INDUSTRIAL TRAINING REPORT

UNDER THE

STUDENTS' INDUSTRRIAL WORK EXPERIENCE SCHEME (SIWES)

AT

TIZETI NETWORK LIMITED, ABEOKUTA, OGUN STATE

BY

ODUNOWO RIDWAN DAMILARE

MATRIC NO: 20193273

TO

THE DEPARTMENT OF PHYSICS

COLLEGE OF PHYSICAL SCIENCES

FEDERAL UNIVERSITY OF AGRICULTURE, ABEOKUTA

JANUARY 2024.

CERTIFICATION

I hereby certify that the work recorded as contained in this Student Industrial Work Experience Scheme (SIWES) report was carried out and submitted by **ODUNOWO RIDWAN DAMILARE** with matriculation number **20193273** within five months at **TIZETI NETWORK LIMITED, ABEOKUTA, OGUN STATE.** In partial fulfillment of the requirements for the award of bachelor's degree in the Department of **PHYSICS** of Federal University of Agriculture Abeokuta, Ogun State, Nigeria.

_____ _____

ODUNOWO RIDWAN DAMILARE **DR. O.T OLURIN**

Student *Supervising Lecturer*

_____

PROF. (Mrs.) I.C OKEYODE

Head of Department

ACKNOWLEDGEMENT

My profound gratitude goes to Allah the omniscient and omnipotent, the giver of life for his never-ending grace and guidance during the course of my students` Industrial Work Experience Scheme (SIWES).

My sincere appreciation goes to my parents, **Engr. And Mrs. Odunowo** who sponsored my educational pursuit unceasingly till this moment, and to the entire physics student of the Federal University of Agriculture, Abeokuta, for being my source of motivation.

I also express my sincere appreciation to my Industry based supervisor, **Engr. Owolabi** and the **NOC OGUN** team; Engr. Adebowale, Engr. Olalekan, Engr. Gabriel, for all their precise, concise, constructive criticism and assistance during the course of my training at Tizeti Network Limited, Abeokuta.

REPORT OVERVIEW

In the present world, it is significant to note that the practical training is very important in our day-to-day activities, irrespective of discipline or area of specialization. There is need for individuals to be practical-oriented in order to be fully equipped and broaden their horizon or in whatever field they have chosen or found themselves.

The students` Industrial Work Experience Scheme (SIWES) program has gone a long way in exposing students (undergraduates) across various levels to the practical world, which has also accorded me the opportunity to deal with real life situation that are in line with **Industrial Physics** likewise how to relate socially with other workers in an organization, how the organization is being run across different levels.

This report made mention of the objectives of SIWES, and also gave a concise and detailed of the establishment of place of attachment, experience gained so far, challenges faced and suggestions on possible ways out of those challenges.

TABLE OF CONTENTS

CHAPTER FOUR: INTRODUCTION TO NETWORKING

CHAPTER FIVE

CHAPTER ONE

1.0 INTRODUCTION TO STUDENTS` INDUSTRIAL WORK EXPERIENCE SCHEME (SIWES)

The students` Industrial Work Experience Scheme (SIWES) is an accepted skills program which forms part of the approved academic standards in the degree program for Nigerian universities. The Federal Government of Nigeria introduced the national policy on industrial training called the students` Industrial Work Experience Scheme (SIWES). This program is under the umbrella of the ministry of education through the Industrial Training Fund (ITF), was designed to help students acquire the necessary practical education /experience in their fields of study and other related professions. It is also intended that the students through a process of relation to academic knowledge and practical industrial application would understand the underlying principles and become better focused and acquire the practical applications towards excellence in his or her discipline.

1.1 BACKGROUND OF SIWES

Students` Industrial Work Experience Scheme (SIWES) introduction, initiation and design were done by the Industrial Training Fund (ITF) in 1974 to acquaint students with the skills of handling employer`s equipment and machinery. The ITF solely funded the scheme during its formative years. However, due to financial constraints, the fund withdrew from the scheme in 1978.

The federal government, noting the significance of the skills training handed the management of the structure to both the National Universities Commission (NUC) and the National Board for Technical Education (NBTE) in 1979. The management and implementation of the scheme was reverted to the ITF by the Federal Government of Nigeria in November, 1984 and the administration was effectively taken over by ITF in July 1985, with the funding solely borne by the Federal Government.

1.2 OBJECTIVES OF SIWES

The main objective or aim of SIWES is to provide the students with the feel of the actual working environment and to gain practical knowledge and skills, which in turn will motivate, develop and build their confidence.

The specific objectives of SIWES were summarized by the government in its Gazette of April, 1978 as follows;

- Prepare students for the industrial work situation they are to find themselves after graduation.
- Provide an avenue for students in institutions of higher learning to acquire industrial skills and experience in their course of study, which are restricted to Engineering and Technology including Environmental studies and other courses that may be approved. Courses of NCE (Technical), NCE (Agriculture), NCE (Business), NCE (Fine and Applied Arts) and NCE (Home Economics) in Colleges of Education are also included.
- Help students have contacts for future job placement.
- Provide avenue for students in institutions of higher learning to acquire industrial skills and experience relevant to their course of study.
- Expose students to work methods and techniques in handling equipment and machinery that may not be available in their institutions.
- Make the transition from school to the world of work easier and enhance students` contacts for later job placement.
- Provide students with the opportunity to apply knowledge in real work situation thereby bridging the gap between theory and practical.
- Enlist and strengthens employers` involvement in the entire educational process and prepare students for employment after graduation.

CHAPTER TWO

2.0DESCRIPTION OF TIZETI NETWORK LIMITED

Tizeti is a fixed wireless broadband internet service provider (ISP or WISP) operated by Tizeti Inc, using wireless to provide unlimited internet to residential and small business customers in Africa. Tizeti is leveraging the large wireless capacity available with Wi-fi and plummeting cost of solar panels to create a low CAPEX/OPEX network owned & operated towers to offer disruptive, customer-friendly pricing for unlimited internet service right across Africa. Tizeti Vision is to provide fast internet service with 99% customer satisfaction, their mission is to become top leading VoIP, video and data service provider in Africa

.

2.1LOCATION AND BRIEF HISTORY OF TIZETI NETWORK LIMITED

Tizeti Network Limited has coverage over 15 states in Nigeria, these are Lagos, Ogun, Rivers, Edo, OYO, Delta, Enugu, Abia, Imo, Kaduna, Kano, Abuja, Anambra, Cross river and Akwa ibom.

Tizeti headquarters is located at Cherub mall, Lekki peninsula II, Lekki 106104, Lagos.

Tizeti, Inc. was publicly announced in TechCrunch in March 2017 by Kendall Ananyi in a TechCrunch interview a week ahead of YC Winter 2017 Demo Day. As of March 2021, it was providing commercial service to customers in Nigeria and Ghana for $30/month. Tizeti is based in Redwood City, has about 300 employees in West Africa, and had raised $5.1 million of funding.

Tizeti operates on the 5.4GHz Wi-Fi and 3.5GHz 4G LTE bands,[2] connecting its Solar Powered Towers to customer premise equipment on customer buildings. Wireless internet propagation is near line-of-sight, not penetrating buildings and windows. The customers connect to the service via wi-fi routers inside their building.

Tizeti operates a number of Services:

- Wifi.com.ng: Unlimited Wi-Fi internet subscription service that provides unlimited internet starting $30 a month to residential and small businesses in Nigeria.
- GhanaWifi.com: Unlimited Wi-Fi internet subscription service that provides plans starting $30 a month to residential and small businesses in Ghana.
- Tizeti Enterprise Solution: Dedicated internet plans that provide high-capacity dedicated internet starting from 10Mbit/s to enterprise customers.
- Express Wi-Fi: Co-branded hotspot partnership with Facebook sold by retailers and targets dense, high traffic locations.
- Wificall.ng: Voice over IP service that provides unlimited calling, cloud PBX features and a voice api for developers.

2.2OBJECTIVES OF TIZETI

Tizeti Objective is to be Africa's top provider of voice, video, and data services.

Tizeti goals include;

- Expanding services: Tizeti aims to expand its services to other locations in Nigeria and some African countries
- Improving Collaboration: Tizeti aims to improve collaboration within growing teams
- Widening digital inclusion: Tizeti wants to widen digital inclusion in Africa with affordable broadband connectivity, particularly to the continent’s underserved populations
- Cost efficiency: Tizeti aims to continue providing affordable internet service to its customers
- Energy efficiency: Tizeti uses solar power in each of its stations as a energy efficient alternative to the use of diesel powered generators
- Unlimited internet plans: Tizeti’ s unlimited internet plans have no data caps, buffering or download limits

2.3TIZETI STRUCTURE AND ORGANOGRAM

Tizeti has hundreds of base stations across Nigeria, 12 across Ogun state and employs hundreds of staffs and interns.

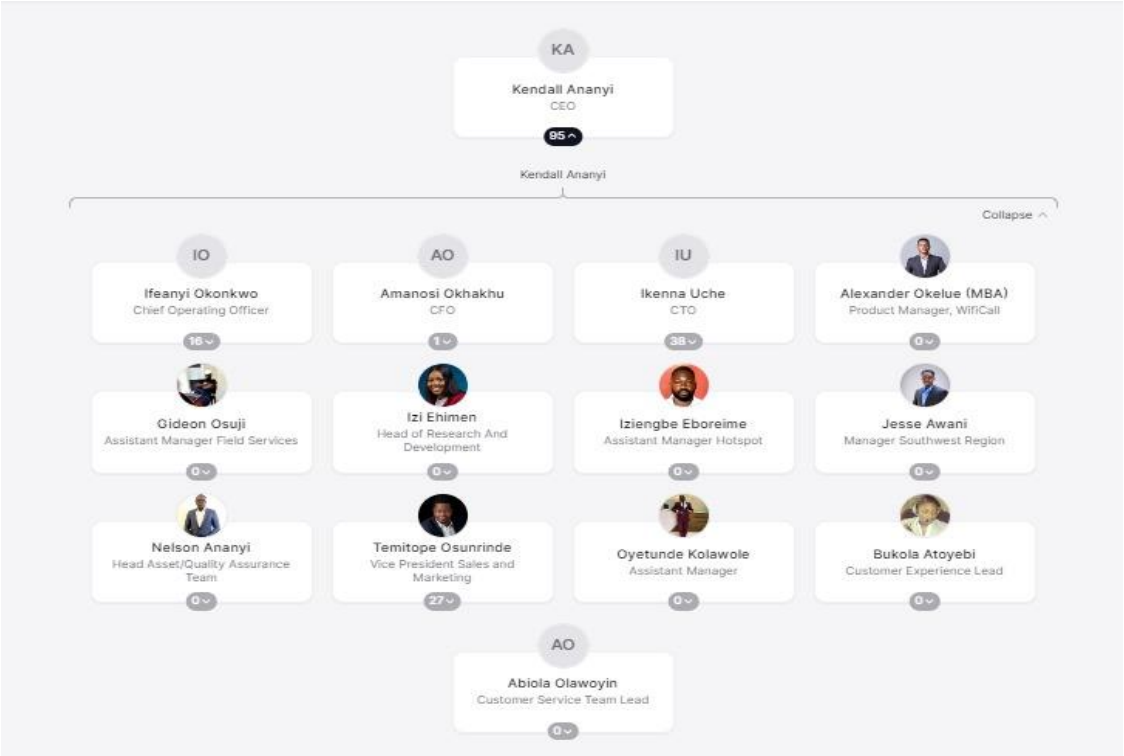


Fig 2.1: Tizeti Organogram

2.4THE VARIOUS DEPARTMENT IN TIZETI NETWORK LIMITED AND THEIR FUNCTION

Currently Tizeti runs on 4 operational departments;

1. SALES DEPARTMENT

The functions and objective of the sales department are;

1. Preparing Sales Plans
2. Prospecting
3. Researching and making sales
4. Managing sales Issues
5. Building customer relationship
6. Training and onboarding

2. FIELD SERVICE ENGINEERS (FSE)

FSE play a crucial role in ensuring smooth operation, maintenance and troubleshooting of equipment and infrastructure deployed in their field. Their primary roles are;

1. Installation and Commissioning of devices at Customers homes and offices
2. Providing Swift physical response to maintenance and repairs
3. Troubleshooting with customers
4. Adherence and compliance to safety standards

3. **NETWORK OPERATION CENTER (NOC)**

NOC serves as the central command and control center responsible for monitoring, managing, and maintaining the network infrastructure. Their primary role include;

1. Network monitoring: Constantly monitoring the network infrastructure, including servers, routers, switches and other network devices, to ensure optimal performance and availability. NOC use specialized monitoring tools like the tycoon monitor to detect and analyze network issues or anomalies
2. Incident Management: Promptly responding to network incidents, such as outages, disruption, or performance degradation, and initiating troubleshooting procedures to resolve issues efficiently.
3. Fault Identification and Resolution: Identifying the root causes of network faults or failures and implementing corrective actions to restore services. This may involve analyzing logs, performing diagnostics, and working closely with technical teams to resolve complex issues.
4. Performance Optimization: Analyzing network performance metrics, identifying potential bottlenecks or areas for improvement, and implementing changes to optimize network performance and reliability.
5. Maintenance and Upgrades: Planning and executing routine maintenance activities, as well as coordinating network upgrades or expansions to enhance network capacity, security, or efficiency.
6. Documentation and Reporting: Maintaining detailed records of network events, incident reports, and actions taken to resolve issues. Generating regular reports on network performance, uptime, and reliability for analysis and improvement purposes.
7. Security Monitoring: Monitoring for security threats and vulnerabilities within the network, implementing security protocols, and collaborating with cybersecurity teams to protect the network against potential attacks.

8. 24/7 Operations: Operating on a 24/7 basis to ensure continuous monitoring and support for the network, including round-the-clock availability for incident response and resolution.

Overall, the NOC plays a critical role in ensuring the smooth operation, stability, and security of a telecom network by proactively monitoring, managing, and maintaining the infrastructure to meet service level agreements and customer expectations.

CHAPTER THREE

3.0 ACTIVITES CARRIED OUT DURING THE PROGRAMME

Below are some of the activities carried out during the program

3.1 NETWORKING SAFETY PRECAUTIONS

Network safety precautions are essential measures taken to protect the integrity, confidentiality, and availability of data within a network. Here are some fundamental network safety precautions:

- Conduct routine security audits
- Implement network monitoring
- Enforce security policies
- Ensure the usage of strong encryption algorithm and protocols
- Regularly Update firmware and software
- Avoid firmware mismatch between devices
- Ensure uninterrupted power supply during configuration of radios
- Avoid unauthorized access to critical network facilities
- Avoid crimping of cable when plugged to the POE
- Avoid using unsecured network, so as to avoid leakage of confidential passwords and access to database
- When connecting Solar panels, charge controller and batteries together, Connect the batteries to the charge controller first before connecting the solar panels.

SAFETY PRECAUTIONS AT THE BASE STATIONS

- Always have on your climbing gears, when climbing masts
- Double check your harness
- Do not climb if you are not a certified rigger or employed as a rigger
- Riggers must have their PPEs and Safety Harness provided before them
- Always remember, safety first.

3.2 NETWORKING EQUIPMENT AND THEIR USES

Networking equipment refers to various devices and hardware components used to facilitate communication and data exchange within computer networks. These devices play different roles in managing, transmitting, and securing data across networks. Some common networking equipment includes:

A. **ROUTERS:** Routers are devices that connect multiple networks together and determine the best path for data packets to travel between them. They use routing tables and protocols to direct traffic efficiently.

Fig 3.1: Cloud core Router

Routers are of different types;

- **. Home Routers:**

- Designed for residential settings and small offices.
- Provides basic functionalities to connect multiple devices to the internet through a single internet connection.
- Often equipped with built-in wireless access points for Wi-Fi connectivity to devices within the home network.
- Easy-to-use web-based interfaces for configuration and management.

FIG 3.2: Home Router

2. Wireless Routers:

- Also known as Wi-Fi routers.
- Equipped with built-in wireless access points to enable devices to connect wirelessly to the network.
- Widely used in both home and small business environments.
- Provides wireless connectivity and supports multiple devices simultaneously.

Fig 3.3: Wireless Router

3. Wired Routers:

- Provides network connectivity through physical wired connections.
- Equipped with Ethernet ports to connect devices via network cables.
- Often used in environments where a stable and high-speed connection is required, such as in offices, data centers, and enterprise networks.

Fig 3.4: Wired Router

4. Core Routers:

- High-end routers used in large-scale networks like internet service providers (ISPs) and major data centers.
- Responsible for forwarding data at the core of the network, connecting multiple high-speed data links.
- Designed for high throughput, low latency, and reliability to handle the massive traffic in backbone networks.

Fig 3.5: Cloud core Router

5. Edge Routers:

- Also known as boundary routers.
- Used at the edge of a network where the network connects to external networks, such as the internet or another organization's network.
- Responsible for routing data between the local network and external networks, implementing security measures, and managing traffic entering or leaving the network.

Fig 3.6: Edge Router

6. Distribution Routers:

- Found in large enterprise networks.
- Connects multiple local networks or segments.
- Responsible for routing traffic between different LANs, ensuring efficient data flow between different parts of the network.
- Performs tasks like VLAN segmentation and quality of service (QoS) management.

Fig 3.7: Distribution Router

7. Access Routers:

- Used in environments like office buildings and campuses.
- Provides connectivity to end-user devices within a local area network.
- Serves as a gateway between the end-user devices and the core or distribution routers in the network.

Fig 3.7: Access Router

8. Virtual Routers:

- Software-based routers that run on virtual machines or cloud platforms.
- Offers the same functionalities as physical routers but are more flexible and scalable.
- Commonly used in virtualized environments, data centers, and cloud computing infrastructure.

Fig 3.8: Virtual Router

9. Modular Routers:

- Allows for the expansion of router capabilities through modular components or line cards.
- Interchangeable interface cards for customization based on specific networking needs.
- Often used in enterprise and data center environments.

Fig 3.9: Modular Router

10. SOHO Routers:

- Designed for small business environments and home offices.
- Offers a balance between features, price, and performance suitable for smaller networks.

Fig 3.9: Mikrotik SOHO Router

The different types of routers cater to various applications and network sizes. The selection of the right router type depends on specific networking requirements and the scale of the network being deployed**.**

B. SWITCHES: A switch is a crucial hardware device that facilitates the interconnection of various devices within a local area network (LAN). Its primary function involves managing and directing the flow of data between devices efficiently.

The vital function of a switch is;

Connectivity: A switch serves as a central point to which multiple devices such as computers, printers, servers, and other networked devices can be connected. It typically features multiple ports (Ethernet ports) to accommodate these connections.

Data Transmission: When data is transmitted between devices connected to a switch, it uses a technique called packet switching. This means that data is broken down into smaller units called packets, and the switch forwards these packets to their intended destinations based on their MAC (Media Access Control) addresses.

MAC Address Learning: Switches maintain a table known as a MAC address table. As data passes through the switch, it learns the MAC addresses of connected devices and their corresponding port locations. This information helps the switch efficiently route data to the correct destination.

Efficient Traffic Handling: Unlike older networking devices like hubs that broadcast data to all connected devices, switches are more intelligent. They forward data selectively, sending it only to the specific device (or devices) for which it is intended. This reduces unnecessary traffic and improves overall network performance.

Collision Domains: Switches create individual collision domains for each port, minimizing collisions (data packet conflicts) on the network. This means that devices connected to different ports can send and receive data simultaneously without causing interference or collisions.

Broadcast Control: Switches control the transmission of broadcast messages within a network. Instead of broadcasting to all devices, a switch will only send a broadcast message to the specific ports where the intended recipient devices are located.

Switches play a vital role in local network setups, enabling efficient communication and data transfer between devices while managing network traffic intelligently. They are a fundamental component in modern networking

infrastructure, available in various sizes and configurations to meet the diverse needs of different network environments.

C. **RADIOS**: In the context of telecommunications and networking, radios refer to devices or components that are used to transmit and receive radio frequency (RF) signals. These signals are utilized for various wireless communication purposes, including but not limited to:

Radio Transceivers: A radio transceiver is a device capable of both transmitting and receiving radio signals. It is a fundamental component in many communication systems, including mobile phones, two-way radios (walkie-talkies), and wireless networking devices like Wi-Fi routers.

Wireless Communication Devices: Radios are integral to various wireless communication devices, such as smartphones, tablets, laptops, and IoT (Internet of Things) devices. They enable wireless connectivity using technologies like Bluetooth, Wi-Fi, cellular networks (2G, 3G, 4G, 5G), and satellite communication.

Broadcasting Equipment: Radios are utilized in broadcasting equipment for AM (Amplitude Modulation), FM (Frequency Modulation), and digital radio transmission. They enable the transmission of audio signals over the airwaves to reach radio receivers for public or private consumption.

Wireless Networking: Radios are essential components in wireless networking equipment, including access points, routers, and wireless adapters. They facilitate the transmission and reception of data signals wirelessly within local area networks (LANs) or extended wireless networks.

Radar Systems: Radar (Radio Detection and Ranging) systems use radio waves to detect and track objects, such as aircraft, ships, weather formations, and more. Radios are vital components in these systems for transmitting and receiving radar signals.

Satellite Communication: Radios play a crucial role in satellite communication systems, where they are used to communicate with satellites orbiting the Earth for purposes such as weather monitoring, global positioning systems (GPS), television broadcasting, and long-distance communication.

Radios operate within specific frequency bands allocated by regulatory authorities, and they employ modulation techniques to carry information on these radio waves. They are essential for enabling wireless communication across various applications, providing connectivity and enabling the transfer of data and information over the air without the need for physical connections.

TIZETI as an ISP, uses mainly two manufacturing type of radios; Cambium and Ubiquity devices

- **UBIQUITY DEVICES:** Ubiquity as an industry design and develop innovative wireless products for both indoor and outdoor environment. Ubiquity, Tizeti uses ubiquity radios for PTP links. Some of these radios are;
    - **Air fiber (AF-60);** with specifications,

Fig. 3.10: Ubiquity AF-60

DIMENSION -> 16.3 x 14.2 inches

ENCLOSURE MATERIAL -> Aluminum, UV stabilized polycarbonate

PROCESSOR -> Quad-core ARM ® Cortex ® A7

NETWORK INTERFACE -> 1GbE port

MAXIMUM POWER CONCUMPTION -> 22W

POWER SUPPLY -> 48V DC, 0.65A Gb POE

SUPPORTED VOLTAGE RANGE -> 44-54 V DC

GPS -> YES

OPERATING MODE -> PTP mode only

NETWORK -> Bridge Mode

SERVICES -> UISP, ping watchdog, NTP client

TOOLS -> Antenna Alignment, discovery utility, ping, trace route, speed test.

MAXIMUM THROUHPUT -> 1.95 Gbps

MAXIMUM SHOOTING RANGE -> 12Km

OPERATING FREQUENCY -> 57- 71 GHz (depends on region)

CHANNEL BANDWIDTH -> 2160, 1080 MHz

BEAM WIDTH -> Azimuth 3db 1.6^0, Elevation 3db 1.6^0

- **Wave Nano:**

FIG. 3.11: UBIQUITY WAVE NANO

The ubiquity wave-nano has varieties of specifications over the AF-60 such as

PROCESSOR -> Dual ARM ® CORTEX ®-A53 cores at 1GHz

It Operates on 5- 95 % non-condensing humidity

It operates on PTP and PTMP (AP) mode

It has Wave AI which automatically pick the suitable frequency for the precise location #

It has a total throughput capacity of 2Gbps (1 Gbps duplex)

It cannot shoot longer than 5Km

Beamwidth of Azimuth 3db 1.4^0, Elevation 3db 1.4^0

Operates on dual link frequency (60 Ghz with antenna gain 41dBi, 5GHz (Back up) with antenna gain 19dBi

Tizeti use Wave nano devices for short ranged PTP connections. AF-60 on the other hand is mostly use to shoot from a Fiber-Base Station to a sub-Station. The only disadvantage is its total Throughput can't exceed 1Gbps.

- **Air Fiber (AF 5U):** Air fiber 5U is a bigger radio with added specifications, one of its versatile advantages is its shooting range of up to 50Km. It has a high transmitting power and emit very intense electromagnetic radiation. The EM radiation emitted might be dangerous to man and might result in nausea, fatigue and loss of libido. It has a total throughput capacity of 1.2+ Gbps.

  It is recommended most for long ranged PTP between base stations, Its way Costlier (around 1.5 million naira) than the Af-60(around 750,000 naira) and Wave nano (around 600, 000 naira).

FIG 3.12: UBIQUITY AF 5U

FIG 3.13: UBIQUITY AF 5U on mast

- **CAMBIUM DEVICES:** The difference in PTP connections using cambium devices and ubiquity devices is that unlike ubiquity, only one device is required during a turbo connection.

  Some of the Cambium devices used are as follows;

1. **ePMP 3000 Access Point.**

FIG 3.14: ePMP 3000 AP

The ePMP 3000™ is the third-generation access point (AP) that carries on the interference tolerance mechanisms from ePMP 2000 but adds the power of Multi-User MIMO (MU-MIMO).

The ePMP 3000 is a 4X4 MU-MIMO access point that can double the throughput at the sector level with the same channel bandwidth by serving two subscribers at the same time.

Key Advantage:

- Frequency Reuse: Supports GPS synchronization and SM Transmit power control to allow for frequency re-use.
- Unmatched Performance and Scalability: With the efficient Cambium Networks MAC protocol and advanced air-fairness scheduler up to 120 simultaneously active subscriber modules can be served without performance degradation.
- Industry-Leading Interference Tolerance: The intelligent filtering capability on the receive side makes ePMP 3000 immune to the effects of strong off-channel interferers and on the transmit side serves to reduce off-channel noise for better radio co-location.
- Industry-Leading Spectral Efficiency: MU-MIMO in the downlink doubles the sector capacity by serving two MIMO users at the same time.

Key Specifications:

- MU-MIMO support with peak throughput of 1.2 Gbps
- 256QAM-5/6, 80 MHz support
- Supports a wide frequency range: 4910 – 5970 MHz
- 802.3at compliant 100/1000BaseT interface
- Frequency re-use with GPS sync, interference mitigation with beam steering antenna and dynamic filtering.

ePMP 3000 are used as access points on masts where customers using Force 180 connects to

2. **ePMP 2000 ACCESS POINT**

Fig 3.16: ePMP 2000 smart antenna

Fig 3.15: ePMP 2000 AP

The ePMP 2000 System consists of high-performance, GPS-Synchronized Access Point (AP) Radio with Intelligent Filtering, a new compact high-performance Sector Antenna, and an optional Smart Antenna.

Intelligent Filtering improves both receive and transmit performance. It protects the network from off-channel interferers with a filter that dynamically moves around the channel. On the transmit side, it protects the RF environment by reducing off-channel transmission noise.

Smart Beamforming drastically reduces the effects of on-channel interference. The System learns the locations of each served Subscriber Module (SM) and forms a narrow beam toward the desired SM while that radio is transmitting in the uplink. This reduces the gain on the uplink for on-channel interferers that are transmitting at an azimuth angle different than the SM, delivering performance gains never before seen.

Key Advantage:

Industry-Leading Interference Tolerance: Intelligent Filtering hardens ePMP 2000 to strong off-channel interferers and reduces off-channel noise for better radio co-location. Smart Beamforming with the optional Smart Antenna delivers dramatic performance improvements when dealing with strong co-channel interference.

Frequency Reuse: GPS Synchronization and Transmit Power Control allow for industry-leading frequency reuse.

Unmatched Performance and Scalability: With the efficient ePMP MAC protocol and advanced air-fairness scheduler, up to 120 simultaneously active Subscriber Modules can be served without performance degradation.

Key Specifications:

Supports up to 120 Subscriber Modules

Supports a wide frequency range: 5150 - 5970 MHz

802.3at compliant 100/1000BaseT Interface

3. **FORCE 300-25**

FIG 3.17: Force 300-25

The Force 300-25 offers a compelling yet affordable point to point product and a future high gain subscriber module for the ePMP3000 Access Point.

Force 300-25 continues the tradition of previous products with an integrated 25dBi dish with a narrow beamwidth and reliable mechanics. Supporting peak throughput greater than 500Mbps, the Force300-25 also supports an always on spectrum analyzer and local Wi-Fi management to take advantage of mobile installation applications.

Features:

Cambium Networks' ePMP Force 300-25 is designed to operate in high interference environments and provides superior throughput of over 500 Mbps of real user data.

The ePMP Force 300-25 supports channel size configuration from 20MHz up to 80MHz and modulates up to 256 QAM.

The Force 300-25 supports a local Wi-Fi connection to allow easy installation, configuration, and monitoring from any Wi-Fi enabled device.

The ePMP Force 300-25 supports constant monitoring of the radio spectrum and allows for live action without bringing down the radio.

Configurable modes of operation ensure robust adaptivity to both symmetrical and asymmetrical traffic while providing high performance and round-trip latency as low as 3-5 ms.

QoS management offers an outstanding quality for triple play services – VoIP, video, and data – and provides three levels of traffic priority.

It is the only cambium device used during PTP turbo/dedicated connections

4. **FORCE 180**

FIG 3.18: Force 180 station

This radio comes in a small, sleek form factor but delivers high performance. The antenna gain is increased by 3 dB to 16 dBi which will provide a 40% increase in range. It comes equipped with a Gigabit Ethernet port so that nothing will limit this product in delivering the maximum throughput. The radio module is powered by PoE and the Ethernet port has the unique capability of being powered from a PoE injector that conforms to standard pinouts or from a PoE injector that conforms

to Cambium pinouts. This makes it possible to upgrade existing radio locations to the Force 180 without changing the PoE injector. It also includes an adjustable mounting bracket that eases the task of installing and properly aligning the radio.

Force 180 is used by FSE team for up to 10Mbps package tolled customers.

D. POWER OVER ETHERNET (POE)

The Power over ethernet **(POE)** is responsible for powering up a radio and also receive/transmit data from/to the radio. The POE is of two ports as illustrated, LAN PORT and POE PORT

The POE port is connected to the radio to power it and at the same time send/receive data to/from the radio.

A radio can be (I) Transmitting radio (A.P) (ii) Receiving radio (Station)

The LAN port on the other hand, transmit data from the router to the POE device.

Radios are of different P.D rating with their respectively rated POE. Examples are ;30W-56V,15W-24V, etc.

Using the wrong POE would surely damage the radio.

E. SURGE

Since radios and routers are E-M transmitting devices; they are open to damage due to thunderstorm and lightening. In other to prevent this, a Surge is connected to the radio. i.e., the POE port will be connected to SURGE then to the router.

F. CABLES

An Ethernet cable is a common type of network cable used with wired networks. Ethernet cables connect devices such as PCs, routers, and switches within a local area network.

These physical cables are limited by length and durability. If a network cable is too long or of poor quality, it won't carry a good network signal. These limits are one reason there are different types of Ethernet cables that are optimized to perform certain tasks in specific situation.

Ethernet cables are of two categories (CAT 5 and CAT 6). CAT 5 cables are 100Mbps transmitting speed cables while CAT 6 cables are 1Gbps transmitting speed cables.

The Ethernet cable are of 8 strands; white of orange, Orange, White of green, Blue, White of Blue, Green, White of brown, Brown. And should be connected in that order

White of Orange, Orange, White of green, green is used for power

White of blue, blue, White of brown, brown. Are used for transmitting and receiving data

The Ethernet Cable are connected to the Lan Connector by using a crimping tool.

G. OPTICAL DISTRIBUTION FIBER (ODF) ALSO KNOWN AS PATCH PANEL

An optical distribution frame (ODF) is a frame used to provide cable interconnections between communication facilities, which can integrate fiber splicing, fiber termination, fiber optic adapters & connectors and cable connections together in a single unit. It can also work as a protective device to protect fiber optic connections from damage.

According to the structure, ODFs can mainly be divided into three types, namely wall mount ODF, floor mount ODF and rack mount ODF.

H. SOLAR PANELS

A solar panel is a device that converts sunlight into electricity by using photovoltaic (PV) cells. PV cells are made of materials that produce excited electrons when exposed to light. The electrons flow through a circuit and produce direct current (DC) electricity, which can be used to power various devices or be stored in batteries. Solar panels are also known as solar cell panels, solar electric panels, or PV modules.

Solar panels are usually arranged in groups called arrays or systems. A photovoltaic system consists of one or more solar panels, an inverter that converts DC electricity to alternating current (AC) electricity, and sometimes other components such as controllers, meters, and trackers. A photovoltaic system can be used to provide electricity for off-grid applications, such as remote homes or cabins, or to feed electricity into the grid and earn credits or payments from the utility company. This is called a GRID CONNECTED PHOTOVOTAIC SYSTEM

Some advantages of solar panels are that they use a renewable and clean source of energy, reduce greenhouse gas emission, and lower electricity bills. Some disadvantages are that they depend on the availability and intensity of sunlight, require cleaning, and have high initial costs. Solar panels are widely used for residential, commercial, and industrial purposes, as well as for space and transportation applications.

I. SOLAR INVERTER

A solar inverter or photovoltaic inverter converts a variable DC output of a photovoltaic solar panels into a utility frequency AC that can be fed into a commercial electrical grid or local devices in the rack, devices such as routers, switches, etc.

Devices can be AC powered or DC powered. Solar inverters can (1) Converts AC to DC (2) Converts DC to AC

J. CHARGE CONTROLLER

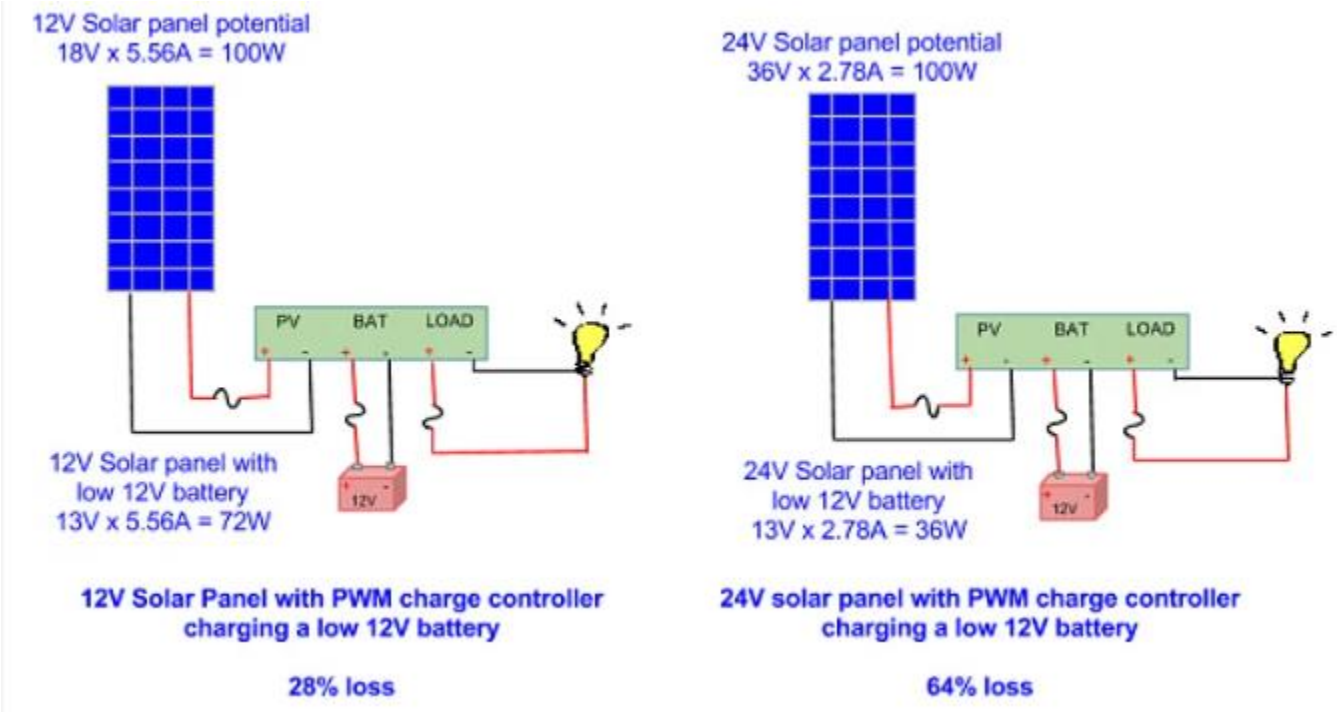
A solar Charge controller manages the power going into the battery bank from the solar array. It ensures that the deep cycle batteries are not overcharged during the day, and that the power doesn't run backwards to the solar panels overnight and drain the batteries. Some charge controllers are available with additional capabilities, like lighting and load control, but managing the power is its primary job.

A solar charge controller is available in two different technologies, PWM and MPPT. How they perform in a system is very different from each other. An MPPT charge controller is more expensive than a PWM charge controller, and it is often worth it to pay the extra money.

PWM SOLAR CHARGE CONTROLLER

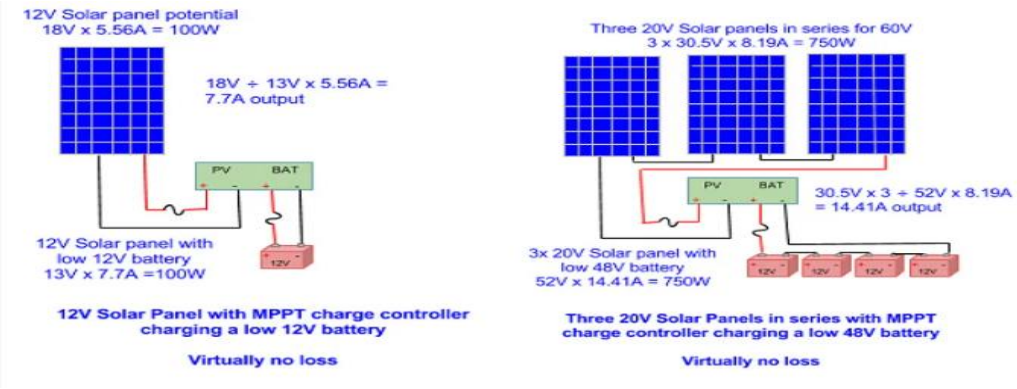
A PWM stands for “Pulse Width Modulation”. These operate by making a connection directly from the solar array to the battery bank. During bulk charging, when there is a continuous connection from the array to the battery bank, the array output voltage is ‘pulled down’ to the battery voltage. As the battery charges, the voltage of the battery rises, so the voltage output of the solar panel rises as well, using more of the solar power as it charges. As a result, you need to make sure you match the nominal voltage of the solar array with the voltage of the battery bank. *Note that when we refer to a 12V solar panel, that means a panel that is designed to work with a 12V battery. The actual voltage of a 12V solar panel, when connected to a load, is close to 18 Vmp (Volts at maximum power). This is because a higher voltage source is required to charge a battery. If the battery and solar panel both started at the same voltage, the battery would not charge.

A 12V solar panel can charge a 12V battery. A 24V solar panel or solar array (two 12V panels wired in series) is needed for a 24V battery bank, and 48V array is needed for 48V bank. If you try to charge a 12V battery with a 24V solar panel, you will be throwing over half of the panel’s power away. If you try to charge a 24V battery bank with a 12V solar panel, you will be throwing away 100% of the panel’s potential, and may actually drain the battery as well.



MPPT SOLAR CHARGE CONTROLLER

An MPPT solar charge controller stands for “Maximum Power Point Tracking”. It will measure the Vmp voltage of the panel, and down-converts the PV voltage to the battery voltage. Because power into the charge controller equals power out of the charge controller, when the voltage is dropped to match the battery bank, the current is raised, so you are using more of the available power from the panel. You can use a higher voltage solar array than battery, like the 60-cell nominal 20V grid-tie solar panels that are more readily available. With a 20V solar panel, you can charge a 12V battery bank, or two in series can charge up to a 24V battery bank, and three in series can charge up to a 48V battery bank. This opens up a whole wide range of solar panels that now can be used for your off-grid solar system.



K. SOLAR BATTERIES

Solar battery stores electrical energy converted from solar energy by the solar panels. Solar batteries hold the key I unlocking the full potential of renewable energy. As sunlight is converted into electrical energy, any extra energy generated during sunny periods can be stored within the batteries for future use

This also ensures a continuous power supply to the devices on the base stations (Data transmitting)

Chemical reactions took place in the batteries to store electricity as potential energy, this stored potential energy is then used during night times overcast days

The stored potential energy is stored as DC in the battery, the stored Dc is then converted to AC for use

SOLAR BATTERY TYPES

1. **Lead -Acid Battery:** Lead Acid batteries are very common battery type used. They have a low energy density (They cannot hold more energy) but are cost -effective and reliable. They can be (i) Flooded (ii) Sealed, Varieties and also classified on the intended function and safe depth of discharge (DOD).
2. **Lithium-ion Battery:** Lithium-ion batteries is much newer than that of other battery types. They have high energy density (i.e., can store much more energy), and they offer a smaller, lighter and more efficient option. They allow the user to access more of the energy stored within the battery before needing to be recharged, making them great for use in laptops and phones. They are way costlier and have high potential of flaming due to thermal runaway when impacted upon contact with a rigid body in accordance to the Newtonian third law of body.

   Lead Acid Batteries are used in powering and storing electricity across base stations.

L. TYCOON MONITORS

The TPDIN-Monitor-WEB2 Based Remote Monitor and Control System is a versatile tool which enables the equipment designer and installer to remotely monitor their equipment and site. The unit can be accessed via the network (web and SNMP) to remotely monitor up to 4 voltages, 4 currents, 2 temperatures and control power to various equipment using 4 on-board relays. The system has built-in surge protection to prevent damage from electrical surges.

On board data-logging and graphing capabilities allow the user to see history of the various parameters

being measured. The graphical interface allows the user to control relays via a single mouse click and monitor all the measurement parameters real-time via any web browser. The web interface allows access and control via desktops, laptops, tablets and smartphones. The Tycoon APP for IOS and Android facilitates remote access.

The system allows control of the relays based on Voltage, Current, Temperature, Time or Ping Watchdog. This provides almost unlimited flexibility.

CHAPTER FOUR

4.0 NETWORKING

4.1 Basic Concepts of Computer Networks

The merging of computers and communications has had a profound influence on the way computer systems are organized. The concept of the "computer center" as a room with a large computer to which users bring their work for processing is now totally obsolete. The old model of a single computer serving all of the organization's computational needs has been replaced by one in which a large number of separate but interconnected computers do the job. These systems are called computer networks.

Computer network means a collection of autonomous computers interconnected by a single technology. Two computers are said to be interconnected if they are able to exchange information. The connection need not be via a copper wire; fiber optics, microwaves, infrared, and communication satellites can also be used. Networks come in many sizes, shapes and forms, as we will see later. Although it may sound strange to some people, neither the

Internet nor the World Wide Web is a computer network. The Internet is not a single network but a network of networks and the Web is a distributed system that runs on top of the Internet.

4.2 Advantages of Networked Computing Relative to Stand alone Computing

The main advantages of using a network over stand-alone computers

- share software
- share information with others on networks
- share peripherals
- speed of sharing software and information files
- cheaper than buying individual software and hardware for each standalone especially if for a school, network software often offers deals for amount being purchased
- security, files can be copy inhibit mode
- centralized software management- software being loaded onto one computer but also this loads software to entire network at one time
- electronic mail(e-mail) between network users, ideal for office memos
- flexible access- access you file from any computer on the network unlike standalone which would mean only being able to access your data from the one computer you uploaded data onto

4.3 Fundamental Types of Networks

a. Peer-to-peer networks

The simplest form of a network is a **peer-to-peer network**. In a peer-to-peer network, every computer can communicate directly with every other computer. By default, no computer on a peer-to-peer network has more authority than another. However, each computer can be con- figured to share only some of its resources and keep

other resources inaccessible to the net- work. Traditional peer-to-peer networks typically consist of two or more general-purpose personal computers, with modest processing capabilities. Every computer is capable of sending and receiving information to and from every other computer, as shown in Figure 1.1. There is no fixed division into clients and servers.

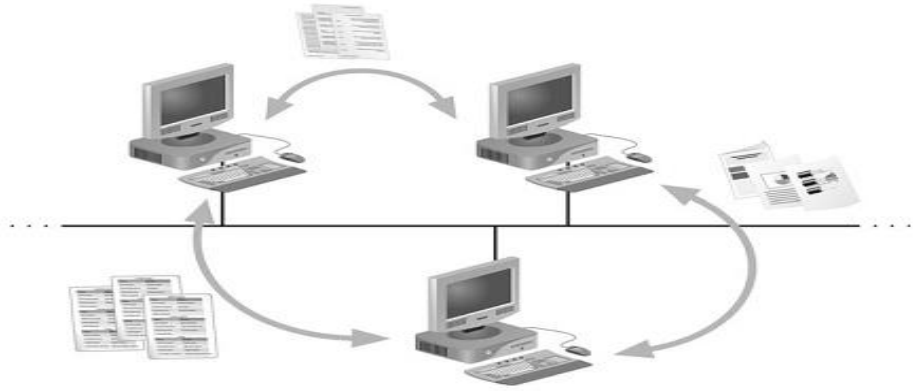


FIGURE 4.1: Resource sharing on a simple peer-to-peer network

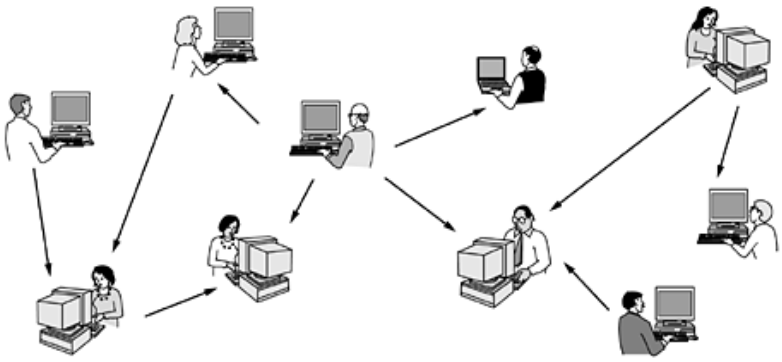


Figure 4.2: In a peer-to-peer system there are no fixed clients and servers

Examples of peer-to-peer communication are fans sharing public domain music or sample tracks that new bands have released for publicity purposes, families sharing photos, movies, and genealogical information, and teenagers playing multi person on-line games. In fact, one of the most popular Internet applications of all, e-mail, is inherently peer-to-peer. This form of communication is expected to grow considerably in the future.

b. Client/server networks

Another way of designing a network is to use a central computer, known as a **server**, to facilitate communication and resource sharing between other computers on the network, which are known as **clients**. Clients usually take the form of personal computers, also known as **workstations**. A network that uses a server to enable clients to share data, data storage space, and devices is known as a **client/server network**. It is widely used and forms the basis of much network usage. It is applicable when the client and server are both in the same building (e.g., belong to the same company), but also when they are far apart. For example, when a person at home accesses a page on the World Wide Web, the same model is employed, with the remote Web server being the server and the user's personal computer being the client. Under most conditions, one server can handle a large number of clients.

If we look at the client-server model in detail, we see that two processes are involved, one on the client machine and one on the server machine. Communication takes the form of the client process sending a message over the network to the server process. The client process then waits for a reply message. When the server process gets the request, it performs the requested work or looks up the requested data and sends back a reply. These messages are shown in **Fig. 4.2**.

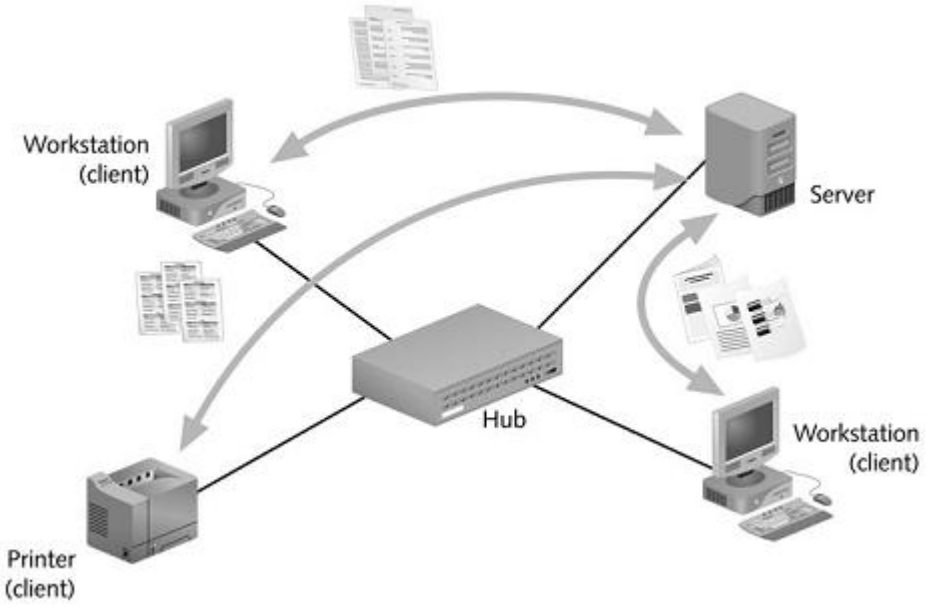


FIGURE 4.3 Resource Sharing On A Client/Server Network

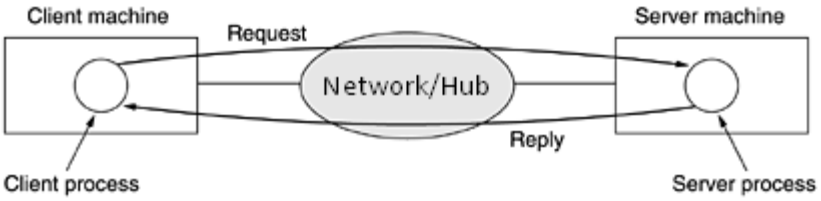


Figure 4.4: The client-server model involves requests and replies.

4.4 Various Classifications of Networks

a. Local Area Network (LAN)

A L**ocal Area Network (LAN)** is a network of computers and other devices that is confined to a relatively small space, such as one building or even one office. LANs are privately-owned networks within a single building or campus of up to a few kilometers in size. They are widely used to connect personal computers and workstations in company offices and factories to share resources (e.g., printers) and exchange information. Today's LANs are typically much larger and more complex client/server networks.

Often separate LANs are interconnected and rely on several servers running many different applications and managing resources other than data. This network may contain many servers, hundreds of workstations, and several shared CD-ROM devices, printers, plotters, and fax machines.

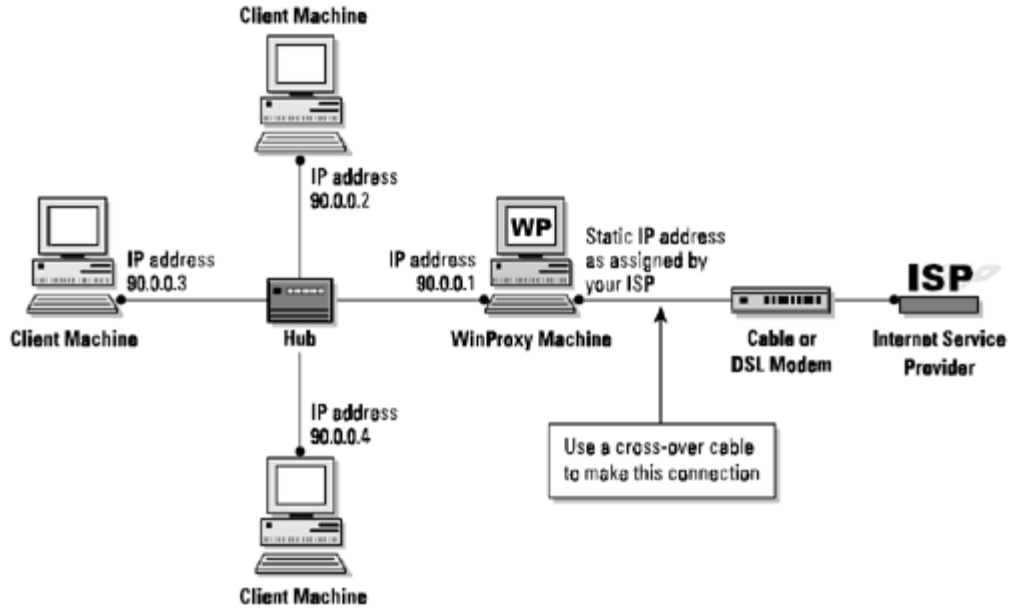


Figure 4.5 A Simple LAN

b. Metropolitan Area Network (MAN)

A Metropolitan Area Network, or MAN, covers a city. The network extends beyond building boundaries that is larger than a LAN and connects clients and servers from multiple buildings - for example, a handful of government offices surrounding a state capitol. Because of the distance it covers, a MAN may use different transmission technology and media than a LAN.

The best-known example of a MAN is the cable television network available in many cities. This system grew from earlier community antenna systems used in areas with poor over-the-air television reception. In these early systems, a large antenna was placed on top of a nearby hill and signal was then piped to the subscribers' houses.

At first, these were locally-designed, ad hoc systems. Then companies began jumping into the business, getting contracts from city governments to wire up an entire city. The next step was television programming and even entire channels designed for cable only. Often these channels were highly specialized, such as all news, all

sports, all cooking, all gardening, and so on. But from their inception until the late 1990s, they were intended for television reception only.

Starting when the Internet attracted a mass audience, the cable TV network operators began to realize that with some changes to the system, they could provide two-way Internet service in unused parts of the spectrum. At that point, the cable TV system began to morph from a way to distribute television to a metropolitan area network. To a first approximation, a MAN might look something like the system shown in Fig. 4.4. In this figure we see both television signals and Internet being fed into the centralized head end for subsequent distribution to people's homes.

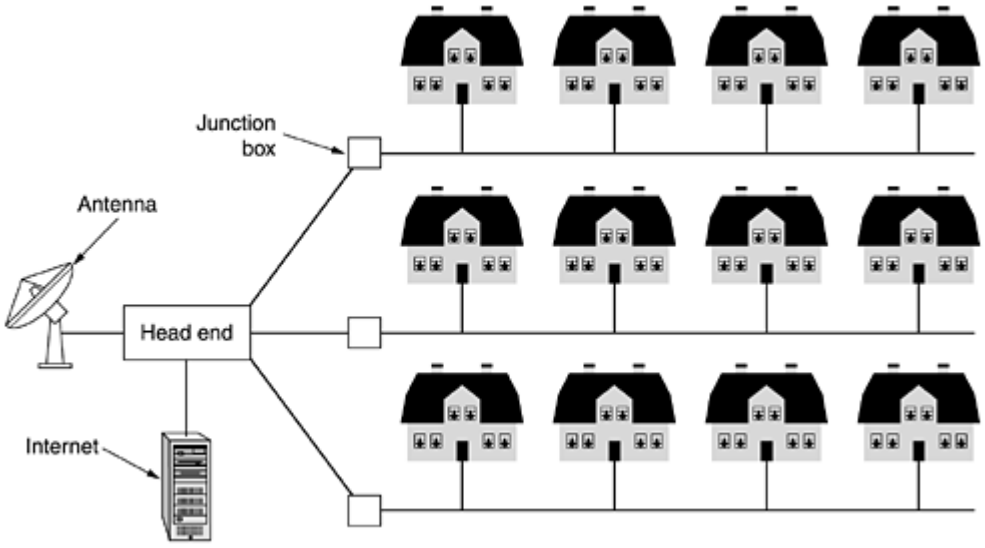


Figure 4.6: A metropolitan area network based on cable TV.

c. Wide Area Network (WAN)

A wide area network, or WAN, connects two or more geographically distinct LANs or MAN. It spans a large geographical area, often a country or continent. It contains a collection of machines intended for running user (i.e., application) programs. Because they carry data over longer distances than LANs, WANs require slightly different transmission methods and media and often use a greater variety of technologies than LANs. Most MANs can also be

described as WANs; in fact, network engineers are more likely to refer to all networks that cover a broad geographical range as WANs.

WANs commonly connect separate offices in the same organization, whether they are across town or across the world from each other

WANs are also used to connect LANs that belong to different organizations. For example, all the public universities within a state might combine and share their resources via a WAN. The largest and most varied WAN in the world is the **Internet**. Figure 4.5 depicts a simple WAN.

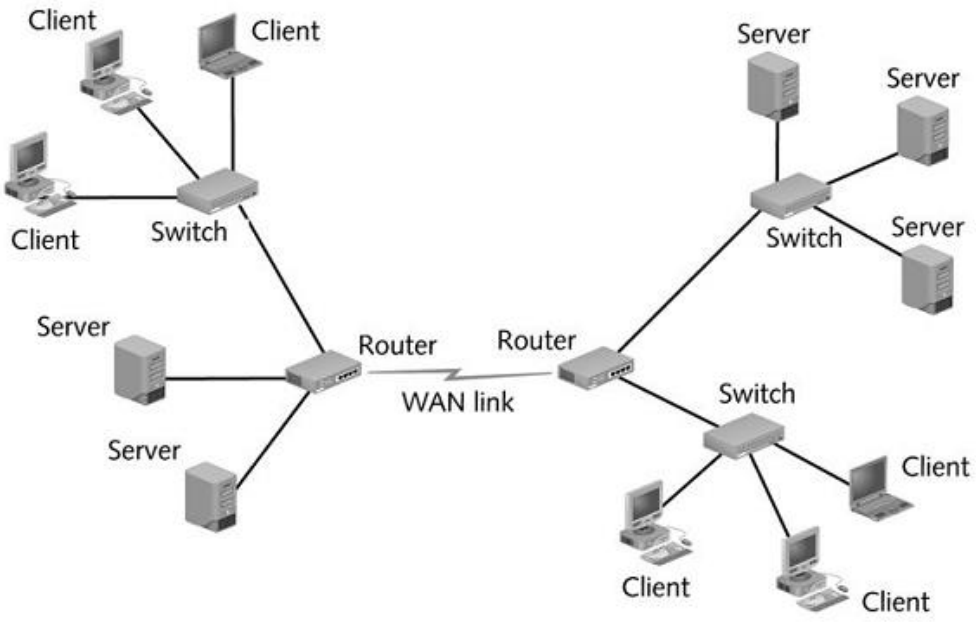


FIGURE 4.7 A simple WAN

4.5 Common element to all client/server networks

5 client

6 server

7 workstation

8 network interface card

9 network operating system

10 node

11 connectivity device

12 backbone

13 segment

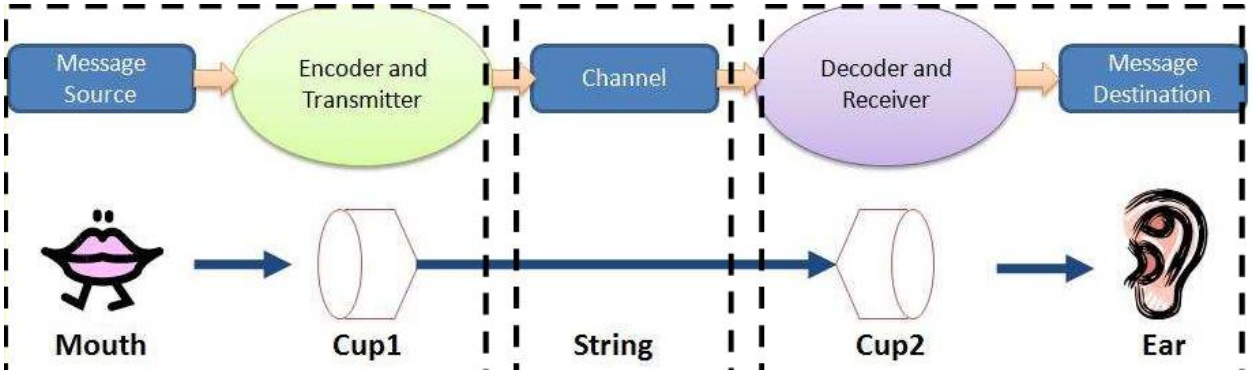
14 topology

15 transmission media.

4.6 PRINCIPLES OF TELECOMMUNICATIONS IN NETWORKING

4.6.1 Source, Channel And Destinations

Basic Elements of a Communication



Source Channel Destination

Basic Elements of a Communication System

•Source

–This device generates the data to be transmitted; examples are telephones and personal computers.

•Channel

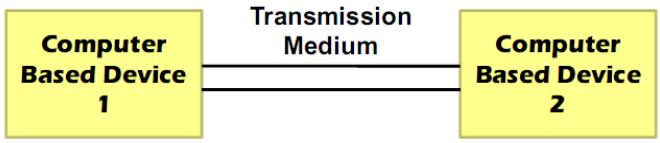
–A medium that carries the message.

•Destination

–The receiver (sink) who receives the message

4.6.2 Rules Of Communications

Rules of communications between two points



There are a number of phases that both devices must pass through in order to perform the common communications function of file transfer

These phases ensure that the software on each device is structured to correct for errors or inconsistencies from the corresponding, remote device.

The rules for each of these phases are clearly defined by a protocol and typical phases are as follows:

- Establish a link
- Issue a command and command qualifier
- Acknowledgment of command
- Dissection messages
- Error detection and correction
- Termination of transmission

Establish a link

- Device 1 checks to see if Device 2 is present on the link by sending a specific "enquiry" message.
- If the link is active and device 2 is active then it should respond by sending back an "acknowledgement" message.
- Device 1 must track the time that device 2 takes to respond.

- If device 2 does not respond within a time interval (defined by the protocol) then device 1 assumes that the link is not active.
- This is called a transmission "time-out" error

Issue a command and command qualifier

- Device 1 sends device 2 a message, in a predefined format, which tells device 2 that a file is to be transferred.
- As a qualifier within the message, device 1 tells device 2 what to do with the file. For example, device 1 may tell device 2 to place the incoming file onto disk storage, with the file-name "FRED".

Acknowledgment of command

- If device 2 has correctly received the command and qualifier from device 1, and is capable of carrying out the command, then it sends device 1 an acknowledgement message.
- The acknowledgement message tells device 1 that it can now proceed with further action needed to fulfil the command.
- If device 2 is unable to act upon the command from device 1, then it must respond with an error message.
- An error could occur on the receiver if, for example, the disk on which the incoming file is to be stored, is already full.
- The error response message would tell device 1 that it should not proceed with its proposed course of action.

Dissection messages

- All messages, command and otherwise, must be broken down into packets of manageable size for transmission.
- Thus, if an error should occur in a packet, then only that packet needs to be re-transmitted (and not the entire message).

- Therefore, when device 1 wishes to transfer a large file to device 2, the file is broken up into packets and transmitted packet by packet.

Error detection and correction

- When device 1 sends a message packet to device 2, it performs a mathematical calculation (manipulation) on every unit of data transmitted.
- This calculation is transmitted to device 2 immediately after the message.
- Device 2 performs exactly the same mathematical calculation on its incoming data as device 1.

- Device 2 also reads in the calculation sent by device 1 and compares it with the local calculation. If the two calculations provide an identical result, then it is assumed that the incoming message was not corrupted on the link.
- Device 2 can then issue a positive acknowledgement to device 1 to indicate that it is ready for the next message. If the two calculations are inconsistent, then it is assumed that incoming data has been corrupted, and device 2 issues a "negative acknowledgement" message to device 1, which indicates that the previous data message must be re-transmitted.

Termination of transmission

- Device 1 transmits a file, piece-wise, ensuring that each packet is correctly received by device 2, using the technique described in (Error Detection and Correction).
- After the last piece of the file is transmitted to device 2 and positively acknowledged, then device 1 must terminate the transmission. Device 1 sends an "end of transmission" message to device 2. This allows device 2 to close the stored file and return to other duties.

4.6.3 Terminologies In Networking (Encoding, Formatting, Size, Timing, Patterns)

Terminologies in relation to communication in networking

- **Message Encoding**

  The effect of the skills, attitudes, and knowledge of the sender on the process of encoding the message.

- **Message Formatting**

  A matter of agreement between two parties as to the form of the data to be exchanged or transmitted. For example, both sides must use the same binary code for characters.

- **Message Size**

The physical dimensions and proportions of message.

- **Message Timing**

Includes speed matching and sequencing of message

- **Message Patterns**

  Patterns of messages occur in two distinct forms: messages between objects, called a Protocol, and messages understood by a particular kind of object, called an Interface.

Communication problem

- **Contract Pattern**

Problem: How can behaviors be defined independent of implementations?

- **Correlation Identifier**

Problem: In any messaging system, a consumer might send several message requests to different service providers.

- **Message Sequence**

Problem: Because of the inherent distributed nature of messaging, communication generally occurs over a network.

- Message Expiration

  Problem: Messages are stored on disk or persistent media. With the growing number of messages, disk space is consumed.

CHAPTER FIVE

5.0 COMMISSIONING A BASE STATION

A base station is a common term used in telecommunications for a radio receiver with one or more antennae. While the base station has many other applications, it's often used for mobile telephony, wireless communications, and even wireless computer networking.

A base station works as the main communication point for one or more wireless mobile devices. It is a fixed transceiver capable of sending and receiving wireless signals via the radio frequency (RF) base station antennas to transmit RF signals to other devices.

Tracking these signals transmitted between devices and base stations is essential, and this is where digital twin software comes into the picture. A digital twin software is a virtual simulation of onsite or remote physical assets, which uses sensor data to monitor, track and manage these assets.

5.1 PROCEDURES TO COMMISSIONING A BASE STATION.

There are several conditions that must be met before considering a site good to be a base station

1. TOPOGRAPHY
2. AVAILABILITY AND PROXY USERS IN THE AREA

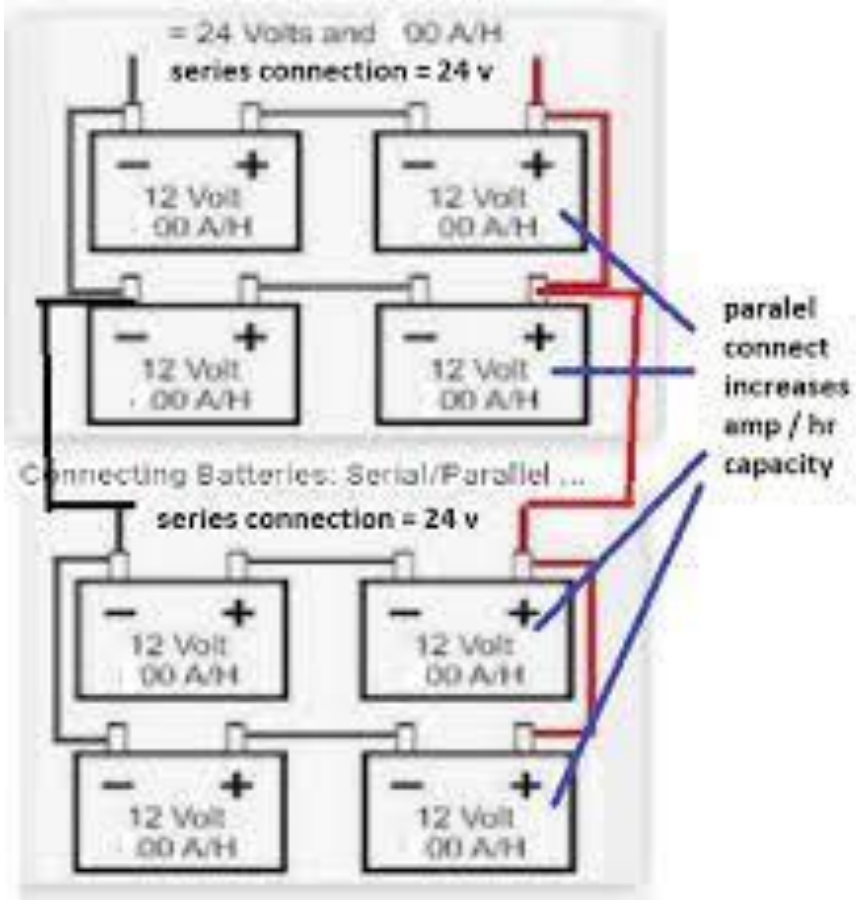
3. SOIL TEST is carried out on the land to test for polarity and rigidness of the soil, this is usually carried out because of the tower to be built on the land (Site)
4. EROSION FREE ENVIRONMENT

Once the above conditions are met, We can then proceed to commissioning a new Base station in the local area.

MATERIALS NEEDED TO BUILD A BASE STATION

- **TOWER (**To be built by a contractor**)**
- **Eight 12V lead-acid batteries**
- **Inverter 24V**
- **Fast Charger / Xantrex**
- **MPPT charge controller**
- **Solar Panels**
- **Router**
- **Switch**
- **ODF**
- **CAT-6 cables**
- **Electrical cables and Solar cables**
- **Racks**
- **Sectors (ePMP 3000™) PTMP radios**
- **POE's**
- **Tycoon Monitor**

The 12V batteries are connected as illustrated below;



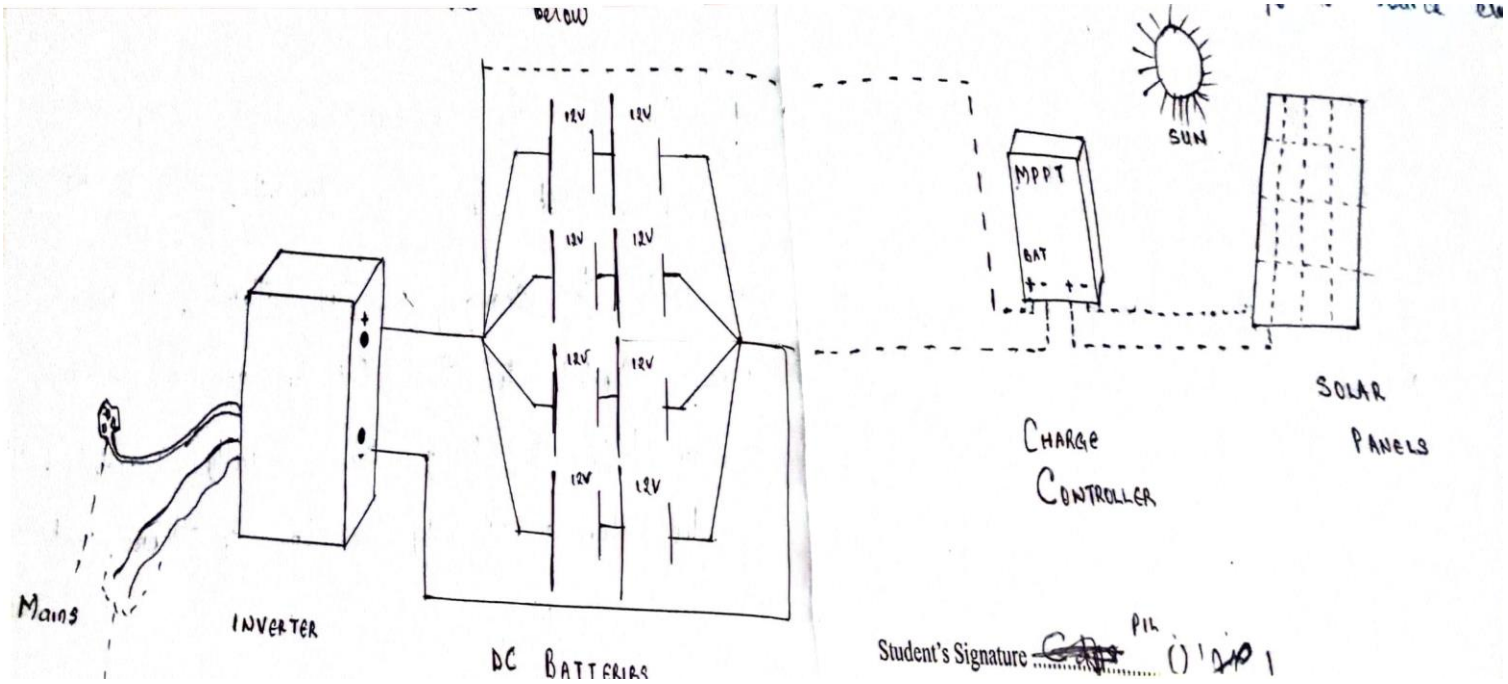
The above connection is similar to that of a bus bar connection.

BUS BAR connection is done to ensure even distribution of current across all batteries, this is done by terminating the terminal of each serially connected 12V + 12V =24V, to a common point with the load, inverter, mains supply and Solar Charge controller

If this isn't done, it is proven that only the terminated sets of batteries tend to charge as they attract more of the current supplied to them since they are the first receiver, they tend to supply other serially connected batteries with low current, resulting in them not charging to their capabilities.

In this case, the Base station tends to depend mainly on the terminated series of batteries, in case of power outage of mains and low Sun intensity, The site battery reading tends to decrease quickly as they are connected in parallel to not well charged batteries.

A 24V inverter is then connected to battery as illustrated below;



The mains supply electricity from either PHCN or the A.C generator. In case of power supply from mains, the inverter would (i) Charge the batteries (2) Supply the mains to the load, thereby releasing the batteries of load pending.

In a case of no power supply from mains, the inverter goes to UPS (Ultra Power Saving) mode, thereby the load solely depends on the batteries to source electricity.

In a case of both Main supply and Solar Supply are available, the batteries can be charged simultaneously by the Mains and the Solar. The sun intensity can be monitored on the charge controller. It is necessary for the Mains supply to be o the range 190-220 V for steady charging

The Xantrex /Fast charger is connected directly to the batteries, if provided a bus bar.

Note: Rack Positioning should have been done prior to this.

A router (cloud core) is then mounted in the rack, the router is said to configured.

If the site is a fiber site, the SFP Port is configured as the gateway port.

If a sub hub (PTP link) site, an ether port is configured as the gateway port

A switch can then be introduced if the site requires more ether ports.

A bandwidth capacity is the size of data that can be transmitted or received by the router per seconds.

Sub hubs are tolled at 200 Mbps and can be increased if demand.

Some fiber sites at close distance at close distance to each other as used as back uplink to each other. This is done by shooting a PTP link using PTP devices such as Wave nano or Af-60.

5.3 HOW TO CONFIGURE UBIQUITY DEVICES (RADIO)

HOW TO CONFIGURE UBIQUITY DEVICES (RADIO)

Below is a step-approach to configure a ubiquity device -:

1. Static your PC to 192.168.1.18, the subnet mask would automatically fill, then set private DNS to 8.8.8.8, and alternative DNS to 8.8.4.4
2. Set your login username and password (Unique details) which should be personal to the owner of the device
3. Go to wireless, Upgrade the firmware to the latest version, set the wireless mode to PTP, and select mains mode, for the A.P only.

   For two radios to associate, they must be of the same SSID and password (Case sensitive)

4. Go to Network,

   Set Network mode to bridge, router mode is only available for PTMP mode

   Static the management IP address to your preferred address and set Gateway IP

   Set Primary DNS to 8.8.8.8

   Set Secondary DNS to 8.8.4.4

   HOW TO CONFIGURE CAMBIUM DEVICES

   The only difference in PTP connections using Cambium devices and ubiquity devices is that unlike ubiquity devices, only one device (Station end) is required

All base stations have cambium ePMP 3000 radios which serves as A.P for PTMP connections.

Since there is a cambium A.P already, only the station end is required.

The station end device is FORCE -> 300

Force 300 have higher beam width and shooting range and can be very easy to pan.

CONFIGURATION OF A MICROTIK ROUTER

To configure a microtik device, we access the device by using either a win box app or web fig.

To access the microtik router, we plug a Lan cable to an ether port on the router

Then open the win box app

- You can login to the router using the router mac ID and this can be gotten by going to neighbors on win box.
- Using a default login username and password of (admin,)
- Every router comes with a default configuration, this default configuration has to be removed. To do this,
  - Go to system
  - Reset, then click remove Config.
  - Go to interface,
  - Add bridge
  - Go to ports
  - Add ports (ports 2-5), Port one is excluded cause it's the gate way port.

By adding ether port 2-5 on bridge have granted have granted access to port 2-5 to pick up internet from the gateway port.

We can also devices to use any other port as the gateway port.

Say, port 2 as gateway, then port 1,2,3 & 5. would be on bridge.

Then go to DHCP client

Add the gateway port e.g., if ether 1 is gateway port.

Then go to the firewall.

Firewall

NAT (add),

General,

The in interface should be left blank, the out interface should be the gateway port

Then, go to actions,

Add masquerade, then ok.

The above configuration would only grant internet access to the other ports.

In order to set up wireless, Go to WIRELESS

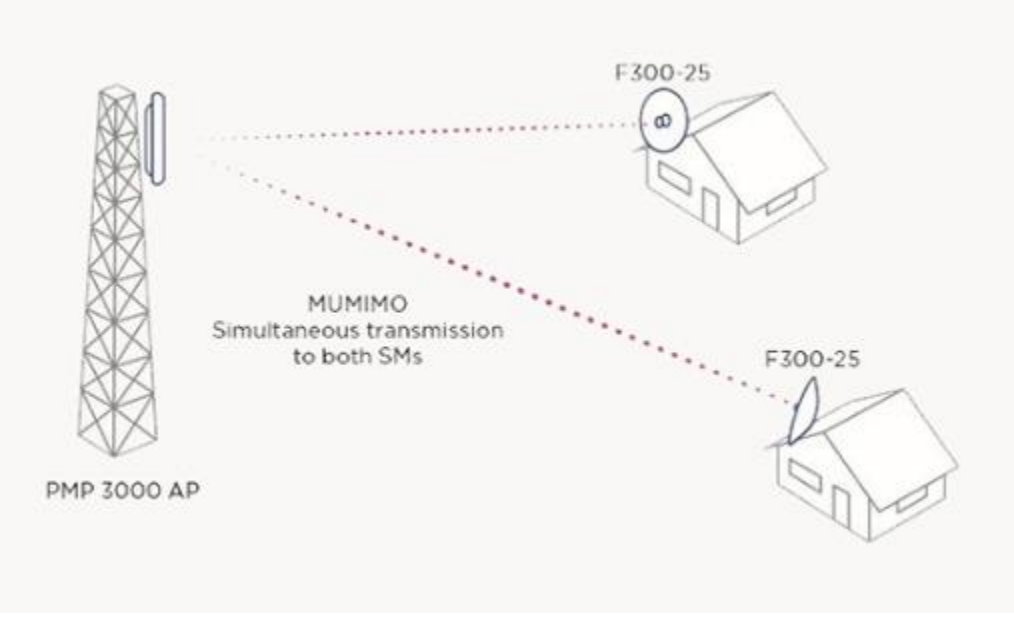
activate WLAN1, put mode on ap bridge, set frequency on auto, then ok.

Go to security Profile.

Edit the default mode to dynamic keys, authentication type to WPA2PSK,

Set SSID and password, if necessary, then reboot the router.

After setting up a base station, then PTMP links can be generated to customers house as illustrated below.



CONCLUSION

The **SIWES** program at **TIZETI NETWORK LIMITED** has been a valuable experience, providing a bridge between theoretical knowledge gained in academic settings and its practical application in the telecommunication industry. The exposure to diverse aspects of telecommunication, from network maintenance to customer service, has enhanced my understanding of the field.

The experience gained during the **SIWES** program has not only improved technical skills but has also fostered professional growth. It has highlighted the need for continuous learning and adaptation in the dynamic field of telecommunication.

Overall, this SIWES program has been an enriching experience, reinforcing the significance of practical exposure in supplementing theoretical education. It has provided a comprehensive understanding of the challenges and opportunities present in the telecommunication industry, preparing me for future endeavors in this dynamic and ever-evolving field.

RECOMMENDATION

To maximize the effectiveness of future SIWES programs, it is recommended that a broader range of experiences be incorporated, allowing students to explore emerging technologies such as 5G, Internet of Things (IoT), and cybersecurity within the telecommunication sector. Additionally, further emphasis on hands-on training and exposure to industry-specific tools and software would greatly benefit aspiring telecommunication engineers.

REFERENCES

Chapter 1 Introduction to networking by May Lia 2022

The fundamentals of networking, IBM 2020

Introduction to telecommunication, Cisco press. 2014

Network fundamentals, Network direction (YOUTUBE). 2019

This conclusion succinctly summarizes the practical experiences gained during the SIWES program in the field of telecommunication, highlighting its significance in bridging the gap between theoretical knowledge and industry application.