter from the list on the left.
  - Click on the Advanced button.
  - Click on the TCP/IP tab to see the IPv4 Address and Subnet Mask.

  Linux:

  - Open a Terminal window.
  - Type "ifconfig" and press Enter.
  - Look for the IPv4 Address and Subnet Mask under the appropriate network adapter.
- **Gateway address:** This is the IP address of the router or gateway device that connects the local network to the internet.

  To check the gateway address in Windows:

  - Press the Windows key + R to open the Run dialog box.
  - Type "cmd" and press Enter to open the Command Prompt.
  - Type "ipconfig" and press Enter.
  - Look for the "Default Gateway" entry, which will display the IP address of the gateway.

  To check the gateway address on a Mac:

  - Click on the Apple icon in the top left corner of the screen.
  - Click on "System Preferences" and then select "Network."
  - Select the active network connection and click on the "Advanced" button.
  - Click on the "TCP/IP" tab and look for the "Router" entry, which will display the IP address of the gateway.
- **DNS server address:** This is the IP address of the Domain Name System (DNS) server that the device uses to translate domain names to IP addresses. To check the DNS server address, you can use the following steps:
  - Open the Command Prompt on a Windows computer, or Terminal on a Mac computer.
  - Type "nslookup" followed by the domain name that you want to look up the DNS information for. For example, if you want to look up the DNS information for Google, you would type "nslookup google.com" and press Enter.

  - The command prompt or terminal will display the DNS server that was used to perform the lookup, as well as the IP address that was returned for the domain name.
  - You can also check the DNS server address on a router or modem by accessing its web interface and looking for the DNS settings. The location of the DNS settings may vary depending on the make and model of the router or modem.
- **Access the configuration interface:** Accessing the configuration interface involves opening a web browser on a computer or mobile device that is connected to the same network as the equipment. The user will then enter the IP address of the equipment into the web browser's address bar, which will bring up the login page for the configuration interface. The user will then enter the username and password for the equipment, which is typically provided in the user manual or can be set during the initial setup process. Once logged in, the user can access the configuration settings for the equipment and make any necessary changes, such as re-configuring the IP address, subnet mask, gateway address, and DNS server address.
- **Make the necessary changes:** Use the configuration interface to adjust the settings that need to be re-configured, such as the IP address and subnet mask.
- **Save and apply the changes:** Once the changes have been made, save them and apply them to the Wi-Fi backhaul equipment.
- **Test the new configuration:** Check that the changes made have been applied and that the Wi-Fi network is working correctly.

4.1.3 Various Indicative Lights on Network Equipment

Indicative lights on network equipment are used to provide visual cues about the status and activity of the device. These lights are usually located on the front or top of the device and are labeled to indicate their function.

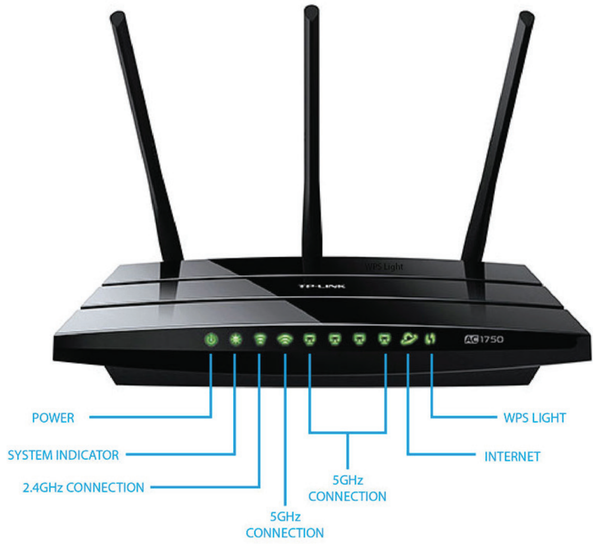


Fig. 4.1.2: Indicative Lights on Network Equipment

The following are some of the most common indicative lights found on network equipment and their meanings:

- **Power:** This light indicates whether the device is receiving power or not. If the light is off, the device is not receiving power, while a steady light means that it is receiving power.

- **Status:** This light indicates the overall status of the device. The meaning of this light varies depending on the specific device, but it often indicates whether the device is operating normally or whether there is an error or issue that needs to be addressed.
- **LAN (Local Area Network):** This light indicates the status of the device's connection to the local network. A blinking or flashing light may indicate network activity, while a steady light indicates a stable connection.
- **WAN (Wide Area Network):** This light indicates the status of the device's connection to the internet or another external network. A blinking or flashing light may indicate network activity, while a steady light indicates a stable connection.
- **Ethernet:** This light indicates the status of the Ethernet connection on the device. A blinking or flashing light may indicate network activity, while a steady light indicates a stable connection.
- **Wi-Fi:** This light indicates the status of the device's Wi-Fi connection. A blinking or flashing light may indicate network activity, while a steady light indicates a stable connection.

4.1.4 Tools Required for Fault Rectification

When it comes to fault rectification in a wireless network setup, there are several tools that can be useful for troubleshooting and resolving issues. Here are some of the most commonly used tools:

- **Wireless network analyzer:** A wireless network analyzer is a tool that can be used to monitor and analyze wireless traffic. It can help identify issues with signal strength, interference, and other factors that can impact network performance.
- **Spectrum analyzer:** A spectrum analyzer can be used to analyze the frequency spectrum to identify any interference that may be affecting the wireless network.
- **Cable tester:** A cable tester can be used to test the integrity of network cables to ensure that they are functioning properly.
- **Multimeter:** A multimeter is a tool that can be used to measure voltage, current, and resistance. It can be useful for identifying issues with power supplies or other electrical components.

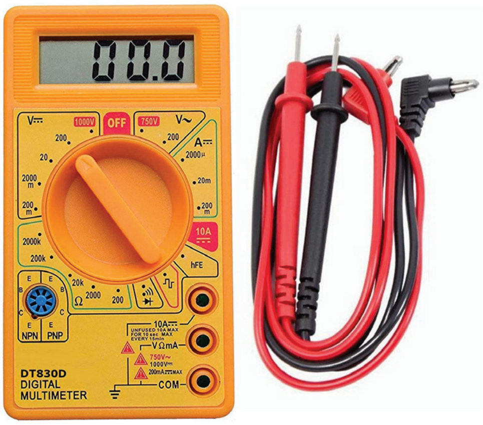


Fig. 4.1.3: Digital Multimeter

- **Power meter:** A power meter can be used to measure the strength of the wireless signal to ensure that it is strong enough to provide reliable connectivity.
- **Ping and traceroute tools:** Ping and traceroute tools can be used to test connectivity and identify network issues.
- **Cable crimping tool:** A cable crimping tool can be used to terminate network cables with connectors.
- **Screwdrivers and pliers:** Basic tools such as screwdrivers and pliers may be needed to open equipment for inspection or to make adjustments.
- **Cleaning tools:** Cleaning tools such as compressed air, cleaning solution, and lint-free cloths may be needed to remove dust or debris from equipment.

4.1.5 Crimping/Soldering Process

Crimping and soldering are two methods used for terminating or connecting electrical wires to a connector or terminal block.

Crimping is the process of using a tool called a crimping tool to press a connector onto the end of a wire, creating a mechanical connection between the wire and the connector. The crimping tool compresses the connector around the wire, causing the metal to deform and tightly grip the wire. Crimping is commonly used for terminating modular plugs, which are commonly used for Ethernet cables.

Soldering, on the other hand, involves heating a soldering iron and melting a soft metal alloy (solder) to create a permanent connection between the wire and the connector. The solder flows into the gap between the wire and the connector, filling any voids and creating a strong, conductive bond between the two. Soldering is commonly used for terminating coaxial cables and other types of wires where a strong, reliable connection is required.

Fig. 4.1.4: Soldering

4.1.6 Risk Assessment Techniques for Network Failures

Risk assessment is the process of identifying, analyzing, and evaluating potential threats that could disrupt a network. For wireless and broadband systems, this includes equipment malfunctions, power outages, interference, cyberattacks, or environmental hazards. Common techniques include:

- **Hazard Identification** – Listing all possible causes of network failure (e.g., faulty cables, overheating equipment, malware attacks, EMI).
- **Probability and Impact Analysis** – Estimating how likely each risk is to occur and its potential impact on service availability, performance, and safety.
- **Vulnerability Assessment** – Evaluating weak points in the system such as outdated firmware, unsecured access points, or poor grounding.
- **Prioritization** – Ranking risks from highest to lowest based on severity and urgency, ensuring that the most critical threats are addressed first.
- **Mitigation Planning** – Developing preventive measures such as redundant links, backup power supplies, and regular maintenance schedules.

4.1.7 Incident Response Protocols for Network Failures

Incident response protocols outline the steps to follow when a network failure occurs, ensuring quick restoration of service and minimal disruption. Typical stages include:

- Detection – Using monitoring tools, alarms, or customer reports to identify a fault or outage.
- Containment – Isolating the affected network segment or equipment to prevent the issue from spreading or worsening.
- Diagnosis – Running tests, checking logs, and analyzing error indicators to determine the root cause of the failure.
- Resolution – Repairing or replacing faulty components, reconfiguring settings, or applying patches to restore functionality.
- Verification – Conducting connectivity and performance tests to confirm that the issue is fully resolved.
- Documentation – Recording the incident details, troubleshooting steps, root cause, and corrective measures taken.
- Post-Incident Review – Analyzing the incident to improve response procedures, prevent recurrence, and enhance network resilience.

4.1.8 Conducting Continuity Tests and Localizing Fault Distance

A continuity test checks whether an electrical path is complete between two points in a cable or circuit. This ensures that signals or current can flow without interruption. Localizing fault distance helps identify where a break, short, or high resistance is located.

Tools Required

- Digital Multimeter (DMM) or Analog Multimeter
- Tone Generator and Probe (for tracing cable routes)
- Time Domain Reflectometer (TDR) (for measuring fault distance in cables)
- Cable Tester (for structured cabling)

Step-by-Step Procedure

Step 1 – Prepare the Cable/System

- Power off the network equipment connected to the cable.
- Disconnect both ends of the cable to avoid interference from other components.

Step 2 – Select Continuity Test Mode

- On a multimeter, set the selector to the continuity or resistance (Ω) mode.
- The continuity mode often gives an audible beep when a complete path exists.

Step 3 – Test for Continuity

- Place one probe on one end of the conductor and the other probe on the corresponding conductor at the other end.
- Pass condition: Audible beep or near-zero resistance reading (e.g., <1 Ω).
- Fail condition: No beep or infinite resistance (OL on digital meter).

Step 4 – Identify Fault Type

- Open Circuit: No continuity (cable break or loose connection).
- Short Circuit: Low resistance between two conductors that should not be connected.
- High Resistance: Resistance higher than expected, indicating partial damage or corrosion.

Step 5 – Localize Fault Distance (if fault found)

- Connect the Time Domain Reflectometer (TDR) to one end of the cable.
- Set the cable type and velocity factor on the TDR.
- Run the test — the TDR sends a pulse and measures the reflection time to calculate the distance to the fault.
- Read the displayed fault distance and mark the cable for repair.

Step 6 – Document Results

- Record the test date, cable ID, results (pass/fail), type of fault, and fault distance.
- Include corrective action taken (e.g., replaced 15 m section, re-crimped connector).

Notes

UNIT 4.2: Troubleshoot Wi-Fi Network Setup

Unit Objectives

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

1. Describe standard commands and procedures for configuring and troubleshooting wireless networking equipment.
2. Explain the parameters affecting signal quality, including interference sources and signal attenuation.
3. Demonstrate how to perform firmware updates and configuration resets, if required.
4. Show how to identify status and diagnostic indicators on Wi-Fi access points.
5. Demonstrate how to connect and utilize network testing tools for fault detection.
6. Show how to interpret output from troubleshooting equipment and software diagnostics.
7. Demonstrate how to access Wi-Fi access point settings through a browser or application to perform configuration checks.
8. Show how to reset, update, or replace malfunctioning Wi-Fi access points based on diagnostic findings.
9. Demonstrate how to record troubleshooting steps and localized faults in logs or digital records.
10. Show how to document all modifications and replacements undertaken during fault rectification.
11. Demonstrate how to restore any worksite changes made during fault repair to meet client and workplace standards.

4.2.1 Locate and Inspect Faults using Portable Tester Device

A portable tester device, such as a network cable tester or Wi-Fi analyzer, can be used to identify faults in the network. These devices can help detect issues such as cable faults, signal interference, or incorrect configuration settings.

A network cable tester is a tool used to verify the quality and integrity of network cabling connections. It can be used to detect faults in network cables, such as broken wires, short circuits, and cross connections.

Here are the steps to use a network cable tester:

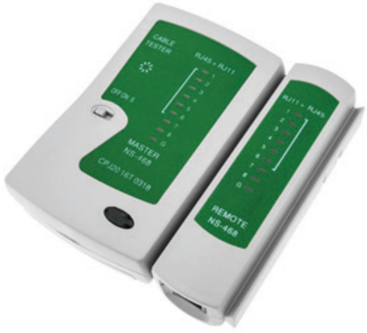


Fig. 4.2.1: Network Cable Tester

- **Prepare the tester:** Turn on the network cable tester and connect the two ends of the tester with the main unit and remote unit.
- **Identify the cable to be tested:** Identify the network cable that you want to test and unplug it from the device or the patch panel.
- **Connect the cable to the tester:** Plug one end of the network cable into the main unit of the network cable tester and the other end into the remote unit of the tester.
- **Test the cable:** Press the test button on the main unit of the tester to start the testing process. The tester will check the cable for continuity, shorts, and other faults. The test results will be displayed on the tester's screen.

- **Interpret the results:** Interpret the test results to identify any faults in the cable. If the cable has passed the test, the tester will display a message indicating that the cable is good. If the cable has failed the test, the tester will display a message indicating the type and location of the fault.
- **Record the results:** Record the test results for future reference. If the cable has failed the test, mark the cable with a label or tape to identify the location of the fault.
- **Fix the faults:** If the cable has failed the test, locate and fix the faults. The faults may be repaired by replacing the damaged connector, cutting and splicing the cable, or replacing the entire cable.
- **Retest the cable:** After fixing the faults, retest the cable to verify that it is working properly.

4.2.2 Replace Feeder Cable/Antenna

If a fault is found with the feeder cable or antenna in a wireless network setup, they may need to be replaced to restore proper functioning of the system. Here are the steps to replace the feeder cable and antenna:

- Identify the location of the faulty feeder cable or antenna. Use a network cable tester or other testing equipment to locate the source of the problem.
- Power off the Wi-Fi access point or o ther wireless device that the feeder cable or antenna is connected to.
- Remove the faulty feeder cable or antenna from the device. If it is a feeder cable, unscrew it from the connector on the device. If it is an antenna, it may be attached with a connector or screws.
- If replacing the feeder cable, attach the new cable to the connector on the device and tighten it securely with the appropriate tool. If replacing the antenna, attach the new antenna in the same way as the old one.
- If the new feeder cable or antenna is a different length than the previous one, it may be necessary to adjust the placement of the antenna to optimize signal strength.
- Power on the wireless device and check for proper functioning of the system. Test the signal strength with appropriate tools to ensure that the new feeder cable or antenna is working correctly.

4.2.3 Troubleshoot Wi- Fi Backhaul Equipment (5Ghz)

Here are the steps to troubleshoot Wi-Fi backhaul equipment (5GHz):

- **Check the power source:** Ensure that the backhaul equipment is receiving power from a reliable source. Check the power cable for any damage and verify that it is properly plugged in.
- **Check the cables and connectors:** Inspect the cables and connectors to ensure that they are properly connected and free from damage or corrosion.
- **Check the antenna alignment:** Check the alignment of the antennas to ensure that they are pointing in the correct direction and are properly oriented.
- **Check the frequency settings:** Verify that the backhaul equipment is set to the correct frequency and channel. The 5GHz band has multiple channels, so it is important to select the appropriate channel that is not being used by other nearby Wi-Fi networks.
- **Check for interference:** Check for any sources of interference, such as other wireless networks, microwaves, or other electronic devices that may be interfering with the signal.
- **Check the firmware:** Ensure that the backhaul equipment is running the latest firmware version. Check the manufacturer's website for any available updates and follow the instructions for updating the firmware.

- **Check the network settings:** Verify that the backhaul equipment is properly configured with the correct IP address, subnet mask, gateway, and DNS settings.
- **Check for hardware faults:** If none of the above steps resolves the issue, it may be necessary to open up the backhaul equipment and inspect for any hardware faults, such as damaged components or loose connections. In this case, it may be best to contact the manufacturer or a professional technician for assistance.

4.2.4 Troubleshoot Wi-Fi Access Points (2.4 GHz)

To troubleshoot Wi-Fi access points (2.4 GHz), you can follow the steps below:

- **Check power and connection:** Ensure that the access point is properly powered on and connected to the network. Check the power source, power cable, and Ethernet cable connections.
- **Check the physical environment:** Verify that there are no physical obstructions or interference that could be impacting the signal, such as metal walls or large objects.
- **Check channel interference:** Use a Wi-Fi scanner to determine if there are other Wi-Fi networks nearby operating on the same channel. If so, change the channel of the access point to one with less interference.
- **Check signal strength:** Check the signal strength by walking around the area with a Wi-Fi signal strength meter or using a mobile device to verify signal strength at different locations. If the signal strength is weak, consider adding additional access points to improve coverage.
- **Check access point configuration:** Review the configuration of the access point to ensure it is correctly set up for the network. Verify that the SSID and password are correct and that the access point is operating on the correct channel.
- **Restart the access point:** Try restarting the access point to see if it resolves any connectivity issues.
- **Check for firmware updates:** Check the access point manufacturer's website for firmware updates that may address known issues or improve performance.

4.2.5 Record Steps Undertaken for Fault Localization/Isolation

Recording the steps undertaken for fault localization and rectification is an important aspect of maintaining a wireless network setup. Here are the steps to record the steps undertaken:

- **Create a document:** Create a document in which you can record the steps undertaken for fault localization and rectification.
- **Record the details:** Record the details of the fault, including when it occurred, the location, and the symptoms of the fault.
- **Record the tests performed:** Record the tests that were performed to isolate the fault, including any tests performed with testing equipment.
- **Record the rectification steps:** Record the steps taken to rectify the fault, including any equipment replaced, repaired or reconfigured.
- **Record the result:** Record the result of the rectification, including whether the fault was successfully resolved or not.
- **Review and update the document:** Review and update the document regularly to ensure that it remains accurate and up-to-date. Add any new faults that were identified, any new tests that were performed, and any new rectification steps that were taken.

4.2.6 Functioning of Laptop (or Other Specific Portable Device) to Carryout Fault Diagnostics

Laptop or other portable device can be a useful tool for carrying out fault diagnostics and repairs in a wireless network setup.

Here are some ways in which a laptop can be used:

- **Network monitoring:** A laptop can be used to monitor the wireless network, including signal strength, noise levels, and interference. This can help in identifying areas of the network that may be experiencing connectivity issues.
- **Network testing:** A laptop can also be used to run network tests, such as pinging network devices, to check for connectivity and response times. This can help in identifying whether there are any issues with the network itself.
- **Configuration:** A laptop can be used to configure network devices, such as access points and routers, to troubleshoot issues related to network settings.
- **Firmware updates:** A laptop can be used to update the firmware on network devices, which can help to resolve any bugs or security vulnerabilities.
- **Remote access:** A laptop can be used to remotely access network devices, which can be particularly useful when troubleshooting issues on devices that are located in hard-to-reach areas.

4.2.7 Documenting Modifications and Replacements During Fault Rectification

Accurate documentation is a critical step in telecom fault management. Every modification or replacement must be recorded to ensure future maintenance teams have a clear service history and to maintain compliance with both organizational and regulatory requirements.

Procedure:

1. **Use Standardized Templates or Digital Platforms**
   - Log all actions in the organization's maintenance management system (MMS), ERP, or site logbook.
   - Include fault ticket number, date, time, and technician ID.
2. **Capture Technical Details**
   - Record the exact component replaced (part number, manufacturer, capacity).
   - Document the nature of the modification (e.g., cable rerouting, software update, equipment recalibration).
3. **Include Justification and Observations**
   - Provide a brief reason for the modification/replacement.
   - Note any secondary issues discovered during the repair.
4. **Attach Supporting Media**
   - Before-and-after photos of the worksite or component.
   - Screenshots of software configuration changes.
5. **Client and Supervisor Sign-Off**
   - Have the record reviewed and approved by the site supervisor or client representative.
   - Ensure it is stored in both physical and digital formats for audit purposes.

4.2.8 Restoring Worksite Changes After Fault Repair

After rectifying a fault, it is essential to return the worksite to its original operational state—or better—while complying with client expectations and workplace safety standards.

Procedure:

1.Inspect the Worksite

- Verify that all tools, cables, and temporary fixings have been removed.
- Ensure all protective covers, access panels, and safety barriers are reinstalled.

2. Restore Structural and Aesthetic Conditions

- Re-secure cable trays, racks, and junction boxes to their original positions.
- Repaint or label areas if markings were removed or damaged.

3. Verify System Functionality

- Test equipment performance against baseline parameters.
- Ensure that no new alarms, interference, or connectivity issues are present.

4. Meet Client-Specific Requirements

- Follow any documented client SOPs (Standard Operating Procedures) for post-repair restoration.
- Have the client sign off on the restored condition before demobilizing.

5. Final Safety and Compliance Check

- Conduct a site walk-through to confirm compliance with workplace safety rules.
- Update documentation to note that restoration is complete.

Summary

- EMI/EMC Concepts
- Re-Configuring the Wi-Fi Backhaul Equipment
- Various Indicative Lights on Network Equipment
- Tools Required for Fault Rectification
- Crimping/Soldering Process
- Locate and Inspect Faults using Portable Tester Device
- Replace Feeder Cable/Antenna
- Troubleshoot Wi-FiBackhaul Equipment (5Ghz)
- Troubleshoot Wi-Fi Access Points (2.4 GHz)
- Record Steps Undertaken for Fault Localization/Isolation
- Functioning of Laptop (or Other Specific Portable Device)to Carryout Fault Diagnostics

Exercise

Multiple-choice Question

1. EMI stands for __________

   a. Electromagnetic Interference   b. Electrical Interference

   c. Elective Interference   d. None of the above

2. __________ is a number that defines the size of the network the device is on

   a. Sunset Mask   b. Subnet Mask

   c. Fishnet Mask   d. None of the above

3. ___________is the IP address of the router or gateway device that connects the local network to the internet

   a. Runway address   b. Hallway address

   c. Gateway address   d. None of the above

4. A __________ is a tool that can be used to measure voltage, current, and resistance

   a. multimeter   b. millimeter

   c. centimeter   d. None of the above

5. ___________ is the process of using a tool called a crimping tool to press a connector onto the end of a wire

   a. Crimping   b. Cramping

   c. Dumping   d. None of the above

Descriptive Questions:

1. Explain EMI and EMC.
2. Explain how to check current IP address on MAC system
3. Explain the process to perform soldering
4. How to use a Network Cable Tester?
5. Elaborate the process to troubleshoot Wi-Fi Access Points (2.4 GHz)

Notes

____

____

____

____

____

____

____

____

____

____

____

____

____

____

____

Scan the QR codes or click on the link to watch the related videos

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

EMI (ElectroMagnetic Interference) & EMC (Electromegetic Compatibility)

सत्यमेव जयते
GOVERNMENT OF INDIA
MINISTRY OF SKILL DEVELOPMENT
& ENTREPRENEURSHIP

5. Installing, Testing, and Maintaining UPS and Domestic Power Supply

Unit 5.1 - Plan for UPS Installation

Unit 5.2 - Install UPS and Check the Electrical Parameter

TEL/N4125

Key Learning Outcomes

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

1. Describe the procedures for installing a UPS system and checking electrical parameters.
2. Explain how to conduct power supply checks and ensure compliance with relevant standards.
3. Determine the steps involved in performing preventive maintenance and troubleshooting UPS systems.

UNIT 5.1: Plan for UPS Installation

Unit Objectives

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

1. Describe standard voltage and current norms for domestic and small commercial power supply systems.
2. Explain guidelines for checking earthing, insulation resistance, and power continuity.
3. Discuss types of UPS systems (Offline, Line-interactive, Online) and their applications.
4. Describe UPS installation best practices, including wiring standards and safety protocols.
5. Determine UPS power ratings, load calculations, and capacity planning.
6. Explain the functioning and use of test equipment (multimeters, clamp meters, insulation testers).
7. Discuss types of batteries used in UPS, battery management practices, and charge cycles.
8. Describe common faults in UPS and troubleshooting methods.
9. Elucidate safety regulations, electrical codes, and protective measures for handling power systems.
10. Explain documentation and reporting procedures for installation, testing, and maintenance activities.
11. Demonstrate how to identify appropriate UPS type and capacity based on the equipment load and power requirements.
12. Demonstrate how to plan installation activities, ensuring adherence to manufacturer guidelines and safety protocols.
13. Show how to read and interpret wiring diagrams and circuit layouts to ensure correct installation.

5.1.1 Uninterruptible Power Supply (UPS)

An Uninterruptible Power Supply (UPS) is a critical component for any organization that relies on electronic equipment to carry out its operations. It is designed to protect electronic devices from power outages, voltage fluctuations, and other power-related issues that may cause damage to the equipment or result in data loss.

UPS systems come in different sizes and capacities to meet the specific needs of different applications. A small UPS, for example, may be used to protect a single computer or workstation, while a larger UPS may be used to provide backup power to an entire server room or telecom site. Large UPS systems may also be used to support critical infrastructure such as hospitals, banks, and other institutions that require a continuous power supply.

UPS systems are commonly used in various applications, including computer systems, network servers, telecommunications equipment, and medical equipment, to name a few. In computer systems, UPS systems provide backup power to prevent data loss and damage to hardware components in case of a power outage or surge. In network servers, UPS systems ensure that the network stays operational even during power outages, preventing any disruption to critical operations.

Telecommunications equipment, such as cell towers and communication centres, rely on UPS systems to provide backup power in case of an outage. This ensures that communication channels remain open during emergencies and critical communication can be maintained without interruption.

Fig 5.1.1: Large UPS

Types of UPS

There are several types of UPS systems used in the Telecom sector. The most common types include:

Online/Double Conversion UPS

This type of UPS provides a continuous power supply to the connected equipment, regardless of the condition of the primary power source. It uses a rectifier to convert the AC power to DC power, which is then used to charge the battery and power the inverter that converts DC power back to AC power. This continuous double-conversion operation isolates connected equipment from problems on the AC line, including blackouts, brownouts, overvoltage, surges, line noise, harmonic distortion, electrical impulses and frequency variations. The output power is regulated by the inverter, which ensures that the voltage and frequency are stable and within a safe operating range. These UPS are used for equipment that is highly critical and cannot tolerate any power disruptions.

Double Conversion Online UPS can be transformer-based or transformer less.

In a traditional transformer-based UPS, the power flows via the rectifier, inverter and transformer to the output, with the transformer used to step up the AC voltage levels, protect the UPS from load disruptions and provide galvanic isolation.

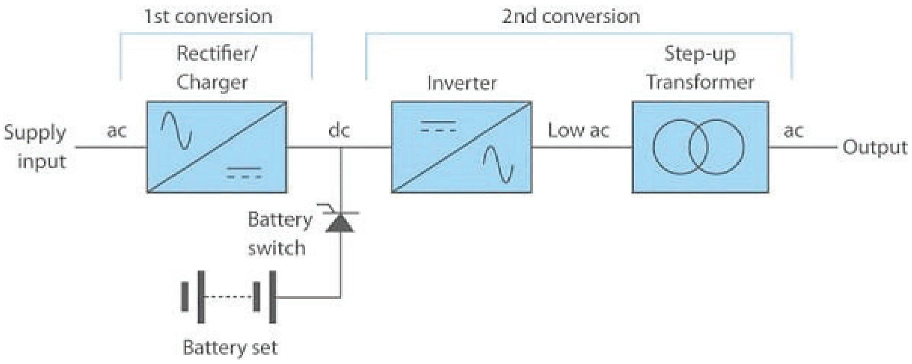


Fig 5.1.2: Block Diagram of a Transformer-Based UPS

Transformer-less UPS operates in the same way, apart from one key difference. They use insulated-gate bipolar transistors (IGBTs) that are capable of dealing with high voltages, eliminating the need for a step-up transformer after the inverter. This improves the energy efficiency of transformer-free uninterruptible power supplies.

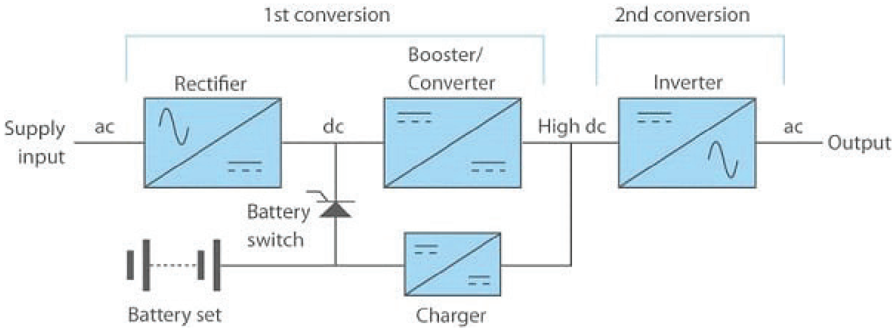


Fig 5.1.3:: Block Diagram of a Transformer less UPS

Offline/Standby UPS

This type of UPS is the most basic and commonly used in the telecom sector. It provides power to the connected equipment only when the primary power source fails. The transfer time from the primary power source to the UPS is typically in the range of 2-10 milliseconds, which may cause a brief interruption in power. These UPS are used for equipment that is not critical and can withstand short power disruptions.

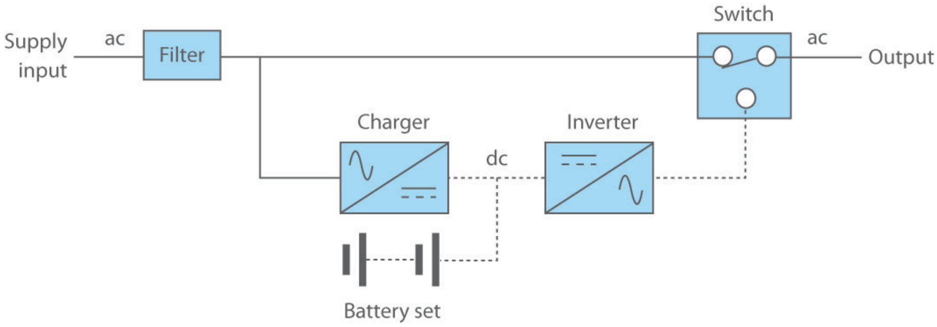


Fig 5.1.4: Block Diagram of an Offline UPS

Line Interactive UPS

This type of UPS is similar to offline/standby UPS, but it has an additional feature of automatic voltage regulation. It regulates the input voltage to the equipment to ensure that it remains within a safe operating range, even during voltage fluctuations. The transfer time from the primary power source to the UPS is typically faster than offline/standby UPS, which reduces the risk of interruption. These UPS are used for equipment that is moderately critical.

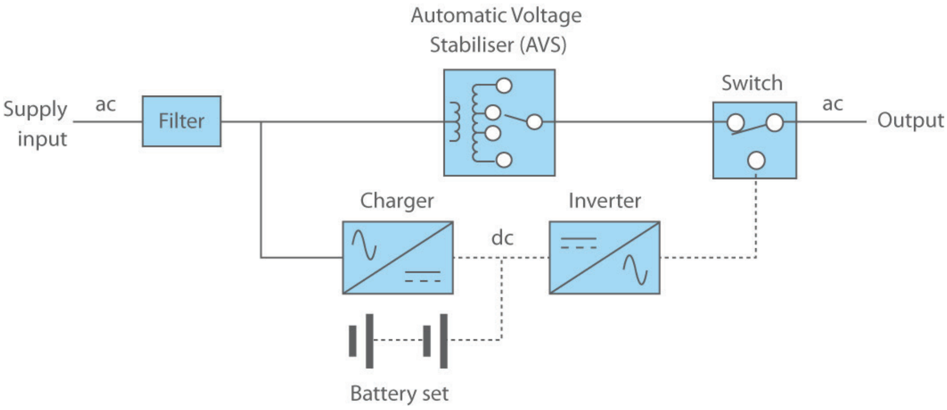


Fig 5.1.5: Block Diagram of a Line Interactive UPS

Modular UPS

This type of UPS consists of multiple UPS modules that can be combined to form a larger system. Each module is self-contained and includes its own battery, inverter, and control unit. This design allows for easy scalability and redundancy, as modules can be added or removed as needed without affecting the entire system. These UPS are used for large telecom installations that require high availability and fault tolerance.

Three-Phase UPS

Three-phase UPS systems are used in the telecom sector to provide backup power to critical equipment that requires a continuous power supply, such as network servers, telecommunications equipment, and telecom sites. These are designed to handle high power loads and are more efficient than single-phase UPS systems. They are able to deliver higher power output while using less energy, making them more cost-effective in the long run.

In addition, three-phase UPS systems are more reliable and offer greater redundancy than single-phase UPS systems. They are able to provide backup power to multiple devices simultaneously, ensuring uninterrupted power supply to critical equipment in case of power failure or voltage fluctuations.

5.1.2 Types of Batteries Compatible with UPS

Large UPS systems used in the telecom sector typically require high-capacity batteries to provide backup power during power outages.

The following are some of the types of batteries that are commonly used with large UPS systems:

Valve-regulated lead-acid (VRLA) batteries

Valve-regulated lead-acid (VRLA) batteries are commonly used in the telecom sector as backup power for UPS systems. These batteries are preferred because they are sealed and maintenance-free, making them easy to install and maintain.

In the telecom sector, an uninterrupted power supply is essential to ensure that communication systems remain functional during power outages or other emergencies. VRLA batteries are used to provide backup power to a range of telecom equipment, including communication towers, telecom sites, and telecom offices. VRLA batteries are also preferred in the telecom sector due to their low cost and long lifespan. They have a high energy density, which means they can store a significant amount of energy in a small space. They are also designed to be highly reliable, providing uninterrupted power for extended periods.

Fig 5.1.6: VLRA Battery

Lithium-ion batteries

Lithium-ion batteries are a type of rechargeable battery that has become increasingly popular in UPS systems due to their high energy density, long life span, and low maintenance requirements. They are also more environmentally friendly than traditional lead-acid batteries, as they do not contain toxic materials such as lead and sulfuric acid.

In the telecom sector, lithium-ion batteries are often used in UPS systems to provide backup power to critical equipment such as base stations, switches, and routers. They are especially useful in remote locations where it may be difficult to maintain traditional lead-acid batteries.

Lithium-ion batteries have a much higher energy density, which means they can store more energy in a smaller space. This makes them ideal for use in small spaces or in applications where size and weight are a concern.

They also have a longer lifespan than lead-acid batteries, with a typical lifespan of 5-10 years compared to 3-5 years for lead-acid batteries. This means that they require less maintenance and replacement over time, which can save costs in the long run.

In addition, lithium-ion batteries can charge and discharge more quickly than lead-acid batteries, which means they can provide backup power more quickly in the event of a power outage or other interruption. They are also more efficient, which means they waste less energy in the charging and discharging process.

Nickel-cadmium (NiCad) batteries

These batteries are known for their long life span and high reliability. They are also able to operate at extreme temperatures, making them ideal for use in harsh environments. The use of these types of batteries has significantly reduced due to their harmful environmental effects.

Flooded lead-acid batteries

Flooded lead-acid batteries are a type of traditional lead-acid battery that has been used for many years in UPS systems. They are also referred to as vented lead-acid batteries or wet-cell batteries. These batteries consist of lead plates immersed in an electrolyte solution of sulfuric acid and water.

While flooded lead-acid batteries have a lower upfront cost compared to VRLA or lithium-ion batteries, they require regular maintenance, such as checking the fluid levels, adding distilled water, and cleaning the terminals. They also have a shorter lifespan than VRLA or lithium-ion batteries.

In the telecom sector, flooded lead-acid batteries may be used in smaller UPS systems or in remote areas where access to regular maintenance is limited. They are also commonly used in backup power systems for critical infrastructure such as telecom sites and telecommunications networks.

Fig 5.1.7: Enhanced Flooded Lead-Acid Batteries

5.1.3 Battery Configuration at Telecom Site

Battery configuration at a telecom site is an essential aspect of ensuring uninterrupted power supply to critical IT equipment. The batteries are typically used in conjunction with a UPS to provide backup power in case of a power outage. The battery configuration in a telecom site depends on various factors, including the power requirement of the IT equipment, the size of the telecom site, the redundancy level required, and the budget.

One common configuration is the use of a battery bank connected to the UPS. The battery bank comprises multiple batteries connected in series or parallels to provide the required voltage and capacity. The batteries used are typically valve-regulated lead-acid (VRLA) or lithium-ion (Li-ion) batteries due to their high energy density, long life span, and low maintenance requirements.

In large telecom sites, multiple battery banks may be used to provide redundancy and increase the backup time. The battery banks are often housed in dedicated battery rooms or cabinets, which are equipped with ventilation systems, fire suppression systems, and other safety features.

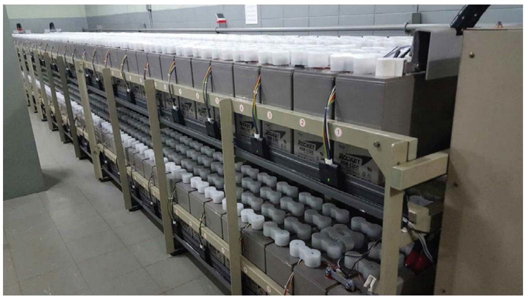


Fig 5.1.8: Battery Configuration in a Telecom site

The battery configuration at a telecom site also involves regular maintenance and testing to ensure that the batteries are functioning correctly and are ready to provide backup power when needed. This includes regular inspections, load testing, and replacement of faulty batteries.

5.1.4 Plan UPS Installation Activity

A wireless technician planning for a UPS installation activity typically follows these steps:

Assessment of power requirements: The technician first assesses the power requirements of the telecom equipment that needs to be powered by the UPS. This includes the power consumption of each device and the total power required.

Selection of UPS: Based on the power requirements, the technician selects an appropriate UPS with the right capacity and specifications to meet the needs of the telecom equipment. Factors such as run time, efficiency, and voltage regulation are considered.

Site survey: The technician conducts a site survey to determine the best location for the UPS installation. This includes assessing the availability of power sources, the placement of the equipment, and any potential obstacles. This also includes plans to connect the UPS to the telecom equipment and test the connections.

Additionally, the technician may also consider factors such as the expected growth of the telecom network, the redundancy requirements for the UPS, and the budget allocated for the installation. They may also consult with other stakeholders, such as the site head, maintenance personnel, and management, to ensure that the UPS installation aligns with the overall objectives and policies of the organization.

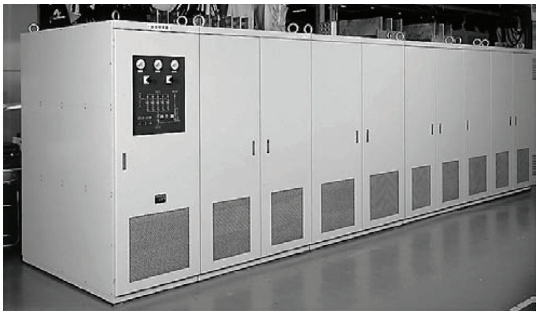


Fig 5.1.9: Large Capacity UPS System

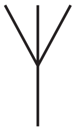
5.1.5 Analysing Basic Wiring Diagrams

A wiring diagram is a visual representation of the physical connections and layout of an electrical system or circuit. It displays how electrical wires are interconnected, and it can also indicate the fixtures and components connected to the system. Wiring diagrams are essential tools for analyzing and understanding the electrical circuits used in UPS installations.

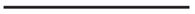
A wiring diagram is different from a schematic diagram. A schematic shows the plan and function of an electrical circuit but is not concerned with the physical layout of the wires. Wiring diagrams show how the wires are connected and where they should be located in the actual device, as well as the physical connections between all the components.

Each symbol in a wiring diagram represents a specific component or device in the circuit and is designed to be easily recognizable and distinguishable from other symbols. For example, a switch symbol typically looks like a break in line with a line at an angle to the wire, much like a light switch you can flip on and off. Similarly, a resistor symbol typically looks like a zigzag line or series of squiggles, symbolizing the restriction of current flow.

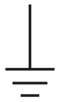
By analyzing a wiring diagram, an installer can gain an understanding of the electrical connections and layout of the system, which can help ensure proper installation of the UPS. This includes understanding how the different components in the circuit are connected and how they work together to provide power to the equipment. The wiring diagram can also help identify potential issues or troubleshooting steps in case of problems in the future.



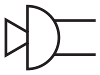
Antenna



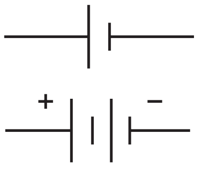
Wire



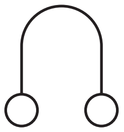
Ground



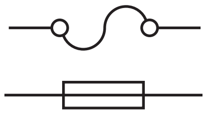
Microphone



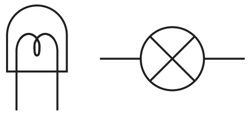
Battery



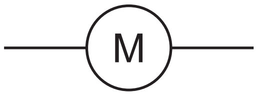
Headphone



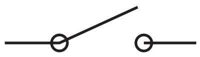
Fuse



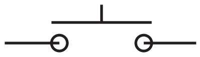
Lamp



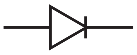
Electric motor



Toggle switch



Push button switch



Diode

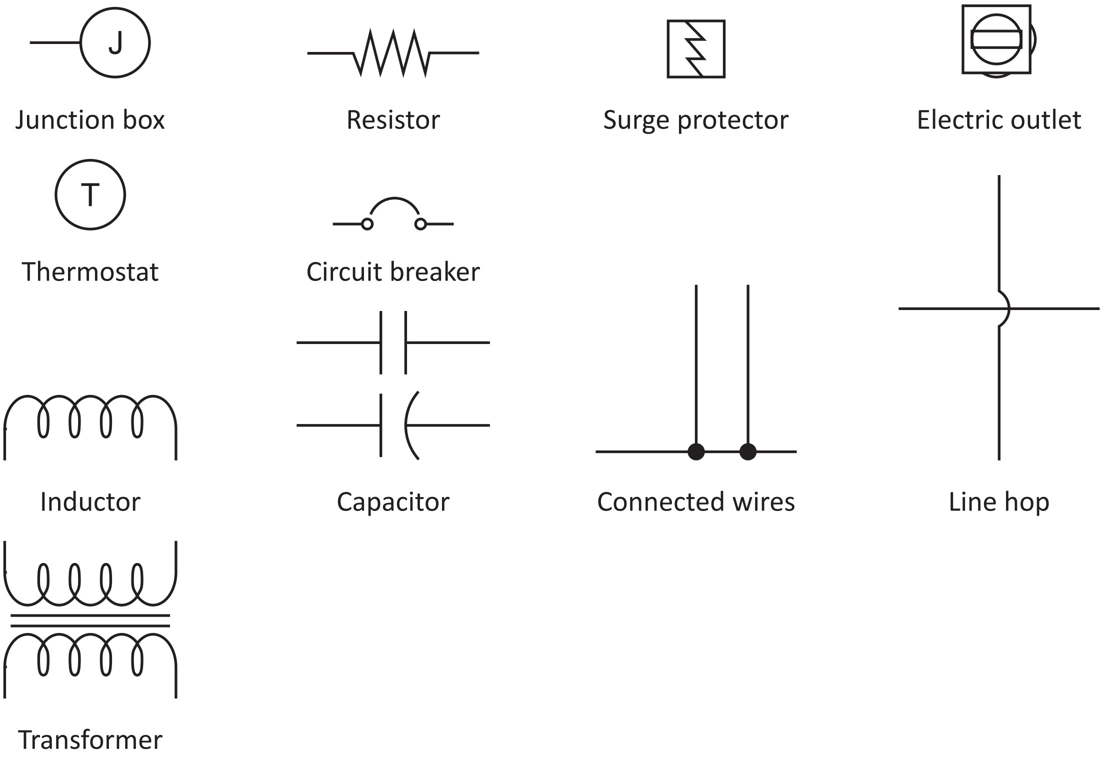


Fig 5.1.10: Standard Wiring Diagram Symbols

Wiring Diagram Rules of Thumb!

Rule #1: Reading Direction

First of all, there is a rule of thumb in standard wiring diagrams that you should read the diagram from left to right and from top-down. Exactly like reading a book!

But sometimes, designers make some exceptions to have a better layout.

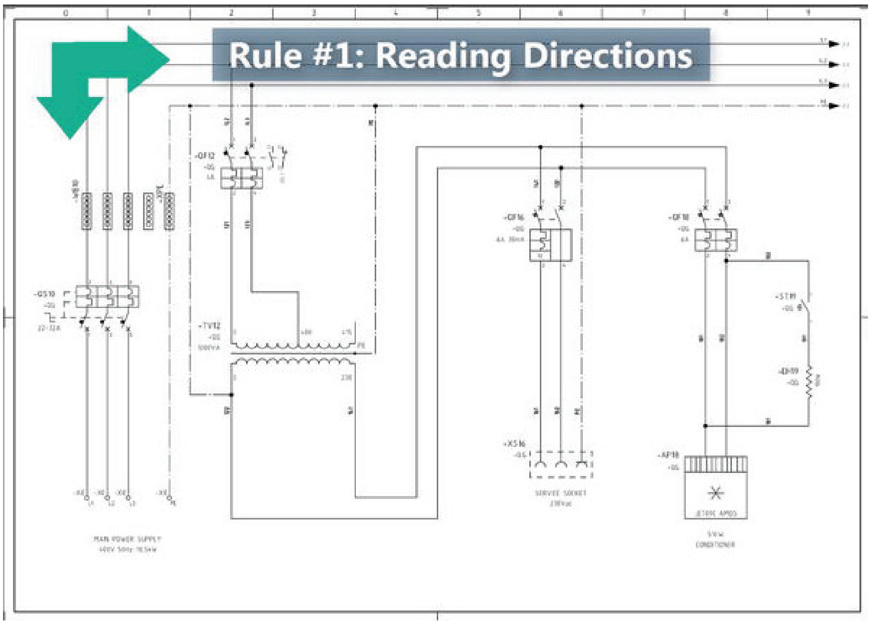


Fig 5.1.11: Reading Direction of Wiring Diagram

Rule #2: Wiring Diagrams Are Drawn in the Neutral Condition

Every standard wiring diagram should be drawn in the neutral condition. This means that all of the contacts, contactors, circuit breakers, etc., are shown in their normal or non-energized condition. Therefore, when you see a closed contact in an electrical wiring diagram, that is a normally closed contact, and the rest of the contacts should be open.

How to Read Wiring Diagrams?

Here are the steps to follow to read a wiring diagram:

Identify the symbols: Each wiring diagram will contain symbols representing different components and electrical devices. It is essential to familiarize yourself with these symbols to understand the diagram.

Follow the lines: The lines on the wiring diagram represent the electrical connections between different components. Follow the lines from one component to another to understand how they are connected.

Determine the power source: The wiring diagram will show the power source for the system or circuit. Identify the power source, whether it is a battery, generator, or other power sources.

Identify the components: Look for the specific components in the diagram, such as switches, relays, and fuses. Determine how these components are connected to each other.

Read the labels: Each component on the diagram may have a label or number. Pay attention to these labels to ensure you are following the correct path.

Follow the flow: The flow of electricity will be indicated by the arrows on the diagram. Follow the flow of electricity to ensure you understand how it moves through the system or circuit.

Check for grounding: The wiring diagram will also show the grounding points in the system. Check these points to ensure they are properly connected and grounded.

Verify the wiring: Once you have followed the diagram and understand how the components are connected, verify that the actual wiring matches the diagram. This step is crucial to avoid misconnections or other errors that can cause system failures or even safety hazards.

5.1.6 Power Rating of UPS

The power rating of a UPS (Uninterruptible Power Supply) refers to the amount of electrical power that the UPS can supply to connected equipment during a power outage or disturbance. It is usually measured in VA (Volt-Ampere) or Watts (W).

The power rating of a UPS is determined by its capacity to support the electrical load of the connected equipment. When selecting a UPS, it is important to consider the power requirements of the equipment that will be connected to it. The UPS should have a power rating that is equal to or greater than the total power requirements of the equipment.

For example, if the total power requirement of the equipment is 800 W, then a UPS with a power rating of at least 800 VA or 800 W should be selected. However, it is recommended to choose a UPS with a slightly higher power rating to ensure that it can handle any sudden spikes or surges in power demand.

It is important to note that the power rating of a UPS is different from its battery backup time. The battery backup time refers to the amount of time that the UPS can provide power to the connected equipment during a power outage, and it depends on the power rating of the UPS and the power consumption of the equipment.

Different factors of power ratings:

- **Apparent Power (VA):** The Apparent Power rating is the product of the RMS voltage and RMS current drawn by the UPS. It indicates the total power that the UPS is capable of delivering to the connected load.
- **Active Power (Watts):** The Active Power rating is the real power that the UPS can deliver to the load. It is the product of the RMS voltage, RMS current, and power factor of the load.
- **Power Factor (PF):** The power factor is the ratio of Active Power (Watts) to Apparent Power (VA). It indicates the efficiency of the UPS in delivering power to the load.
- **Crest Factor:** The crest Factor is the ratio of the peak voltage to the RMS voltage of the output waveform of the UPS. It indicates the amount of distortion in the output waveform.
- **Efficiency:** Efficiency is the ratio of Active Power (Watts) to Input Power (Watts) of the UPS. It indicates the efficiency of the UPS in converting input power to output power.

Standby/Offline UPS is generally the most affordable and has a power rating typically ranging from 350VA to 1500VA. Line Interactive UPS has a power rating typically ranging from 500VA to 3000VA. It provides better protection against power fluctuations than a standby UPS and typically has a faster response time. Online/Double Conversion UPS offers the highest level of protection and has a power rating typically ranging from 1kVA to 20kVA or higher.

UPS systems can be categorized based on their power ratings into the following types:

- **Low-Power UPS:** These are the most commonly used UPS systems and typically have a power rating of up to 5 kVA. They are suitable for personal computers
- **Medium Power UPS:** These UPS systems have a power rating of 5 kVA to 50 kVA and are suitable for mid-sized businesses and telecom sites.
- **High Power UPS:** These UPS systems have a power rating of 50 kVA to 1000 kVA and are suitable for telecom sites
- **Extra High Power UPS:** These UPS systems have a power rating of over 1000 kVA and are used for critical applications.

5.1.6 Guidelines for Checking Earthing, Insulation Resistance, and Power Continuity

1. Earthing (Grounding) Check

Earthing is a critical safety measure in electrical installations. It provides a low-resistance path for fault currents to flow into the ground, thereby preventing electric shock, equipment damage, and fire hazards.

Procedure:

1. Visual Examination:

Inspect the earthing conductor, clamps, and electrodes for signs of corrosion, damage, or loose connections. Ensure that the earthing strip or wire is of the correct size and is mechanically protected against physical damage.

Measurement of Earth Resistance:

- Use an Earth Resistance Tester (megger-type or clamp-on type).
- Disconnect the earthing conductor from the main earthing terminal before measurement to avoid parallel paths.
- Record the resistance value; as per IS 3043 standards, it should generally be less than 1 ohm for sensitive installations and not exceed 5 ohms for general systems.

Verification of Equipotential Bonding:

Ensure that all exposed conductive parts (metal enclosures, frames, conduits) are connected to the main earthing system.

Safety Note:

Earthing measurements should only be conducted on de-energized systems. Under no circumstances should the earthing conductor be disconnected while the system is live.

2. Insulation Resistance (IR) Check

Insulation resistance testing determines the integrity of the insulation surrounding live conductors. Adequate insulation prevents leakage currents, short circuits, and accidental contact with live parts.

Procedure:

1. Preparation:

- Isolate the equipment or circuit from the power supply.
- Discharge any stored electrical energy in capacitors or cables.
- Remove or disconnect sensitive electronic components to avoid damage during testing.

2. Testing Method:

Use an Insulation Resistance Tester (megger) set to the appropriate voltage:

- 500 V DC for low-voltage circuits (up to 1 kV).
- 1 kV or above for high-voltage cables.

Test between:

- Phase to Earth
- Phase to Neutral
- Neutral to Earth

Maintain the test voltage for at least one minute for a stable reading.

3. Acceptance Values:

- Low-voltage systems: Minimum 1 MΩ (preferably above 2 MΩ).
- High-voltage systems: Generally above 100 MΩ per kV of operating voltage.

Safety Note:

Only trained personnel should conduct IR testing. Avoid touching test leads during operation to prevent electric shock.

3. Power Continuity Check

Continuity testing ensures that conductors, protective earth connections, and circuit paths are unbroken and capable of carrying current without excessive resistance.

Procedure:

1. Preparation:

- Isolate the circuit from all power sources.
- Verify isolation using an appropriate voltage tester.

2. Testing Method:

- Use a Continuity Tester or a Digital Multimeter in the resistance (Ω) mode.
- Place the test probes at each end of the conductor under test.
- A good conductor should show a very low resistance reading (close to zero ohms).

3. Polarity and Protective Earth Continuity:

- Verify that all phase, neutral, and earth conductors are connected to the correct terminals.
- For protective earth conductors, the resistance from the equipment body to the main earth terminal should not exceed 0.5 Ω.

Safety Note:

Never conduct continuity testing on live circuits. Ensure complete isolation before starting.

5.1.7 Power Rating of UPS

Different factors of power ratings:

- Apparent Power (VA): The Apparent Power rating is the product of the RMS voltage and RMS current drawn by the UPS. It indicates the total power that the UPS is capable of delivering to the connected load.
- Active Power (Watts): The Active Power rating is the real power that the UPS can deliver to the load. It is the product of the RMS voltage, RMS current, and power factor of the load.
- Power Factor (PF): The power factor is the ratio of Active Power (Watts) to Apparent Power (VA). It indicates the efficiency of the UPS in delivering power to the load.
- Crest Factor: The crest Factor is the ratio of the peak voltage to the RMS voltage of the output waveform of the UPS. It indicates the amount of distortion in the output waveform.
- Efficiency: Efficiency is the ratio of Active Power (Watts) to Input Power (Watts) of the UPS. It indicates the efficiency of the UPS in converting input power to output power.

Standby/Offline UPS is generally the most affordable and has a power rating typically ranging from 350VA to 1500VA. Line Interactive UPS has a power rating typically ranging from 500VA to 3000VA. It provides better protection against power fluctuations than a standby UPS and typically has a faster response time. Online/Double Conversion UPS offers the highest level of protection and has a power rating typically ranging from 1kVA to 20kVA or higher.

UPS systems can be categorized based on their power ratings into the following types:

- Low-Power UPS: These are the most commonly used UPS systems and typically have a power rating of up to 5 kVA. They are suitable for personal computers
- Medium Power UPS: These UPS systems have a power rating of 5 kVA to 50 kVA and are suitable for mid-sized businesses and telecom sites.
- High Power UPS: These UPS systems have a power rating of 50 kVA to 1000 kVA and are suitable for telecom sites
- Extra High Power UPS: These UPS systems have a power rating of over 1000 kVA and are used for critical applications.

5.1.8 Common Faults in UPS Systems and Troubleshooting Methods

A Uninterruptible Power Supply (UPS) is designed to provide continuous power to critical equipment during interruptions or fluctuations in the main supply. Despite their reliability, UPS systems may experience faults due to electrical, environmental, or operational issues. Timely fault detection and troubleshooting ensure uninterrupted protection for connected loads.

1. Battery-Related Faults

Common Symptoms:

- Reduced backup time
- Battery not charging
- Battery overheating or swelling
- UPS shuts down prematurely during power outage

Possible Causes:

- Aged or sulfated battery cells
- Loose battery connections
- Faulty battery charger circuit
- Overcharging or deep discharging

Troubleshooting Methods:

- **Visual Inspection:** Check for corrosion, leakage, swelling, or loose terminals.
- **Voltage Test:** Measure battery voltage with a digital multimeter; compare with manufacturer's specification.
- **Load Test:** Apply a known load and monitor discharge performance.
- **Charger Check:** Verify charger output voltage and current.
- Replace defective batteries or charger components if required.

2. Inverter Faults

Common Symptoms:

- UPS not supplying power during outages
- Distorted output waveform
- Excessive heat from inverter section
- Inverter overload alarm

Possible Causes:

- Failed power transistors (MOSFETs/IGBTs)
- Faulty driver circuits
- Overload or short circuit on output
- Cooling fan failure

Troubleshooting Methods:

- **Check Output:** Use an oscilloscope or RMS voltmeter to verify output voltage and waveform.
- **Component Testing:** Test switching devices and driver circuits.
- **Load Inspection:** Reduce or disconnect load to verify fault clearance.
- **Cooling Check:** Ensure fans and heatsinks are clean and functional.

3. Input Power Problems

Common Symptoms:

- UPS does not switch to mains power
- Frequent changeover to battery mode
- Input over/under-voltage alarm

Possible Causes:

- Loose or damaged input wiring
- Supply voltage outside acceptable range
- Faulty input filter or relay

Troubleshooting Methods:

- **Measure Input Voltage:** Compare with UPS input specifications.
- **Inspect Wiring:** Tighten connections, replace damaged cables.
- **Component Check:** Test relays, input filters, and surge protection devices.

4. Overload and Short-Circuit Conditions

Common Symptoms:

- UPS alarm indicating overload
- Sudden shutdown under heavy load
- Tripped circuit breakers or blown fuses

Possible Causes:

- Load exceeding rated capacity
- Faulty connected equipment
- Internal short in UPS output section

Troubleshooting Methods:

- **Load Audit:** Disconnect non-critical loads and check UPS performance.
- **Measure Current Draw:** Ensure total load is within UPS capacity.
- **Inspect Internal Circuits:** Check for burnt components or traces.

5. Overheating Faults

Common Symptoms:

- Over-temperature alarm
- UPS shuts down after prolonged operation
- Fans running at high speed continuously

Possible Causes:

- Blocked air vents
- Dust accumulation on heatsinks and components
- Faulty cooling fans
- High ambient temperature

Troubleshooting Methods:

- **Clean Air Paths:** Remove dust from vents, filters, and heatsinks.
- **Check Fan Operation:** Replace if defective.
- **Monitor Room Temperature:** Maintain as per manufacturer's recommendation (usually 20–25°C).

6. Control and Communication Faults

Common Symptoms:

- Display panel not functioning
- Incorrect status indications
- UPS not responding to remote commands

Possible Causes:

- Faulty control PCB
- Damaged cables or connectors
- Software/firmware errors

Troubleshooting Methods:

- **Cable & Connector Check:** Ensure proper seating and continuity.
- **Firmware Reset/Update:** Follow manufacturer's procedure.
- **Replace Control PCB:** If confirmed faulty.

5.1.9 Safety Regulations, Electrical Codes, and Protective Measures for Handling Power Systems

Handling electrical power systems involves significant hazards, including electric shock, arc flash, equipment damage, and fire. To minimize these risks, strict safety regulations, adherence to electrical codes, and implementation of protective measures are essential.

1. Safety Regulations

Safety regulations provide the legal and procedural framework for safe work practices in electrical installations and maintenance.

1.1 Regulatory Bodies and Standards

- **International Electrotechnical Commission (IEC)** – Publishes global standards such as IEC 60364 (Electrical Installations of Buildings).
- **Institute of Electrical and Electronics Engineers (IEEE)** – Publishes guidelines like IEEE Std 1584 for arc-flash hazard calculations.
- **National Fire Protection Association (NFPA)** – NFPA 70 (National Electrical Code, USA) and NFPA 70E (Electrical Safety in the Workplace).

- **Bureau of Indian Standards (BIS)** – Publishes IS codes such as IS 3043 (Earthing) and IS 732 (Electrical Wiring Installations).
- **Directorate General of Mines Safety (DGMS)** – For mining and industrial electrical safety in India.

1.2 Key Safety Rules

- Work only when authorized and qualified.
- Always isolate and lockout–tagout (LOTO) before starting work.
- Test circuits before touching, using a calibrated voltage tester.
- Maintain safe approach distances from live parts.
- Ensure adequate illumination and non-slip flooring in electrical areas.

2. Electrical Codes

Electrical codes specify technical requirements for designing, installing, and maintaining electrical systems to ensure safety and performance.

2.1 Purpose of Electrical Codes

- Prevent electrical fires.
- Minimize electric shock hazards.
- Ensure safe operation and maintainability.
- Provide standardization for installations.

2.2 Commonly Referenced Codes

- **IS 732** – Code of Practice for Electrical Wiring Installations.
- **IS 3043** – Code of Practice for Earthing.
- **IEC 60364** – Low-voltage electrical installation requirements.
- **NFPA 70 (NEC)** – Electrical installation code (USA).
- **DGMS Technical Circulars** – Electrical equipment use in hazardous mining areas.

2.3 Code Compliance Essentials

- Use correct cable sizing to prevent overheating.
- Install proper earthing and bonding for fault current return.
- Use overcurrent protection devices (MCB, MCCB, fuses) rated for the load.
- Ensure phase identification and proper color coding of conductors.
- Maintain clearances for switchboards and panels as per code.

3. Protective Measures for Handling Power Systems

Protective measures are designed to safeguard personnel and equipment from electrical hazards.

3.1 Personal Protective Equipment (PPE)

- Insulating gloves (as per IEC 60903).
- Arc-rated clothing to protect from arc flash.
- Safety footwear with electrical insulation.
- Face shields and goggles for eye protection.
- Hearing protection in high-noise electrical environments.

3.2 Engineering Controls

- **Circuit Breakers and Fuses** – Protect against overloads and short circuits.
- **Residual Current Devices (RCDs)** – Provide protection against earth leakage currents.
- **Surge Protective Devices (SPD)** – Protect equipment from voltage spikes.
- **Isolation Transformers** – Provide galvanic isolation for safety.
- **Earthing Systems** – Ensure safe dissipation of fault currents.

3.3 Safe Work Practices

- **Lockout–Tagout (LOTO):** Ensure all sources of electrical energy are isolated and tagged before work begins.
- **Test Before Touch:** Always verify zero voltage before handling conductors.
- **Use Insulated Tools:** Tools should conform to IEC 60900 standards.
- **Follow the "One Hand Rule":** Keep one hand away from live work to reduce current path through the heart.
- **Maintain Clearance:** Keep a safe working distance from exposed live parts.

4. Hazard Identification and Risk Control

4.1 Electrical Hazards

- Electric shock
- Burns from arc flash or contact with hot components
- Fires due to overload or short circuit
- Explosion in hazardous atmospheres

4.2 Risk Control Measures

- **Conduct a Job Safety Analysis (JSA) before starting work.**
- **Use lockout–tagout and proper isolation.**
- **Regular preventive maintenance of electrical equipment.**
- **Install warning signs and safety barriers around hazardous areas.**

5. Documentation and Training

- Maintain as-built electrical drawings and update them after modifications.
- Keep test records of insulation resistance, earth resistance, and RCD performance.
- Conduct regular safety training on electrical hazards and emergency procedures.
- Display emergency contact numbers and first aid instructions in electrical rooms.

5.1.10 Planning Installation Activities in Compliance with Manufacturer Guidelines and Safety Protocols

Proper planning of installation activities ensures that equipment operates efficiently, meets warranty requirements, and complies with legal and safety standards. It involves coordination between technical specifications, workplace safety rules, and step-by-step execution.

1. Understanding Manufacturer Guidelines

Manufacturers provide detailed instructions in their installation manuals to ensure optimal performance and avoid premature failure.

1.1 Key Aspects to Review

- **Technical Specifications:** Voltage, current rating, operating environment limits.
- **Pre-Installation Requirements:** Space clearance, ventilation, foundation, anchoring.
- **Tools and Materials Needed:** As listed in the manual.
- **Assembly Instructions:** Sequence of parts installation.
- **Wiring Diagrams:** For correct electrical connections.
- **Commissioning Procedures:** Initial checks before energizing.

1.2 Compliance Importance

- Prevents voiding the product warranty.
- Ensures equipment functions as intended.
- Reduces the risk of safety incidents.

2. Pre-Installation Planning

2.1 Site Assessment

- Evaluate physical space for accessibility, ventilation, and clearance.
- Verify structural capacity to support equipment weight.
- Check environmental factors — temperature, humidity, dust levels.

2.2 Resource Planning

- Allocate qualified personnel for electrical, mechanical, and safety tasks.
- Prepare materials as per the Bill of Materials (BOM).
- Arrange specialized tools (torque wrench, insulation tester, crimping tools).

2.3 Permits and Approvals

- Obtain work permits as per company policy or statutory regulations.
- Get client and safety department approval before starting work.

3. Integrating Safety Protocols

3.1 Before Starting Work

- Follow Lockout–Tagout (LOTO) procedures to isolate energy sources.
- Wear appropriate PPE — safety helmet, gloves, arc-rated clothing, safety shoes.
- Display warning signs in the work area.

3.2 During Installation

- Maintain safe working distances from energized parts.
- Use insulated tools in compliance with IEC 60900.
- Keep the area clean and free of trip hazards.

3.3 Post-Installation Safety Checks

- Verify earthing and bonding as per IS 3043 or IEC 60364.
- Perform insulation resistance and continuity tests before energizing.
- Ensure overcurrent and leakage protection devices are installed and functional.

4. Step-by-Step Installation Plan

Step	Activity	Reference / Guidelines
1	Review manufacturer's manual and safety codes	Manufacturer Manual, IS/IEC Codes
2	Conduct site survey and prepare layout	IS 732 (Wiring), NEC/NFPA 70
3	Arrange tools, materials, and skilled manpower	BOM, Work Order
4	Secure work permits and safety clearance	Company Safety SOPs
5	Isolate power sources and implement LOTO	IS 5216, NFPA 70E
6	Install equipment as per specified torque, alignment, and wiring	Manufacturer Manual
7	Perform pre-commissioning tests (IR, earth resistance, polarity)	IS 3043, IS 732
8	Record installation details in logbook and obtain sign-off	Documentation Standards
9	Energize system under controlled observation	Commissioning Checklist

5. Documentation and Handover

- **Installation Report:** Includes diagrams, test results, and deviations from design (if any).
- **Test Certificates:** For insulation resistance, earth resistance, and functional tests.
- **As-Built Drawings:** Reflecting actual installed conditions.
- **Sign-Off Forms:** Approved by installer, supervisor, and client representative.

6. Example – Planning UPS Installation

Objective: Install a 10 kVA online UPS in a data center.

Planning Steps:

- Review UPS manufacturer manual — ensure room temperature is within 20–25°C, maintain clearance of 300 mm on all sides.
- Conduct site inspection — verify floor strength, locate dedicated earthing point.
- Arrange MCB, copper cables of specified size, and battery bank as per load capacity.
- Assign certified electrician and technician for installation.
- Isolate main power, implement LOTO, and post warning boards.
- Follow wiring diagram for AC input, output, and battery connections.
- Test insulation resistance at 500 V DC; verify earth resistance < 1 Ω.
- Record results in installation log and obtain commissioning approval.

5.1.11 Identifying Appropriate UPS Type and Capacity Based on Equipment Load and Power Requirements

Selecting the correct UPS (Uninterruptible Power Supply) type and capacity is essential to ensure uninterrupted operation of connected equipment, protect against power disturbances, and prevent overloading. This process involves load analysis, runtime requirements, and environmental considerations.

1. Step 1 – Determine the Equipment Load

1.1 List All Connected Devices

- Identify all equipment that will be powered by the UPS during an outage.
- Record the power ratings from the equipment's nameplate or manufacturer's datasheet.

Equipment	Power Rating (W)	Quantity	Total Power (W)
Server	400	2	800
Network Switch	50	2	100
Desktop Computers	300	3	900
CCTV DVR	60	1	60
Total Load	–	–	**1,860 W**

1.2 Convert Watts to Volt-Amperes (VA)

UPS capacity is rated in VA or kVA. Since most loads are not purely resistive, apply the **Power Factor (PF)**:

VA=WattsPower Factor\text{VA} = \frac{\text{Watts}}{\text{Power Factor}}VA=Power FactorWatts

For IT loads, PF ≈ 0.8:

VA=1,8600.8=2,325 VA (≈2.3 kVA)\text{VA} = \frac{1,860}{0.8} = 2,325 \ \text{VA} \ (\approx 2.3 \ \text{kVA})VA=0.81,860=2,325 VA (≈2.3 kVA)

2. Step 2 – Apply Safety Margin

To account for future expansion and avoid overloading, add 20–30% spare capacity:

UPS Capacity Required=2.3 kVA×1.25=2.875 kVA\text{UPS Capacity Required} = 2.3 \ \text{kVA} \times 1.25 = 2.875 \ \text{kVA}UPS Capacity Required=2.3 kVA×1.25=2.875 kVA

Select nearest standard size: 3 kVA UPS.

3. Step 3 – Determine Runtime Requirement

- **Short Runtime (5–15 minutes):** For safe shutdown of systems.
- **Medium Runtime (30–60 minutes):** For bridging short outages.
- **Long Runtime (>1 hour):** For critical operations until backup generator starts.

Battery capacity must be chosen based on the runtime and load, as per manufacturer's battery sizing charts.

4. Step 4 – Select Appropriate UPS Type

4.1 UPS Types

1. **Offline / Standby UPS**
   - Switches to battery power when mains fails.
   - Suitable for small office/home electronics.
   - Low cost, limited protection.
2. **Line-Interactive UPS**
   - Regulates voltage fluctuations using an autotransformer.
   - Suitable for small-to-medium IT setups, point-of-sale systems.
3. **Online / Double Conversion UPS**
   - Converts incoming AC to DC and back to AC continuously.
   - Provides clean, uninterrupted power.
   - Best for data centers, medical equipment, and critical industrial loads.

4.2 UPS Type Selection Criteria

Factor	Offline UPS	Line-Interactive UPS	Online UPS
Voltage Regulation	Poor	Good	Excellent
Transfer Time	2–10 ms	2–4 ms	0 ms
Cost	Low	Medium	High
Protection Level	Basic	Moderate	High
Application	Home PCs	SMEs, Retail	Data Centers, Medical

5. Step 5 – Environmental and Operational Considerations

- **Power Quality Issues:** For frequent surges, sags, or noise, choose an Online UPS.
- **Installation Location:** Ensure adequate ventilation and dust protection.
- **Expansion Needs:** Choose a UPS with scalable battery options.
- **Maintenance Requirements:** Verify ease of battery replacement and availability of spares.

5.1.12 Documentation and Reporting Procedures for Installation, Testing, and Maintenance Activities

Proper documentation and reporting are critical elements of electrical project management. They ensure traceability, compliance with standards, and facilitate efficient troubleshooting, preventive maintenance, and audits.

1. Purpose of Documentation and Reporting

- **Compliance:** Meet legal and regulatory requirements such as IS standards, IEC codes, or organizational SOPs.
- **Quality Assurance:** Provide evidence that installation and maintenance activities meet design specifications and safety norms.
- **Traceability:** Maintain historical records for future reference, modifications, and warranty claims.
- **Communication:** Share information between technicians, supervisors, and clients in a standardized format.

2. Documentation During Installation

2.1 Pre-Installation Records

- **Site Survey Report:** Includes layout drawings, load calculations, and environmental considerations.
- **Material Inspection Report:** Confirms receipt of correct components (e.g., cables, breakers, UPS units) with test certificates.
- **Work Permits and Approvals:** Signed authorization to begin installation.

2.2 Installation Records

- **As-Built Drawings:** Updated diagrams reflecting the actual installed configuration, cable routing, and equipment placement.
- **Installation Checklists:** Step-by-step verification of work stages such as cable termination, earthing, and panel wiring.
- **Photographic Evidence:** Before-and-after images of key installation points.

3. Documentation During Testing and Commissioning

3.1 Test Records

- **Insulation Resistance Test Report:** Lists test voltage, measured values, and acceptance criteria.
- **Earth Resistance Test Report:** Includes measured values, test method, and date.
- **Continuity and Polarity Test Records:** Verification of conductor paths and connections.
- **Functional Test Report:** Confirms correct operation of equipment under normal and fault conditions.

3.2 Certificates

- **Test Certificates:** Signed by authorized personnel confirming compliance with standards.
- **Commissioning Certificate:** Declares the system ready for operational use.

4. Documentation During Maintenance

4.1 Routine Maintenance Records

- **Maintenance Checklists:** Daily, weekly, monthly, or annual inspection points (e.g., visual checks, tightening connections).
- **Service Logs:** Dates, technician name, work performed, and parts replaced.
- **Calibration Records:** For measuring instruments and protective devices.

4.2 Fault and Repair Reports

- **Fault Diagnosis Report:** Symptom description, root cause analysis, and corrective actions.
- **Breakdown Maintenance Report:** Urgent repair details, downtime, and restoration steps.

5. Reporting Procedures

5.1 Standard Report Structure

1. **Title Page:** Project name, report title, date, and responsible person's name.
2. **Summary:** Brief overview of the activity and key findings.
3. **Detailed Findings:** Test results, inspection notes, photographs.
4. **Compliance Statement:** Reference to relevant codes and standards met.
5. **Recommendations:** Suggested improvements or follow-up actions.
6. **Signatures and Approvals:** Technician, supervisor, and client acknowledgment.

5.2 Report Submission

- Submit to **project manager or client** within the agreed timeframe.
- Keep **digital and physical copies** for archival purposes.
- Store documents in **centralized repository** for easy retrieval.

6. Regulatory and Standards References

- **IS 732** – Code of Practice for Electrical Wiring Installations.
- **IS 3043** – Code of Practice for Earthing.
- **IEC 60364** – Electrical Installations for Buildings.
- **NFPA 70 / NEC** – National Electrical Code (USA).
- **DGMS Circulars** – For mining sector installations.

7. Best Practices for Documentation

- Use **clear and concise language** with standard electrical symbols.
- Ensure all records are **signed, dated, and version-controlled**.
- Maintain **legible, high-resolution copies** of drawings and test results.
- Implement **digital reporting systems** (e.g., CMMS – Computerized Maintenance Management Systems) for real-time updates.

Notes

UNIT 5.2: Install UPS and Check the Electrical Parameters

Unit Objectives

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

1. Review wiring standards, polarity, and phase alignment for UPS systems.
2. Understand procedures for verifying grounding and power quality after installation.
3. Demonstrate how to inspect and verify power supply connections for voltage, current, earthing, and continuity.
4. Demonstrate how to install and securely mount UPS as per the specified standards.
5. Show how to route and connect power supply through UPS, ensuring proper input and output wiring.
6. Demonstrate how to check for polarity and phase alignment to avoid incorrect wiring.
7. Show how to verify the proper grounding of the UPS and connected equipment.
8. Demonstrate how to use multimeters and clamp meters to measure and validate voltage, current, and earthing resistance.
9. Show how to test power backup functionality by simulating a power failure scenario.
10. Demonstrate how to ensure the UPS output matches the required power quality standards.
11. Show how to identify and report fluctuations or irregularities in power supply that may affect equipment performance.
12. Demonstrate how to apply safety precautions while handling high-voltage connections and power tools.
13. Show how to inspect and test UPS batteries for charge retention and health status.
14. Demonstrate how to replace faulty or degraded batteries following standard replacement procedures.
15. Show how to clean and secure UPS ventilation to prevent overheating.
16. Demonstrate how to diagnose and troubleshoot common UPS faults such as overloading, short circuits, and failed inverters.
17. Show how to document test results, maintenance actions, and reported issues as per standard procedures.
18. Demonstrate how to communicate findings and recommendations to customers or supervisors.

5.2.1 Installing UPS

Installing a large UPS at a telecom site requires careful planning and execution to ensure that the UPS is properly installed and integrated with the existing telecom equipment.

Plan for installation

Planning for the installation of UPS at the telecom site includes conducting a site survey, assessing the power requirement and selecting the UPS basis the power requirement. Factors such as run time, efficiency, and voltage regulation are also considered during the selection.

Preparation of site

Prepare the site for installation, including any necessary electrical work, mounting of the UPS, and installation of any necessary wiring or cabling. The process starts with identifying a suitable location for the UPS that meets the requirements of the equipment it will be powering. The location should be easily accessible for maintenance and repair work and should have adequate ventilation and cooling.

Ensure that the electrical infrastructure at the site is capable of handling the electrical load that the UPS will be supplying. This may require the installation of additional electrical circuits, wiring, or transformers. Once the electrical infrastructure is in place, mount the UPS in the designated location. Ensure that it is level, secure, and protected from any potential hazards.

Installation of UPS

Install the UPS and any necessary equipment required for the installation. If the UPS requires batteries, connect them to the system. Ensure that the batteries are correctly sized and configured to provide the necessary backup power. Install any necessary wiring and cabling to connect the UPS to the telecom equipment. This may include power cables, signal cables, and communication cables.

Testing

After the UPS is installed and wired, test the installation to ensure that it is functioning correctly. This may include testing the battery backup system, the voltage regulation, and the communication between the UPS and the telecom equipment. Configure the required settings, set up monitoring and reporting systems, and perform any necessary calibration or adjustment of the UPS.

5.2.2 UPS Redundancies

In order to achieve high uptime requirements at telecom sites, it is essential to implement UPS redundancies. This ensures that the site remains operational even in the event of a UPS failure. There are several types of UPS redundancies that can be implemented:

N+0 or Non-Redundant: Relative to other levels of redundancy, this is designated as N+0, where N represents a unit of the UPS. This type of UPS configuration is where there is no redundancy built into the system. This means that there is only one UPS unit providing power to the critical load, and if that unit fails, the load will be without power until the unit is repaired or replaced.

N+1 Redundancy: In this configuration, one extra UPS is added to the system, which can take over the load in case of a failure in any of the other UPS systems. This configuration provides a 1:1 ratio of UPS units to the maximum load capacity of the telecom site.

2N Redundancy: In this configuration, two independent UPS systems are installed, each capable of handling the full load of the telecom site. This ensures that even if one UPS system fails, the other one can handle the full load and provide uninterrupted power.

N+2 Redundancy: In this configuration, two extra UPS systems are added to the system, which can take over the load in case of a failure in any of the other UPS systems. This configuration provides an additional level of redundancy to ensure high uptime requirements.

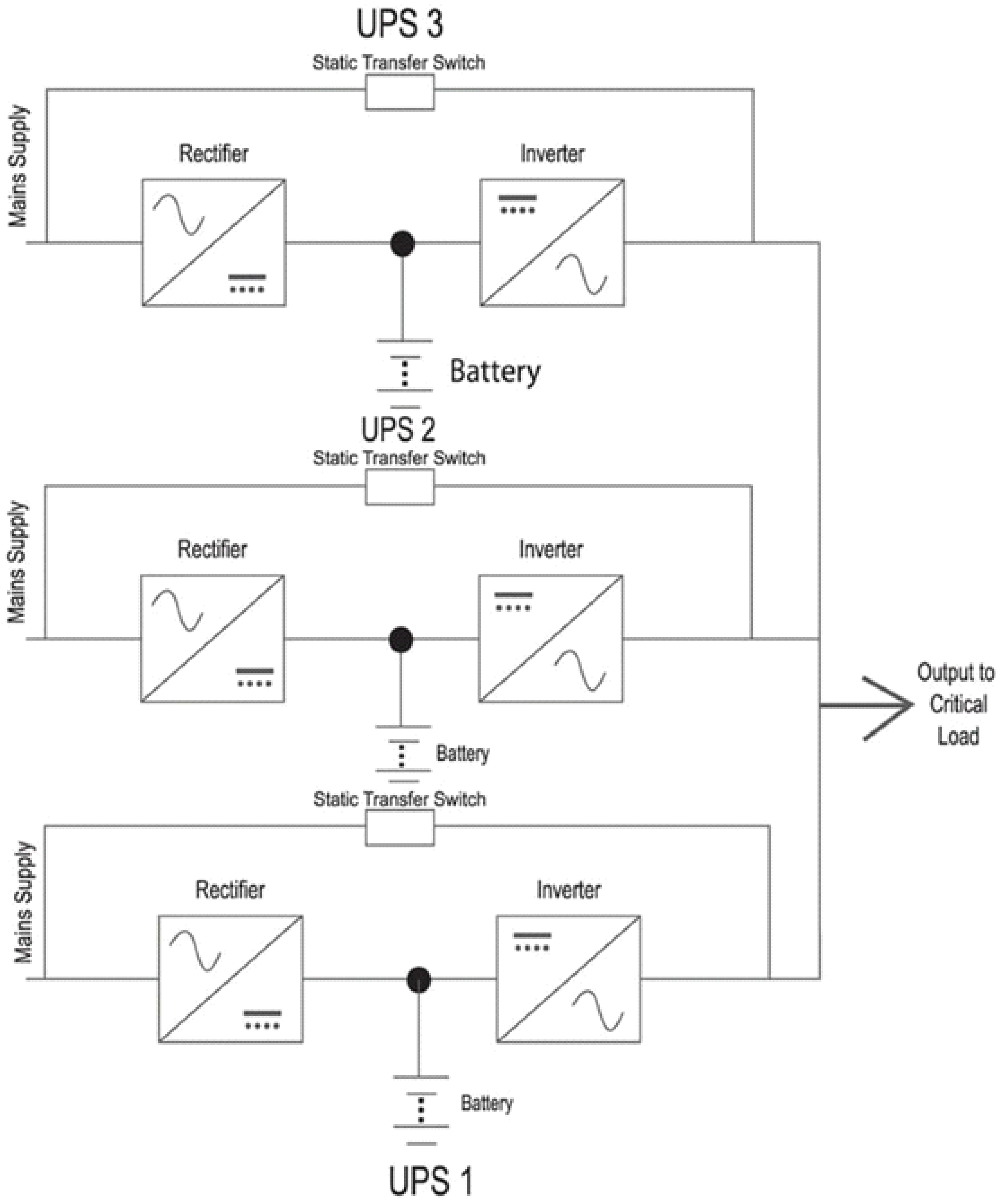


Fig 5.2.1: Parallel redundant configuration (N +1)

2N+1 Redundancy: In this configuration, three independent UPS systems are installed, with two capable of handling the full load of the telecom site and the third acting as a backup. This configuration provides an even higher level of redundancy to ensure an uninterrupted power supply.

5.2.3 Check the Electrical Parameters

To test the UPS voltage, current, and earth for the power supply:

- **Check the input voltage:** Use a voltmeter to check the input voltage of the UPS. This should match the voltage rating of the UPS and should be within the acceptable range for the equipment connected to the UPS.
- **Measure the output voltage:** Connect a load to the output of the UPS and use a voltmeter to measure the output voltage. This voltage should be within the acceptable range for the equipment connected to the UPS.
- **Measure the output current:** Use a clamp meter to measure the output current of the UPS. This current should be within the acceptable range for the equipment connected to the UPS.
- **Check the UPS earthing:** Use a multimeter to measure the voltage between the UPS chassis and the earth. This voltage should be zero or very low, indicating that the UPS is properly grounded.
- **Perform a battery test:** Test the UPS batteries to ensure that they are functioning properly and providing the required backup power in the event of a power outage. This can be done using the UPS's built-in battery testing feature or with an external battery tester.
- **Conduct a load test:** Test the UPS with a load that is equal to or greater than the rated load of the UPS to ensure that it is operating properly and providing the required backup power. This can be done by simulating a power outage or by gradually increasing the load on the UPS while monitoring its output voltage and current.

5.2.4 Route Power Supply through UPS

Routing power supply through large UPS in a telecom site is a critical task that requires careful planning and execution to ensure a reliable power supply to the site equipment. The following steps can be followed for routing power supply through a large UPS:

- **Plan the power distribution system:** Plan the power distribution system carefully to ensure that the power supply is distributed evenly to all the telecom site equipment. The power distribution system should be designed based on the power requirements of the equipment and the capacity of the UPS.
- **Install the input circuit breaker:** Install the input circuit breaker to protect the UPS and the equipment from overloads and short circuits. The circuit breaker should be rated according to the power requirements of the equipment. The circuit breaker should be installed as close as possible to the UPS input terminals, preferably in a dedicated panel or breaker box.
- • **Connect the power cables:** Connect the power cables to the input terminals of the UPS. Make sure that the cables are properly rated for the current and voltage requirements of the UPS. They should be connected to the input terminals of the UPS, which are usually labelled as L1, L2, and L3 for the phases and N for the neutral. The ground cable should be connected to the designated ground terminal.

- **Connect the output cables:** Connect the output cables from the UPS to the distribution panels or the equipment to be powered. Make sure that the cables are properly rated for the current and voltage requirements of the equipment. They should be connected to the distribution panels or the equipment to be powered. It is important to follow the manufacturer's instructions for proper cable routing and termination to avoid any electrical interference or grounding issues.
- **Test the power supply:** After connecting the power and output cables, it is essential to test the power supply to ensure that it is providing the correct voltage and current to the equipment. This can be done using a multimeter to measure the voltage and current at various points in the system. It is important to verify that the voltage and current measurements match the equipment's requirements and the UPS's rating.

5.2.5 Replace Faulty Battery

Replacing a faulty battery from a UPS involves the following steps:

Step 1. Turn off the UPS

Before beginning the battery replacement process, the UPS must be turned off to avoid any electrical hazards.

Step 2. Remove the battery cover

Depending on the type of UPS, the battery cover may be located on the side or top of the UPS. Remove the cover by using a screwdriver or by pressing the release buttons if they are present.

Step 3. Identify the faulty battery

Once the battery cover is removed, the faulty battery needs to be identified. The batteries are usually arranged in a series or parallel configuration and are connected to the UPS via a battery cable. Carefully disconnect the battery cable from the faulty battery.

Step 4. Remove the faulty battery

Remove the faulty battery from the UPS by gently lifting it out of its slot. Some UPS systems may have a locking mechanism that needs to be disengaged before removing the battery.

Step 5. Insert the new battery

Insert the new battery into the slot, ensuring that the battery terminals are aligned with the UPS terminal. Carefully connect the battery cable to the new battery, making sure that the positive and negative terminals are properly aligned.

Step 6. Replace the battery cover

Once the new battery is installed, replace the battery cover by securing it with screws or pressing the release buttons.

Step 7. Turn on the UPS

Finally, turn on the UPS and monitor the system to ensure that the new battery is functioning properly. It may take some time for the UPS to charge the new battery, so allow the UPS to run for a few hours before checking the battery status.

5.2.6 Checking for Polarity and Phase Alignment to Avoid Incorrect Wiring

In any electrical installation, ensuring correct **polarity** and **phase alignment** is critical for the safe and efficient functioning of equipment, especially in systems like **UPS (Uninterruptible Power Supply)**. Incorrect wiring can lead to hazards such as electric shocks, equipment damage, malfunction, or fire hazards.

- **Polarity:** The direction of current flow in a circuit, typically marked as **positive (+)** and **negative (−)** in DC systems, or **line (L)**, **neutral (N)**, and **earth (E)** in AC systems.
- **Phase Alignment:** The correct arrangement of multiple AC phases (L1, L2, L3) so that they match the intended sequence for proper operation of three-phase equipment.

Importance of Polarity and Phase Alignment

- Prevents damage to sensitive electronic components.
- Ensures correct operation of motors and phase-sensitive equipment.
- Reduces the risk of electric shocks and short circuits.
- Maintains compliance with **IEC standards** and local **electrical codes**.

Tools and Instruments Required

- **Multimeter** – for voltage and continuity testing.
- **Phase Sequence Indicator / Rotating Field Tester** – for verifying phase sequence in three-phase systems.
- **Polarity Tester** – for confirming correct line and neutral connection.
- **Insulated Screwdrivers** – for making adjustments safely.
- **Personal Protective Equipment (PPE)** – gloves, safety shoes, insulated mats, and safety glasses.

Procedure for Checking Polarity

Step 1: Isolate Power Supply

- Switch off the main breaker and ensure no voltage is present before starting work.
- Use **Lockout/Tagout (LOTO)** procedures to prevent accidental energizing.

Step 2: Connect the Polarity Tester or Multimeter

- For **AC circuits**:
  - Place the **black probe** on **Neutral (N)**.
  - Place the **red probe** on **Line (L)**.
  - A correct reading will show the expected voltage (e.g., ~230V in single-phase).
- For **DC circuits**:
  - Connect probes to positive (+) and negative (−) terminals and verify correct polarity.

Step 3: Identify Incorrect Polarity

- If voltage readings are reversed or significantly different, swap the connections at the terminal block as per manufacturer guidelines.

Procedure for Checking Phase Alignment

Step 1: Use a Phase Sequence Indicator

- Connect the indicator to L1, L2, L3 terminals of the incoming supply.
- The device will display either correct phase sequence (clockwise) or incorrect phase sequence (anticlockwise).

Step 2: Correcting Phase Misalignment

- If the phase sequence is incorrect:
    - Swap any two of the three phase wires at the supply terminals.
    - Recheck with the phase sequence indicator to confirm correctness.

Safety Precautions

- Always work with insulated tools and wear appropriate PPE.
- Do not perform polarity or phase checks on live circuits without proper authorization and precautions.
- Never bypass protective devices (MCBs, fuses, RCDs) during testing.
- Comply with local and international electrical standards such as IEC 60364.

Documentation and Reporting

- Record polarity test results, phase sequence verification, and any corrective actions taken in the installation log.
- Ensure test certificates are prepared as part of the commissioning documentation.
- Maintain these records for future maintenance and compliance audits.

5.2.7 Ensuring UPS Output Matches Required Power Quality Standards

A Uninterruptible Power Supply (UPS) is designed to provide clean, stable, and reliable power to connected equipment. To ensure the UPS output meets the required power quality standards, technicians must verify electrical parameters and waveform quality according to manufacturer specifications, electrical codes, and industry standards (e.g., IEC 62040).

1. Understanding Power Quality Parameters

Before testing, it is important to identify the parameters that define acceptable UPS output quality:

Parameter	Acceptable Range (Typical)	Impact if Out of Range
Output Voltage	±2–5% of nominal rating (e.g., 230V ±5%)	Equipment malfunction, overheating, or shutdown
Frequency	50 Hz ±0.1 Hz (or 60 Hz ±0.1 Hz)	Data loss, motor speed variation, audio/video distortion
Total Harmonic Distortion (THD)	≤ 3–5% for sensitive loads	Overheating, signal interference, reduced equipment life
Power Factor	Close to unity (0.9–1.0)	Increased losses, reduced efficiency
Voltage Regulation	Minimal fluctuation under load changes	Unstable operation of sensitive devices

2. Tools and Instruments Required

- **True RMS Digital Multimeter (DMM)** – for accurate voltage and frequency readings.
- **Power Quality Analyzer** – for THD, waveform distortion, and power factor measurement.
- **Oscilloscope** – to visually check waveform purity and phase stability.
- **Load Bank** – for simulating operational loads.

3. Step-by-Step Procedure

Step 1: Preparation

- Review manufacturer specifications for the UPS output parameters.
- Isolate non-essential loads to prevent disruption during testing.
- Ensure the UPS is in operational mode and connected to the intended load or test load bank.
- Wear appropriate PPE and follow lockout/tagout (LOTO) safety procedures.

Step 2: Voltage and Frequency Verification

- Connect the DMM to the UPS output terminals.
- Record the no-load voltage and frequency.
- Compare readings with nominal rated values (e.g., 230V, 50 Hz).
- Apply incremental loads using the load bank and observe if voltage and frequency remain within specified tolerances.

Step 3: Harmonic Distortion Measurement

- Connect the power quality analyzer at the UPS output.
- Measure THD under different load conditions.
- If THD exceeds recommended limits (usually <5%), check for:
  - Overloaded UPS
  - Poor grounding or shielding
  - Faulty internal inverter components

Step 4: Waveform and Phase Alignment Check

- Use an oscilloscope to visualize the output waveform.
- Confirm that it is a pure sine wave (for sensitive loads) without flattening or distortion.
- Check phase alignment to ensure no phase shift that could affect synchronized equipment.

Step 5: Load Response and Recovery

- Apply a sudden load increase and decrease.
- Record recovery time for voltage and frequency to stabilize.
- Ensure recovery meets manufacturer guidelines (usually within a few milliseconds).

Step 6: Documentation

- Record all measured values in the maintenance log.
- Note any deviations from standard values and recommend corrective actions.
- Include instrument calibration records for traceability.

4. Troubleshooting If Standards Are Not Met

Fault	Possible Cause	Remedy
Low output voltage	Inverter fault, battery weakness, overload	Check battery health, reduce load, service inverter
High THD	Damaged inverter, harmonic interference from load	Replace faulty components, add harmonic filters
Frequency instability	Control circuit malfunction	Inspect and replace faulty control board
Poor waveform shape	Inverter MOSFET/IGBT damage	Test and replace defective components

5. Safety Precautions

- Never touch live terminals while measuring output.
- Use insulated tools and category-rated test equipment.
- Do not test during battery replacement or UPS bypass mode unless approved by procedure.
- Maintain minimum clearance from energized components.

5.2.8 Identifying and Reporting Power Supply Fluctuations or Irregularities

Power supply stability is crucial for the reliable operation of electrical and electronic equipment. Fluctuations such as voltage sags, surges, frequency deviations, and harmonics can lead to reduced efficiency, overheating, data loss, or permanent damage to connected systems. Technicians must be able to detect these irregularities promptly and report them for corrective action.

i. Common Types of Power Supply Irregularities

Irregularity	Description	Possible Causes	Impact on Equipment
Voltage Sag/Dip	Temporary drop in voltage level	High load startup, utility faults	Equipment reset, malfunction
Voltage Surge/Spike	Sudden increase in voltage	Lightning strikes, switching loads	Component damage, overheating
Frequency Variation	Deviation from nominal frequency (e.g., 50 Hz)	Generator instability, grid issues	Speed mismatch in motors, process disruption
Harmonic Distortion	Waveform distortion due to non-linear loads	VFDs, rectifiers, UPS malfunction	Overheating of transformers, misoperation of relays
Brownout	Sustained low voltage	Overloaded power grid	Reduced motor torque, flickering lights
Blackout	Total loss of power	Grid failure, breaker trip	System shutdown, data loss

ii. Methods to Identify Power Fluctuations

1. Visual Indicators

- Flickering lights or displays
- Unusual noises from motors or transformers
- Frequent equipment restarts

2. Measurement Tools

- **Digital Multimeter (DMM)**: Measures voltage and frequency.
- **Power Quality Analyzer**: Detects sags, swells, harmonics, and waveform distortion.
- **Oscilloscope**: Monitors waveform quality.
- **Event Recorder**: Captures transient events for later analysis.

3. Testing Procedure

- **Preparation**: Wear PPE and ensure proper safety isolation procedures.
- **Baseline Measurement**: Record normal voltage, frequency, and waveform under load.
- **Load Variation Testing**: Measure during different load conditions (startup, peak operation).
- **Event Capture**: Use analyzers to log data over 24–48 hours to catch intermittent fluctuations.
- **Comparison**: Compare readings with manufacturer specifications and local electrical code limits (e.g., ±6% voltage variation, ±1% frequency deviation).

iii. Reporting Procedure

1. Information to Include

- **Date & Time** of observation
- **Type of Irregularity** detected
- **Measurement Data** (voltage, frequency, THD values, waveform screenshots)
- **Duration & Frequency** of occurrence
- **Affected Equipment**
- **Immediate Impact** (e.g., downtime, overheating)

2. Reporting Format

- **Log Sheet** for daily monitoring
- **Incident Report Form** for major fluctuations
- **Digital Reports** generated by power quality analyzers (PDF/CSV)

3. Communication

- Notify the maintenance supervisor or control room immediately for severe cases.
- Share recorded data with the engineering team for root cause analysis.
- If required, escalate to utility provider for grid-related issues.

iv. Safety Considerations

- Never attempt measurements without proper training and insulated tools.
- Use lockout/tagout (LOTO) when connecting monitoring equipment.
- Maintain safe clearance from live conductors.

5.2.9 Cleaning and Securing UPS Ventilation to Prevent Overheating

Introduction

Uninterruptible Power Supply (UPS) units generate heat during operation. To maintain optimal performance and prevent component damage, proper ventilation is essential. Dust, debris, or obstructions in the ventilation openings can restrict airflow, leading to overheating and reduced equipment lifespan. Cleaning and securing the ventilation system is a crucial part of preventive maintenance.

1. Understanding the Importance of Ventilation in UPS

- **Heat Dissipation:** UPS systems contain power conversion circuits and batteries that generate heat during normal operation.
- **Airflow Path:** Cooling fans draw air through vents to dissipate heat and maintain internal temperature within safe operating limits.
- **Risk of Overheating:** Blocked or clogged vents increase internal temperature, potentially causing:
    - Battery degradation
    - Reduced UPS efficiency
    - Component failure
    - Unexpected shutdowns

2. Preparatory Safety Measures

Before cleaning the UPS ventilation:

- **Switch Off and Disconnect Power**
  - Shut down the UPS as per manufacturer's instructions.
  - Disconnect from mains power supply and isolate battery connection.
- **Wear Protective Gear**
  - Use safety gloves and anti-static wrist straps to avoid static discharge damage.
- **Ensure Adequate Lighting and Workspace**
  - Work in a clean, dry, and well-lit environment.

3. Cleaning Procedure

Step 1: External Vent Cleaning

- Use a soft-bristled brush or compressed air to remove dust from external vents.
- Hold the compressed air can at a slight angle and at least 15–20 cm away to avoid pushing dust inside.

Step 2: Internal Dust Removal (if permitted by manufacturer)

- Open the UPS casing only if it is designed for user maintenance and warranty terms allow.
- Use a low-powered vacuum cleaner or compressed air to remove internal dust from:
  - Cooling fans
  - Air filters (if present)
  - Heat sinks

Step 3: Cleaning Fan Blades

- Gently wipe fan blades using a lint-free cloth slightly dampened with isopropyl alcohol.
- Ensure no liquid drips into the circuitry.

4. Securing Ventilation Openings

- **Check Vent Covers:** Ensure that vent grills or covers are firmly attached and free from cracks.
- **Maintain Clearance:** Keep at least 10–15 cm of space around all sides of the UPS for airflow.
- **Avoid Blockages:** Do not place UPS near walls, curtains, or paper stacks that could obstruct airflow.
- **Reinstall Filters:** If the UPS has removable dust filters, ensure they are properly reinstalled after cleaning.

5. Post-Cleaning Verification

- **Reconnect and Power On:** Follow proper startup procedures.
- **Check Fan Operation:** Ensure cooling fans run smoothly without unusual noise.
- **Monitor Temperature:** Use UPS monitoring software or inbuilt display to check operating temperature.

- **Log Maintenance Activity:** Record date, cleaning actions, and observations in the UPS maintenance log.

6. Maintenance Frequency

- **Office Environment:** Every 6 months
- **Dusty/Industrial Environment:** Every 2–3 months
- **High Humidity Zones:** Check monthly to avoid moisture-related dust accumulation.

5.2.10 Diagnosing and Troubleshooting Common UPS Faults

UPS (Uninterruptible Power Supply) systems protect critical equipment from power disturbances, but faults can occur due to improper operation, component failure, or environmental factors. Understanding common issues and their troubleshooting methods is essential for safe and reliable operation.

1. Overloading

Description: Occurs when the connected load exceeds the UPS's rated capacity, leading to overheating, reduced battery runtime, or shutdown.

Symptoms:

- UPS alarm or warning lights indicating overload
- Sudden shutdown under load
- Frequent switching to bypass mode

Diagnosis Steps:

- Check the UPS load indicator on the control panel.
- Compare load reading with UPS capacity (kVA/kW rating).
- Identify devices drawing excessive current using a clamp meter.

Troubleshooting Methods:

- Disconnect non-critical loads until the load is within limits.
- Redistribute loads across multiple power circuits.
- Upgrade UPS capacity if load demands are consistently high.

2. Short Circuit

Description: A direct connection between live conductors or between a conductor and ground, causing excessive current flow.

Symptoms:

- Tripped circuit breakers or blown fuses
- Audible pop or spark before UPS shutdown
- Burning smell or visible damage to wiring

Diagnosis Steps:

- Isolate the UPS from both input and output power.
- Inspect connected cables and devices for visible damage.
- Use a multimeter in continuity mode to detect abnormal zero-resistance paths.

Troubleshooting Methods:

- Replace damaged cables and connectors.
- Repair or replace faulty connected equipment.
- Reset circuit breakers after resolving the fault.

3. Failed Inverter

Description: The inverter, which converts DC battery power to AC output, fails due to component malfunction or prolonged overload.

Symptoms:

- UPS only operates in bypass mode
- No power output during mains failure
- Alarm codes indicating inverter failure

Diagnosis Steps:

- Check the UPS event log for inverter fault codes.
- Measure inverter output voltage using a multimeter.
- Visually inspect for burnt components or capacitor leakage inside the inverter section.

Troubleshooting Methods:

- Replace faulty inverter boards or modules as per manufacturer guidelines.
- Ensure adequate cooling to prevent component overheating.
- Perform post-repair testing under controlled load.

4. Safety Considerations

- Always de-energize the UPS before opening any covers.
- Wear insulated gloves and use rated tools.
- Follow Lockout/Tagout (LOTO) procedures to prevent accidental energization.
- Never bypass safety interlocks.

5. Documentation

After troubleshooting:

- Record fault type, diagnosis steps, corrective actions, and replaced parts.
- Update maintenance logs for future reference.
- Report any recurring faults to the manufacturer for further analysis.

5.2.11 Documenting Test Results, Maintenance Actions, and Reported Issues

Accurate documentation ensures equipment reliability, compliance with standards, and traceability for future troubleshooting.

1. Preparation Before Documentation

- **Gather Required Tools & Forms**:
  - ○ Standard maintenance logbook or digital CMMS (Computerized Maintenance Management System)
  - ○ Manufacturer's test sheet or checklist template
  - ○ Pen or electronic device for entries
  - ○ UPS model & serial number details
- **Verify Standards**: Follow ISO 9001: Quality Management, IEC 62040 (UPS systems), and organizational maintenance SOPs.

2. Recording Test Results

Steps:

1. Identify the Test Performed
   - ○ e.g., Load Test, Battery Voltage Test, Continuity Test, Inverter Output Test
2. Record Test Parameters & Values
   - ○ Date & Time of test
   - ○ Equipment ID & location
   - ○ Test readings (e.g., Voltage: 230V, Frequency: 50Hz, Load: 65%)
3. Include Pass/Fail Status
   - ○ Mark test outcome as per threshold values
4. Attach Supporting Evidence (if applicable)
   - ○ Photos, graphs, or screenshots from test equipment

3. Recording Maintenance Actions

Steps:

1. Describe the Task Performed
   - ○ e.g., Cleaned UPS ventilation filters, Replaced battery module, Adjusted load connections
2. Note Any Parts Replaced
   - ○ Include part number & quantity
3. Mention Duration & Downtime
   - ○ Start & finish time
4. State Technician's Name & Signature
5. Link to Preventive Maintenance Schedule

4. Recording Reported Issues

Steps:

1. Log the Problem as Reported by Operator/User
   - Include exact wording from the report
2. Assign Priority Level
   - Critical / Major / Minor
3. Link to Incident Number or Job Ticket
4. Mark Resolution Status
   - Pending / In Progress / Resolved
5. Add Remarks for Follow-up

5.2.12 Communicating Findings and Recommendations to Customers or Supervisors

1. Purpose of Communication

Effective communication ensures that technical issues, inspection results, or maintenance updates are clearly understood by the concerned stakeholders. The objective is to provide accurate, concise, and actionable information for decision-making.

2. Key Principles

1. **Accuracy** – All findings must be fact-based, supported by evidence such as test results, photographs, or data logs.
2. **Clarity** – Use simple, jargon-free language when addressing non-technical customers; use precise technical terms when reporting to supervisors or engineering teams.
3. **Timeliness** – Communicate as soon as possible after the activity to ensure immediate action can be taken.
4. **Confidentiality** – Share sensitive information only with authorized personnel.

3. Steps for Communicating Findings

a) Preparation

- Review and verify all collected data (test readings, measurements, visual inspections).
- Identify the key points that need to be conveyed (e.g., faults found, performance issues, deviations from standards).

b) Structuring the Message

- **Introduction** – State the purpose (e.g., "Report on UPS performance test results").
- **Findings** – Present observed conditions and evidence (e.g., "Output voltage fluctuated between 215–230V during load test").

- **Analysis** – Briefly explain possible causes (e.g., “Likely due to inconsistent input supply or faulty voltage regulation circuit”).
- **Recommendations** – Suggest corrective actions (e.g., “Replace AVR module and monitor load distribution”).
- **Conclusion** – Summarize key takeaways and urgency level.

c) Delivery Methods

- **Verbal Briefing** – For urgent issues, use face-to-face or phone communication.
- **Written Reports** – For formal documentation and record-keeping.
- **Email Summary** – For quick reference and follow-up actions.

4. Best Practices for Customer Communication

- Avoid overly technical language unless the customer is technically trained.
- Use analogies or visual aids (charts, graphs, photos) to explain complex issues.
- Remain professional and objective—focus on facts, not personal opinions.

5. Best Practices for Supervisor Communication

- Provide full technical details, including reference to standards or manufacturer manuals.
- Highlight safety concerns and compliance issues.
- Suggest both short-term fixes and long-term preventive measures.

6. Sample Communication Format

Subject: UPS Load Test Report – 12th Aug 2025
To: [Recipient]
From: [Your Name]
Summary: During routine testing, the UPS was found to have voltage fluctuations under 70% load.
Findings: Output voltage range 215–230V; Battery health at 80% capacity.
Recommendations: Replace AVR module, rebalance load, and schedule full battery replacement within 6 months.
Attachments: Test logs, photographs, maintenance checklist.

Summary

- Various types of UPS, such as offline/standby, line-interactive, and online/double conversion, are available in the market.
- Different types of batteries, such as lead-acid, lithium-ion, nickel-cadmium, and alkaline batteries, are compatible with UPS.
- UPS installation activities include selecting the appropriate location, identifying and installing the necessary equipment, and ensuring proper grounding and ventilation.
- Basic wiring diagrams must be analyzed before installing the UPS to understand the circuitry and ensure proper installation.
- UPS can be distinguished based on their power ratings, such as VA (volt-ampere) and watts.
- The equipment load must be calculated to determine the appropriate UPS rating required to support the load.
- The procedure for installing UPS should follow the manufacturer's instructions and include steps such as mounting the unit, connecting the battery, and connecting the load.
- Checks for voltage, current, and earthing must be performed during UPS installation to ensure that the unit is installed safely and securely.
- The power supply should be routed through the UPS to ensure uninterrupted power supply to the equipment.
- Precautions must be taken while handling power supplies, such as avoiding contact with live wires and disconnecting the power supply before working on equipment.
- In case of a defective UPS, the battery must be replaced, and checks must be performed to ensure that the UPS is functioning correctly after the replacement.

Exercise

A. Multiple Choice Questions:

1. What precautions should be taken while handling power supplies?

   a. Avoid contact with water   b. Use insulated tools

   c. Disconnect power before maintenance   d. All of the above

2. Which types of batteries are compatible with the UPS?

   a. Lead-acid   b. Nickel-cadmium

   c. Lithium-ion   d. All of the above

3. What is the purpose of calculating equipment load vis-à-vis UPS rating?

   a. To ensure the UPS is not overloaded

   b. To calculate the battery backup time

   c. To determine the maximum number of devices that can be connected to the UPS

   d. To ensure the UPS is properly grounded

4. Which of the following is NOT a step to replace a faulty battery in a UPS?

   a. Disconnect the power supply

   b. Remove the battery cover

   c. Disconnect the battery cables

   d. Replace the battery with any type of battery available

5. What are the standard UPS and voltage/current norms to be followed in the installation process?

   a. IEEE and EN standards   b. ANSI and IEC standards

   c. DIN and ISO standards   d. None of the above

B. Descriptive Questions:

1. What are the precautions that should be taken while handling power supplies, and why are they important?
2. Describe the different types of batteries that are compatible with a UPS, and what factors should be considered when choosing a battery.
3. Compare different types and power rating of UPS, and explain which factors should be considered when selecting a UPS for a specific application.
4. What are the steps involved in planning installation activities for a UPS, and why is planning important?
5. What are the steps involved in replacing a faulty battery in a UPS, and why is it important to follow these steps carefully?

Notes

____

____

____

____

____

____

____

____

____

____

____

____

____

____

____

____

Scan the QR codes or click on the link to watch the related videos

https://www.youtube.com/watch?v=bj5KpFR_LPU

What is a UPS?

https://www.youtube.com/watch?v=3S0poIviRac

Three Types of UPS System Technologies

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

How to Connect UPS to Home Distribution Board

https://www.youtube.com/watch?v=iNpizBLXao8

Dangers of Electricity, and Appropriate Safety Measures

सत्यमेव जयते
GOVERNMENT OF INDIA
MINISTRY OF SKILL DEVELOPMENT
& ENTREPRENEURSHIP

6. Sustainability Practices in Telecom Infrastructure Installation

Unit 6.1- 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 6.1: 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.

6.1.1 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.

6.1.2 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.

6.1.3 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. 6.1.1 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.

6.1.4 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.

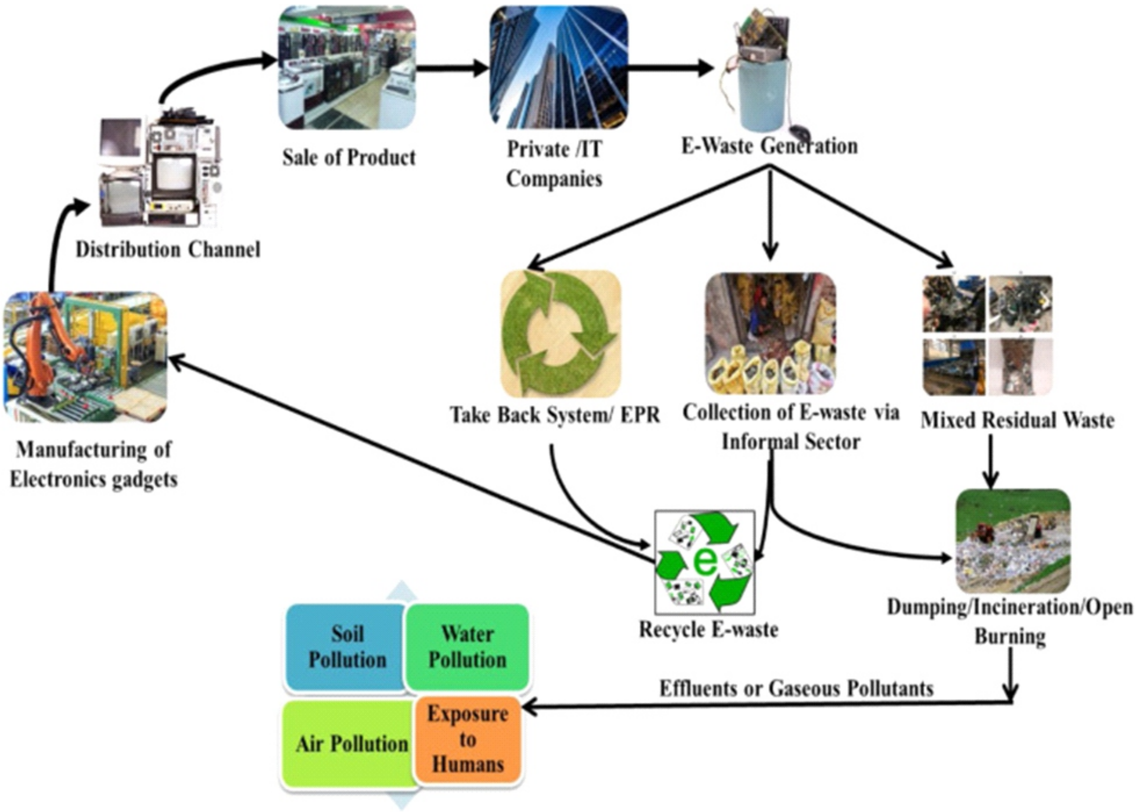


Fig. 6.1.2 E-waste Management

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.

6.1.5 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.

6.1.6 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.

6.1.7 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.

6.1.8 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

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

7. Employability Skills (60 Hours)

It is recommended that all training include the appropriate. Employability Skills Module. Content for the same can be accessed

https://www.skillindiadigital.gov.in/content/list

DGT/VSQ/N0102

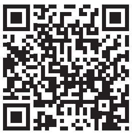
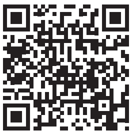
सत्यमेव जयते
GOVERNMENT OF INDIA
MINISTRY OF SKILL DEVELOPMENT
& ENTREPRENEURSHIP

8. Annexure

Annexure I - QR Codes –Video Links

Annexure - I

QR Codes –Video Links

Module No.	Unit No.	Topic Name	Page No	Link for QR Code (s)	QR code (s)
1. Introduc-tion to the Role of a Wireless Technician	1.1: Introduction to Telecom Sector	1.1.1 Telecom Sector in India	15	https://www.youtube.com/watch?v=tha-DJhkih8	 Telecom Sector in India
		1.1.2 Wi-Fi Broadband Industry in India	15	https://www.youtube.com/watch?v=x3c1ih2NJEg	 How does the INTERNET work?
		1.1.3 Role and Re-sponsibilities of a Wireless Techni-cian	15	https://www.youtube.com/watch?v=cppHX2bMjEc	 Technical Support Jobs
		1.1.4 Electrical and Electronic Com-ponents used for Wireless Instal-lations	15	https://www.youtube.com/watch?v=6UTOTgbJ_8E	 Basic Electronic components
		1.1.6 Safety, Health and Environ-mental Regula-tions for Work-place	15	https://www.youtube.com/watch?v=IZVxBlX18Dw	 Environment, Health & Safety (EHS) Effectiveness

Module No.	Unit No.	Topic Name	Page No	Link for QR Code (s)	QR code (s)
2. Pre-requisites of Wiring and Wi-Fi Backhaul Equipment	2.1: Installation of Wi-Fi System	2.1.1 Analysing Work Orders and Job Sheets	44	https://www.youtube.com/watch?v=P8j2H5J4fU4	How to Set Up a Wi-Fi Network
		2.1.2 Wi-Fi Backhaul	44	https://www.youtube.com/watch?v=-DIbLZ3hL9M	Wireless OR Wired Backhaul Benefits
		2.1.6 Wi-Fi System Instal-lation	44	https://www.youtube.com/watch?v=P8j2H5J4fU4	How to Set Up a Wi-Fi Network
	2.2: Complete Docu-mentation	2.2.1 Im-portance of Satisfactory Customer Service	74	https://www.youtube.com/watch?v=WnQ7L4WFrcQ	Why is customer service important?
		2.2.3 Differ-ent Payment Modes	74	https://www.youtube.com/watch?v=GUurzvS3DlY	What is a payment gateway and how does it work?

Module No.	Unit No.	Topic Name	Page No	Link for QR Code (s)	QR code (s)
3. Configur-ing Equipment and Establishing Connectivity	3.1: Setting up Wi-Fi Network	3.1.1 Concept of Wireless Technology	94	https://www.youtube.com/watch?v=I2PKJslPObM	Wireless Technology
		3.1.4 Gateways	94	https://www.youtube.com/watch?v=pCcJFdYNamc	Wireless OR Wired Backhaul Benefits
		3.1.5 TCP/IP	94	https://www.youtube.com/watch?v=CsektxtqA8c	TCP/IP Protocol Explained
		3.1.9 Ether-net address / MAC Address	94	https://www.youtube.com/watch?v=TIiQiw7fpsU	MAC Address Explained
	3.2: Establishing Connectivity	3.2.3 First-Aid Box	94	https://www.youtube.com/watch?v=8assGpZvwG4	What Should be in a First Aid Kit?

Module No.	Unit No.	Topic Name	Page No	Link for QR Code (s)	QR code (s)
4. Trouble-shoot to Lo-calize and Rectify Faults	4.1: Prepare for Trouble-shooting Wi-Fi Backhaul Equipment	4.1.1 EMI/EMC Concepts	94	https://www.youtube.com/watch?v=cWo_sVDTszY	EMI (ElectroMagnetic Interference) & EMC (Electromegetic Compatibility)
5. UPS In-stallation and Domes-tic Power Supply Checks	5.1: Plan for UPS Installation	5.1.1 Unin-terruptible Power Supply (UPS)	94	https://www.youtube.com/watch?v=bj5KpFR_LPU	What is a UPS?
		5.1.2 Types of Batteries Compatible with UPS	94	https://www.youtube.com/watch?v=3S0polviRac	Three Types of UPS System Technologies
	5.2: Install UPS and Check the Electrical Parameters	5.2.1 In-stalling UPS	143	https://www.youtube.com/watch?v=sjopLdwFJSw	How to Connect UPS to Home Distribution Board
		5.2.6 Precau-tions While Handling Power Sup-plies	143	https://www.youtube.com/watch?v=iNpizBLXao8	Dangers of Electricity, and Appropriate Safety Measures

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