RQF LEVEL 4

NITWO401

NETWORKING AND INTERNET TECHNOLOGIES

Wireless Network Outdoor

TRAINEE'S MANUAL

October, 2024

WIRELESS NETWORK OUTDOOR

KOICA Korea International Cooperation Agency

TQUM TVET Quality Management Project

2024

AUTHOR'S NOTE PAGE (COPYRIGHT)

- This work has been produced initially with the Rwanda TVET Board with the support from KOICA through TQUM Project
- This work has copyright, but permission is given to all the Administrative and Academic Staff of the RTB and TVET Schools to make copies by photocopying or other duplicating processes for use at their own workplaces.
- This permission does not extend to making of copies for use outside the immediate environment for which they are made, nor making copies for hire or resale to third parties.
- The views expressed in this version of the work do not necessarily represent the views of RTB. The competent body does not give warranty nor accept any liability
- RTB owns the copyright to the trainee and trainer's manuals. Training providers may reproduce these training manuals in part or in full for training purposes only. Acknowledgment of RTB copyright must be included on any reproductions. Any other use of the manuals must be referred to the RTB.

© Rwanda TVET Board
Copies available from:
- *HQs: Rwanda TVET Board-RTB*
- *Web: www.rtb.gov.rw*
- **KIGALI-RWANDA**

Original published version: October 2024

ACKNOWLEDGEMENTS

The publisher would like to thank the following for their assistance in the elaboration of this training manual:

Rwanda TVET Board (RTB) extends its appreciation to all parties who contributed to the development of the trainer's and trainee's manuals for the TVET Certificate IV in in Networking and Internet Technologies, specifically for the module "**NITWO401: Wireless Network Outdoor**".

We extend our gratitude to KOICA Rwanda for its contribution to the development of these training manuals and for its ongoing support of the TVET system in Rwanda.

We extend our gratitude to the TQUM Project for its financial and technical support in the development of these training manuals.

We would also like to acknowledge the valuable contributions of all TVET trainers and industry practitioners in the development of this training manual.

The management of Rwanda TVET Board extends its appreciation to both its staff and the staff of the TQUM Project for their efforts in coordinating these activities.

This training manual was developed:

Under Rwanda TVET Board (RTB) guiding policies and directives

Under Financial and Technical support of

COORDINATION TEAM

RWAMASIRABO Aimable

MARIA Bernadette M. Ramos

MUTIJIMA Asher Emmanuel

Production Team

Authoring and Review

TUYISABE Annoncee

SHEMA Innocent

Validation

NSHIMIYIMANA Eugene

MUKANDAYISENGA Annualite

GATETE Patrick

Conception, Adaptation and Editorial works

HATEGEKIMANA Olivier

GANZA Jean Francois Regis

HARELIMANA Wilson

NZABIRINDA Aimable

DUKUZIMANA Therese

NIYONKURU Sylvestre

KWIZERA INGABIRE Diane

Formatting, Graphics, Illustrations, and infographics

YEONWOO Choe

SUA Lim

SAEM Lee

SOYEON Kim

WONYEONG Jeong

NDAYISABA Olivier

Financial and Technical support

KOICA through TQUM Project

TABLE OF CONTENT

ACRONYMS

ACL: Access Control List

AP: Access Point

BoQ: Bill of Quantities

BSSID: Basic Service Set Identifier

CA: Coverage Area

CAT5e: Category 5 Enhanced

CAT6: Category 6

CAT6a: Category 6 Augmented

CBT/A: Competent Based Training/Assessment

CCNA/CCNP : Cisco Certified Network Associate / Cisco Certified Network Professional

CPE: Customer Premises Equipment

CR: Cognitive Radio

DHCP: Dynamic Host Configuration Protocol

DSSS: Direct Sequence Spread Spectrum

EIGRP: Enhanced Interior Gateway Routing Protocol

EMI/RFI :(Electromagnetic/Radio Frequency Interference)

GHz: Gigahertz

GNS3: Graphical Network Simulator

IEEE: Institute of Electrical and Electronics Engineers

IM: interference Management

IoT : Internet of Things

IP: Internet Protocol:

KOICA: Korea International Cooperation Agency

LAN: Local Area Network

LED: Light-Emitting Diode

MAC – Media Access Control:

MIMO: Multiple Input Multiple Output

MU-MIMO: Multi-User MIMO

NAT: Network Address Translation

NIC: Network Interface Card

OFDM: Orthogonal Frequency-Division Multiplexing

OFDMA: Orthogonal Frequency-Division Multiple Access

OSI: Open Systems Interconnection Model

OSPF: Open Shortest Path Firstk.

PoE: Power-Over-Ethernet

PSK – Pre-Shared Key:

PtMP: Point-to-Multipoint

PtP: Point-to-Point

QAM: Quadrature Amplitude Modulation

RF: Radio Frequency

RIP: Routing Information Protocol.

RJ45: Registered Jack 45

RTB: Rwanda TVET Board

SSID : Service Set Identifier

TPC: Transmit Power Control

TQUM Project: TVET Quality Management Project

TWT: Target Wake Time

UPS: Uninterruptible Power Supply

WPA – Wi-Fi Protected Access:

WPA2/**WPA3**: Wi-Fi Protected Access

INTRODUCTION

This trainee's manual includes all the knowledge and skills required in Networking and Internet Technologies specifically for the module of **“Wireless Network Outdoor ".** Trainees enrolled in this module will engage in practical activities designed to develop and enhance their competencies. The development of this training manual followed the Competency-Based Training and Assessment (CBT/A) approach, offering ample practical opportunities that mirror real-life situations.

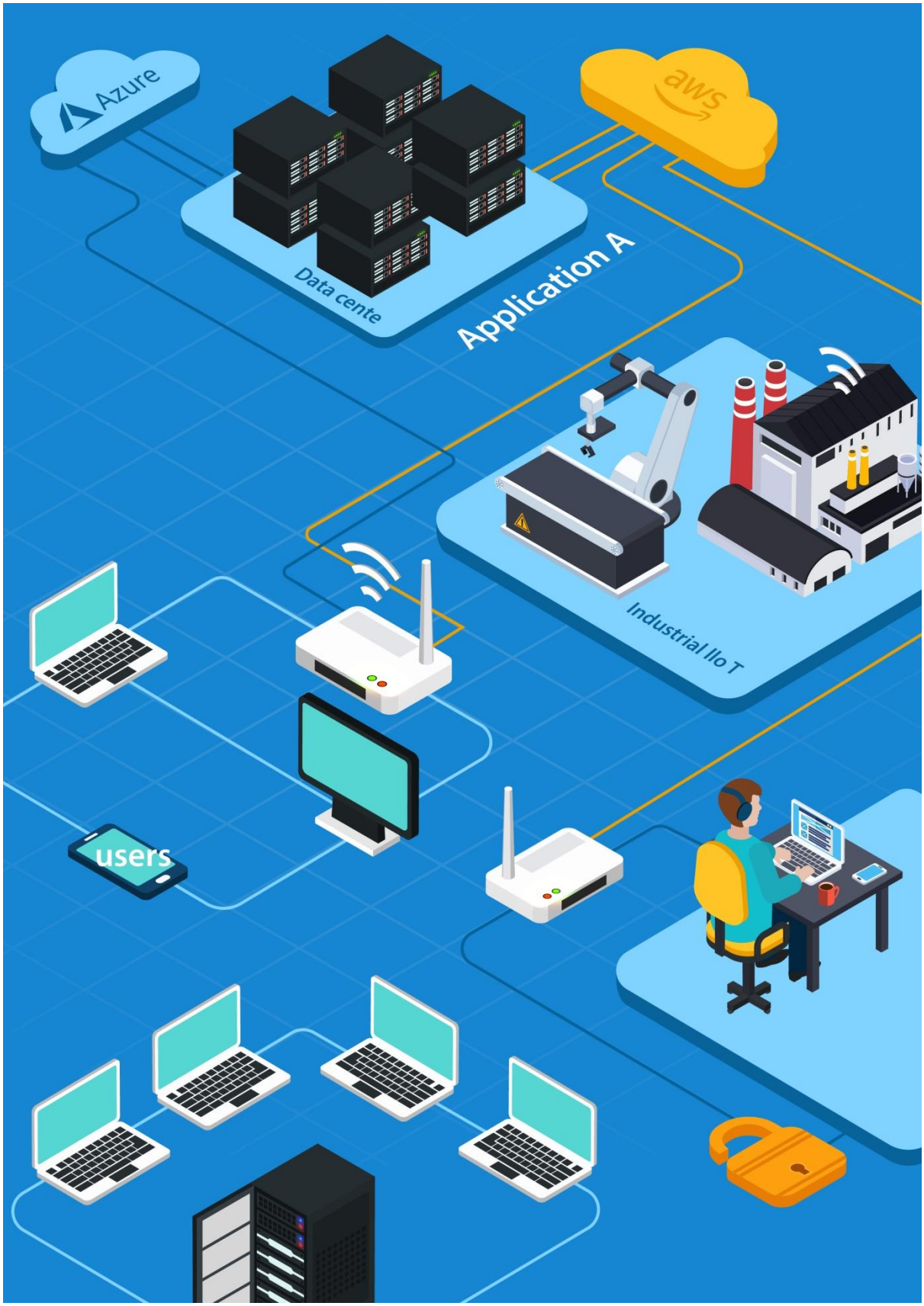
The trainee's manual is organized into Learning Outcomes, which is broken down into indicative content that includes both theoretical and practical activities. It provides detailed information on the key competencies required for each learning outcome, along with the objectives to be achieved.

As a trainee, you will start by addressing questions related to the activities, which are designed to foster critical thinking and guide you towards practical applications in the labor market. The manual also provides essential information, including learning hours, required materials, and key tasks to complete throughout the learning process.

All activities included in this training manual are designed to facilitate both individual and group work. After completing the activities, you will conduct a formative assessment, referred to as the end learning outcome assessment. Ensure that you thoroughly review the key readings and the 'Points to Remember' section.

MODULE CODE AND TITLE: NITWO401 WIRELESS NETWORK OUTDOOR

Learning Outcome 1: Plan wireless network outdoor installation
Learning Outcome 2: Deploy wireless network outdoor
Learning Outcome 3: Maintain wireless network outdoor


Azure
aws
Data cente
Application A
Industrial Iio T
users

Indicative contents
1.1 Identification of network requirements
1.2 Identification of Materials and Equipment
1.3 Design wireless network topology

Key Competencies for Learning Outcome 1: Plan wireless network outdoor installation

Knowledge	Skills	Attitudes
• Description of wireless network outdoor • Identification of wireless network outdoor areas of applications • Identification of Materials and Equipment used in wireless network outdoor installation • Description of radio frequency • Description of network topologies used to setup wireless network outdoor	• Conducting site survey for wireless network outdoor installation • Analysing site survey findings • Selecting tools, materials and equipment • Producing bill of quantity • Designing wireless network topology diagram	• Being attentive to details while recording site information • Being analytical thinker on analysing site survey • Having Accuracy on development of topology and producing bills of quantity. • Being Comprehensive by Including all relevant network components

Duration: 20hrs

Learning outcome 1 objectives:

By the end of the learning outcome, the trainees will be able to:

1. Describe clearly wireless network outdoor concepts based on network standard
2. Conduct correctly site survey based on user requirements
3. Identify correctly tools, materials and equipment used in wireless network outdoor installation based on site survey findings.
4. Develop correctly bill of quantity based on network requirements
5. Design properly wireless network outdoor topology based on site survey findings

Resources

Equipment	Tools	Materials
● Access points ● Router ● Repeater ● Wireless Extender ● Antennas ● Firewall ● PoE ● Switch ● Rack amount ● Computer ● UPS ● Lightning Arrestor	● Edrawmax ● Draw.io ● Cisco packet tracer ● Lucidchart	● Connector ● Network Cables ● Cable ties ● Screws ● Internet Bundles ● Nails

Indicative content 1.1: Identification of Network Requirements

Duration: 8 hrs

Theoretical Activity 1.1.1: Description of wireless network outdoor concepts

Tasks:

1: Answer the following questions related to the wireless network outdoor concepts:

i. What do you understand by wireless network outdoor?

ii. Describe these key terms related to wireless network outdoor:

a. Coverage area

b. Frequency spectrum

c. Antenna types and direction

d. Interference management

iii. Identify the application areas of wireless network outdoor

2: Write your findings on paper or flipchart

3: Present your findings in front of the whole class

4: Ask for clarification where necessary

5: Read the key readings 1.1.1

Key readings 1.1.1.:Description of wireless network outdoor concepts

1. **Definition**

Wireless network outdoor: A wireless network outdoor is a communication system designed to provide wireless internet and network connectivity across open spaces or outdoor environments

2. **Key Terms of Wireless Network Outdoor**

2.1 Coverage Area: Refers to the geographical region where the wireless network's signal is strong enough to provide reliable connectivity to users

- In outdoor wireless networks, coverage area is a crucial aspect of

design and planning. It determines how far and how effectively the wireless signal can travel from an access point (AP).

- The size of the coverage area depends on factors like the power of the AP, the type of antennas used, the terrain, and the presence of obstacles (e.g., buildings, trees).
- The goal is to ensure that the entire desired area is covered with minimal gaps (dead zones) and overlaps, which requires strategic placement of APs and consideration of environmental factors.

2.2 Frequency Spectrum: Refers to the range of electromagnetic frequencies used to transmit data wirelessly. In outdoor wireless networks, common frequency bands include the 2.4 GHz and 5 GHz bands, and sometimes higher frequencies for specific applications.

- Different frequencies have different properties that affect range, data throughput, and interference. Lower frequencies (like 2.4 GHz) tend to have longer ranges and better penetration through obstacles, but are more prone to interference. Higher frequencies (like 5 GHz) offer faster data rates and less interference but have shorter ranges and are more easily obstructed.
- The choice of frequency spectrum impacts the network's performance and coverage. Spectrum management and the careful selection of channels are essential to minimize interference and optimize network efficiency

2.3 Antenna & antenna Types and Direction:

An antenna is a device that transmits and receives electromagnetic waves, such as radio waves, television signals, and cellular phone signals. It serves as the interface between a transmitting or receiving device

Antenna types refer to the different designs and functionalities of antennas used in outdoor wireless networks, while direction refers to the orientation and focus of the antenna's signal. Choosing the right type of antenna is crucial for the success of an outdoor wireless network. Factors such as the desired coverage area, environmental conditions, and the specific application will determine which antenna is best suited for the job

2.3.1. Types of antennas

A. Omnidirectional Antennas

Omnidirectional antennas radiate signals uniformly in all directions (360 degrees horizontally). They are often used when coverage is needed in all directions around the antenna.

Type of omnidirectional antennas

- ✓ **Outdoor Omni Antennas**
  Used to improve WiFi signal outdoors. To successfully improve the wireless coverage outside, they are typically connected to a router, access point, or an outdoor access point.
- ✓ **Ceiling Dome Antennas**
  Connect to a WiFi router or access point via coaxial cable and are installed on the ceiling of a home, office building, or warehouse.
- ✓ **Rubber Duck Antennas or Dipole Antennas**
  Typically found on routers, access points, and WiFi USB adapters. Have a look the antennas on the Tenda Wi-Fi 4G+ LTE AC1200 Dual-Band Router

B. Directional antennas

As their name suggests, focus all their power in one direction. A directional antenna works similarly to a flashlight. When you turn on a flashlight, it illuminates the area that the light is being shined on.

Directional Wi-Fi antennas are often used for long-range point-to-point Wi-Fi networks to bridge the internet connection between two buildings

Types of Directional Wi-Fi antennas

- ✓ **Yagi Antennas**
  The most popular directional antenna. Most Yagi antennas are shaped like arrows. To work, they must point in the direction they are sending a signal to or receiving a signal from. A typical Yagi antenna has a radiation pattern of 45 degrees
- ✓ **Mini Panel Antennas**
  Low-profile antennas designed to send radio waves to and from a specific area. These antennas are most commonly used to improve your WiFi signal indoors. They could replace a rubber duck antenna on a router, access point, or WiFi USB adapter. To drop connectivity issues, the antenna must point in the direction where you want to send a signal to and receive a signal from. These types of antennas have a radiation pattern of 60 degrees.
- ✓ **Panel Antennas**
  Strong antennas that can be used to send or receive a signal from far distances. They can either be connected to a router to transmit data further or to a USB Wi-Fi adapter to receive data from further distances. Panel antennas are more directional than mini panel antennas; they have a radiation pattern of 35 degrees. For example, the Tenda 5GHZ 16dBi 11ac Outdoor CPE antennas can be either panel or parabolic
- ✓ **Parabolic Grid Ante**

High gain and are extremely directional. They tend to have a very narrow beam width, usually between 3-20 degrees.

Because of this, parabolic antennas are able to send and receive signals from miles away, making them perfect for point-to-point Wi-Fi networks. Plus, due to their design, they can withstand extreme weather conditions

- ✓ **CPE antennas:** "CPE" antennas stand for "Customer Premise Equipment" antennas, and can be either panel or parabolic. They are used to create point to point networks and broadcast your wireless signal over a distance. The CPE antennae's that we offer cover 12 miles and 6.5 miles respectively. CPE antennas can be deployed both indoors and outdoors to create a reliable WiFi connection in outlying buildings such as barns, rural areas and surveillance cameras. Check out the Tenda 5GHz 23dBi 11ac Outdoor CPE

2.4 Interference Management

Interference in wireless networks refers to any unwanted signal that can disrupt or degrade the quality of communication between devices.

Is a strategies such as channel selection, power control, and spatial separation to minimize and mitigate the impact of interference from other wireless networks and environmental sources

2.4.1 Interference Management strategy strategies

- ✓ **Frequency Planning:**
  Allocate different frequency bands or channels to nearby wireless networks or cells to reduce co-channel interference. Proper frequency planning can help ensure that neighboring networks operate on non-overlapping channels.
- ✓ **Power Control**
  Adjust the transmit power of wireless devices based on their proximity to the access point or base station. Devices closer to the access point can reduce their transmit power to avoid interfering with devices farther away, and vice versa.
- ✓ **Antenna Design and Placement**
  Use directional antennas to focus signals in specific directions and reduce interference from other directions. Proper antenna placement can also help minimize interference from reflective surfaces and obstacles.
- ✓ **Spectrum Management**
  Employ spectrum sensing techniques to detect and identify interference sources, including unauthorized devices or sources of interference in unlicensed frequency bands.
- ✓ **Cognitive Radio**
  Implement cognitive radio technology, which allows wireless devices to adapt their transmission parameters, such as frequency, power, and modulation, to operate in the least congested and interfered-with portions of the spectrum.

- ✓ **Coexistence Protocols**
  Use protocols and standards that are designed to enable the coexistence of multiple wireless networks in the same environment, such as Wi-Fi's Clear Channel Assessment (CCA) and Listen Before Talk (LBT) mechanisms.

3 Area of application Wireless network outdoor

Wireless networks are widely used in outdoor environments for various applications. Here are some common areas of application for outdoor wireless networks

- ✓ **Public Wi-Fi Hotspots**
  Outdoor wireless networks are deployed in public spaces such as parks, stadiums, and city centers to provide free or paid Wi-Fi access to the public. These networks enhance connectivity for residents and tourists.
- ✓ **Smart Cities**
  Outdoor wireless networks play a crucial role in smart city initiatives, enabling the deployment of various IoT devices, smart streetlights, traffic management systems, and environmental monitoring sensors.
- ✓ **Wireless Surveillance**
  Outdoor wireless networks are used for video surveillance systems in cities, campuses, and industrial areas. These networks allow for real-time monitoring of public spaces and critical infrastructure
- ✓ **Remote Connectivity:**
  We can use outdoor wireless networks to extend internet access to remote areas, supporting activities such as rural telemedicine, remote education, and connecting isolated IoT devices or sensors for monitoring and control.

Theoretical Activity 1.1.2: Description of environment survey evaluation.

Tasks:

1: Answer the following questions related to the Environment survey evaluation:

i. What do you understand by environment survey evaluation?
ii. Describe Physical Environment Survey?
iii. Describe Analysing Existing System?
iv. Describe Radio Frequency (RF) Site Survey
v. Identify the main factors that should be analysed during a site survey for a wireless network to ensure optimal performance and reliability.

2: Write your findings on paper or flipchart
3: Present your findings in front of the whole class
4: Ask for clarification where necessary
5: Read the key readings 1.1.2

Key readings 1.1.2.: Description of Environment survey evaluation

1. **Definition**

An environment survey evaluation is a process of assessing the environmental conditions and their potential impact on a specific project or activity. It involves collecting and analysing data about various environmental factors to determine their suitability and potential risks.

2. **Physical Environment Survey:**

Is a systematic assessment of the physical characteristics of a specific location or area. It involves collecting data about various environmental factors that can impact human activities, infrastructure, and the overall well-being of a community.

- ✓ **Analyze Environmental Factors**

  Study the effect of various terrains (flat vs. hilly) and structures (buildings, trees, etc.) on wireless signal propagation. Consider the impact of weather conditions like rain and wind on signal degradation.

- ✓ **Map Hypothetical Obstructions**

  Use a topographic map or aerial image of an area to hypothesize where signal blockages might occur due to physical obstacles.

- ✓ **Mounting Considerations**

  Theorize the best mounting locations (e.g., rooftops, towers) based on the physical landscape, height requirements, and proximity to user density zones.

3. **Analyzing Existing System:**

Is a critical step in any project or initiative. It involves evaluating the current state of a system, identifying its strengths, weaknesses, and areas for improvement. This analysis provides valuable insights for making informed decisions about system maintenance, upgrades, or replacements.

- ✓ **Review Network Architecture**

Analyze the architecture of an existing wireless network to understand its strengths and weaknesses. Theorize what can be reused or upgraded.

- ✓ **Capacity Estimation**

Examine user demand data (e.g., number of users, bandwidth usage) to estimate whether the existing system meets demand or requires expansion.

- ✓ **Hypothetical Integration**

Conceptualize how new wireless systems could integrate with or replace the current network. Predict how upgrading equipment or adding more access points might improve performance.

4. **Radio Frequency (RF) Site Survey:**

It is a process of assessing the radio frequency of a specific location to

determine the suitability for wireless network deployment.

It involves measuring signal strength, identifying interference sources, and evaluating the potential impact of environmental factors on network performance.

- ✓ **Frequency Spectrum Analysis**

  Study theoretical frequency bands (e.g., 2.4 GHz, 5 GHz) and analyze how different environmental conditions impact them.

- ✓ **Simulate Coverage**

  Use mapping tools or software to simulate wireless signal coverage in a given area. Hypothesize the effect of non-line-of-sight (NLOS) scenarios and obstructions.

- ✓ **Interference Prediction**

  Identify potential sources of RF interference (e.g., nearby networks, electronic devices) in the theoretical environment and predict their impact on signal quality and performance.

5.Analysing Site Survey Findings

When conducting a site survey for a wireless network, several critical factors must be analysed to ensure optimal performance and reliability. These factors include bandwidth, network coverage, security, scalability, and weatherproofing. Below is a detailed analysis of each factor based on survey findings.

- ✓ **Bandwidth**

  Bandwidth is a crucial metric that determines the data transmission capacity of the network. During site surveys, measurements such as throughput, data rates, and latency are assessed to ensure that the network can handle the expected load. Active site surveys provide detailed metrics on upstream and downstream data rates, helping identify potential bottlenecks or areas requiring additional access points (APs) to maintain adequate bandwidth for users.

  Bandwidth Requirements = (Data Rate per User) * (Number of Users) * (Safety Factor)

  Safety factor: account for unexpected traffic spikes or future growth.

- ✓ **Network Coverage**

  Network coverage refers to the area where users can connect to the wireless network effectively. Site surveys typically generate heat maps that visualize signal strength across different areas, highlighting "dead zones" where coverage is insufficient. This information is vital for determining optimal AP placements to ensure comprehensive coverage. Additionally, identifying sources of interference such as other wireless networks or electronic devices can help mitigate connectivity issues and enhance overall performance.

- ✓ **Security**

Security is paramount in wireless networks.

Site surveys assess potential vulnerabilities by analysing existing security protocols and identifying any unauthorized access points (rogue APs). The survey can also evaluate the effectiveness of encryption methods and suggest improvements to safeguard sensitive information. Regular assessments help maintain a secure environment as new devices are added or existing configurations change.

- ✓ **Scalability**

  Scalability involves planning for future growth in network demand. A well-executed site survey not only addresses current requirements but also anticipates future needs based on projected user growth and increased device connectivity. This foresight allows organizations to design networks that can accommodate additional users and high-bandwidth applications without compromising performance.

- ✓ **Weatherproofing**

  For outdoor or semi-outdoor installations, weatherproofing is essential to ensure the longevity and reliability of network equipment. Site surveys should evaluate environmental factors such as humidity, temperature fluctuations, and exposure to elements like rain or snow. Recommendations may include using weather-resistant enclosures for APs or selecting equipment specifically designed for outdoor use.

Practical Activity 1.1.3: Conducting site survey of wireless network outdoor

Task:

1: Read carefully and do the stated activity

WPX School want to deploy wireless network in sport field, you are requested to evaluating the environment, analysing the current system and measure RF signal strength to ensure efficient signal propagation and coverage area and then present the survey findings

2: Follow the work instructions given by the teacher and under his guidance, perform the stated activity

3: Ask for clarification where necessary

4: Present your survey findings to the class.

5: Read key readings 1.1.3 and perform the application of learning 1.1

Key readings 1.1.3:Conducting a Site Survey for a Wireless Network Outdoor

A site survey is a crucial step in planning and deploying a wireless network outdoors. It involves evaluating the physical environment, identifying potential challenges, and collecting data to optimize network performance.

Here are the key steps involved in conducting a site survey for a wireless network outdoors:

1. **Define the Scope:**

- **Determine the area to be covered:** Identify the specific locations or buildings that need wireless coverage.
- **Set objectives:** Define the desired network performance goals, such as coverage, capacity, and reliability.

2. **Gather Existing Information:**

- **Collect site maps:** Obtain detailed maps of the area, including building layouts and terrain.
- **Review existing infrastructure:** Assess the current wireless network infrastructure, if any, and identify potential limitations or challenges.

3. **Conduct a Physical Site Visit:**

- **Inspect the environment:** Examine the physical conditions of the site, including buildings, trees, and other obstacles that could affect signal propagation.
- **Identify potential interference sources:** Look for sources of electromagnetic interference, such as nearby radio towers, power lines, or other wireless networks.
- **Assess power availability:** Determine the availability of power outlets for network devices.

4. **Measure RF Signal Strength:**

- **Use a signal strength meter:** Measure the strength and quality of the existing wireless signal at different locations within the coverage area.
- **Identify dead zones:** Identify areas with weak or no signal coverage.

5. **Analyze Environmental Factors:**

- Consider terrain: Evaluate the impact of hills, valleys, and other topographical features on signal propagation.
- Assess line-of-sight: Determine if there are any obstructions between the access

points and the intended coverage areas.

- **Evaluate weather conditions:** Consider how weather factors like rain, snow, and temperature can affect signal strength.

6. **Plan Antenna Placement:**

- **Choose appropriate antenna types:** Select antennas that are suitable for outdoor environments and the desired coverage area (e.g., omnidirectional or directional).
- **Determine mounting locations:** Identify suitable locations for mounting antennas, considering factors like height, line of sight, and physical accessibility.

7. **Estimate Network Capacity:**
    - **Assess user density:** Estimate the number of users who will be connected to the network.

- **Calculate bandwidth requirements:** Determine the required bandwidth based on user activity and applications.

8. **Develop a Network Design:**

- **Create a network topology:** Design the layout of the network, including the placement of access points and cables.

9. **Conduct a Pilot Deployment:**

- **Install and test a limited number of access points:** Deploy a small-scale network to verify the design and identify any issues.
- **Make adjustments as needed**: Modify the network design based on the pilot deployment results.

10. **Document the Site Survey:**

Create a detailed report: Document all findings, including site measurements, network design, and recommendations.

By following these steps, you can conduct a comprehensive site survey for your outdoor wireless network, ensuring optimal performance and coverage.

Practical Activity 1.1.4: Analysing site survey evaluation findings of wireless network outdoor.

Task:

1: Read carefully and do the stated activity

Refer to the previous practical activity 1.1.3, validate the effectiveness of the wireless network outdoor in terms of the following aspects: Bandwidth, Network Coverage, Security, Scalability, and Weatherproofing and then elaborate the data validation report.

2: Follow the work instructions given by the trainer
3: Using site survey documentation given by trainer and under his guidance , perform the stated activity
4: Ask for clarification where necessary
5: Read key readings 1.1.4 and perform the application of learning 1.1

Key readings 1.1.4: Analyzing site survey evaluation findings of wireless network outdoor

Analyzing site survey evaluation findings of wireless network outdoor

Analyzing site survey evaluation findings of a wireless network outdoor refers to the process of reviewing, interpreting, and making sense of the data collected during a site survey to determine how well the wireless network performs in an outdoor environment.

During the site survey evaluation findings analysis, the following aspects are considered:

Bandwidth, Network Coverage, Security, Scalability, and Weatherproofing.

1. Bandwidth Assessment

Objective: Measure the speed and capacity of the network to determine whether it meets user needs.

Steps:

1: **Preparation:**
- Select testing tools (e.g., Ookla Speed test, iPerf, or PingPlotter).
- Identify test locations across the coverage area (e.g., center, edges, and blind

spots).

2: **Measurement**:

- Test download speed, upload speed, and latency at each location.
- Perform multiple tests during different times of the day (peak vs. off-peak hours).

3: **Comparison**:

- Compare measured bandwidth against the expected or advertised values from the network provider.
- Note any significant drops or fluctuations.

Reporting Findings of data validation:

- Present speed test results in tabular or graphical format.
- Highlight areas with significant bandwidth issues or inconsistencies.

2. Network Coverage Assessment

Objective: Evaluate how well the network covers the outdoor area and identify weak or dead zones.

Steps:

1: **Signal Strength Measurement:**

- Use tools like Wi-Fi analyzers (e.g., NetSpot, Ekahau, or inSSIDer) to measure signal strength (RSSI) in dBm.
- Check for dead zones or weak spots (<-70 dBm indicates poor coverage).

2: **Heatmap Creation:**

- Create a Wi-Fi heatmap to visually display the network coverage.
- Use heatmap software to overlay signal strength data on a map of the site.

3: **Obstacle Impact Assessment:**

- Test signal strength near physical barriers (e.g., trees, walls, or vehicles).
- Note any significant coverage reduction caused by obstacles.

Reporting Findings:

- Include heat maps, RSSI values, and dead zone locations.
- Recommend adding access points or antennas to address poor coverage areas.

3. Security Assessment

Objective: Ensure the network is secure from unauthorized access and data breaches.

Steps:

1: **Encryption Validation:**

- Check the encryption standard used (e.g., WPA3, WPA2).
- Use network analyzers to detect open or unencrypted networks.

1: **Access Control Verification:**

- Confirm if the network uses MAC filtering, user authentication (e.g., RADIUS), or a guest network policy.

2: **Vulnerability Scanning:**

- Use tools like Wireshark or Aircrack-ng to detect security vulnerabilities (e.g., weak passwords, rogue devices).
- Simulate unauthorized access attempts to test the effectiveness of security measures.

3: **Physical Security Check:**

- Inspect outdoor hardware for tamper-proof installations (e.g., locked enclosures, secured cabling).

Reporting Findings:

- List vulnerabilities found and their severity levels.
- Provide specific recommendations, such as enabling stronger encryption or implementing multi-factor authentication.

4. Scalability Assessment

Objective: Determine the network's ability to handle additional devices and increased traffic.

Steps:

1: **Current Capacity Testing:**

- Simulate multiple simultaneous device connections (e.g., laptops, smartphones).
- Monitor bandwidth usage and latency with tools like iPerf or SolarWinds.

2: **Stress Testing:**

- Gradually increase the number of devices until performance degradation

is noticeable.
- Record the maximum number of users the network supports without significant issues.

3: **Future Growth Assessment:**

- Evaluate the network's ability to add access points or expand coverage without major hardware changes.
- Check if the router/access points support high-density features (e.g., MU-MIMO).

Reporting Findings:

- Include the maximum user capacity and performance metrics under load.
- Suggest hardware upgrades or configuration changes to improve scalability.

5. Weatherproofing Assessment

Objective: Test the resilience of network equipment under various environmental conditions.

Steps:

1: **IP Rating Verification:**

- Confirm the equipment's ingress protection (IP) rating (e.g., IP67 ensures protection against dust and water).

2: **Simulated Environmental Testing:**

- Use artificial rain or sprinklers to test water resistance.
- Expose devices to heat or cold conditions to simulate temperature variations.

3: **Physical Inspection:**

- Check for rust, corrosion, or damage to outdoor enclosures, cables, and connectors.
- Verify proper sealing and installation.

4: **Real-World Testing:**

- Monitor network performance during actual weather conditions (e.g., rain, wind, snow).

Reporting Findings:

- Document any equipment failures or performance degradation.
- Provide recommendations, such as upgrading to higher IP-rated equipment or improving installation methods.

6. Elaborating the Data Validation Report

Once the data has been collected and analyzed for all five aspects, compile it into a comprehensive report.

Points to Remember

- The right type of antenna should be chosen based on the coverage area and specific application needs
- A wireless network outdoor is a communication system designed to provide wireless internet and network connectivity across open spaces or outdoor environments
- The right type of antenna should be chosen based on the coverage area and specific application needs
- To avoid interference, Consider outdoor factors such as weather, physical obstacles, and the scale of deployment
- You need to identify potential sources of interference and Implement strategies to minimize interference, such as selecting appropriate channels and using advanced technologies like beamforming.
- The appropriate frequency bands is selected based on range, bandwidth requirements, and regulatory constraints.
- Network outdoor can be applied in many deferent area such as Public Wi-Fi hotspot, Smart City infrastructure, Wireless Surveillance and Security and Remote Connectivity
- An environment survey evaluation is a process of assessing the environmental conditions and their potential impact on a specific project or activity
- For clearly evaluate wireless outdoor environment you must survey the Physical Environment , Analyzing Existing System and Radio Frequency (RF) site survey
- A clearly Environment survey evaluation finds: bandwidth needs, network coverage area ,security measurement , network scalability option and weatherproof techniques
- A site survey is a crucial step in planning and deploying a wireless network outdoors
- The key steps involved in conducting a site survey includes

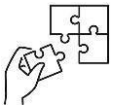
- ✓ Define the Scope
- ✓ Gathering Existing Information
- ✓ Conducting a Physical Site Visit
- ✓ Measuring RF Signal Strength
- ✓ Analyzing Environmental Factors
- ✓ Plan Antenna Placement
- ✓ Estimate Network Capacity
- ✓ Estimate Network Capacity
- ✓ Develop a Network Design
- ✓ Conduct a Pilot Deployment
- ✓ Conduct a Pilot Deployment
- ✓ Document the Site Survey

• Ensure the appropriate bandwidth is proportional to the number of users.

• Ensure that the distance coverage is properly measured.

• Think of wireless network outdoor protection against theft, physical damage and unauthorized intruders.

• The better selection of appropriate wireless access points frequency band based on the nature of the medium.



Application of learning 1.1.

ABC school located in Kigali city want to deploy a network that interconnect both primary and secondary, the distance between primary and secondary is 1km. Secondary building is surrounded by trees and power transmission antenna. As network technician you are hired to conduct a site survey, plan the antenna placement based on description and measure the signal strength of current infrastructure

Indicative content 1.2: Identification of Materials and Equipment

Duration: 6 hrs

Theoretical Activity 1.2.1: Description of wireless network outdoor materials and equipment

Tasks:

1: answer the following questions relating to wireless network outdoor Materials and Equipment

i. What do you understand by Materials and Equipment

ii. Describe the following Materials and Equipment of wireless outdoor network:

   a. Connectors
   b. Cable manager (Ties, clips, Sockets)
   c. Ethernet Cable
   d. Outdoor Access Points
   e. Antennas
   f. Wireless Extender
   g. Power-Over-Ethernet
   h. Lightning Arrestor
   i. UPS
   j. Network switch
   k. Routers
   l. Repeater
   m. Firewall
   n. Rack mount

iii. Describe bill of quantities

2: Write your findings on paper or flipchart

3: Present your findings in front of the whole class

4: Ask for clarification where necessary

5: Read the key readings 1.2.1

Key readings 1.2.1.:Wireless network outdoor materials and equipment

1. **Definition**

   Materials: are the physical components and substances used to construct and install the wireless infrastructure These materials play a crucial role in ensuring the network's reliability, durability, and performance.

   Equipment : Equipment refers to the tools and devices used to install, test, and manage the wireless outdoor network

2. **Identification of Materials**

   ✓ **Connectors**

   Connectors are components used to join cables or other hardware elements in a network. They ensure secure and reliable electrical connections between devices and cables. Examples include RJ45 connectors for Ethernet cables and SMA connectors for antennas.

   ✓ **Cable Manager (Ties, Clips, Sockets)**

   Cable managers are tools used to organize and secure cables to prevent tangling, damage, or interference

   - **Ties:** Plastic or velcro strips used to bundle and secure cables.
   - **Clips:** Small devices used to attach cables to surfaces or structures.
   - **Sockets:** Junction boxes or cable management enclosures where multiple cables connect or are routed.

   ✓ **Ethernet Cable**

   Ethernet cables are used to connect network devices, such as routers, switches, and access points, to each other or to a network. They come in various categories (e.g., Cat5e, Cat6, Cat6 a) that determine their speed and bandwidth capabilities.

3. **Identification of equipment**

   ✓ **Outdoor Access Points**

   Outdoor access points (APs) are wireless devices designed for outdoor environments to provide Wi-Fi coverage. They are built to withstand harsh weather conditions and have enhanced range and signal strength compared to indoor APs.

   ✓ **Antennas**

   Antennas are devices that transmit and receive radio signals. They come in different types, such as omnidirectional (which radiate signals in all directions) and directional (which focus signals in a specific direction), and are essential for establishing and maintaining wireless communication.

   ✓ **Wireless Extender**

   A wireless extender, also known as a Wi-Fi extender or range extender, is a

device used to expand the coverage of an existing wireless network.

- **Network Management**: Some extenders come with management apps or web interfaces that allow users to monitor and manage their extended networks, including setting up parental controls and scheduling access times.
- **LED Indicators**: Wireless extenders often have LED indicators that display the connection status and signal strength, making it easier to find the best location for placement.

✓ **Power-Over-Ethernet (PoE)**

Power-Over-Ethernet technology allows Ethernet cables to carry both data and electrical power to devices such as access points and IP cameras, eliminating the need for separate power sources and simplifying installation.

✓ **Lightning Arrestor**

A lightning arrestor is a device used to protect network equipment from electrical surges caused by lightning strikes. It diverts excess electrical energy away from sensitive equipment to prevent damage.

✓ **UPS (Uninterruptible Power Supply)**

A UPS provides backup power to network equipment during electrical outages or disturbances. It ensures that network devices remain operational and helps prevent data loss and hardware damage.

✓ **Network Switch:**

A network switch is a device that connects multiple network devices within a local area network (LAN). It receives incoming data packets and redirects them to their destination devices based on their MAC addresses, improving network efficiency and performance.

✓ **Routers:**

Routers are devices that manage network traffic between different networks, such as between a local network and the internet. They route data packets to their destination and can provide additional functions such

as NAT (Network Address Translation) and DHCP (Dynamic Host Configuration Protocol).

- ✓ **Repeater**

  Repeaters and wireless extenders serve similar purposes in terms of improving network coverage, but they operate differently and have distinct characteristics.

  - **Operational Layer:** Repeaters operate at the physical layer (Layer 1) of the OSI model. They amplify and retransmit signals without understanding the data packets they carry.
  - **Signal Boosting:** Repeaters amplify signals, increasing their strength before retransmission. They are used in both wired and wireless networks to extend coverage.

- ✓ **Firewall**

  A firewall is a network security device or software that monitors and controls incoming and outgoing network traffic based on predetermined security rules. It helps protect the network from unauthorized access and cyber threats.

- ✓ **Rack Mount**

  Rack mounts are enclosures or mounting brackets used to house and organize network equipment within a standard server rack or cabinet. They allow for efficient use of space and easy access to equipment.

- ✓ **Bill of Quantities (BoQ)**

  A Bill of Quantities (BoQ) is a detailed document that lists all the materials, labor, and equipment required for a project, along with their respective quantities and costs. It serves as a key tool in construction, infrastructure, and network deployment projects, providing a structured breakdown of all components needed for completion.

3.1. Key Features:

- ✓ **Itemization**

The BoQ specifies every material, component, or piece of equipment needed for the project.

- ✓ **Costing**

  Along with the quantities, the BoQ includes estimated costs for each item or task, allowing for accurate budgeting.

- ✓ **Labor**

  It often includes labor costs based on estimated hours or effort required for different tasks.

- ✓ **Quantities**

  It provides precise measurements or counts of each item, ensuring accurate procurement.

Note The header in a Bill of Quantities (BoQ) is crucial as it provides key information that frames the context of the document and helps identify important project details. Here are the main reasons why the header is important:

1. Project Identification

- The header clearly identifies the project, including the name, location, and type of work (e.g., "Wireless Outdoor Network Project for Nyandungu Urban Wetland Ecotourism Park").
- This ensures that the BoQ is correctly linked to the specific project, especially in cases where multiple projects are handled by the same contractor or team.

2. Client and Contractor Information

- The header often includes the name of the client (the organization or individual who requested the project) and the contractor or supplier responsible for creating the BoQ.
- This clarifies the parties involved and can be useful for accountability, communication, and reporting purposes.

3. Date and Version Control

- Including the date in the header allows for version control. As projects progress, multiple revisions of the BoQ may be required, and having a clear date helps avoid confusion over which version is current.
- This is particularly important in dynamic projects where costs, quantities, and specifications may change over time.

4. Reference for Documentation

- The header serves as a reference for other project-related documents such as contracts, invoices, and progress reports. It provides essential context for anyone reviewing the document, such as auditors, accountants, or project managers.

- It makes it easier to cross-reference with other project documents.

5. Clarity and Professionalism

- A well-structured header enhances the professionalism of the BoQ, making it clear, easy to understand, and visually organized.
- It contributes to the overall organization of the document, helping stakeholders navigate the details more easily.

6. Legal and Contractual Significance

- In many cases, the BoQ is a formal part of a contract or tender document.

  The header ensures that all relevant details, such as project name, client, contractor, and date, are present, providing legal clarity about what the document covers.

Example of bill of quantity

XYZ Company Bill of Quantities for Networking Devices

Date: 22/10/2024

Project Location: Kigali-Gasabo

Prepared by: K J

Contact Information: 0788000000

Summary:

Networking Devices:

Description	**Quantity**	**Unit Price (USD)**	**Total Cost (USD)**
Cisco Catalyst 3850 Switch	5	2,000.00	10,000.00
Cisco ISR 4451 access point	2	6,000.00	12,000.00
Yagi Antenna TP-Link TL-	20	150.00	3,000.00

ANT2424B			
Parabolic Grid Antenna Ubiquiti AirGrid M5 HP	3	1,500.00	4,500.00
Cisco ASA 5506-X Firewall	1	3,500.00	3,500.00
Ethernet cable cat 8	50meter	800.00	1,600.00
Wife extend TP-Link RE650 AC2600	1	1,200.00	1,200.00
APC Smart-UPS 1500VA UPS	5	500.00	2,500.00
Subtotal for Networking Devices			**$38,800.00**

Other Expenses, Subtotals, and Grand Total:

Expense	**Subtotal (USD)**
Networking Devices	$38,800.00

Cabling and Installation	$10,000.00
Configuration and Labor	$7,500.00
Grand Total (Including Markup)	**$56,300.00**

Practical Activity 1.2.2: Producing bill of quantity

Task:

1: Read and perform this activity

Referring to survey report that was produced in the previous practical activities (1.1.3).you are requested to produce bill of quantity of all requirement needed for deploying wireless network outdoor

2: Listen to the instructions given by trainer
3: Follow the demonstrations process of producing bills of quantity
4: Perform the activity of step 3 by following the procedures.
5: Ask questions if necessary
6: Read the key readings 1.2.2 and perform the application of learning 1.2

Key readings 1.2.2: Producing bill of quantity

Producing bill of quantity

network deployment projects, providing a structured breakdown of all components needed for completion

Step 1:Create a List

Identify all materials and equipment required for the project based on the site survey finds.

Step 2:Specify Quantities

Calculate the amount of each item needed based on the site survey and project requirements.

Step 3: Cost Estimation

- Research current market prices for each item on your list.
- Use the formula for each item and sum them up
- Estimate the cost of labor required for installation, configuration, and testing.

Step 4: Add Contingency

Add a contingency amount (typically 5-10% of the total cost) to cover unexpected expenses or price fluctuations.

Step 5: Compile the BoQ

- Present the items in a clear, itemized format, including descriptions, quantities, unit prices, and total costs.
- Double-check the quantities and prices to ensure accuracy and completeness.

Step 6: Presentation

- Summarize the BoQ in a formal report or spreadsheet format.
- Provide explanations for the quantities and costs where necessary, especially for significant items.

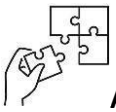
Step 7: Feedback and Revision

- Present the BoQ to peers or instructors for review and feedback.
- Make any necessary adjustments based on feedback or new information.

Points to Remember

- Materials are the physical components and substances used to construct and install the wireless infrastructure
- Equipment refers to the tools and devices used to install, test, and manage the wireless outdoor network
- While describing tools equipment and materials, identify the specifications of each based on functionality
- Some tools, materials and equipment differ from their type, manufacturer and the use case
- A Bill of Quantities (BoQ) is a detailed document that lists all the materials, labor, and equipment required for a project, along with their respective quantities and costs.
- The key steps involved in producing a bill of quantity

- ✓ Create a List
- ✓ Specify Quantities
- ✓ Cost Estimation
- ✓ Add Contingency
- ✓ Compile the BoQ
- ✓ Presentation
- ✓ Feedback and Revision



Application of learning 1.2.

A non-profit organization plans to establish a community center in a remote rural area in Rwanda. They require a reliable and efficient wireless network to provide internet access to the community members. You are required to identify all required materials, equipment and produce a bill of quantity.

Indicative content 1.3: Design Wireless Network Topology

Duration: 6 hrs

Theoretical Activity 1.3.1: Description of wireless network topology

Tasks:

1: Answer the following questions relating to related to wireless topology

i. Define network topology

ii. Describe Network topology types

iii. Identify Advantages and disadvantages of wireless topology

iv. Identify network designing tools

2: Write your findings on reserved space

3: Present your findings in front of a whole class

4: Take short notes on given expert view and clarifications

5: Read the **key readings 1.3.1** in this manual

Key readings 1.3.1.: Description of wireless network topology

Description of wireless network topology

Network topology refers to the arrangement or layout of various elements (such as nodes, links, routers, and switches) in a computer or communication network. The topology defines how different devices in a network are connected and how data is transmitted between them. It plays a critical role in the performance, reliability, and scalability of the network.

1. Wireless Network Topology Types

1.1. Infrastructure Mode:

In this mode, wireless devices connect to a central wireless access point (AP) or multiple APs connected to a wired network.

Advantages:

- Centralized management and control of wireless connections.
- Easy to add or remove devices.
- Effective for larger networks with multiple users and devices.

Disadvantages:

- Single points of failure in the form of APs.
- Limited to the coverage area of the APs.

1.2. Ad-Hoc Mode (Peer-to-Peer):

Devices communicate directly with each other without the need for a central AP. Often used for peer-to-peer connections between devices.

Advantages:

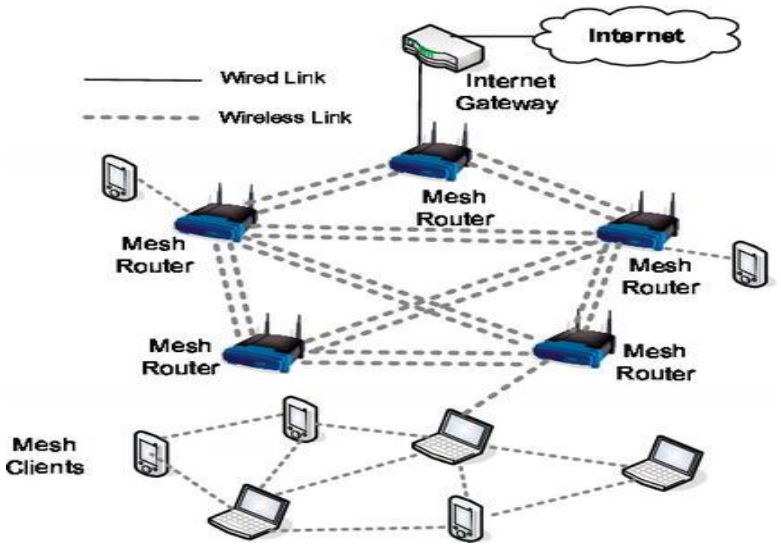
- No need for central infrastructure; devices can connect spontaneously.
- Useful for small, temporary networks or device-to-device communication.

Disadvantages:

- Limited scalability; not suitable for larger networks.
- Security concerns due to the absence of a central authority.

1.3. Mesh Topology:

Devices are interconnected in a mesh-like fashion, allowing multiple paths for data transmission. Mesh networks can be either fully meshed or partially meshed.



Advantages:

- High redundancy and fault tolerance; network remains operational even with device or link failures.
- Self-healing capabilities; data can reroute through alternate paths.

Disadvantages:

- Complex to configure and manage due to multiple connections.

- Costlier to implement due to the need for multiple devices.

1.4. Hybrid Topology:

A combination of different topologies, such as infrastructure and ad-hoc modes.

Advantages: Flexibility to suit various network requirements.

Disadvantages: complex to manage

2. Advantages of Wireless Network Topologies

- **Mobility**: Wireless networks provide the flexibility for devices to connect and move freely within the coverage area.
- **Ease of Installation**: Wireless networks eliminate the need for physical cables, simplifying installation and reducing infrastructure costs.
- **Scalability**: Wireless networks can be easily expanded by adding more access points to increase coverage or capacity.
- **Convenience**: Wireless networks are suitable for environments where it's challenging or impractical to lay physical cables, such as historic buildings or outdoor areas.
- **Adaptability: Wireless networks can adapt to changing network demands and reconfigure themselves dynamically.**

3. Disadvantages of Wireless Network Topologies:

- **Limited Range**: Wireless signals have limited range, and coverage can be affected by physical obstacles and interference.
- **Interference**: Wireless networks are susceptible to interference from other electronic devices, neighboring networks, and physical obstacles.
- **Security Concerns**: Wireless networks can be vulnerable to unauthorized access and security breaches if not properly secured.
- **Slower Speeds**: In some cases, wireless connections may offer slower data transfer speeds compared to wired connections.
- **Reliability**: Wireless networks may be less reliable than wired networks in environments with high interference or congestion.
- **Complexity**: Setting up and managing wireless networks, especially larger ones, can be complex and may require expertise.

4. Network designing tools

Network designing tools are software applications or platforms used by network engineers and architects to plan, design, and visualize network architectures. These tools help in creating network diagrams, simulating network performance, managing IP addresses, and ensuring optimal configurations. They can also assist in assessing the impact of changes, troubleshooting, and documenting the network design.

4.1. Cisco Packet Tracer

Cisco Packet Tracer is arguably the most well-known network simulation tool, especially among networking students and professionals preparing for Cisco certifications.

✓ **Key Features**:

- Simulates Cisco devices (routers, switches, firewalls) and configurations.
- Intuitive drag-and-drop interface to design topologies.
- Built-in support for testing routing protocols (e.g., OSPF, EIGRP, RIP) and VLANs.
- Real-time and simulation modes for viewing live data flow.

✓ **Best For**

Learning and preparing for Cisco certifications (CCNA, CCNP), building and testing network topologies before deployment.

4.2. GNS3 (Graphical Network Simulator 3)

GNS3 is widely recognized for its ability to simulate real network devices and supports a wide range of network hardware and software, not just Cisco.

✓ **Key Features**:

- Emulates real-world hardware using real Cisco IOS images and other network operating systems (Juniper, Palo Alto, etc.).
- Supports complex network topologies, including multi-vendor setups.
- Integration with real hardware for hybrid physical-virtual simulations.
- Open-source and community-driven.

✓ **Best For**

Advanced network professionals and engineers simulating real-world network environments with real OS images.

4.3. Microsoft Visio

Microsoft Visio is a household name in network design, known for its ease of use in creating **visual network diagrams**. It's part of the Microsoft Office suite and is widely used for network documentation and presentations.

✓ **Key Features**:

- Large library of pre-built networking symbols (routers, switches, firewalls, etc.).
- Easy-to-use drag-and-drop interface.
- Extensive template library for creating various types of network diagrams.
- Integrates with Microsoft Office for professional reporting.

✓ **Best For**

Creating professional, visual network diagrams and documentation for IT

managers and network engineers.

4.4. SolarWinds Network Topology Mapper

SolarWinds is well-known in the IT world for its **network monitoring** and management tools, and the Network Topology Mapper is a key part of its ecosystem. It automatically maps existing networks, saving network administrators a lot of time.

✓ **Key Features**:

- Automatic network discovery and topology mapping.
- Layer 2 and Layer 3 mapping capabilities.
- Export maps to Visio for documentation.
- Real-time network monitoring with performance data.

✓ **Best For**

IT administrators who need automatic network mapping and real-time monitoring of their environments.

4.5. IDraw Max

is a professional drawing and diagramming software used for creating network diagrams, flowcharts, business process diagrams, and other technical illustrations. It is particularly popular in industries where clear and detailed visual documentation is required, including IT and engineering.

✓ **Key Features:**

- **Extensive Templates**: Offers a wide range of pre-designed templates and shapes for quick diagram creation.
- **Customizable**: Users can easily customize shapes, colors, and sizes to fit specific needs.
- **Export Options**: Supports multiple export formats, including PNG, JPEG, and PDF.
- **User-Friendly Interface**: Intuitive drag-and-drop functionality makes it accessible for beginners.
- **Collaboration Tools**: Allows for easy sharing and collaboration with team members.

✓ **Best For**

IDraw Max is ideal for professionals and teams looking to create clear, professional diagrams for presentations, project planning, or network design without needing extensive graphic design skills.

Practical Activity 1.3.2: Designing wireless network topology

Task:

1: Read carefully and perform this activity

Based on the survey report which is produced in practical activity 1.1.3, design a topology of wireless network outdoor using any designing software that is available in the computer lab.

2: Listen to the instructions given by trainer and then follow the demonstrations process of designing wireless network topology

3: Perform the activity by following the procedures performed by the trainer.

4: Present the work done to the trainer

5: Ask questions if necessary

6: read the key readings 1.3.2 and perform the application of learning 1.3

Key readings 1.3.2: Designing wireless network topology

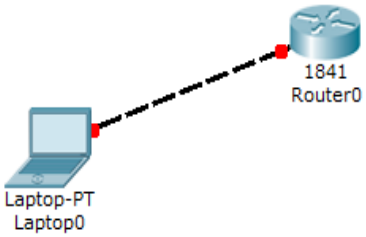
Designing wireless network topology

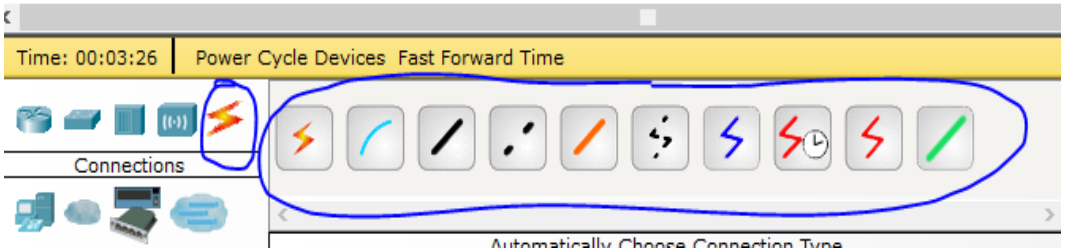
Wireless network topology determining how devices communicate with each other without physical connections.

1: **Identify Key Components**

Select all devices and components of the network:

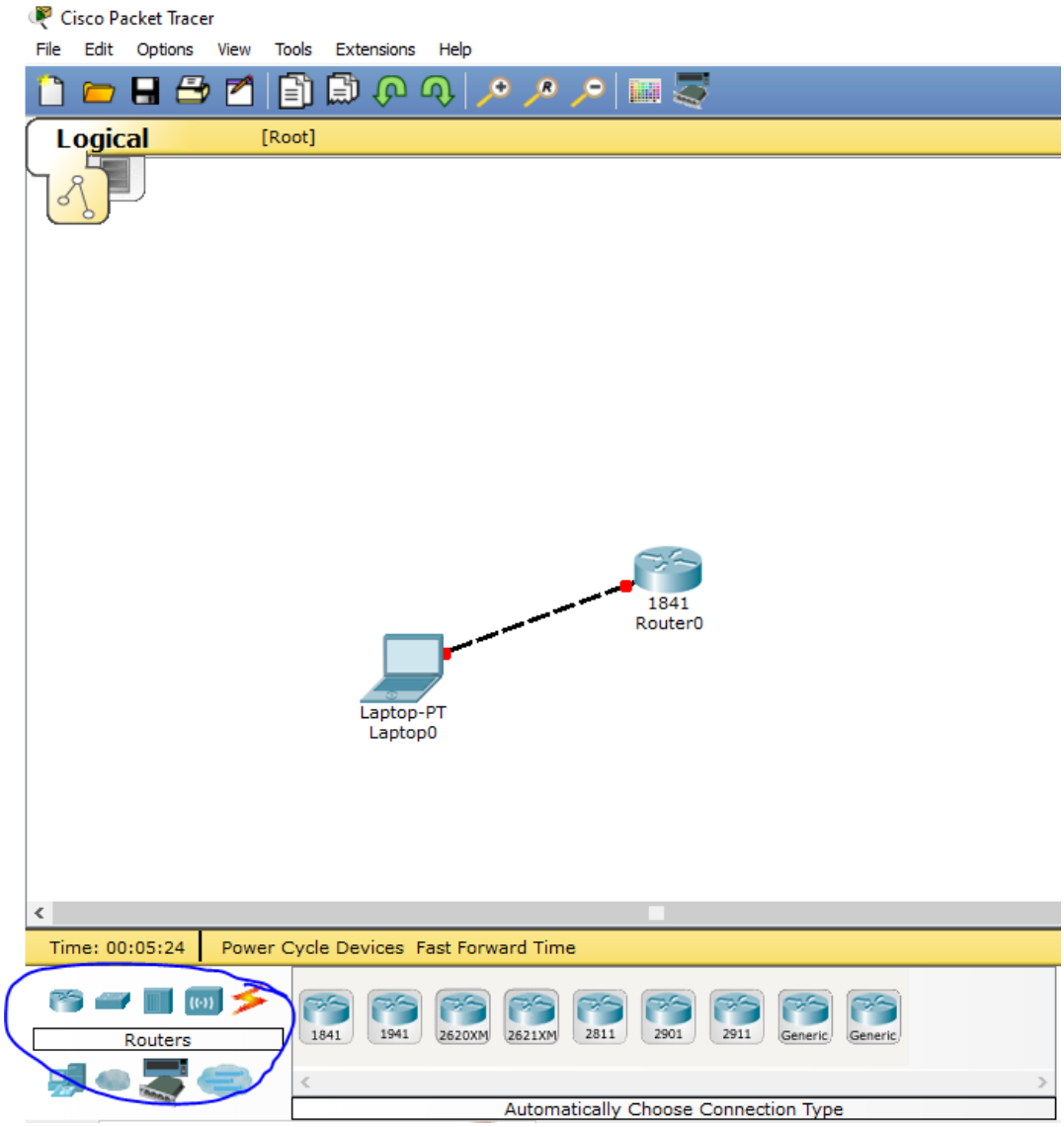
- **Access Points (APs)**: Central devices for infrastructure mode.
- **Client Devices**: Laptops, smartphones, tablets, etc.
- **Routers/Switches**: For wired connections and network management.
- **Network Interface Cards (NICs)**: Wireless NICs for client devices.
- **Cabling and Power Sources**: For APs and other hardware.





2: **Connected**

Connect device appropriate according to transmission medium (wired or wireless).



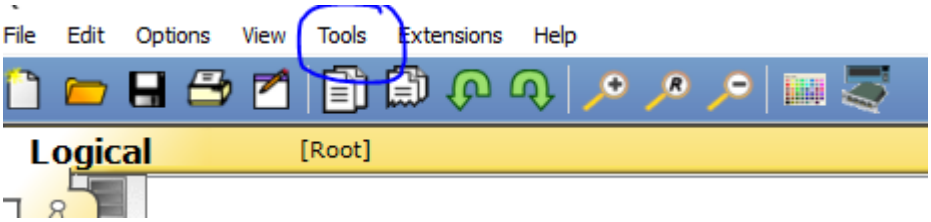
3: **Labeling**

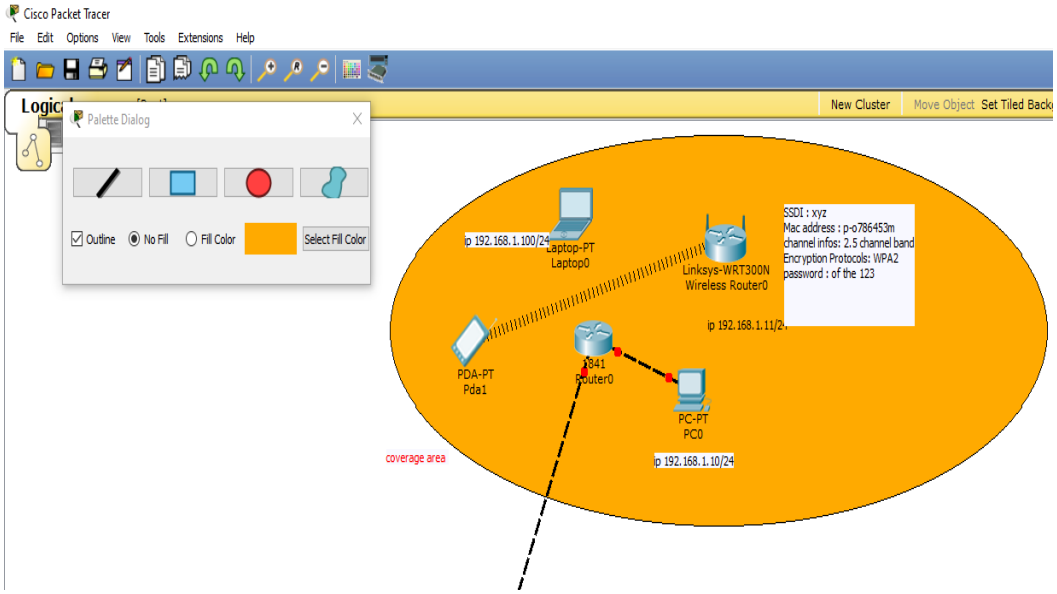
✓ Label all component

✓ Indicate coverage areas for each AP:

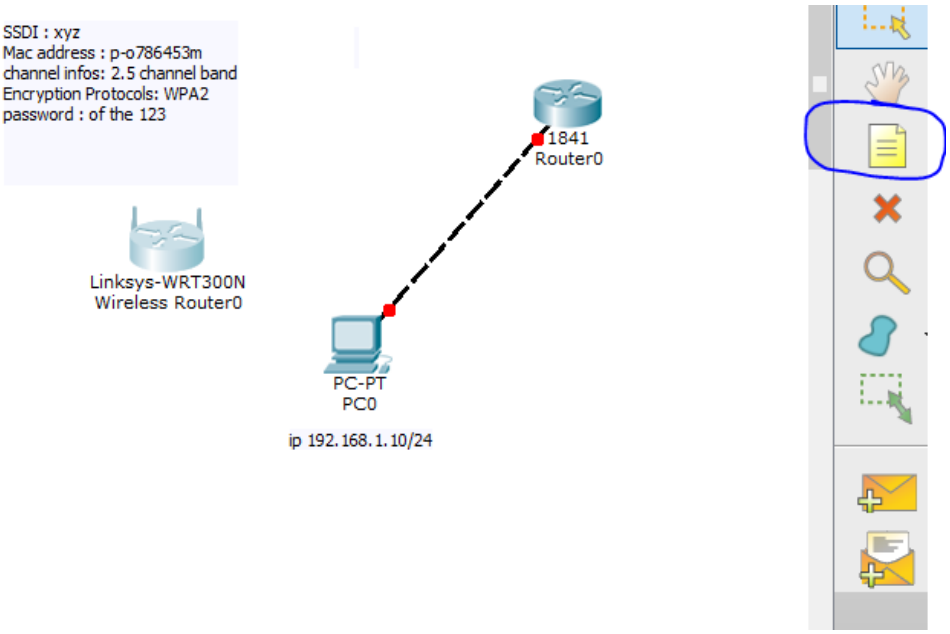
- Basic Service Area (BSA): Define the coverage range of each AP.
- Use shading or color coding on the diagram to represent areas of overlap or dead zones.

Go to tool>drawing palette ?





Or



4: **Document Configuration Details**

✓ document relevant configuration details:

- **SSID (Service Set Identifier)**: The name of the wireless network.
- **BSSID (Basic Service Set Identifier)**: The MAC address of the AP.
- **Channel Information**: Specify the channels used by each AP to avoid interference.
- **IP Addressing Scheme**: Outline the IP addressing used for devices on the

network.

✓ Include Security Features

- **Encryption Protocols:** WPA2, WPA3, etc.
- **Access Control Lists (ACLs):** Define who can access which parts of the network.
- **Guest Networks:** If applicable, indicate separate SSIDs for guest access.

5: **Review and Validate**

Ensure that all components are accurately represented and labeled:

- **Peer Review**: Have team members review the documentation for accuracy.
- **Test Connectivity**: Verify that all connections work as intended.

6: **Maintain Documentation**

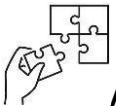
Keep your documentation up to date:

- **Regular Updates**: Modify diagrams and documentation as changes occur in the network.

Points to Remember

- Network topology refers to the arrangement or layout of various elements (such as nodes, links, routers, and switches) in a computer or communication network.
- Wireless Topologies Include Infrastructure Mode, Ad-Hoc Mode, Mesh Topology, and Hybrid each with unique advantages and challenges.
- Advantages of Wireless Networks is Mobility, ease of installation, scalability, convenience, and adaptability.
- Disadvantages of Wireless Networks is Limited range, interference, security concerns, slower speeds, and complexity.
- Network designing tools are software applications or platforms used by network engineers and architects to plan, design, and visualize network architectures
- Design Tools like Cisco Packet Tracer, GNS3, Microsoft Visio, and Solar Winds help in designing, simulating, and documenting network topologies**.**
- Wireless network topology determining how devices communicate with each other without physical connections.
- The key steps involved in designing Wireless network topology
    - ✓ Identify Key Components

- ✓ Connected
- ✓ Labeling
- ✓ Document Configuration Details
- ✓ Review and Validate
- ✓ Maintain Documentation



Application of learning 1.3.

You are tasked by your school to Design a wireless outdoor network topology of your school that combine sport field area and staff department using one of the designing tools available in the computer lab.

Learning outcome 1 end assessment

Written assessment

Section A: Read the following statement and answer by TRUE if is correct otherwise by FALSE

1. A wireless network's coverage area is the total area that the network can serve effectively.
2. The frequency spectrum used in outdoor wireless networks is limited to 2.4 GHz only.
3. Directional antennas can focus signal strength in a specific direction, making them useful for long-distance communication.
4. Public Wi-Fi hotspots are typically designed for high-security applications.
5. A radio frequency site survey helps assess potential interference sources in a wireless network.
6. Bandwidth refers to the maximum data transfer rate of a network.
7. Outdoor access points require weatherproofing to ensure durability in harsh environmental conditions.
8. A repeater is used to amplify and extend the range of a wireless signal.
9. Analysing site survey findings helps determine the best placement for antennas.
10. The firewall is used to enhance the physical security of a wireless network.

Section B: Multiple Choice Questions: Select the right answer

Circle the letter corresponding to the correct answer

1. Which of the following is NOT a type of outdoor antenna?
    a) Omni-directional
    b) Bi-directional
    c) Sub-directional
    d) Directional
2. What is the main purpose of a lightning arrestor in an outdoor network?
    a) To increase signal strength
    b) To protect equipment from lightning strikes
    c) To extend the coverage area

d) To connect multiple devices

3. What type of network topology connects all devices to a central hub?
    a) Mesh
    b) Star
    c) Ring
    d) Bus
4. Which application would most likely utilize wireless surveillance?
    a) Smart home automation
    b) Public Wi-Fi
    c) Smart city infrastructure
    d) Remote connectivity
5. When conducting a site survey, which factor is most important for determining network coverage?
    a) Number of users
    b) Frequency interference
    c) Type of devices
    d) Bandwidth
6. What does UPS stand for in networking equipment?
    a) Uninterruptible Power Supply
    b) Universal Power System
    c) United Power Supply
    d) Unifying Power Source
7. Which material is commonly used for outdoor network cables?
    a) PVC
    b) Fiber optic
    c) Teflon
    d) Polyethylene
8. In a wireless network, which element manages the data traffic?
    a) Repeater
    b) Network switch
    c) Firewall
    d) Antenna

9. What is the main disadvantage of a mesh topology?
    a) Complexity
    b) Cost
    c) Redundancy
    d) Scalability
10. For which application is weatherproofing particularly important?
    a) Indoor networks
    b) Remote connectivity
    c) Smart city infrastructure
    d) Outdoor access points

Section C Match the following terms with their descriptions by writing the letter corresponding to the correct description

Answer	Term	Description
1……..	**1.** Antenna Types	**A.** A document listing materials and costs for a project
2…….	**2.** Interference Management	**B.** Ability to expand a network as needed
3……..	**3.** Public Wi-Fi Hotspot	**C.** Device that directs data traffic between devices
4…….	**4.** Radio Frequency Site Survey	**D.** Survey that identifies potential signal issues
5……..	**5.** Scalability	**E.** Provides security by monitoring incoming and outgoing traffic
6……..	**6.** Power-Over-Ethernet (PoE)	**F.** Outdoor location providing internet access to the public
7…….	**7.** Network Switch	**G.** Use of antennas to focus or disperse signal
8……..	**8.** Remote Connectivity	**H.** System to manage and reduce signal interference
9…….	**9.** Firewall	**I.** Connects devices and provides power over Ethernet cables
10……..	**10**. Bill of Quantities	**J.** Enables users to access the network from different locations

Practical assessment

You have been hired by a city council to design an outdoor wireless network of public Wi-Fi hotspots. Your task is to assess the area then identify requirements, select appropriate materials and equipment, create a bill of quantity and create a topology diagram.

END

References

Adams, G. (2022, March 18). Effective Upgrading of Wireless Networks. Retrieved from IT Network Guides: www.itnetworkguides.com/upgrading-wireless

Brown, D. (2023, June 25). Troubleshooting Outdoor Wireless Networks. Retrieved from Network Troubleshooting: www.networktroubleshooting.com/outdoor

Brown, S. (2023, June 20). RF Site Survey Best Practices. Retrieved from Network World: www.networkworld.com/rf-site-survey

Doe, J. (2023, October 10). Outdoor Wireless Networks. Retrieved from Network Solutions: www.networksolutions.com/outdoor-wireless

Johnson, A. (2023, September 10). Monitoring Wireless Networks. Retrieved from Network Performance Solutions: www.networkperformancesolutions.com/monitoring

Johnson, E. (2022, August 15). Designing a Public Wi-Fi Network. Retrieved from Wi-Fi Alliance: www.wi-fi.org/public-network-design

Lee, B. (2023, August 5). Understanding Signal Strength and SNR. Retrieved from Wireless Tech Insights: www.wirelesstechinsights.com/signal-strength

Miller, F. (2023, April 30). Analyzing Packet Loss in Wireless Networks. Retrieved from Network Analysis Today: www.networkanalysistoday.com/packet-loss

Roberts, A. (2023, February 8). Weatherproofing Outdoor Equipment. Retrieved from Tech Innovations: www.techinnovations.com/weatherproofing

Smith, C. (2022, July 15). Tools for Monitoring Wi-Fi Performance. Retrieved from Tech Monitoring Hub: www.techmonitoringhub.com/wifi-tools

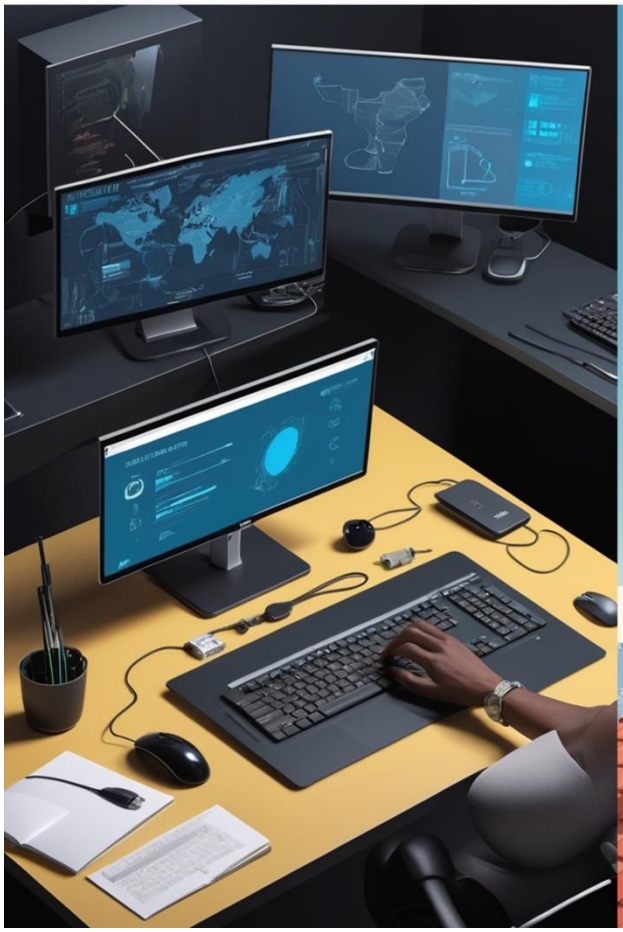
Smith, J. (2023, September 25). Understanding Wireless Technologies. Retrieved from TechRadar: www.techradar.com/wireless-tech

White, E. (2023, May 20). Firmware Management for Wi-Fi Devices. Retrieved from Cybersecurity Best Practices: www.cybersecuritybestpractices.com/firmware

White, L. (2022, April 18). Interference in Wireless Networks. Retrieved from TechSpot: www.techspot.com/interference

Wilson, J. (2023, December 1). Documenting Wireless Network Changes. Retrieved from IT Documentation Hub: www.itdocumentationhub.com/wireless

Wilson, T. (2023, May 30). Antenna Types Explained. Retrieved from Antenna World: www.antennaworld.com/types



Indicative contents

2.1 Selection of tools, Materials and Equipment

2.2 Installation of wireless network devices

2.3 Configuration of wireless devices

2.4 Testing of deployed wireless network outdoor

Key Competencies for Learning Outcome 2 : Deploy wireless network outdoor

Knowledge	Skills	Attitudes
● Identification of tools, materials and equipment used in deploying wireless network outdoor ● Description of wireless standards used in wireless network outdoor ● Description of Wireless Network Outdoor-Specific Features ● Description of wireless network devices configurations parameters	● Selecting tools, Materials and Equipment used in deploying wireless network outdoor ● Mounting network equipment ● Making and testing network cable ● Connecting network devices ● Configuring wireless network devices ● Testing deployed wireless network outdoor	● Being Attention to Detail when Selecting tools, Materials and Equipment and mounting them in proper space ● Being Patience and Perseverance while deploying and testing wireless outdoor network ● Having Problem-Solving Mindset during mounting network devices ● Being Analytical Thinker reviewing configuration options such as SSID, channels, security protocols (e.g., WPA3), and bandwidth.

Duration:40 hrs

Learning outcome 2 objectives:

By the end of the learning outcome, the trainees will be able to:

1. Identify correctly tools, materials and equipment used in deploying wireless network outdoor
2. Select appropriately tools, materials and equipment used in deploying wireless network outdoor
3. Mount correctly wireless network components based on the user requirements
4. Describe clearly Wireless Network Outdoor-Specific Features based on manufacturers standard
5. Describe clearly wireless network devices configurations parameters based on device specification
6. Perform correctly network cabling based on device placement
7. Configure correctly wireless network devices based on network standard
8. Test correctly the deployed outdoor wireless network

Resources

Equipment	Tools	Materials
● Access points ● Router ● Repeater ● Wireless Extender ● Antennas ● Firewall ● PoE ● Switch ● Rack amount	● Edrawmax ● Draw.io ● Cisco packet tracer ● Lucidchart	● Connector ● Network Cables ● Cable ties ● Screws ● Internet Bundles ● Nails

● Computer ● UPS ● Lightning Arrestor		

Indicative content 2.1 : Selection of Tools, Materials and Equipment

Duration: 5 hrs

Theoretical Activity 2.1.1: Description of tools, materials and equipment used in deploying wireless network outdoor

Tasks:

1: Answer the following questions

i. Differentiate these key terms: tools, materials and equipment

ii. Describe these tools and mention their role in wireless network outdoor deployment:

a. Cutting tools

b. Patching tools

c. Crimping tools

d. Drilling tools

e. Testing tools

f. Fixing tools

2: Write your findings on reserved space

3: Present your findings in front of a whole class

4: Take notes for the clarifications given

5: Read key readings 2.1.1 and address question if any.

Key readings 2.1.1.: Description of tools, materials and equipment used in deploying wireless network outdoor

Description of tools, materials and equipment used in deploying wireless network outdoor

1. **Difference between tools, materials and equipment:**

1.1. Tools: Instruments or devices used to perform specific tasks.

- ✓ Purpose: Tools are often handheld and assist in performing precise or manual tasks.
- ✓ Examples: Hammer, wrench, screwdriver, measuring tape, power drill.

1.2. Materials: Raw or processed substances used to construct, build, or manufacture products.

- ✓ Purpose: Materials are the components or ingredients that are transformed or combined to create the final product.
- ✓ Examples: Connectors, cable manager(Tiers, clips, Sockets),Ethernet cables

1.3 Equipment: Larger, more complex machinery or devices used in various operations.

- ✓ Purpose: Equipment typically involves more advanced technology and is used for tasks that cannot be done efficiently with hand tools alone.
- ✓ Examples: Outdoor access points, Antennas, Network switch, routers, repeater, Rack mount.

2. Description of tools used and its role in wireless network outdoor deployment

2.1. Cutting Tools: Tools used to cut through cables, wires, or other materials during installation. These tools are used to trim cables to the proper length, remove insulation from wires, and make precise cuts for proper cable management in outdoor installations.

- ✓ **Examples:**

Cable cutters

Used to cut through cables and wires. They are designed to cleanly cut through various types of cables, including electrical cables, coaxial cables, and network cables, without crushing or fraying the wire

Wire strippers:

Designed to remove the insulation from electrical wires without damaging the conductors inside. This is crucial for making proper connections during electrical or network installations.

- Utility knives: used for cutting a variety of materials, including cable jackets, insulation, tape, and other packaging. They are versatile tools useful in many tasks beyond just working with cables.

2.2. Patching Tools: Tools used to connect and secure network cables, typically in patch panels or outlets. These tools are crucial for terminating cables in outdoor environments, ensuring secure connections between different sections of the network.

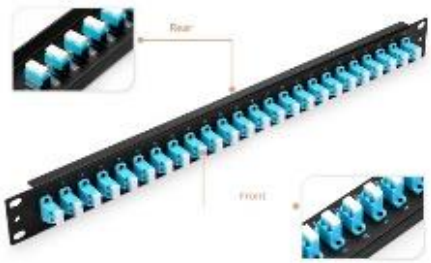
✓ **Examples:**

- **Punch-down tools:** A punch-down tool is a hand tool used primarily in telecommunications and networking to connect wires to specific types of connectors, such as patch panels, keystone jacks, and punch-down blocks. It is essential for terminating twisted pair cables (like Cat5, Cat6, and Cat6a) when setting up network infrastructure.

- **Patch panels.**

  A patch panel is a hardware device that acts as a central point for managing and organizing network cables. It is used in structured cabling systems for

data, voice, and sometimes video networks, providing a way to connect different devices, such as computers, routers, and switches, within a network.



2.3. Crimping Tools: Tools used to attach connectors, like RJ45, to cables by compressing or crimping them. Crimping tools are used to secure connectors to cables, such as Ethernet or coaxial cables, ensuring reliable signal transmission in outdoor network deployments.

✓ **Examples:**

- RJ45 crimping tools
- Coaxial crimpers.

2.4. Drilling Tools: Power tools designed to create holes in surfaces, often for mounting hardware or routing cables.

✓ **Examples:**

- Electric drills
- hammer drills
- Cordless drills.

✓ **Role in Deployment:**

- Drilling tools are used to mount antennas, brackets, or other network hardware on outdoor walls, poles, or other structures. They may also be used to route cables through walls or other barriers.

2.5. Testing Tools: Tools used to check and verify the functionality of network installations, including signal strength and cable integrity.

✓ **Examples**: Cable testers, spectrum analyzers, signal meters.

✓ **Role in Deployment:**

- Testing tools ensure that the wireless network is functioning optimally by verifying proper connections, signal quality, and overall network performance.

2.6. Fixing Tools: Tools used to fasten and secure network components in place.

✓ **Examples:** Screwdrivers, wrenches, cable ties, fasteners.

✓ **Role in Deployment:**

- Fixing tools are necessary for securely mounting wireless access points, antennas, or other hardware. They help ensure that components are fixed properly to withstand outdoor conditions like wind or rain.

Practical Activity 2.1.2: Selecting tools, materials and equipment

Task:

1: Read carefully and perform this task

Refer to the practical activity 1.1.2 and 1.3.2, select tools, materials and equipment that will be used to deploy the wireless network outdoor.

2: Follow the trainer's work instruction

3: Based on the work instructions given by your trainer, select tools, materials and equipment as seen in design.

4: Verify whether all needed tools, materials and equipment are selected

5: For more clarifications read the key readings 2.1.2 and do the application of learning 2.1

Key readings 2.1.2: Selecting tools, materials and equipment

Selecting tools, materials and equipment

1. Selecting tools, materials and equipment require the various steps including

1.1. Analyze the Survey Report and Network topology

Before selecting tools, materials, and equipment, you need to review the survey report and Network topology in detail.

- Key aspects to consider:
  - ✓ Site Layout: Distance and Coverage
  - ✓ Obstacles and Interference
  - ✓ Environmental Conditions
  - ✓ Power and Cabling

1.2. Selection of Tools:

Choose tools for cutting, connecting, testing, and securing the network hardware.

- Key features to consider when selecting tools

- ✓ Durability and Weather Resistance:
- ✓ Portability: Tools used in outdoor deployments should be easy to transport, as the technician may need to carry them over long distances or to elevated locations.
- ✓ Precision and Versatility:
  - **Multi-functionality:** Tools that serve multiple purposes (e.g., combo crimpers/strippers) reduce the need to carry multiple devices and simplify tasks in the field.
  - **Accuracy**: Precision is essential for tasks like cutting cables to the correct length, ensuring proper terminations, and accurate alignment when mounting antennas or access points.

1.3. Selection of Materials:

Choosing durable, weather-resistant materials is critical for an outdoor wireless deployment.

- **Key features to consider when selecting Materials**

✓ **Environmental Resilience:**

- Cables and enclosures should be UV-resistant to prevent degradation from long-term sun exposure.
- Waterproofing: Materials used in cable jackets, connectors, and enclosures must be water-resistant to handle rain, snow, and humidity.
- Temperature Resistance: Ensure materials can withstand extreme temperatures, both hot and cold, especially in areas with variable climates.

✓ **Durability and Strength:** Materials like cables and conduits must withstand wear and tear from outdoor conditions, including sharp surfaces, weather, and possible animal interference.

- Materials should have sufficient strength to resist stretching, pulling, or bending, especially for long cable runs in outdoor environments.

✓ **Shielding and Interference Protection:**

- Shielded Cables: For areas with high electromagnetic interference (EMI) or radio-frequency interference (RFI), use shielded cables to protect the network from interference and ensure data integrity.
- Surge Protection: Outdoor installations should include surge-protected cables or grounding systems to protect against lightning strikes and power surges.

1.4. Selection of Equipment:

✓ Select the best Wireless Access Points (APs)

✓ Select Antennas:

- Omnidirectional Antennas: For broad coverage in open spaces (playgrounds,

courtyards).

- Directional Antennas: For focused coverage in areas where more concentrated signals are required, such as along corridors or outdoor areas between buildings.

✓ Select Power over Ethernet (PoE) Switches:

✓ Select Network Switches:

- Switches with sufficient ports and bandwidth to handle the connections from all access points.
- Managed switches with VLAN and QoS support are recommended for network control.

✓ Surge Protectors: Devices to protect sensitive equipment from electrical surges, particularly in areas prone to lightning.

Note: While doing selection , pay attention also on Cost and Budget

✓ **Equipment Cost**: Ensure the selected tools, materials, and equipment fit within the school's budget while meeting performance and durability requirements.

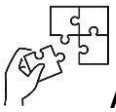
✓ **Licensing and Support**: Consider whether the APs or network switches require additional software licenses or subscription services for management and support.

✓ **Maintenance Costs**: Evaluate long-term maintenance costs for weatherproofing, replacing damaged components, and upgrading network equipment as needed.

Points to Remember

- While describing tools equipment and materials, identify the specifications of each based on manufacturer
- Tools are often handheld and assist in performing precise or manual tasks.
- Materials are the components or ingredients that are transformed or combined to create the final product
- Equipment typically involves more advanced technology and is used for tasks that cannot be done efficiently with hand tools alone.
- tools, materials and equipment differ from their type, manufacturer and the use case
- Some tools, materials and equipment are of the same types, you need to provide clear identifications and specifications to differentiate them.
- Before selecting tools, materials, and equipment, you need to review the survey report and network topology in detail.

- While selecting tools, materials and equipment, consider the Environmental Conditions, Coverage Area and Range, Frequency Bands and Spectrum Availability, Network Equipment Specifications to ensure reliable performance, coverage, and durability.
- When selecting tools consider the Durability and Weather Resistance, Portability, Precision and Versatility
- When selecting materials consider the Environmental Resilience, Durability and Strength, Shielding and Interference Protection
- When selecting equipment consider the Licensing and Support, Equipment Cost and Maintenance Costs
- Bad selections result in failed deployment, thus ensure that the tools, materials and equipment you select are the best for deployment



Application of learning 2.1.

LMT Cyber café located near of your school has recently conducted a site visit for the new a reliable and weather-resistant wireless outdoor deployment. The survey report and the network design were obtained. The manager of café need you to go in their store and select the necessary tools, materials, and equipment for deploying a reliable and weather-resistant outdoor wireless network.

Indicative content 2.2: Installation of Wireless Network Devices

Duration: 15 hrs

Theoretical Activity 2.2.1: Description of wireless standards

Tasks:

1: Respond to the following questions

i. Describe these wireless network standard, their applications and their use case. Along with these details, give the advantage and disadvantages for each.

   a. IEEE802.11a

   b. IEEE802.11b

   c. IEEE802.11n

   d. IEEE802.11ac

   e. IEEE802.11ax

2: Write your answers on paper or flipchart

3: Share your answers with other members of your group

4: Present your answers in front of a whole class

5: Ask questions or clarification if any

6: Read key readings 2.2.1 for more clarification

Key readings 2.2.1.: Description of wireless standards

Description of Wireless Standards:

1. **IEEE 802.11a (1999):** IEEE 802.11a is one of the early wireless networking standards released in 1999 alongside 802.11b. It was developed by the Institute of Electrical and Electronics Engineers (IEEE) as part of the 802.11 family of standards.

1.1. Key Features of IEEE 802.11a:

✓ **Frequency Band**

- Operates in the 5 GHz frequency band, which is less crowded compared to the 2.4 GHz band used by 802.11b.

- The use of the 5 GHz band helps reduce interference from devices like microwaves, Bluetooth devices, and other household gadgets that typically use the 2.4 GHz band.

✓ **Data Transfer Rates**

- Supports maximum data rates of 54 Mbps. This was a significant improvement over 802.11b, which could only reach 11 Mbps.
- Actual throughput typically ranged between 20 to 25 Mbps under real-world conditions, accounting for network overhead and signal quality.

✓ **Modulation Technique**

- Uses Orthogonal Frequency Division Multiplexing (OFDM), which allows for higher data rates by splitting the signal into multiple smaller sub-signals (sub-carriers) transmitted simultaneously.
- OFDM is more efficient than the Direct Sequence Spread Spectrum (DSSS) used in 802.11b, allowing for faster and more reliable data transmission.

✓ **Range and Coverage**

- While 802.11a provides higher speeds, it has a shorter range compared to 802.11b.
- The 5 GHz signals have less ability to penetrate walls and other obstacles, leading to reduced coverage areas.

✓ **Channels and Bandwidth**

- The 5 GHz band has more channels available than the 2.4 GHz band, which allows for less interference and better performance in environments with multiple Wi-Fi networks.
- Supports 20 MHz channels, and the larger number of channels available on the 5 GHz band reduces the chance of overlapping channels, which can cause interference.

✓ **Compatibility**

- Not backward compatible with 802.11b or 802.11g because they operate on different frequency bands (5 GHz vs. 2.4 GHz).
- Devices would need dual-band support (5 GHz and 2.4 GHz) to connect to both 802.11a and 802.11b/g networks.

1.2. Applications and Use Cases

The IEEE 802.11a (1999) wireless standard had several applications and use cases, primarily focused on environments that required higher data rates and less interference.

Here are some notable applications:

✓ **Enterprise Networks**

- **Corporate Offices:** Due to its higher data rates (up to 54 Mbps) and less crowded 5 GHz frequency, 802.11a was well-suited for enterprise environments. Businesses could set up wireless networks for tasks like file

sharing, web browsing, and accessing internal resources without the risk of interference from common 2.4 GHz devices.

- **Conference Rooms and Meeting Spaces:** 802.11a provided reliable connections for presentations, video conferencing, and collaborative work, where fast and stable network performance was crucial.

✓ **Multimedia Streaming**

- **Video and Audio Streaming**:
  - The higher bandwidth of 802.11a made it ideal for streaming high-quality audio and video content.
  - It was used in scenarios that required uninterrupted, high-speed wireless connections, such as streaming video to multiple screens in office settings or public venues.
- **Digital Signage:** In locations like airports, shopping malls, and conference centers, 802.11a could be used to stream content to digital signs, displays, and monitors without the interference issues common in the 2.4 GHz band.

✓ **High-Density Environments**

- **Stadiums and Arenas:**
  - 802.11a was useful in high-density environments where many users needed to connect simultaneously.
  - The availability of more non-overlapping channels in the 5 GHz band allowed network administrators to create multiple, stable connections, reducing congestion.
- **Trade Shows and Conventions:** Event organizers could set up reliable networks for exhibitors and attendees, supporting activities like product demonstrations, presentations, and high-volume data transfers.

✓ **Industrial and Warehouse Operations**

- **Manufacturing Plants:** 802.11a was used in industrial settings to connect devices, machines, and control systems, where stable and interference-free connections were essential for operations.
- **Warehouses:** Wireless scanners, inventory systems, and logistics management tools often relied on 802.11a to provide fast, reliable data connections. The reduced interference in the 5 GHz band meant fewer disruptions during operations.

✓ **Educational Institutions**

- **Universities and Schools:**
  - Educational institutions used 802.11a for campus-wide networks to provide internet access for students, faculty, and staff.
  - It was especially useful in environments where multiple devices needed to connect without interference, such as libraries, lecture halls, and dormitories.
- **Classroom Multimedia**: Teachers and students could use 802.11a to stream

educational content, share large files, and connect devices for interactive learning activities.

✓ **Healthcare Facilities**

- **Hospitals and Clinics:**
  - 802.11a could be used to connect medical devices, patient monitoring systems, and administrative equipment, ensuring stable and fast data transmission.
  - It was particularly beneficial in areas where interference from other devices (such as wireless phones and medical equipment) needed to be minimized.

✓ **Point-to-Point and Backhaul Connections**

- **Wireless Backhaul:**
  - The 802.11a standard was often used for short-range point-to-point backhaul connections between access points or from access points to routers.
  - Its higher data rates made it suitable for connecting different parts of a network wirelessly.
- **Outdoor Campus Networks**: Schools, companies, and campuses could set up point-to-point connections using 802.11a to link buildings or extend network reach across outdoor areas.

✓ **Airports and Transportation Hubs**

- **Passenger Wi-Fi**: Airports and transportation hubs could use 802.11a to provide Wi-Fi services to passengers without worrying about interference from other wireless devices operating on the 2.4 GHz band.
- **Operations and Security:** The standard was used for connecting security systems, surveillance cameras, and other operational devices that needed reliable, high-speed connections.

1.3. Advantages of IEEE 802.11a

✓ **Higher Data Rates:** 54 Mbps data rates were significantly faster than those provided by 802.11b.

✓ **Less Interference**: Operating in the 5 GHz band helped reduce interference from common household devices using the 2.4 GHz spectrum.

✓ **More Channels**: Availability of more non-overlapping channels enabled better performance in environments with multiple wireless networks.

1.4. Limitations of IEEE 802.11a

✓ **Shorter Range:** The 5 GHz band had less range and penetration capability than the 2.4 GHz band, limiting coverage.

✓ **Limited Compatibility**: Lack of compatibility with 802.11b/g meant fewer devices supported 802.11a, especially in consumer markets.

2. **IEEE 802.11b (1999):** IEEE 802.11b was one of the early wireless networking standards released in 1999, alongside 802.11a. It became the first widely

adopted Wi-Fi standard, contributing significantly to the growth of wireless networking. Here's a detailed description of 802.11b:

2.1. Key Features of IEEE 802.11b:

- ✓ **Frequency Band**
  - Operates in the 2.4 GHz frequency band, which was already in use by many consumer devices, making it easy to adopt.
  - The 2.4 GHz band allowed for longer range and better penetration through walls and obstacles compared to the 5 GHz band used by 802.11a.
- ✓ **Data Transfer Rates**
  - Supported maximum data rates of 11 Mbps, which was much higher than the original 802.11 standard's 2 Mbps.
  - Actual throughput typically ranged between 4 to 6 Mbps in real-world conditions, due to network overhead and signal quality.
  - It offered various data rates, including 1 Mbps, 2 Mbps, 5.5 Mbps, and 11 Mbps, allowing devices to automatically switch to lower speeds if the signal was weak.
- ✓ **Modulation Technique**
  - Utilized Direct Sequence Spread Spectrum (DSSS), which helped in spreading the signal over a wide range of frequencies, making it more resistant to interference.
  - Complementary Code Keying (CCK) was introduced to enhance the data rate up to 11 Mbps, improving the overall performance over the original standard.
- ✓ **Range and Coverage**
  - 802.11b had a longer range compared to 802.11a. Its signals could cover a wider area, even in environments with obstacles.
  - The 2.4 GHz band provided better signal penetration, making 802.11b suitable for use in homes, offices, and other areas with walls and barriers.
- ✓ **Compatibility**
  - Devices supporting 802.11b were compatible with the original 802.11 standard, but not with 802.11a, which operated on a different frequency band.
  - Later standards like 802.11g were designed to be backward-compatible with 802.11b, ensuring a smooth transition for users upgrading to newer technology.

2.2. Applications and Use Cases of IEEE 802.11b

- ✓ **Home Networking**
  - **Internet Sharing:** 802.11b became the standard for setting up home Wi-Fi networks, allowing multiple devices like laptops, PCs, and smartphones to

share an internet connection wirelessly.

- **Home Media Devices:** Early smart TVs, media players, and other home electronics began to incorporate 802.11b for wireless connectivity.

✓ **Small Business Networks**

- **Office Wi-Fi:** Small businesses could set up wireless networks without the need for extensive cabling, providing flexible and easy internet access for employees.
- **Point of Sale (POS) Systems:** Retailers and restaurants adopted 802.11b for wireless POS systems, enabling mobility and convenience.
- Public Wi-Fi Hotspots
- **Cafes, Airports, and Hotels:** The widespread adoption of 802.11b made it the go-to standard for providing public Wi-Fi in places like cafes, airports, hotels, and shopping centers.
- **Internet Service Providers (ISPs):** ISPs began offering wireless access points that supported 802.11b, making it easier for customers to connect to the internet.

✓ **Education**

- **Schools and Universities:** Educational institutions deployed 802.11b networks across campuses, providing students and staff with wireless access to learning resources and the internet.
- **Libraries:** Libraries used 802.11b to offer patrons wireless access for research and information retrieval.

2.3. Advantages of IEEE 802.11b

✓ **Cost-Effective:** As one of the earliest Wi-Fi standards, 802.11b was more affordable than 802.11a, making it widely accessible for home and small business use.

✓ **Good Range and Coverage**: With better range and penetration capabilities, 802.11b was effective in various environments, including homes, offices, and outdoor areas.

✓ **Ease of Adoption**: Using the 2.4 GHz band allowed existing devices to communicate easily, and the relatively lower cost of equipment encouraged widespread adoption.

2.4. Limitations of IEEE 802.11b

✓ **Lower Data Rates:** Although 11 Mbps was an improvement over earlier standards, it was still slower compared to 802.11a's 54 Mbps and later standards like 802.11g and 802.11n.

✓ **Interference Issues:** The 2.4 GHz band was already crowded with other devices like cordless phones, microwaves, Bluetooth devices, and other household electronics. This led to more interference, which could degrade the performance of 802.11b networks.

- ✓ **Limited Scalability:** The lower data rates and susceptibility to interference made it less suitable for environments with high-density usage or heavy bandwidth requirements.

3. **IEEE 802.11n (2009):** IEEE 802.11n, also known as Wi-Fi 4, was released in 2009 as an improvement over previous wireless standards (802.11a, 802.11b, and 802.11g). It brought significant advancements in speed, range, and reliability, making it a major breakthrough in Wi-Fi technology

3.1. Key Features of IEEE 802.11n:

- ✓ **Frequency Bands**
  - Operates on both the **2.4 GHz** and **5 GHz** frequency bands, making it a **dual-band** standard.
  - This dual-band capability allowed users to choose between the wider coverage of the 2.4 GHz band and the less congested 5 GHz band, which provided better performance in environments with heavy Wi-Fi usage.
- ✓ **Data Transfer Rates**
  - Supports maximum data rates of up to **600 Mbps**, depending on the configuration.
  - This was a significant improvement over **802.11g** (54 Mbps) and **802.11a** (also 54 Mbps). In real-world usage, users could experience throughput speeds between **150 Mbps to 300 Mbps**.
  - Higher data rates were achieved through various advanced technologies such as **MIMO**, **channel bonding**, and **frame aggregation**.
- ✓ **MIMO (Multiple Input, Multiple Output) Technology**
- **802.11n** introduced **MIMO**, which uses multiple antennas at both the transmitter and receiver to improve performance.
- MIMO allows multiple data streams to be sent and received simultaneously, significantly increasing the throughput and improving the range and reliability of connections.
- Typical configurations included **2x2**, **3x3**, or **4x4** MIMO setups, where the first number represents the number of transmitting antennas and the second the number of receiving antennas.
- **Channel Bonding**
- **802.11n** could combine two **20 MHz channels** into a single **40 MHz** channel, effectively doubling the available bandwidth and allowing for faster data rates.
- This feature was particularly useful on the 5 GHz band, where there were more non-overlapping channels available, reducing the risk of interference.
- ✓ **Backward Compatibility**
- **802.11n** was designed to be **backward compatible** with **802.11a/b/g** devices,

allowing older devices to connect to **802.11n** networks. However, when older devices were connected, the network's performance could be limited to the capabilities of the older standard.

✓ **Improved Range and Coverage**

- Due to MIMO technology and better data transmission techniques, **802.11n** provided a **greater range** than its predecessors.
- Signals could travel farther and penetrate obstacles (like walls) more effectively, making **802.11n** a better choice for larger areas or environments with physical barriers.

✓ **Frame Aggregation**

- Combined multiple frames into a single transmission, reducing the overhead and increasing the overall efficiency of data transfer.
- This technique helped improve throughput and reduced latency, especially in environments with high data traffic.

3.2. Applications and Use Cases of IEEE 802.11n

✓ **Home Networking**

- **HD Video Streaming and Online Gaming**: With higher speeds and better range, **802.11n** was well-suited for streaming HD videos, playing online games, and other bandwidth-heavy tasks.
- **Smart Home Devices**: **802.11n** networks became the standard for connecting smart home devices like security cameras, smart lights, and home assistants.

✓ **Enterprise and Office Networks**

- **Corporate Wi-Fi**: Businesses used **802.11n** to provide robust wireless networks that could handle the growing number of devices, including laptops, tablets, and smartphones.
- **Video Conferencing**: Reliable connections with higher speeds supported smooth video conferencing for businesses, helping with remote communication and collaboration.

✓ **Educational Institutions**

- **Campus-Wide Networks**: Universities and schools could set up campus-wide **802.11n** networks, providing students and staff with fast, reliable Wi-Fi access across large areas.
- **E-Learning and Online Resources**: **802.11n** networks allowed seamless access to online educational resources, video lectures, and collaborative tools.

✓ **Retail and Hospitality**

- **Wi-Fi for Guests**: Hotels, cafes, and other venues could offer fast, reliable Wi-Fi to guests, improving the overall customer experience.
- **Point-of-Sale (POS) Systems**: Retailers could use wireless POS systems, inventory tracking devices, and other wireless gadgets more effectively with

the faster speeds and improved reliability of **802.11n**.

✓ **Industrial Applications**

- **Warehouse Management**: Warehouses and distribution centers used **802.11n** networks to connect wireless scanners, tablets, and inventory systems, enabling efficient logistics management.
- **Remote Monitoring and Control**: Industrial sites could set up **802.11n** for reliable remote monitoring and control of machines, equipment, and security systems.

3.3. Advantages of IEEE 802.11n

✓ **Higher Speeds**: With potential data rates up to 600 Mbps, **802.11n** was a significant upgrade over **802.11a/b/g**, making it suitable for bandwidth-intensive applications like HD video streaming, online gaming, and large file transfers.

✓ **Greater Range**: Improved range and coverage, thanks to MIMO technology, made **802.11n** ideal for larger homes, offices, and open spaces.

✓ **Dual-Band Flexibility**: The ability to operate on both 2.4 GHz and 5 GHz bands provided flexibility, allowing users to switch between better coverage and less interference.

3.4. Limitations of IEEE 802.11n

✓ **Interference on 2.4 GHz Band**: While **802.11n** could operate on both bands, the 2.4 GHz band was still prone to interference from other devices (like microwaves, cordless phones, and Bluetooth), which could affect performance.

✓ **Shared Performance with Older Devices**: Backward compatibility meant that if older **802.11b/g** devices were connected, it could drag down the overall network speed due to the need to accommodate those devices.

4. **IEEE 802.11ac (2013): IEEE 802.11ac**, also known as **Wi-Fi 5**, was introduced in **2013** as an improvement over the previous **802.11n** standard. It brought significant enhancements in terms of speed, capacity, and efficiency, making it the preferred Wi-Fi standard for modern high-performance networks.

4.1. Key Features of IEEE 802.11ac:

✓ **Frequency Band**

- **802.11ac** operates exclusively in the **5 GHz** frequency band.
- By using the 5 GHz band, **802.11ac** avoids much of the interference seen in the 2.4 GHz band, which is crowded with devices like Bluetooth gadgets, microwaves, and older Wi-Fi networks.

✓ **Data Transfer Rates**

- **802.11ac** supports maximum data rates of up to **6.9 Gbps**, depending on the

configuration (though more common implementations provide speeds up to **1.3 Gbps** or **3.5 Gbps**).

- This was a massive leap from **802.11n**'s top speed of **600 Mbps**, making **802.11ac** ideal for high-bandwidth activities like 4K video streaming, online gaming, and large file transfers.

✓ **Channel Width**

- **Wider Channels**: While **802.11n** could combine two **20 MHz** channels into a **40 MHz** channel, **802.11ac** expanded this capability by supporting channels up to **80 MHz** and **160 MHz**.
- Wider channels allow for greater data throughput by increasing the amount of data that can be transmitted in a single transmission, boosting overall performance.
- **MIMO (Multiple Input, Multiple Output) and MU-MIMO**
- **MIMO** technology was enhanced in **802.11ac**, with support for up to **8 spatial streams** (compared to **802.11n's** 4 spatial streams).
- Introduced **MU-MIMO** (**Multi-User MIMO**), which allows an access point to communicate with multiple devices simultaneously. This reduces the wait time for each device, especially in high-density environments like offices or public hotspots.
- **MU-MIMO** makes the network more efficient by enabling better utilization of available bandwidth, which is particularly beneficial for environments where many devices are connected at once.

✓ **Beamforming**

- **802.11ac** uses **beamforming**, a technique that directs Wi-Fi signals more precisely towards a receiving device, rather than broadcasting signals in all directions.
- This leads to better signal strength, improved range, and more stable connections, especially in environments where devices are spread out or separated by obstacles.

✓ **Backward Compatibility**

- **802.11ac** is backward compatible with **802.11a/n**, meaning that devices using older standards can still connect to **802.11ac** networks, though at their respective lower speeds.
- The ability to support older devices made it easy for users to upgrade their networks without replacing all their equipment.

4.2. Applications and Use Cases of IEEE 802.11ac

✓ **Home Networking**

- **Ultra HD Streaming and Gaming**: With the ability to handle large amounts of data, **802.11ac** is perfect for households streaming 4K videos on multiple

devices or engaging in online gaming, where low latency and fast speeds are crucial.

- **Smart Homes**: Modern smart homes with numerous connected devices (smart TVs, voice assistants, security cameras) benefit from the improved capacity and bandwidth management of **802.11ac**.

✓ **Enterprise and Office Networks**

- **High-Density Office Environments**: Offices with many employees using laptops, tablets, and smartphones simultaneously can provide fast, stable connections across multiple devices, thanks to **MU-MIMO** and wider channels.
- **Video Conferencing and Collaboration**: Businesses using video conferencing and real-time collaboration tools rely on **802.11ac** to provide smooth, uninterrupted service.

✓ **Public Wi-Fi and Hotspots**

- **Airports, Malls, and Stadiums**: Public areas where thousands of people connect to Wi-Fi at the same time benefit from **802.11ac's** ability to manage high-density environments efficiently.
- **Cafes and Restaurants**: Smaller venues can also offer faster and more reliable Wi-Fi connections to their patrons, improving customer experience.

✓ **Educational Institutions**

- **Campus-Wide Wi-Fi**: Universities and schools can deploy **802.11ac** networks to cover large areas, providing reliable and fast connections for students and staff.
- **E-Learning and Media Streaming**: Faster speeds allow for the use of e-learning tools, multimedia resources, and online exams without performance issues.

✓ **Industrial and IoT Applications**

- **Warehouses and Manufacturing Plants**: Industrial environments can use **802.11ac** to connect a variety of devices, from inventory scanners to robots, ensuring efficient data flow and communication.
- **IoT Devices**: **802.11ac**'s improved bandwidth and reduced latency make it ideal for IoT devices that require consistent, high-speed connections.

4.3. Advantages of IEEE 802.11ac

✓ **Much Higher Speeds**: With data rates reaching up to **6.9 Gbps**, **802.11ac** made it possible to support multiple high-bandwidth applications simultaneously, like HD video streaming, cloud services, and gaming.

✓ **Improved Performance in High-Density Environments**: Features like **MU-MIMO** and **beamforming** ensured that even when many devices were connected, the network remained efficient and fast.

- ✓ **Better Signal Quality and Range**: Beamforming and support for more spatial streams allowed for better overall coverage and stability, even at extended ranges.
- ✓ **Less Interference**: Operating exclusively in the 5 GHz band reduced the chances of interference, improving network performance.

4.4. Limitations of IEEE 802.11ac

- ✓ **Limited to 5 GHz Band**: While the 5 GHz band is less crowded, it has a shorter range compared to the 2.4 GHz band. This means that **802.11ac** signals do not penetrate walls and obstacles as effectively as **802.11n** signals on the 2.4 GHz band.
- ✓ **Wider Channels and Interference**: Although wider channels provide more speed, they also increase the risk of overlapping with neighboring Wi-Fi networks if not properly managed, which can lead to interference and reduced performance.

5. **5.IEEE 802.11ax (Wi-Fi 6, 2019):** IEEE 802.11ax, known as Wi-Fi 6, was introduced in 2019 as the next-generation Wi-Fi standard, designed to enhance performance, efficiency, and scalability in high-density environments. It builds on the foundation of 802.11ac (Wi-Fi 5), introducing new technologies to support more devices and improve overall network capacity and speed.

5.1. Key Features of IEEE 802.11ax:

- ✓ **Frequency Bands**
- **Wi-Fi 6** operates on both **2.4 GHz** and **5 GHz** frequency bands, offering better flexibility and coverage.
- Unlike **802.11ac**, which only supported the 5 GHz band, **802.11ax** reintroduced and optimized the 2.4 GHz band, making it suitable for connecting a wide variety of devices.
- ✓ **Data Transfer Rates**
- **Wi-Fi 6** supports maximum data rates up to **9.6 Gbps**, a noticeable increase from **Wi-Fi 5's** 6.9 Gbps.
- While the peak speeds are higher, the real focus is on improving the overall network performance, especially when multiple devices are connected, rather than just achieving higher speeds.
- ✓ **OFDMA (Orthogonal Frequency Division Multiple Access)**
- One of the key features of **Wi-Fi 6** is **OFDMA**, which enables more efficient use of available bandwidth by dividing channels into smaller sub-channels.
- This allows multiple devices to communicate simultaneously, reducing latency

and improving overall network efficiency. It's similar to how cellular networks handle multiple connections.

✓ **MU-MIMO Enhancements**

- **Wi-Fi 6** enhances **MU-MIMO (Multi-User, Multiple Input, Multiple Output)** by supporting up to **8 devices** simultaneously, both for uplink and downlink.
- Unlike **Wi-Fi 5**, which only supported downlink MU-MIMO (from router to devices), **Wi-Fi 6** allows for both uplink and downlink, enabling faster and more efficient data transfer even when multiple devices are uploading data at the same time.

✓ **1024-QAM (Quadrature Amplitude Modulation)**

- **Wi-Fi 6** uses **1024-QAM**, which allows more data to be packed into each signal, resulting in **25% more data throughput** compared to **256-QAM** used in **Wi-Fi 5**.
- This leads to faster speeds and better performance, particularly when devices are closer to the access point.

✓ **Target Wake Time (TWT)**

- **Target Wake Time (TWT)** is a feature designed to improve battery life for devices by scheduling specific times for devices to communicate with the router.
- This reduces the need for devices to continuously listen for signals, conserving power. This is especially beneficial for IoT devices, smartphones, and other battery-powered gadgets.

✓ **Improved Range and Signal Efficiency**

- **Wi-Fi 6** uses technologies like **BSS Coloring**, which helps in reducing interference by distinguishing between overlapping networks, allowing for better performance even in crowded areas.
- The improved signal efficiency helps extend range and maintain stronger connections, even when there are obstacles between the router and devices.

✓ **Backward Compatibility: Wi-Fi 6** is backward compatible with previous Wi-Fi standards, including **802.11a/b/g/n/ac**, meaning that devices using older standards can still connect to a **Wi-Fi 6** network, though they won't experience the benefits of the newer technology.

5.2. Applications and Use Cases of IEEE 802.11ax (Wi-Fi 6)

✓ **Home Networking**

- **Smart Homes**: **Wi-Fi 6** is ideal for smart homes with numerous connected devices, from smart TVs and cameras to smart lights and voice assistants. It ensures all devices can connect seamlessly without network congestion.
- **4K/8K Video Streaming**: Faster speeds and lower latency make **Wi-Fi 6** perfect for streaming high-definition video content on multiple devices

simultaneously.

- ✓ **Enterprise and Office Networks**
- **High-Density Office Environments**: Offices with a high number of devices (laptops, tablets, smartphones) benefit from the increased capacity and efficiency of **Wi-Fi 6**.
- **Real-Time Collaboration and Video Conferencing**: Enhanced network stability and speed enable smooth, real-time collaboration, which is essential for businesses relying on video conferencing and cloud-based services.
- ✓ **Public Wi-Fi and Hotspots**
- **Airports, Stadiums, and Malls**: Public venues with large crowds of users can maintain strong and reliable Wi-Fi connections, thanks to **Wi-Fi 6's** ability to handle multiple devices efficiently.
- **Public Transport**: Buses, trains, and other forms of public transport can offer better internet connectivity with **Wi-Fi 6**, catering to a large number of passengers.
- ✓ **Educational Institutions**
- **Campus-Wide Networks**: Universities and schools can deploy **Wi-Fi 6** to cover large campuses, ensuring that students, staff, and IoT devices are connected without performance issues.
- **E-Learning and Multimedia Resources**: **Wi-Fi 6** supports streaming of educational videos, interactive e-learning tools, and online exams without lag or buffering.
- ✓ **Industrial and IoT Applications**
- **Factories and Warehouses**: **Wi-Fi 6** can be used for connecting robots, sensors, and other IoT devices in industrial environments, ensuring reliable and low-latency communication.
- **Smart Cities**: As cities adopt more connected devices, **Wi-Fi 6** provides the necessary bandwidth and efficiency to support smart city infrastructure, from traffic monitoring systems to public safety networks

5.3. Advantages of IEEE 802.11ax (Wi-Fi 6)

- ✓ **Higher Network Capacity**: With features like **OFDMA** and enhanced **MU-MIMO**, **Wi-Fi 6** can handle more devices simultaneously without degrading performance, making it ideal for homes, offices, and public spaces with many connected devices.
- ✓ **Better Efficiency**: **Wi-Fi 6** improves data handling, resulting in faster, more reliable connections even in crowded environments.
- ✓ **Lower Latency**: The combination of OFDMA, MU-MIMO, and other technologies reduces latency, which is crucial for real-time applications like gaming, video calls, and IoT operations.

- ✓ **Extended Battery Life**: **Target Wake Time (TWT)** helps conserve power for connected devices, leading to longer battery life for devices that need to be always connected.

5.4. Limitations of IEEE 802.11ax (Wi-Fi 6)

- ✓ **Higher Cost**: **Wi-Fi 6** routers and devices are generally more expensive than their **Wi-Fi 5** counterparts, although prices have been decreasing as the technology becomes more common.
- ✓ **Dependent on Device Compatibility**: To fully utilize **Wi-Fi 6** features, both the router and the devices must support **802.11ax**. Older devices can still connect but won't benefit from the new features.
- ✓ **5 GHz Range Limitation**: Although **Wi-Fi 6** enhances the 2.4 GHz band, the range limitations of the **5 GHz** band still exist. This may affect performance over long distances or through multiple walls.

Theoretical Activity 2.2.2: Description of Wireless Network Outdoor-Specific Features

Tasks:

1: Read these questions and respond to them accordingly:

i. Describe these Wireless Network Outdoor-Specific Features:

a. Point-to-Point (PtP) Bridging

b. Point-to-Multipoint (PtMP) Bridging

c. Wireless Mesh Networking

d. Outdoor Antenna Alignment

e. Long-Range Considerations

f. Quality of Service (QoS)

2: Write your findings on the paper or flipchart

3: Present your findings in front of a whole class

4: Ask questions or clarification

5: Read key readings 2.2.2

Key readings 2.2.2: Description of Wireless Network Outdoor-Specific Features

Wireless network outdoor-specific features are essential considerations that ensure reliable, high-performance, and secure wireless communication in outdoor environments. These features address the unique challenges posed by outdoor installations, such as environmental factors, signal interference, and coverage requirements

Here are some key outdoor-specific features:

1. **Point-to-Point (PtP) Bridging:**

Point-to-Point (PtP) bridging refers to the wireless connection between two fixed locations using directional antennas. It is used to create a direct, high-speed link between two network nodes over long distances without relying on a wired infrastructure.

✓ **Key Features:**

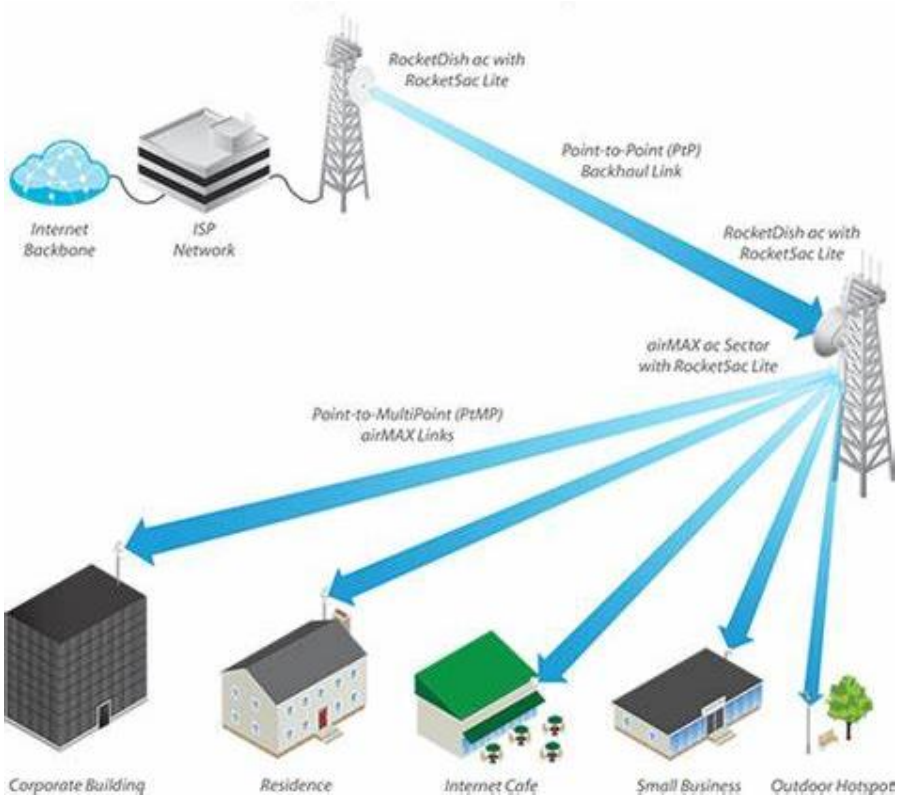
- Directional Antennas: High-gain directional antennas (such as parabolic or Yagi antennas) are used to focus the signal and extend the range.
- Clear Line of Sight (LoS): PtP links typically require clear LoS between the two locations to ensure reliable connectivity and reduce interference.
- High Throughput: PtP bridges are capable of providing high data rates over long distances, making them suitable for connecting buildings, remote offices, or outdoor cameras.

✓ **Applications:** Used for inter-building communication on a campus, connecting remote sites, or linking a main network to a secondary location across large distances (kilometers).

✓ **Use Case:**

A school wants to connect two campuses that are located 2 km apart. A PtP bridge is established between the buildings using high-gain antennas to provide a high-speed wireless link.

2. Point-to-Multipoint (PtMP) Bridging:



Point-to-Multipoint (PtMP) bridging involves using a central base station or access point to connect multiple remote nodes or client devices. It allows for a single access point to serve multiple locations or users over long distances.

✓ **Key Features:**

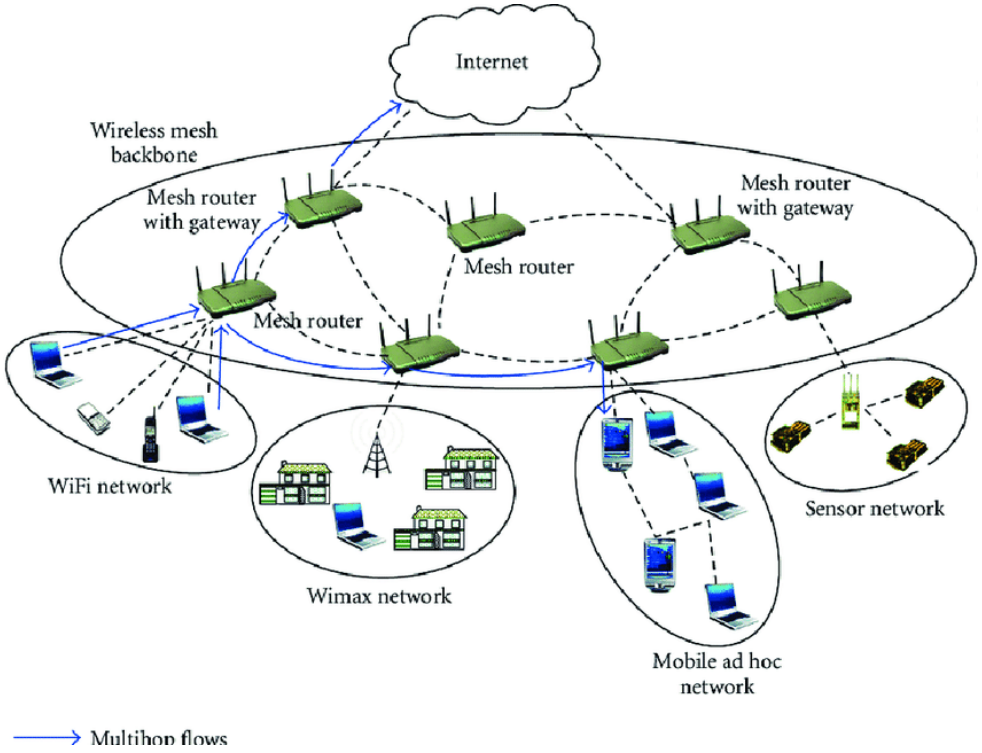
- Central Access Point: A single high-powered access point, often with a sector antenna, serves as the "hub" to communicate with multiple client devices or remote stations.
- Multiple Clients: Several client devices, such as outdoor access points or bridges, are connected to a central hub, creating a wide coverage area.
- Scalability: PtMP systems are highly scalable, allowing the addition of more clients as the network grows.

✓ **Applications:** Used for public Wi-Fi networks, security camera connectivity, or connecting multiple offices, buildings, or houses in rural areas.

✓ **Use Case:**

A park installs a PtMP system to provide Wi-Fi to various areas, with one central access point serving multiple wireless nodes distributed throughout the park.

3. Wireless Mesh Networking:



Wireless Mesh Networking is a type of network topology where multiple wireless nodes (access points or routers) work together to form a self-healing, interconnected network. Each node in a mesh network can communicate with other nodes, ensuring redundancy and broader coverage.

✓ **Key Features:**

- Self-Healing: If one node fails or goes offline, the network automatically reroutes traffic through other available nodes.
- Redundancy: Multiple pathways between nodes increase reliability and minimize the risk of a single point of failure.
- Dynamic Routing: Traffic dynamically hops from node to node, optimizing the best possible route for data transmission.

✓ **Applications:** Ideal for outdoor environments where a large area needs coverage without the need for extensive cabling, such as in citywide Wi-Fi networks or large campuses.

✓ **Use Case:**

A university deploys a wireless mesh network across its campus to provide seamless wireless connectivity. If one access point fails, the others continue to function, ensuring uninterrupted service.

4. Outdoor Antenna Alignment:

Outdoor antenna alignment refers to the precise adjustment of directional

antennas to ensure that the wireless signal is properly focused and directed toward the desired target (for PtP or PtMP setups). Proper alignment is critical for maximizing signal strength and minimizing interference or signal loss.

✓ **Key Features:**

- Alignment Tools: Many outdoor devices come with built-in signal strength meters or apps to assist in aligning antennas correctly.
- Fine-Tuning: Adjusting both the vertical (elevation) and horizontal (azimuth) angles ensures that the antenna is properly oriented.
- Signal Optimization: Proper alignment reduces signal degradation and interference, ensuring maximum throughput and link reliability.

✓ **Applications:** Essential for long-distance PtP bridges or sector antennas in PtMP systems.

✓ **Use Case:** A technician aligns the antennas of a PtP bridge between two buildings to ensure the strongest signal strength by using a signal meter to guide the alignment.

5.Long-Range Considerations

Long-range considerations refer to the specific factors that need to be addressed when deploying wireless networks over extended distances, especially in outdoor environments. These include ensuring proper signal propagation, handling interference, and accounting for environmental factors like terrain and weather.

✓ **Key Features:**

- Line of Sight (LoS): Clear LoS is typically required for long-range wireless communication, as obstacles like trees, buildings, or hills can significantly degrade the signal.
- Antenna Gain: High-gain antennas are necessary to transmit signals over long distances. Directional antennas are commonly used for this purpose.
- Fresnel Zone: The Fresnel Zone is an elliptical area around the LoS path that should remain clear of obstacles to avoid signal degradation. Proper planning ensures that the Fresnel Zone is unobstructed.
- Environmental Factors: Weather, such as rain, snow, or fog, can impact signal quality, particularly in the 5 GHz band, which is more susceptible to attenuation.

✓ **Use Case:**

A rural ISP deploys a long-range PtP bridge over a 10 km distance to provide internet connectivity to a remote village. The installation team ensures a clear LoS and uses high-gain antennas for the deployment.

6. Quality of Service (QoS):

Refers to the prioritization and management of different types of network traffic to ensure that critical applications receive the necessary bandwidth and low-latency connections. In outdoor wireless networks, QoS helps manage bandwidth usage across various services and users.

✓ **Key Features:**

- Traffic Prioritization: Critical traffic such as VoIP, video conferencing, or emergency communication is given higher priority over less essential services (e.g., general browsing).
- Bandwidth Allocation: QoS policies allow network administrators to allocate specific bandwidth limits to different devices or applications, ensuring fair distribution and preventing congestion.
- Latency Control: Minimizes latency for real-time services by prioritizing their traffic over non-time-sensitive data.

✓ **Applications**: Useful in environments where multiple users are accessing the network simultaneously, such as schools, parks, or public Wi-Fi networks.

✓ **Use Case:** A public park's wireless network uses QoS to ensure that critical applications such as video surveillance get priority over users streaming videos or browsing the web.

Theoretical Activity 2.2.3: Description of key considerations in Mounting network equipment and connecting devices

Tasks:

1. Read these questions and respond to them accordingly:
   i. What do you understand by mounting network equipment
   ii. Identify the Importance of Mounting Network Equipment
   iii. Describe the key factors to consider when connecting devices and mounting network equipment
   iv. Describe the following terms:
      a. cable management
      b. Cable Security
2. Write your findings on paper or any other reserved space
3. Present your findings in front of a whole class
4. Ask questions or clarification if any
5. Read the key readings 2.2.3 and do the application of learning 2.2

Key readings 2.2.3: Description of the key considerations in Mounting network equipment and connecting devices

1. **Mounting network equipment** refers to the process of securely installing network devices, such as antennas, access points, routers, switches, and other networking hardware, onto a fixed surface or structure.
   This is a critical step in deploying outdoor networks, ensuring that the devices are safely positioned for optimal performance and reliability. The process typically involves selecting the right location, using appropriate mounting hardware, and aligning the equipment for efficient operation.

1.1. Key Components of Mounting Network Equipment

- ✓ **Selection of Location:**
  For wireless equipment (e.g., access points or antennas), the location is chosen to maximize signal coverage and performance. In outdoor deployments, it is essential to ensure line-of-sight (LoS) between connected devices for optimal connectivity.
- ✓ **Mounting Surfaces**:
  Equipment can be mounted on various surfaces, such as walls, poles, rooftops, or ceilings, depending on the deployment scenario. Choosing the right surface and hardware is crucial to ensure stability.
- ✓ **Mounting Hardware**:
  The correct brackets, clamps, or mounting frames are selected based on the weight, size, and type of equipment being installed. For outdoor installations, weather-resistant materials like stainless steel or aluminum are often used to prevent corrosion and withstand environmental factors.
- ✓ **Alignment and Positioning:**
  For wireless installations, proper alignment of the equipment (especially for antennas) is necessary to ensure the strongest possible signal. In point-to-point (PtP) or point-to-multipoint (PtMP) configurations, precise positioning is crucial for maintaining strong, stable connections.
- ✓ **Cable Management**:
  Ensuring proper routing and securing of cables to prevent damage or interference is an important part of the mounting process. In outdoor installations, this often includes waterproofing measures to protect cables from the elements.
- ✓ **Security and Safety:**
  Mounting should ensure that the equipment is secure against tampering, theft, or vandalism. Additionally, the mounting hardware should be able to

withstand environmental challenges such as wind or heavy rain in outdoor settings.

1.2. Importance of Mounting Network Equipment:

- ✓ **Performance**: Properly mounted equipment ensures efficient network performance, maximizing coverage and minimizing signal interference.
- ✓ **Reliability:** Secure mounting ensures that equipment remains operational even in harsh weather or challenging environments.
- ✓ **Maintenance:** Well-mounted equipment is easier to maintain, with considerations for access and adjustments when needed.
- ✓ **Safety:** Ensuring that network devices are securely mounted minimizes the risk of accidents, equipment falls, or damage to property and people.

2. key factors to consider when and mounting network equipment and connecting devices

When connecting devices and mounting network equipment, several key factors must be considered to ensure optimal performance, safety, and durability. These factors include physical, environmental, technical, and security considerations. Below is a detailed description of the critical aspects:

- ✓ **Equipment Placement and Location**
- Signal Coverage and Line-of-Sight (LoS): For wireless devices, especially in outdoor installations, ensure a clear line-of-sight between devices (e.g., access points, antennas) to minimize signal interference and maximize coverage. The placement should reduce obstacles like trees, buildings, or other physical barriers.
- Optimal Height: Mount devices at a height that provides the best signal propagation. For outdoor environments, this usually means mounting antennas on rooftops or poles high enough to avoid obstructions.
- Proximity to Connected Devices: Wired devices should be positioned to minimize cable lengths between devices to reduce latency and signal degradation.

✓ **Environmental Conditions**

- Weather Resistance: For outdoor installations, ensure the equipment is rated for exposure to rain, wind, UV light, and extreme temperatures. Use weatherproof mounting hardware and enclosures to protect devices from the elements.
- Wind and Vibration Resistance: Ensure that mounted equipment can withstand strong winds, especially antennas and poles in high-wind areas. Vibration can also affect performance, so secure equipment to avoid movement.

- Temperature and Humidity: Ensure the equipment's operating range matches the environmental conditions. For outdoor setups, consider equipment with ventilation or temperature control features to prevent overheating or damage from cold.

✓ **Equipment Compatibility**

- Hardware Compatibility: Verify that the mounting hardware is compatible with the specific network devices, considering their size, weight, and installation requirements. Mismatched hardware may lead to instability or difficulty in proper alignment.
- Frequency Band and Interference: For wireless devices, consider the frequency band (e.g., 2.4 GHz or 5 GHz) and choose equipment that avoids overcrowded channels and interference from nearby networks.

✓ **Load Capacity and Mounting Surface**

- Weight Support: The mounting hardware must be capable of supporting the weight of the equipment, especially for heavier devices like large antennas or cameras. Overloading mounts can lead to instability and failure.
- Mounting Surface Compatibility: Ensure the mounting hardware is designed for the surface (e.g., wall, pole, or roof). Different surfaces require specific brackets, anchors, or fasteners. Poles often require clamps or straps that adjust to the correct size.

✓ **Cable Management**

- Cable Length and Routing: Ensure that cables are long enough to reach from the device to the power source or connected device. Avoid tension or sharp bends in cables that can damage connections.
- Protection Against the Elements: For outdoor setups, protect cables from weather exposure by using weatherproof enclosures, conduits, or cable glands to seal openings. Use UV-resistant materials for cables exposed to direct sunlight.
- Interference and Cross-Talk: Keep power and data cables separated to avoid electrical interference. For PoE (Power over Ethernet) setups, use high-quality Ethernet cables with shielding if necessary.

✓ **Security and Access Control**

- Physical Security: Protect mounted equipment from theft, tampering, or vandalism, especially in public areas. Use tamper-resistant mounting hardware or secure enclosures.
- Access for Maintenance: Ensure that devices are mounted in accessible locations to allow for routine maintenance, repairs, or upgrades. Avoid hard-to-reach areas that complicate troubleshooting.

✓ **Alignment and Orientation**

- Precise Alignment: For wireless installations such as point-to-point (PtP) or point-to-multipoint (PtMP) setups, ensure antennas are properly aligned to maximize signal strength and reduce latency. Use built-in tools like signal strength meters for precise adjustments.
- Orientation: Ensure that devices such as antennas or directional access points are mounted in the correct orientation (e.g., vertical or horizontal) for optimal performance.

✓ **Power Supply Considerations**

- Power Source Proximity: Devices should be mounted near reliable power sources. For outdoor devices, ensure power connections are weatherproof and protected from water ingress.
- PoE (Power over Ethernet): If using PoE, ensure that the Ethernet cable run is within the maximum length limit (usually 100 meters for Cat5e/Cat6 cables) and that the switch or injector supports the necessary power level.
- Backup Power: Consider battery backups (UPS) or surge protectors for critical network equipment, especially in areas prone to power outages or fluctuations.

✓ **Safety Standards and Compliance**

- Building Codes: Ensure mounting and installation meet local safety and building codes, especially in terms of load-bearing, wind resistance, and cable routing.
- Electrical Safety: When connecting devices that require power, ensure proper grounding and surge protection to prevent electrical shocks or damage to the equipment during lightning storms or power surges.

✓ **Documentation and Labeling**

- Documentation: Maintain proper documentation for all connections and mounting configurations. Record details such as IP addresses, mounting locations, cable routes, and device configurations.
- Labeling: Label cables and devices clearly to simplify troubleshooting and future maintenance.

3. Definitions for the terms:

3.1. Cable Management

✓ **Cable management** refers to the process of organizing, routing, and securing cables to ensure a neat and functional setup. Proper cable management reduces clutter, prevents damage to cables, enhances airflow in equipment spaces, and makes it easier to identify and troubleshoot cables when necessary. It also minimizes hazards like tripping or cable interference with other equipment.

- **Techniques used for cable management** include cable ties, cable trays, conduits, and cable organizers to keep power and data cables separated and well-arranged.

✓ **Cable Security**

- Cable security involves protecting network and power cables from physical damage, tampering, or unauthorized access. This includes ensuring that cables are securely fastened, routed in safe areas, and shielded from potential environmental or human risks (e.g., vandalism or accidental disconnection).
- For sensitive installations, cable security can also involve using tamper-proof conduits, locks, or cable alarms to prevent unauthorized access or interference with the network infrastructure.
- In data networks, cable security also helps prevent signal degradation or interference that could affect network performance.

Practical Activity 2.2.4: Mounting network equipment, cabling and connecting devices

Task:

1: Read carefully this task and perform it accordingly

Refer to the practical activity 2.1.2, go to the area where network equipment will be mounted and then mount network equipment in strategic locations. After mounting device, perform cabling based on device placement and ensure proper connectivity between devices. Take all needed tools, materials and equipment for Mounting network equipment and connecting devices

2: Follow the demonstration process of Mounting network equipment, cabling and connecting devices.

3: Repeat yourself the task of mounting network equipment, cabling and connecting devices

4: Ask questions or clarifications

5: Read key readings 2.2.4 and do the application of Learning 2.2

Key readings 2.2.4: Mounting network equipment and connecting devices

- **Mounting network equipment and connecting devices**

Connecting Devices and Mounting Network Equipment refers to the

process of physically installing and setting up networking hardware, such as routers, switches, access points, and antennas, to ensure they are properly secured, connected, and configured to function as part of a network infrastructure

Mounting Network Equipment Connecting Devices and involves these steps:

Step 1:Equipment Preparation: prepare all needed devices

- ✓ Devices to be installed:
- Wireless Access Points
- Network Switch (to connect multiple devices)
- Router (for internet distribution)
- Outdoor Antenna (for long-range coverage)
- Necessary mounting hardware (brackets, clamps, screws)
- Ethernet cables, power cables, and cable ties.

Note that the number of devices to be installed depend on the network topology that should be designed from the survey report.

Step 2: Identify Mounting Locations:

- ✓ Indoor Setup:
- Mount the wireless access point in a central indoor location, such as the school's main hallway or cafeteria, ensuring optimal Wi-Fi coverage.
- Install the network switch in the network rack (or cabinet), ensuring it's accessible for maintenance.
- ✓ Outdoor Setup:
- Mount the outdoor access point on an external wall or pole, ensuring it covers the school's parking lot or playground.
- Mount the outdoor antenna on the roof or a pole, ensuring it has a clear line of sight for long-range connectivity.

Considerations:

- Ensure the mounting locations have proper ventilation and are protected from direct sunlight (for outdoor setups) or water exposure.
- Make sure there's easy access to power sources for the devices.
- While selecting mounting hardware for network equipment, ensure that the hardware is appropriate for the environment, equipment, and specific application by considering the following: Type of Equipment Being Mounted, environment conditions, load capacity and ease of installation.

Step 3:Mounting the Network Equipment:

- ✓ Mounting Indoor Wireless Access Point:
- Use the provided mounting brackets to securely install the indoor access

point on the ceiling or high wall.

- Ensure the access point is centrally located for maximum coverage and minimal signal interference.

✓ Mounting the Outdoor Access Point and Antenna:

- Use heavy-duty weather-resistant brackets to mount the outdoor access point on the building's exterior wall or a pole. Ensure that it is high enough to avoid obstacles and interference.
- Securely mount the outdoor directional antenna using the provided brackets and align it for optimal signal strength.
- Use a signal strength meter or a smartphone app to fine-tune the antenna's position if needed.

Step 4:Make and Test Ethernet cable

✓ **Gather Tools and Materials**

- Tools: Wire cutter/stripper, crimping tool, cable tester.
- Materials: Ethernet cable (Cat5e/Cat6), RJ45 connectors.

✓ **Choose Wiring Standard**

- Use T568B (most common) or T568A.
  T568B Color Order: White-Orange, Orange, White-Green, Blue, White-Blue, Green, White-Brown, Brown.

✓ **Prepare the Cable**

- Cut the cable to the desired length.
- Strip 1 inch of the outer sheath.
- Untwist and align wires according to the chosen standard.

✓ **Terminate the Cable**

- Trim wires to the same length.
- Insert wires into the RJ45 connector in order.
- Crimp the connector with a crimping tool.

✓ **Repeat for the Other End**

- Follow the same steps for the other end of the cable.

✓ **Test the Cable**

- Use an Ethernet cable tester: plug one end into the main unit and the other into the remote unit.
- Check the lights:

Step 5:Connect Devices:

✓ Power Supply:

- Connect all network devices to power using nearby outlets or PoE (Power over Ethernet) for the access points if supported.
- Ensure that outdoor devices are powered using weatherproof cables or enclosures to protect the connections from the elements.

✓ Cable Management:

- Use Ethernet cables to connect the access points and switches.
- Ensure that cables are routed neatly using cable ties or conduits to avoid tangling and physical damage.
- For outdoor cables, use waterproof conduits or cable glands to protect them from weather exposure.

✓ Network Connections:

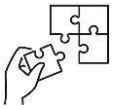
- Connect the indoor access point to the network switch using an Ethernet cable.
- Connect the switch to the router for internet access.
- Use long-range outdoor-rated Ethernet cables to connect the outdoor antenna and access point to the switch.

Points to Remember

- 802.11a and 802.11b were among the earliest standards, offering moderate speeds, with 802.11b providing wider adoption and range at the cost of slower speed.
- 802.11n improved both speed and range with MIMO technology and dual-band support.
- 802.11ac (Wi-Fi 5) brought much faster speeds and better performance on the 5 GHz band, while 802.11ax (Wi-Fi 6) focuses on efficiency, higher throughput, and handling many devices at once in dense environments, with improved performance in both the 2.4 GHz and 5 GHz bands. Wi-Fi 6E further extends this by adding the 6 GHz band for even higher performance and capacity.
- Point-to-Point (PtP) Bridging Requires clear line-of-sight (LOS) between two points to ensure optimal performance whereas point to multipoint can sometimes operate in near-line-of-sight (NLOS) conditions depending on the technology used.
- When aligning an outdoor antennas Take into account environmental factors (e.g., wind, rain) that might impact antenna stability and alignment over time.
- Ensure low-latency communication for applications like VoIP and video conferencing by setting appropriate QoS rules.
- When mounting network equipment and connecting devices, it is crucial to focus on physical stability, environmental protection, alignment, power supply, and security. Ensuring that equipment is properly mounted and connections are secure

guarantees reliable network performance, ease of maintenance, and safety in both indoor and outdoor installations.

- Ensure the antennas are compatible with the 5 GHz band for reduced interference and higher throughput
- Ensure that antennas are accurately aligned. Use alignment tools such as compasses, laser levels, or smartphone apps to help achieve precise alignment.
- Mount antennas high enough to maintain clear LoS between the two locations.
- Mount the network equipment in appropriate locations.
- Properly connect network devices such as routers, access points, and switches.
- Ensure safe cable routing and management.
- You have to check the coverage, signal strength, and stability of the wireless connection across different locations for verifying that devices can reliably connect to a network and communicate with each other.
- Ensure that the network is secure and resilient against potential threats by evaluating the safety measures of a network to protect it against unauthorized access, data breaches, and other security threats.
- Use properly the tools which corresponds to the testing type for getting accurate result.
- For connectivity testing, focus on coverage, signal strength, stability, and user experience.
- For security testing, assess vulnerabilities, conduct penetration testing, monitor for threats, and ensure compliance.
- For performance testing, measure throughput, latency, jitter, packet loss, and conduct load testing.
- Make sure that you use specialized tools for each testing type to ensure thorough and accurate assessments.



Application of learning 2.2.

You are hired for deploying a robust wireless network solution for a remote campus. The campus consists of multiple buildings, some of which are far apart, requiring both indoor and outdoor connectivity solutions. The project involves deploying access points based on different wireless standards, establishing outdoor connections between buildings, ensuring coverage in all areas, and setting up the necessary infrastructure (cabling, mounting equipment, etc.).

You must also ensure optimal performance with Quality of Service (QoS) for specific applications.

Indicative content 2.3: Configuration of Wireless Devices

Duration: 15 hrs

Theoretical Activity 2.3.1: Description of wireless devices configurations

Tasks:

1: Respond to the following questions

i. Define these key terms:

   a. DHCP

   b. DNS

   c. NAT

   d. VPN

   e. Wireless extender

   f. Firewall

   g. Proxy server

   h. Content filtering

   i. Quality of service

   j. Logging and reporting

ii. Describe the access point settings

2: Write your answers on reserved space

3: Present your answers to the whole class

4: Ask questions or clarification if necessary

5: Read the key readings 2.3.1 and do the application of learning 2.3

Key readings 2.3.1: Description of wireless devices configurations

Description of needed wireless devices configurations

1. Description of key terms:

1.1. DHCP (Dynamic Host Configuration Protocol)

DHCP is a network protocol that automatically assigns IP addresses to

devices on a network. It eliminates the need for manually configuring IP addresses for each device, making network management simpler. DHCP servers handle the assignment of IP addresses, default gateways, and other important network settings, allowing devices to connect to the network efficiently.

1.2. DNS (Domain Name System)

DNS is a system that translates human-readable domain names (like www.example.com) into IP addresses (like 192.168.1.1) that computers use to identify each other on a network. This makes it easier for users to access websites without needing to remember long numerical IP addresses.

1.3. NAT (Network Address Translation)

NAT is a method used by routers to map multiple private IP addresses to a single public IP address, allowing multiple devices within a local network to share a single IP for internet access. NAT helps conserve the number of public IP addresses and improves security by hiding internal IP addresses from external networks.

1.4. VPN (Virtual Private Network)

A VPN is a secure connection that allows users to access a private network over a public network (such as the internet). It encrypts the data being sent and received, providing privacy and security. VPNs are commonly used by remote workers to access a company's internal network securely.

1.5. Wireless Extender

A wireless extender, also known as a Wi-Fi range extender, is a device that boosts the coverage of an existing wireless network by receiving the wireless signal and retransmitting it. This helps eliminate dead spots and expands the Wi-Fi signal in areas where it might be weak.

1.6. Firewall

A firewall is a security device, either hardware or software that monitors and controls incoming and outgoing network traffic based on predefined security rules. Firewalls act as a barrier between trusted internal networks and untrusted external networks, helping to protect systems from unauthorized access and cyber threats.

1.7. Proxy Server

A proxy server acts as an intermediary between a client and the internet. When a user makes a web request, the proxy server retrieves the requested content on behalf of the user. Proxy servers are often used to hide the user's real IP address, improve security, and cache data for faster retrieval of frequently accessed websites.

1.8. Content Filtering

Content filtering is a technique used to block access to certain websites, content, or services based on specific criteria. It is commonly used by organizations, schools, or parents to prevent access to inappropriate or harmful content on the internet. This is done using software or hardware tools that scan and filter out specific content.

1.9. Quality of Service (QoS)

QoS refers to the ability of a network to prioritize certain types of traffic, ensuring that critical applications like voice, video, or gaming receive the necessary bandwidth and low latency to perform well. It helps in managing network resources efficiently by reducing delays and improving performance for important services.

1.10. Logging and Reporting

Logging refers to the process of recording events or activities that occur within a system or network. Reporting involves analyzing these logs and generating summaries or detailed reports to provide insight into the system's operation, security events, or network performance. Logs are essential for troubleshooting and maintaining network security, as they help in tracking incidents or anomalies.

2. Description of the access point settings

When configuring an access point (AP) for a wireless network, several settings need to be adjusted to ensure proper operation, security, and performance. Here's an overview of the key access point settings:

2.1. SSID (Service Set Identifier)

The SSID is the name of the wireless network that devices will see when scanning for available networks. Each access point can broadcast one or more SSIDs, which users will select to connect to the network.

2.2. **Operating Frequency Band**

- ✓ Access points can operate on different frequency bands, typically 2.4 GHz and 5 GHz, or both.
- ✓ 2.4 GHz: Longer range but more prone to interference because it's shared with many other devices (Bluetooth, microwaves, etc.).
- ✓ 5 GHz: Shorter range but less interference and supports higher speeds.
- ✓ Dual-band or tri-band access points can simultaneously broadcast on both bands, allowing for more flexibility and better performance.

2.3. Channel Selection

- ✓ Channels are specific frequencies within the chosen frequency band. Proper channel selection can help avoid interference with other nearby networks or devices.
- ✓ Automatic Channel Selection: Many access points offer this feature to select the least congested channel.
- ✓ Manual Channel Selection: Advanced users may choose channels manually to optimize performance based on local conditions.
- ✓ Non-overlapping Channels: On 2.4 GHz, channels 1, 6, and 11 are non-overlapping, and using these reduces interference.

2.4. Wireless Security

- ✓ Encryption: This is critical for securing the wireless network.
- ✓ WPA3: The latest and most secure wireless encryption standard.
- ✓ WPA2: Still widely used and secure, though less advanced than WPA3.
- ✓ WEP: Older and insecure, should not be used.
- ✓ Passphrase/Password: Set a strong passphrase to prevent unauthorized access.
- ✓ Enterprise Security (WPA2-Enterprise/WPA3-Enterprise): For business networks, access points can use RADIUS authentication, adding a layer of user-level authentication.

Guest Network

Many access points support the creation of a guest network, which provides internet access but isolates guests from the internal network.

2.5. Configuration:

- ✓ Separate SSID for guest access.
- ✓ Limit bandwidth for guest users.
- ✓ Enable client isolation to prevent guests from communicating with each other.

DHCP Settings

- o Dynamic Host Configuration Protocol (DHCP) assigns IP addresses to devices on the network. Access points can act as DHCP servers, assigning addresses to connected devices.
- o Alternatively, they can be set to use an external DHCP server, typically handled by the router.

Transmit Power Control

- o Transmit Power: Controls the strength of the wireless signal.
- o Lower power settings can reduce interference and make the network more secure by limiting the range of the signal. Higher

power is used when covering large areas or when more range is needed.
    - Adjusting transmit power can help in environments where multiple access points are deployed, reducing overlap and interference.

MAC Filtering

- MAC Address Filtering: Allows you to specify which devices (by their MAC addresses) are allowed or denied access to the network. This adds another layer of security but can be cumbersome to manage in larger networks.

QoS (Quality of Service)

- QoS Settings allow prioritizing certain types of network traffic, such as video streaming, VoIP, or gaming, to ensure those services get more bandwidth and lower latency.
- Configuring QoS is particularly important in environments with multiple users or bandwidth-sensitive applications.

VLAN (Virtual Local Area Network) Configuration

- VLAN support allows the segregation of network traffic on a single access point.
- You can configure different VLANs for various user groups (e.g., guests, staff) to improve security and network performance.

Firmware Updates

- It’s important to keep the access point's firmware up to date. Firmware updates often include security patches, bug fixes, and performance improvements.
- Most modern access points allow for automatic updates, but this should be managed to avoid interruptions.

Roaming Settings

- If there are multiple access points in the network, seamless roaming can be configured to allow devices to move between access points without losing connection.
- 802.11r (Fast Roaming) and 802.11k/v are protocols used to optimize roaming between access points.

Band Steering

- Band Steering encourages dual-band devices to connect to the 5 GHz band (which typically has more capacity and less congestion) instead of the 2.4 GHz band.
- This helps balance the load between the two frequency bands and improves overall network performance.

Mesh Network Settings

- If the access point is part of a wireless mesh network, configuration

options will involve setting up nodes (other access points) to extend the coverage without requiring wired connections between them.

Client Isolation

- Client Isolation prevents devices connected to the access point from communicating with each other directly, which is useful for public networks or guest networks to improve security.

Logging and Monitoring

- Logging tracks connection attempts, device status, and other events, providing useful data for troubleshooting and monitoring.
- Many access points offer real-time monitoring tools to view connected devices, signal strength, data usage, and other network metrics.

Practical Activity 2.3.2: Configuring wireless Network Devices

Task:

1: Read carefully and perform this task accordingly
Refer to the previous practical activity 2.2.4, go where the wireless devices were installed and then configure those Wireless devices.

2: Listen to the work instructions and guidelines

3: Follow the demonstration for the process of configuring wireless network outdoor devices

4: Configure wireless network devices by yourself by following the demonstrated process

5: Ask questions or clarifications if any.

6: Read key readings 2.3.2 and do the application of learning 2.3

Key readings 2.3.2: Configuring wireless network devices

1. Access Point Configurations for Wireless Network Outdoor

When deploying wireless networks outdoors, configuring the access points (APs) correctly is crucial to ensure optimal coverage, performance, and security. Here are the key configurations required for outdoor access points:

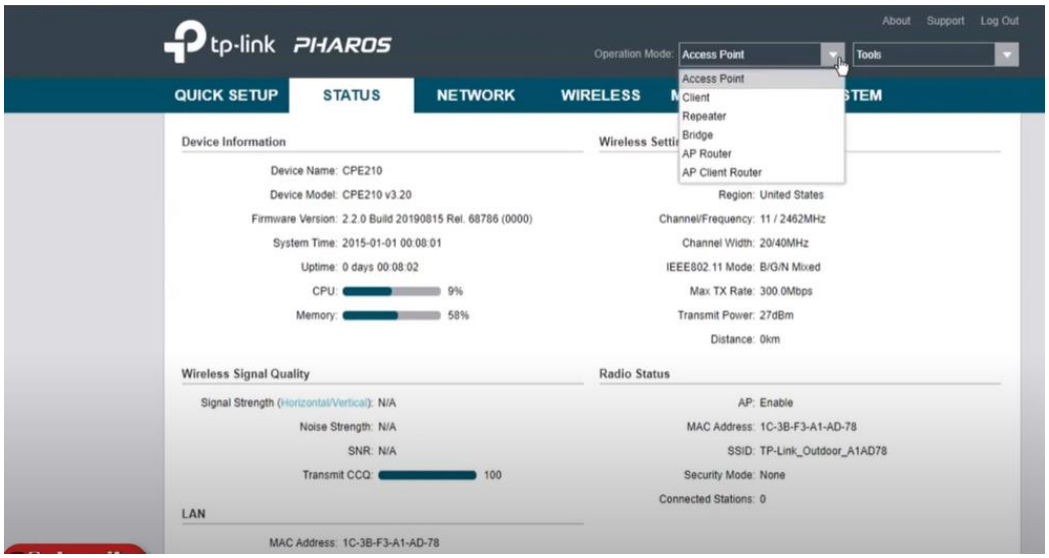
1.1. Basic Wireless Settings

✓ **Follow these steps to configure basically access point:**

Step 1:Assign SSID

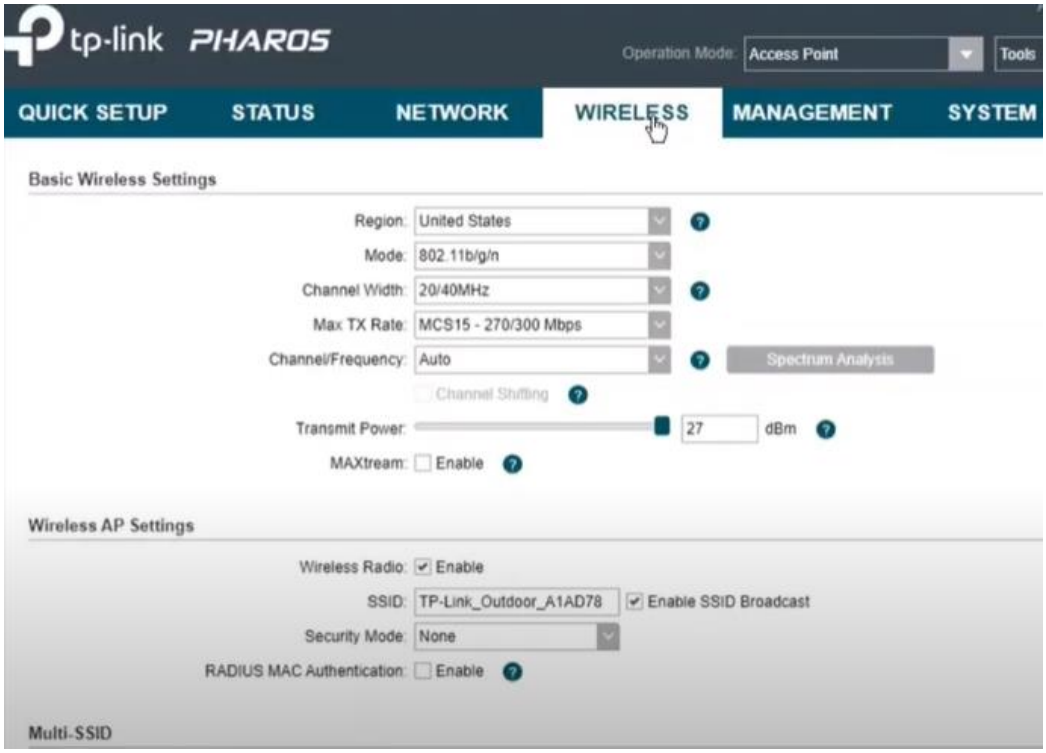
- Assign a clear, identifiable SSID for the outdoor network (e.g., "CampusOutdoorWiFi").
- Consider creating a separate guest network with limited access by enabling multiple **SSIDs (e.g., "GuestWiFi").**

Step 2:Choose operation mode



- Access Point (AP) Mode: Typically, outdoor APs should be configured in AP mode to broadcast the wireless network.
- Bridge Mode: In cases of connecting two locations via Point-to-Point (PtP) or Point-to-Multipoint (PtMP) links, one AP may be set as the transmitter (Access Point) and the other as a receiver (Client Mode).
- Mesh mode: configuring multiple APs to work together as a single, seamless wireless network

Step 3:Select Frequency Band



- **5** GHz Band: Preferable for outdoor deployments because it offers more channels and less interference compared to 2.4 GHz. It's especially useful in environments with high Wi-Fi traffic.
- 2.4 GHz Band: Offers better range but is more prone to interference. It might still be used in open, less crowded areas or for legacy devices.

- Channel Width

- 20 MHz, 40 MHz, or 80 MHz: Configure wider channel widths (40 MHz or 80 MHz) for higher data rates, but keep in mind that wider channels are more prone to interference.

- Channel Selection

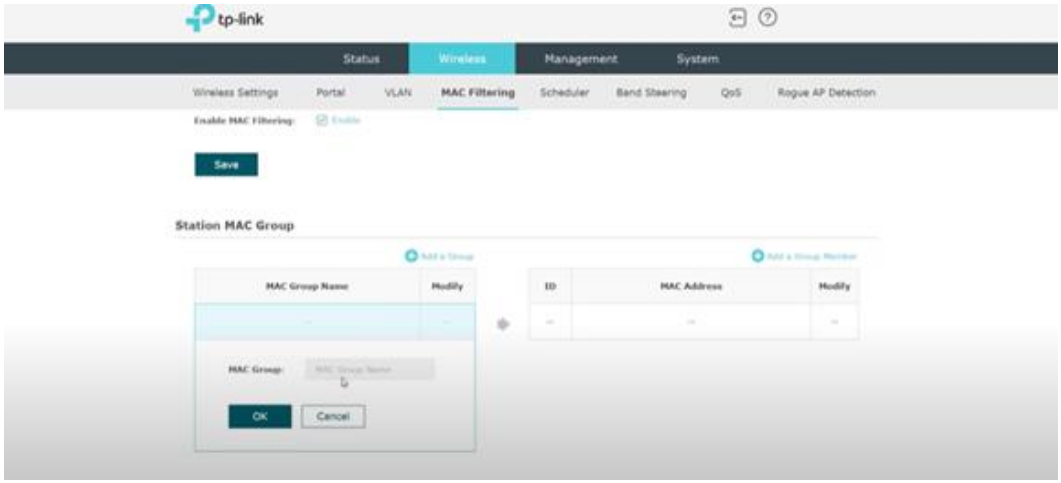
- Auto or Manual: It is often recommended to manually choose channels to avoid interference with nearby networks. Use a Wi-Fi analyzer tool to select the least congested channel**.**

Step 4:Configure Security Settings

✓ **Encryption and Authentication**

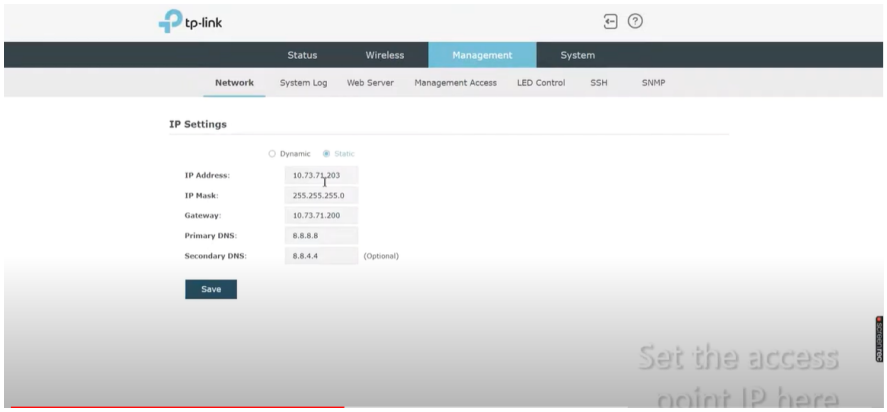
- WPA2/WPA3 Encryption: Set the wireless security mode to WPA2-PSK (Pre-Shared Key) or WPA3-PSK for stronger encryption.
- Password/Passphrase: Ensure a strong password to prevent unauthorized **access.**

✓ **MAC Address Filtering**



- You can enable MAC address filtering to limit access to specific devices (e.g., only authorized laptops or phones can connect).

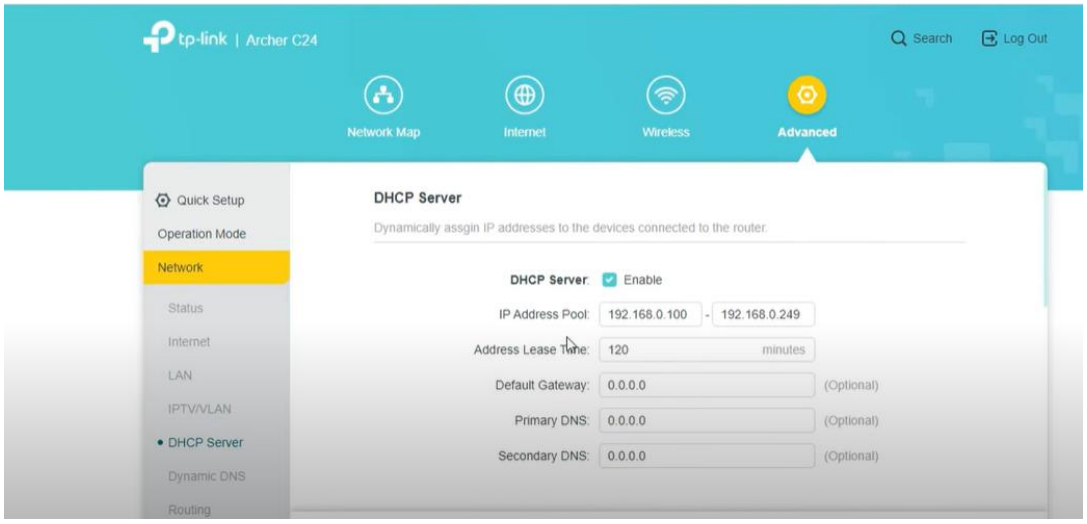
Step 5:Configure IP Addressing and Networking



✓ **IP Address Configuration**

- Assign static IP addresses to each outdoor AP for easier management and troubleshooting.
- Make sure the IP addresses of the APs are in the same subnet as the rest of your network or define a new management subnet for outdoor devices.

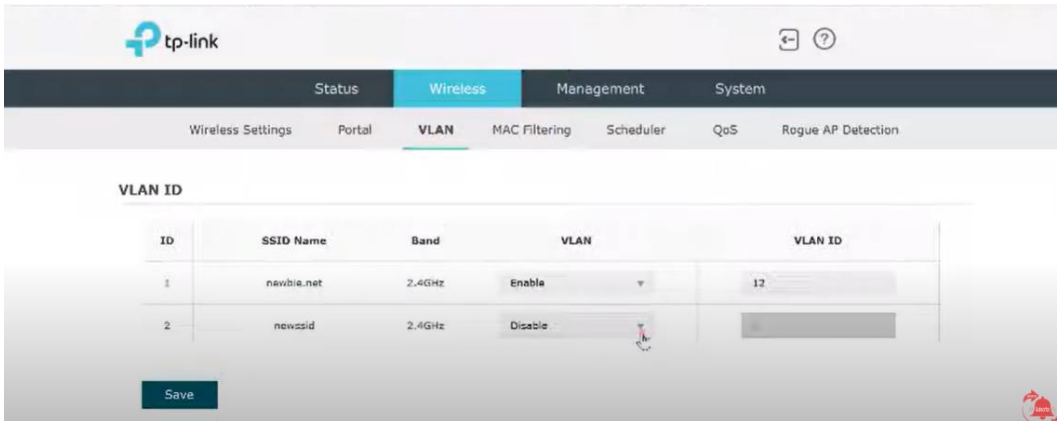
Step 6:Enable DHCP Settings



APs can be configured to either:

- Obtain an IP address dynamically from a DHCP server on the network (useful for client devices).
- Act as a DHCP server in some cases (this is rare for outdoor APs unless you're setting up an isolated network).

Step 7:Configure VLAN



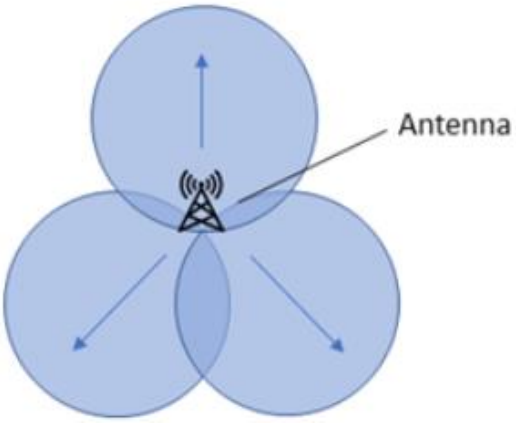
- Assign VLAN IDs to separate traffic for different SSIDs or to segment guest traffic from internal network traffic**.**

2. Advanced Wireless Settings

✓ **Adjust the Transmit Power**

- Adjust the transmit power to control the coverage area of the AP.
- High power for long-range links or large open areas.
- Lower power for smaller, more focused coverage to prevent interference**.**

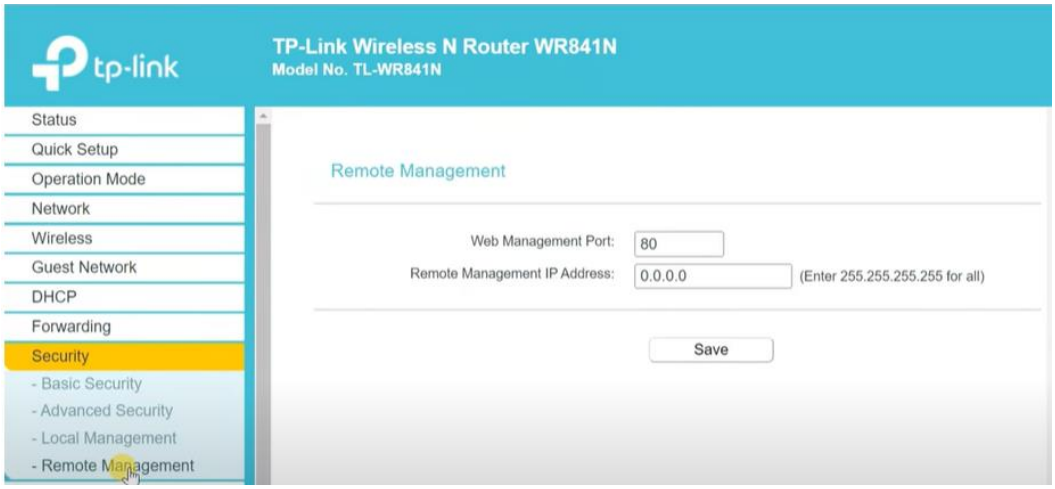
✓ **Align antennas in good direction (For Directional Antennas)**



- Proper alignment is critical for Point-to-Point (PtP) or Point-to-Multipoint (PtMP) links. Use built-in signal meters or external tools to fine-tune the antenna alignment for the strongest signal.

✓ **Configure QoS settings** to prioritize certain types of traffic, such as VoIP, video conferencing, or critical applications, to ensure these services get sufficient bandwidth.

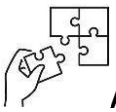
3. Configure Remote Management



- Enable remote management to access and control the outdoor APs from a centralized location or a cloud-based controller.

Points to Remember

- Choose a recognizable and unique SSID.
- Optionally, hide the SSID to prevent it from being visible to casual users (though this does not add significant security).
- Properly configuring access point settings ensures optimized performance, strong security, and reliable coverage for all users on the wireless network.
- Any issues identified can be resolved by reconfiguring settings or adjusting the network design, ensuring the school has a robust wireless system in place for seamless communication across campuses.
- Ensure the network is secure and protected from unauthorized access.
- Set strong password to enhance security
- Record key configurations for each access point, such as the SSID, security settings, IP addresses, and channels used
- Ensure that the selected channels are free from heavy interference from neighbouring networks.



Application of learning 2.3.

You are tasked with configuring a robust outdoor wireless network for a university campus. The network must provide consistent and reliable connectivity across various outdoor areas, including courtyards, walkways, and sports fields, ensuring that students, staff, and guests can access the internet and campus resources seamlessly.

Indicative content 2.4: Testing of Deployed Wireless Network Outdoor

Duration : 5hrs

Theoretical Activity 2.4.1: Description of the basic tests for the deployed wireless network

Tasks:

1: Respond to the following questions:

i. Describe the following terms:

a. Connectivity testing

b. Security testing

c. Performance testing

ii. Identify the main tools used to test connectivity , security and performance

2: Write your answers on a paper or flipchart

3: Present your answers to the whole class

4: Ask questions or clarification if necessary

5: Read the key readings 2.4.1 and do the application of learning 2.4

Key readings 2.4.1: Description of the basic tests for the deployed wireless network

- **Description of the terms:**

✓ **Connectivity Testing**

- Connectivity testing refers to the process of verifying that devices can reliably connect to a network and communicate with each other.
- It involves checking the coverage, signal strength, and stability of the wireless connection across different locations.
- This type of testing ensures that the network provides consistent and uninterrupted connectivity, even in challenging environments or at various distances from access points.

✓ **Security testing** :

- Security testing involves evaluating the safety measures of a network to protect it against unauthorized access, data breaches, and other security threats.
- It checks for vulnerabilities in encryption protocols, authentication mechanisms,

and network configurations that could be exploited by attackers.

- This process may include activities like penetration testing, monitoring for unauthorized devices, and verifying compliance with security standards. The goal is to ensure that the network is secure and resilient against potential threats.

✓ **Performance testing**

- Performance testing assesses the efficiency and speed of a network by measuring key metrics such as throughput (data transfer rate), latency (response time), jitter (variation in response time), and packet loss.
- This type of testing ensures that the network can handle the expected load and deliver consistent performance, even under heavy usage.
- It involves stress testing the network by connecting multiple devices, running speed tests, and analyzing data to identify any bottlenecks or areas for improvement.

- **Main tools used to test connectivity , security and performance**

2.1. Connectivity Testing Tools

✓ **Wi-Fi Analyzer**: Tools like NetSpot, inSSIDer, and WiFi Explorer are used to scan wireless networks, check signal strength, and identify available Wi-Fi channels. They help in detecting issues related to coverage and interference.

✓ **Ekahau Site Survey:** A professional tool for planning, deploying, and validating wireless networks. It helps in conducting site surveys and checking the overall connectivity of the network.

✓ **Acrylic Wi-Fi:** A tool for monitoring and analyzing Wi-Fi connections, showing details like signal quality, coverage, and access point performance**.**

2.2. Security Testing Tools

✓ **Wireshark:** A network protocol analyzer that captures and inspects data packets. It can be used to monitor network traffic for suspicious activity and identify security vulnerabilities.

✓ **Aircrack-ng:** A suite of tools for testing Wi-Fi network security, including packet sniffing, WEP and WPA cracking, and network monitoring.

✓ **Nmap:** A network scanning tool used for network discovery and security auditing. It helps identify open ports, services, and potential vulnerabilities on connected devices.

✓ **Kali Linux:** A specialized Linux distribution containing multiple tools (e.g., Metasploit, Burp Suite, John the Ripper) for penetration testing and security analysis.

✓ **WPA3 Compliance Test Tools:** Tools specifically designed to check the encryption protocols and authentication mechanisms, ensuring they adhere to security standards like WPA3.

2.3. Performance Testing Tools

✓ **iPerf:** A network testing tool that measures bandwidth, latency, and packet loss.

It is commonly used to test network throughput between two points on the network.

- ✓ **NetFlow Analyzer**: A performance monitoring tool that tracks network traffic, analyzes bandwidth usage, and detects network anomalies.
- ✓ **Speedtest by Ookla**: A simple and widely-used tool to test internet speed, providing information on download and upload speeds as well as latency.
- ✓ **SolarWinds Network Performance Monitor (NPM):** An enterprise-level tool that monitors network performance, tracks real-time data, and helps identify bottlenecks.
- ✓ **PingPlotter:** A visual tool to measure latency, packet loss, and network path issues, providing insights into the performance and stability of the network.

Practical Activity 2.4.2: Testing the deployed wireless network outdoor

Task:

1: Read carefully and perform this task accordingly

Referring to the practical activity 2.3.2, test the Deployed wireless network for connectivity, security, and performance to ensure that the network meets the required standards for reliable and secure wireless communication.

2: Listen to the instructions and guidelines

3: Follow the demonstration for the process of testing the deployed wireless network

4: Perform the activity of testing the deployed wireless network 3 by yourself

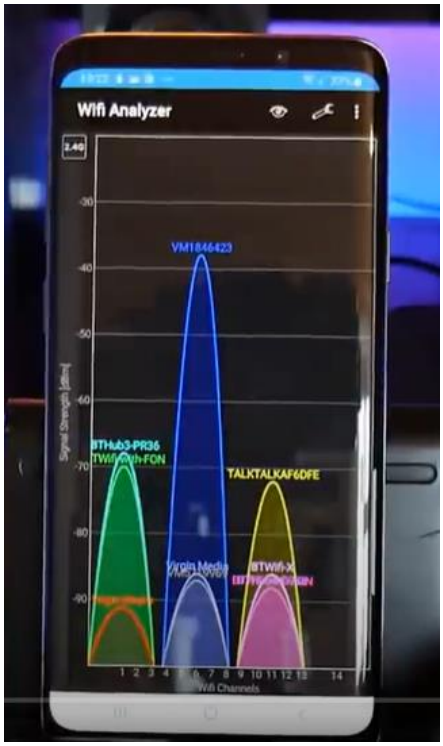
5: Ask questions or clarifications if any.

6: Read key readings 2.4.2 and do the application of learning 2.4.

Key readings 2.4.2: Deployed wireless network outdoor can be tested for connectivity, security and performance through the following steps:

1. **Connectivity Testing:** Verify that all areas within the coverage range of the access points have strong and stable connectivity**.**

Step 1:Check Wireless Signal Strength:



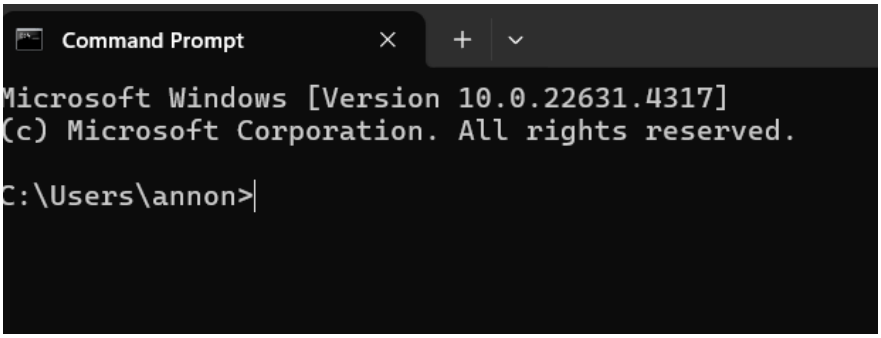
- Use a Wi-Fi analyzer or mobile app (such as WiFi Analyzer for Android or AirPort Utility for iOS) to measure signal strength (in dBm) at various locations on the campus.
- Record signal strength values at key points: outdoor playgrounds, walkways, and between buildings.
- Criteria: Signal strength should ideally be between -30 dBm (excellent) and -70 dBm (acceptable).

Step 2: Perform the Roaming Test:

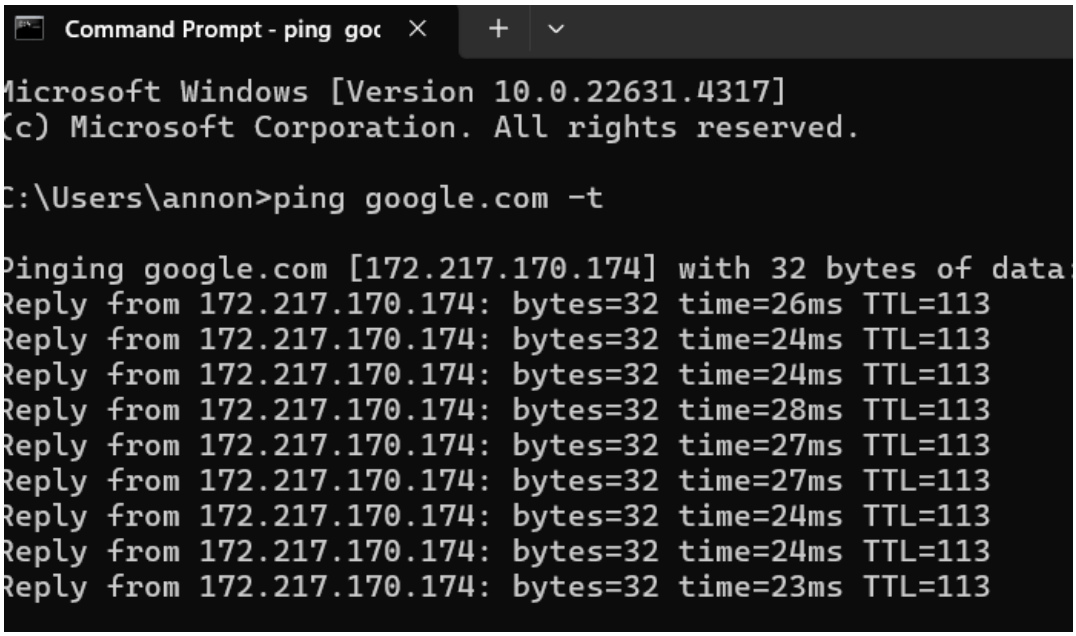
- Walk around the campus with a connected device (laptop, smartphone, or tablet) to test seamless handoff between access points.
- Monitor whether the device switches between access points smoothly without dropping the connection.
- Criteria: No noticeable loss of connection or drop in signal during handoff between access points.

Step 3: Ping Test:

- Open command prompt from server side.



✓ Type the following command: ”ping google.com-t” and get the result.



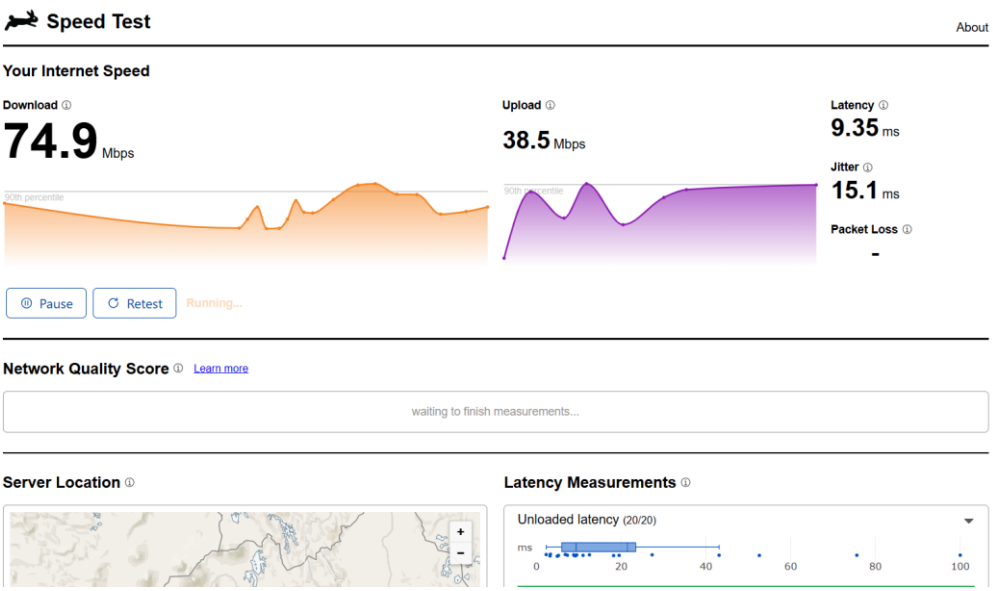
- From various locations, perform a ping test to a server or a known IP address on the network.
- Record the latency (in milliseconds) and any packet loss.
- Criteria: Latency should be low (<50ms), with minimal to no packet loss.

2. **Performance Testing**: Measure the network's throughput and performance under normal and high-load conditions**.**

✓ **Bandwidth and Throughput Test:**

✓ **Speed Test:**

– Use speed test app to measure network speed in downloading and uploading streams



- Perform a speed test (e.g., using Speedtest.net) from different locations on the campus to measure download and upload speeds.
- Criteria: Speeds should be close to the service provider's promised rate.

✓ **Load Testing:**

- Simulate high user traffic by connecting multiple devices to the network simultaneously (e.g., 20+ devices).
- Measure how the network handles the increased load and whether it maintains consistent performance.
- Criteria: No significant drop in network speed or connectivity issues under heavy load.

3. **Security Testing:** Ensure the wireless network is secure and that only authorized users can access it.

Steps:

✓ **Verify Encryption Settings:**

- Check that the network is using WPA2 or WPA3 encryption and that no unencrypted networks are available.
- Attempt to connect to the network without entering a password to confirm that encryption is enforced.
- Criteria: Only authorized devices with the correct credentials should be able to connect to the network.

✓ **Access Control Testing:**

- Test MAC address filtering (if enabled) by attempting to connect unauthorized devices to the network.
- Check whether guest networks are isolated from the primary network and have limited access.
- Criteria: Unauthorized devices should not be able to connect to the main

network**.**

✓ **Firewall and Intrusion Detection:**

- If the network includes a firewall, attempt to access restricted services (e.g., servers or admin panels) to ensure the firewall blocks unauthorized access.
- Test the intrusion detection system (IDS) by simulating abnormal network behavior (such as multiple failed login attempts).
- Criteria: The firewall should block unauthorized access, and the IDS should detect any suspicious activities.

4. **Signal Interference Testing:** Identify and mitigate any potential interference that may degrade wireless signal quality.

   Steps:

✓ **Channel Overlap Test:**

- Use a Wi-Fi analyzer to check if any other nearby networks are operating on the same channels as your network.
- If interference is detected, change the Wi-Fi channel on the access points to reduce overlap.
- Criteria: Ensure that the selected channels are free from heavy interference from neighboring networks.

✓ **Environmental Interference Test:**

- Walk around the campus with a connected device and note any locations where signal quality drops significantly, possibly due to physical obstructions (trees, walls) or electromagnetic interference (e.g., from nearby electrical equipment).
- Criteria: Identify and mitigate areas of interference by repositioning access points or adjusting the antenna orientation.

5. **Reporting and Documentation:** Record all findings from the tests to ensure future maintenance and troubleshooting can be handled effectively.

   Steps:

✓ **Document the Results:**

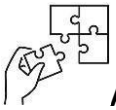
- Write a report detailing signal strength measurements, ping test results, speed test results, and any identified issues.
- Provide recommendations for improving network performance or resolving any issues encountered.

✓ **Log Configuration Settings:**

- Record key configurations for each access point, such as the SSID, security settings, IP addresses, and channels used.
- This will be useful for future maintenance or network expansion.

Points to Remember

- You have to check the coverage, signal strength, and stability of the wireless connection across different locations for verifying that devices can reliably connect to a network and communicate with each other.
- Ensure that the network is secure and resilient against potential threats by evaluating the safety measures of a network to protect it against unauthorized access, data breaches, and other security threats.
- Use properly the tools which corresponds to the testing type for getting accurate result.
- For connectivity testing, focus on coverage, signal strength, stability, and user experience.
- For security testing, assess vulnerabilities, conduct penetration testing, monitor for threats, and ensure compliance.
- For performance testing, measure throughput, latency, jitter, packet loss, and conduct load testing.
- Make sure that you use specialized tools for each testing type to ensure thorough and accurate assessments.



Application of learning 2.4.

XYZ School has recently deployed wireless network outdoor for their new building, they need you to test that network for connectivity, security, and performance to ensure that the network meets the required standards for reliable and secure wireless communication.

Learning outcome 2 end assessment

Written assessment

Multiple choice questions

1. **Circle the correct answer**

I. Which of the following is a cutting tool?

a) Ethernet Cable

b) Wire Stripper

c) Outdoor Antenna

d) Nano Station

II. Which equipment is used to prevent power surges from damaging network devices?

a) Firewall

b) Lightning Arrestor

c) Ethernet Cables

d) Access Point

III. What does IEEE802.11ac refer to?

a) Cable manager

b) Wireless standard

c) Testing tool

d) Power-Over-Ethernet

IV. Which device connects multiple network devices and forwards data based on MAC addresses?

a) Router

b) Network switch

c) Wireless extender

d) Nano Station

2. **Write true if the statement is correct and false if it is not correct**

I. Ethernet cables are materials used in network installation.

II. A Point-to-Multipoint (PtMP) wireless bridge is used to connect a single device to a network.

III. A crimping tool is used to terminate cables by attaching connectors.

IV. IEEE802.11n is a wireless standard that supports only outdoor wireless networks.

V. A UPS is used to ensure continuous power to network equipment during power outages.

3. Match The elements/ devices in the column A with their role in column B by writing the letter corresponding to the correct uses

Answer	Column A	Column B
1……..	1.Wireless extender	A. Ensures uninterrupted power
2……..	2. Patch tools	B. Used for cable management
3……..	3.PoE (Power-Over-Ethernet)	C. Extends the wireless network
4……..	4. Rack mount	D. Provides power through Ethernet cable
5……..	5. Cable manager	E. Used for cable repairs

Practical assessment

You have been hired by a small business located in a multi-building campus environment to deploy an outdoor wireless network. The business requires seamless and reliable wireless connectivity across the entire campus to support day-to-day operations, including secure communication, video conferencing, and file sharing. You are tasked with selecting the appropriate tools, materials, and equipment, install and configure wireless devices, connect three main buildings and an outdoor recreational area and then test the deployed network for connectivity, performance and security.

END

References

Ciprian Adrian Rusen (Mars, 2020), How to choose a wireless router: 10 things to consider, URL: https://www.digitalcitizen.life/things-consider-when-buying-wireless router Accessed on April 17 2023.

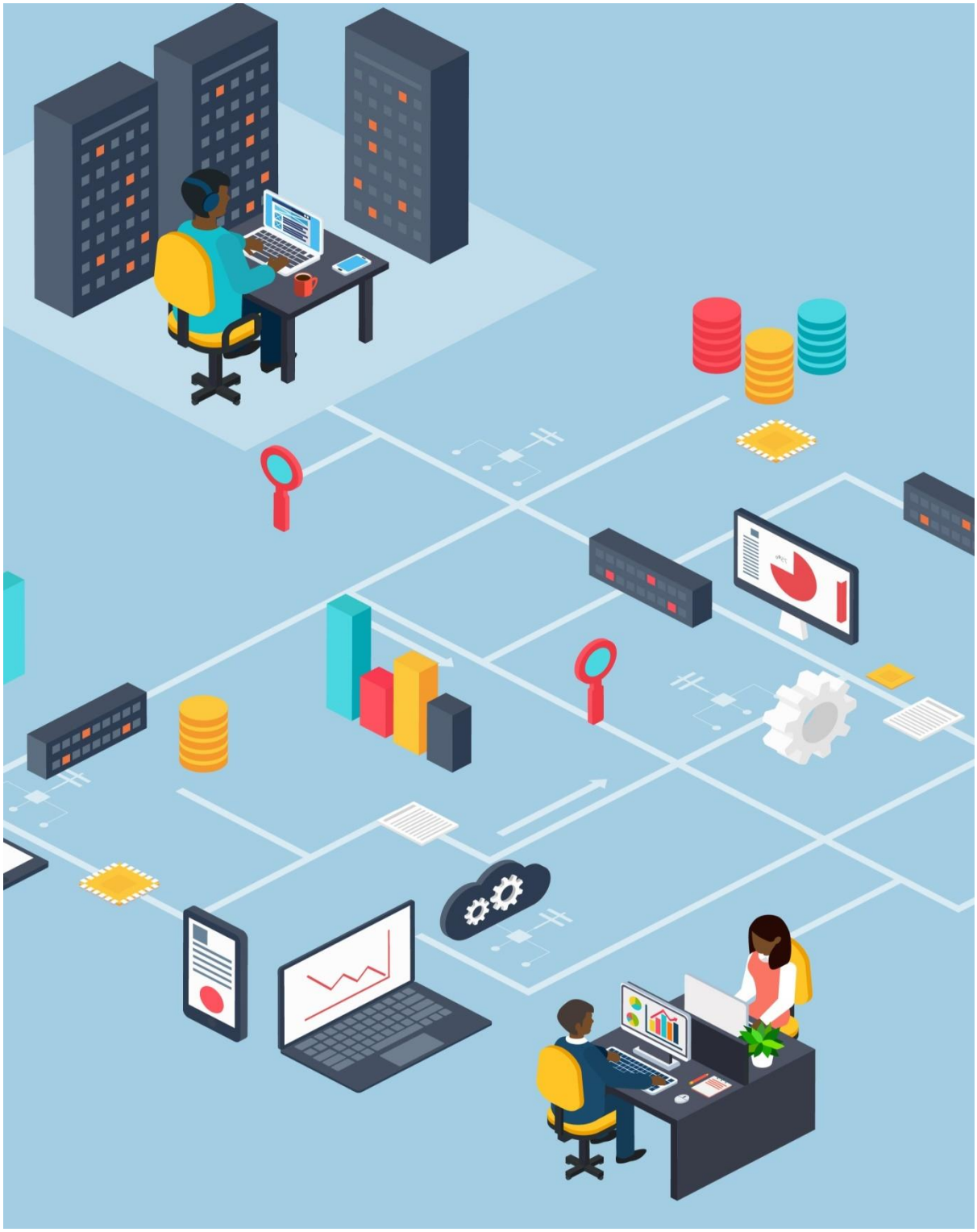
https://www.akibia.com/what-factors-to-consider-when-selecting-network-cabling/

Lee, B. (2023, August 5). Understanding Signal Strength and SNR. Retrieved from Wireless Tech Insights: www.wirelesstechinsights.com/signal-strength

Mark Kyrnin (June 2020), Installing a PCI Adapter Card, URL: https://www.lifewire.com/pci-adaptercard-installation-833860

Matthew S. Gast (2005). 802.11 Wireless Networks. The Definitive Guide, Second Edition. O'Reilly Media. Pp 187-317.

URL: http://blog.dlink.com/how-to-extend-your-network-with-a-wireless-bridge/



Indicative contents

3.1 Monitoring wireless network Outdoor

3.2 Troubleshooting wireless network Outdoor

3.3 Upgrading wireless network Outdoor

3.4 Document wireless network Outdoor

Key Competencies for Learning Outcome 3: Maintain wireless network outdoor

Knowledge	Skills	Attitudes
• Description of wireless network outdoor Monitoring Metrics • Identification of tools used in network performance monitoring • Description of wireless controllers in managing multiple access points • Description of hardware components potential failure points. • Description of diagnostic commands for network troubleshooting • Description of wireless network	• Analysing wireless outdoor monitoring metric findings • Selecting monitoring metric tools used in wireless outdoor • Conducting physical inspections of wireless hardware • using diagnostic commands • Developing technical reports • Generating a technical journal for tracking wireless outdoor network changes	• Being Attentive to Detail while Analysing wireless outdoor monitoring metric and conduct physical inspections of wireless hardware • Being analytical thinker on Selecting monitoring metric tools • Being Proactive while monitoring and troubleshooting wireless network outdoor • Being Problem-Solver while troubleshooting wireless network outdoor • Being organized while Developing technical reports and maintaining a technical journal

outdoor upgrade ● Description of technical report and Technical Journals		

Duration:20 hrs

Learning outcome 3 objectives:

By the end of the learning outcome, the trainees will be able to:

1. Describe clearly Monitoring Metrics as used in wireless network outdoor
2. Describe clearly Monitoring Tools used in wireless network outdoor
3. Describe clearly Access Point Controllers based on monitoring metric
4. Conducting clearly physical inspections of wireless outdoor network hardware.
5. Describe clearly hardware components for potential failure points
6. Troubleshoot correctly wireless network Outdoor based environment fact
7. Use correctly troubleshooting Diagnosing commands of wireless network outdoor
8. Upgrade correctly wireless network Outdoor based on factor of wireless network outdoor
9. Generate properly technical reports and Technical journal of wireless network Outdoor

Resources

Equipment	Tools	Materials
• Router • Wireless Extender • Firewall • PoE • Switch • UPS	• Ladder • Drilling machine • Tape Measure • Hummer • Networking tool Kit • Cable tester • Clipping tools • Cisco packet tracer • Edrawmax	• Connector (RJ45) • Cable ties • Screws • Internet Bundles • Nails • Network cables

	● GSN3 ● Wireshark ● Solar Wind network performance ● Wi-Fi Analyser(insider, NetSpot) ● PRTG Network Monitor ● Wi-Spy Spectrum Analyze ● PingPlotter	

Indicative content 3.1: Monitoring wireless Network Outdoor.

Duration: 4hrs

Theoretical Activity 3.1.1: Description of monitoring metrics and tools

Tasks:

1: Answer the following questions:

i. Describe the following monitoring metrics :
   a. Signal Strength (Bandwidth and Latency)
   b. Signal to noise Ratio
   c. Data throughput
   d. Jitter
   e. Packet Loss and Re-transmissions

ii. Describe the following monitoring tools
   a. Monitoring Tools
   b. Wireshark
   c. Solar Winds Network Performance
   d. Wi-Fi Analyser

iii. Describe clearly Access points controllers

2: Write your findings on paper or flipchart

3: Present your findings in front of the whole class

4: Ask for clarification where necessary

5: Read the key readings 3.1.1

Key readings 3.1.1.: Description of monitoring metrics and tools

1. **Definition**

Network performance refers to the quality and effectiveness of a network system. It involves evaluating and reviewing the speed, connectivity, reliability, and efficiency of a network.

Key indicators of network performance include bandwidth, latency, throughput, jitter, and error rate. High-performing networks reliably transmit high volumes of data quickly and securely, with minimal delays or errors, improving productivity and user experience.

Wireless network monitoring metrics are measurements used to assess the

performance, reliability, and efficiency of a wireless network

2. Key indicators of network performance

2.1. Signal Strength

Signal strength is a measurement of the power level that a wireless device, such as a laptop, smartphone, or tablet, receives from a wireless access point (AP**)**

2.2. Bandwidth

Bandwidth represents the utmost data volume that can be transmitted between network points within a specified timeframe, usually quantified as bits per second (bps), kilobits per second (Kbps), or megabits per second (Mbps).

Administrators reference bandwidth when planning network expansions or when troubleshooting slow network speeds to ensure capacity aligns with demands.

2.3. Latency

This is the delay that occurs while data is being transferred from one point to another, impacted by factors like distance and network congestion, and measured in milliseconds (ms). In applications where real-time communication is vital, such as VoIP or video conferencing, administrators monitor latency to ensure seamless data transmission.

2.4. Signal-to-Noise Ratio (SNR)

The ratio of the signal power to the noise power or is a measure that compares the level of the wireless signal (signal strength) to the level of background noise. A higher SNR indicates a clearer and stronger signal, which generally results in better network performance and reliability

2.5. Data Throughput

It measures the actual quantity of data that is successfully transferred from one point to another over a given period, and is usually lower than bandwidth due to hindrances like data errors or network congestion.

Administrators analyze throughput to verify if a network is performing at its expected efficiency and to identify any potential bottlenecks.

2.6. Jitter

Jitter refers to the variability in packet arrival times in a network. It is the fluctuation in the time taken for data packets to travel from the source to the destination. Jitter is especially important for time-sensitive applications like VoIP (Voice over IP), video conferencing, and online gaming, where consistent packet delivery is crucial.

2.7. Packet Loss and Re-transmissions

The percentage of packets that are lost during transmission. High packet loss can degrade network performance and impact applications.

2.8. Re-transmissions

The process of sending packets again due to loss or errors. Frequent re-transmissions can indicate network issues and affect overall performance.

3. Monitoring Tools

Are software applications or hardware devices used to track and analyze the performance, health, and security of a network or system.

3.1. Wireshark

✓ **Overview:**

Wireshark is a powerful open-source network protocol analyzer that allows you to capture and inspect data traffic on a network. It is commonly used for troubleshooting, analyzing, and monitoring wired and wireless network communications

✓ **Key Features**

- **Packet Capture**: Wireshark can capture and display real-time data packets passing through the network, making it possible to see what data is being transmitted and received.
- **Protocol Analysis**: It supports a wide range of protocols (e.g., TCP, UDP, ICMP) and can help identify specific issues such as high latency, packet loss, or re-transmissions.
- **Filtering Capabilities:** Wireshark allows users to filter packets based on specific protocols, IP addresses, ports, or other parameters, making it easier to focus on relevant data.
- **Decryption Support:** It can decrypt traffic for some protocols, including wireless protocols like WPA2, allowing deeper analysis of wireless network traffic.

✓ **Use Cases:**

- **Diagnosing network issues** such as slow performance, packet loss, or jitter by analyzing traffic flow and identifying where problems arise.
- **Capturing wireless traffic** to analyze signal strength, interference, and potential security vulnerabilities.

✓ **Strengths:**

- Extremely detailed packet-level analysis.
- Wide protocol support and powerful filtering options.
- Can be used for both wired and wireless networks.

✓ **Limitations:**

- Requires in-depth knowledge to interpret complex network data.

- Real-time analysis can be resource-intensive on large networks.

3.2. SolarWinds Network Performance Monitor (NPM)

✓ **Overview:**

SolarWinds Network Performance Monitor is a commercial, enterprise-grade tool designed to monitor and manage the performance of a network. It provides comprehensive visibility into network devices and infrastructure, making it ideal for large-scale environments, including wireless outdoor deployments.

✓ **Key Features**

- **Network Performance Monitoring:** SolarWinds NPM can track key performance metrics such as latency, packet loss, jitter, and throughput for wireless and wired devices.
- **Customizable Dashboards:** Users can create personalized views that show real-time network health, with data presented via charts, graphs, and alerts**.**
- **Network Mapping**: It provides visual representations of the network topology, showing how devices are connected, helping to easily locate performance bottlenecks**.**
- **Wireless Heat Maps:** It can create wireless heat maps, showing the coverage and signal strength of access points in specific areas**.**
- **Alerting System:** Configurable alerts can notify users of network performance issues such as high packet loss or bandwidth saturation**.**

✓ **Use Cases:**

- Proactive network monitoring by tracking the performance of wireless access points and other network devices.
- Generating reports and alerts to respond quickly to performance degradation or hardware failure.
- Monitoring wireless environments to optimize signal strength, bandwidth usage, and device configuration.

✓ **Strengths:**

- Scalable and suitable for both small and large networks.
- Provides clear visualizations and in-depth monitoring.
- Supports automated alerting for quick issue resolution.

3.2.1. Limitations:

- Requires a subscription or license, making it less accessible for smaller operations.
- Setup can be complex for new users or smaller networks

3.3. Wi-Fi Analyzer

✓ **Overview:**

Wi-Fi Analyzer is a user-friendly tool that helps monitor and analyze wireless networks by visualizing the signal strength and channel usage of nearby Wi-Fi networks. It is commonly used for quick and basic analysis of wireless environments, helping users to optimize access points and network performance.

✓ **Key Features**

- **Signal Strength Measurement:** Wi-Fi Analyzer shows real-time graphs of signal strength for all detected Wi-Fi networks, making it easy to identify which networks provide the strongest signals in a given area.
- **Channel Utilization:** It identifies which channels are most used or congested, helping you choose less crowded channels for your wireless network, reducing interference.
- **Network Graphs:** Displays graphical information about access points, their signal strengths, and their interference with neighboring networks.
- **Real-Time Analysis:** Provides live updates on the performance and strength of the Wi-Fi signal as you move around, allowing for easy adjustments to access points or antenna positions.

✓ **Use Cases:**

- **Optimizing wireless coverage** by identifying weak signal areas and adjusting access point placement.
- **Reducing interference** by switching to less congested Wi-Fi channels, improving performance and signal quality.
- **Troubleshooting network performance** by checking signal strength in different areas and finding optimal AP locations.

✓ **Strengths:**

- Easy to use for both beginners and advanced users.
- Ideal for quick wireless troubleshooting and optimization.
- Available on multiple platforms (Windows, Android, iOS)..

✓ **Limitations:**

- Limited in-depth analysis compared to tools like Wireshark or SolarWinds.
- Primarily used for signal strength and channel interference analysis, not deep packet inspection.

4. Access Point Controllers

Access Point Controllers are network devices or software solutions designed to manage and control multiple wireless access points (APs) within a network.

They provide centralized management and coordination to ensure optimal performance, security, and coverage across the wireless network.

4.1. Function

- **Centralized Management**: Provides a unified platform for configuring, managing, and monitoring multiple access points from a single location. This simplifies network administration and ensures consistency across the network.
- **Coordination**: Coordinates the operation of all connected access points to ensure seamless coverage and performance. It manages channel assignments, power levels, and load balancing among APs.
- **Load Balancing**: Distributes client connections evenly across access points to prevent overloading any single AP and to maintain optimal network performance.
- **Configuration**: Enables centralized configuration of network settings such as SSID (Service Set Identifier), security protocols, and network policies.

✓ **Key Features**

- **Unified Dashboard**: Offers a central interface where network administrators can view and manage the status and performance of all connected APs. It provides insights into network health, usage patterns, and potential issues.
- **Firmware Updates**: Allows administrators to push firmware updates to all APs simultaneously, ensuring that all devices run the latest software for security and performance enhancements.
- **Network Optimization**: Includes tools for optimizing network performance, such as automatic channel selection to minimize interference and adjusting power levels to enhance coverage.
- **Security Management**: Implements and enforces security policies across all APs, including encryption standards, authentication methods, and access controls.
- **Monitoring and Reporting**: Provides real-time monitoring of metrics such as signal strength, client connectivity, and network traffic. It generates reports to help analyze performance trends and diagnose issues.

✓ **Benefits**

- **Ease of Management**: Simplifies network administration by consolidating control of all access points into a single platform, reducing the complexity of managing a large network.
- **Scalability**: Facilitates the addition of new access points without extensive reconfiguration, making it easier to expand network coverage as needed.
- **Consistency**: Ensures uniform configuration and policies across all access points, improving network reliability and user experience.

- **Troubleshooting**: Helps identify and resolve network issues by providing detailed performance metrics and diagnostic tools.

Practical Activity 3.1.2 : Measuring Signal Strength, signal to noise Ratio(SRN), Data throughput, Jitter, Packet Loss and Re-transmissions using Acrylic Wi-Fi Analyzer network monitoring tool

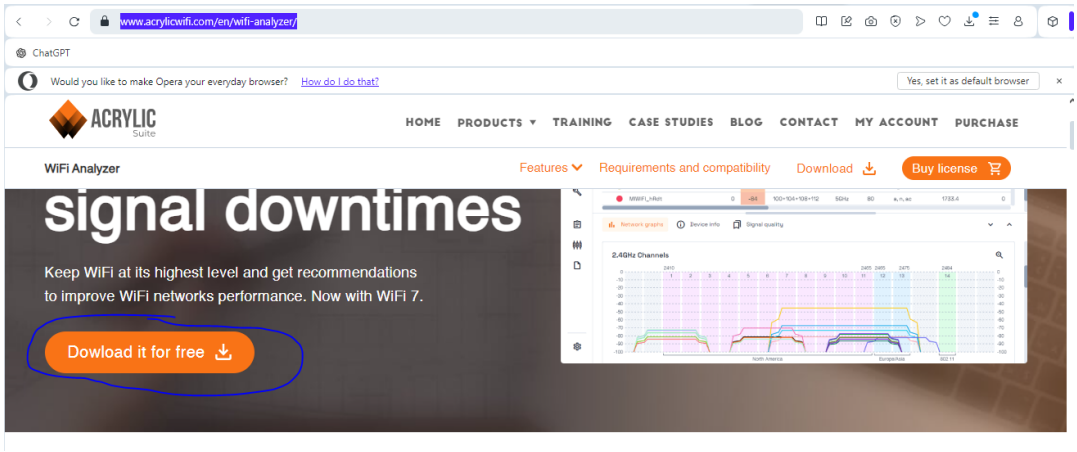
Task:

1. Read and perform this activity
   Measure Signal Strength, signal to noise Ratio(SRN), Data throughput, Jitter, Packet Loss and Re-transmissions of your school wireless network in various locations using Acrylic Wi-Fi Analyzer network monitoring tool to identify areas of strong and weak coverage.
2. Listen to the instructions given by trainer
3. Follow the demonstrations process of Measure Signal Strength, signal to noise Ratio(SRN), Data throughput, Jitter, Packet Loss and Re-transmissions
4. Perform the activity of Measure Signal Strength, signal to noise Ratio(SRN), Data throughput, Jitter, Packet Loss and Re-transmissions by following the procedures
5. Read key readings 3.1.2 and do the application of learning 3.1

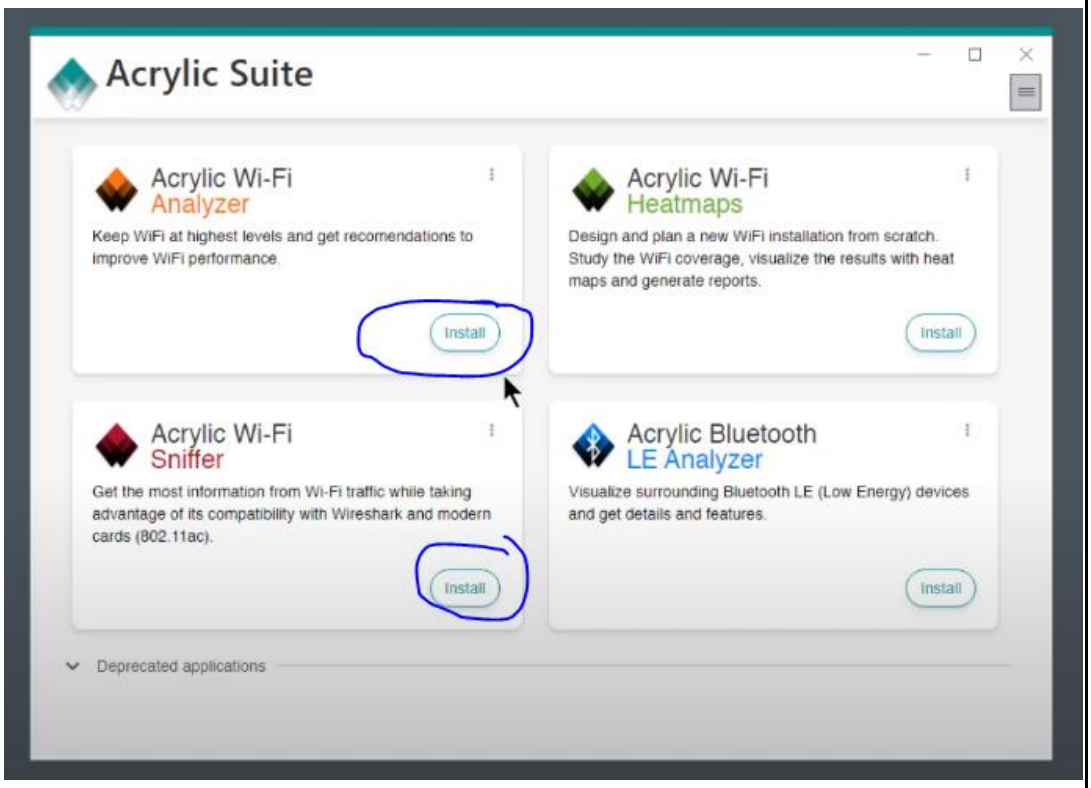
Key readings 3.1.2.: Measuring Signal Strength, signal to noise Ratio(SRN), Data throughput, Jitter, Packet Loss and Re-transmissions using Acrylic Wi-Fi analyser network monitoring tool

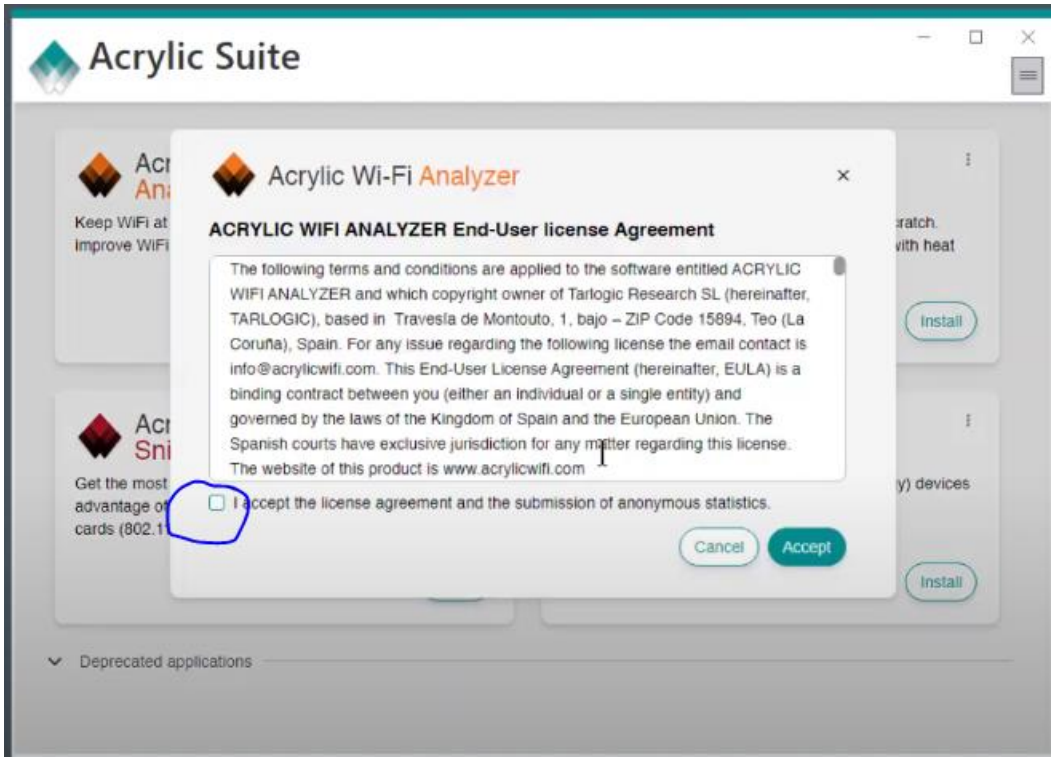
Follow these steps to measure Signal Strength, signal to noise Ratio(SRN), Data throughput, Jitter, Packet Loss and Re-transmissions using Acrylic Wi-Fi analyser network monitoring tool

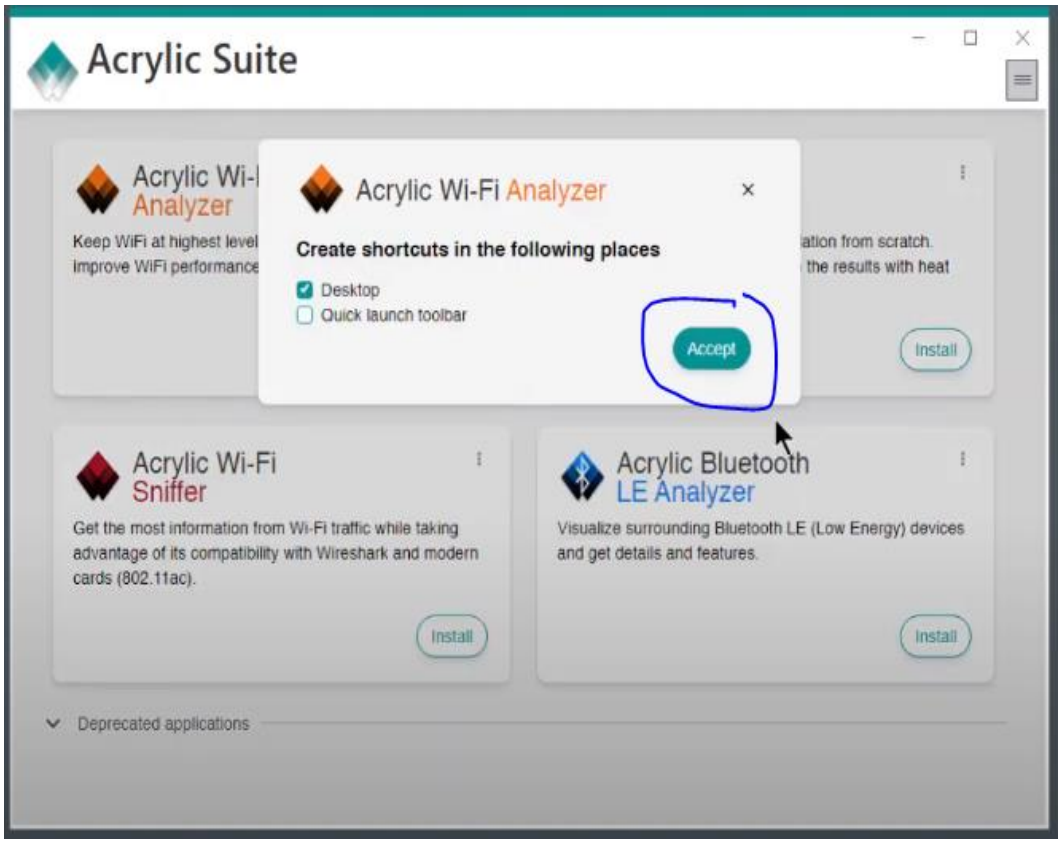
1. Download Acrylic Wi-Fi Analyzer network monitoring tool through the following url :https://www.acrylicwifi.com/en/wifi-analyzer/



2. Install by following the step make sure you install both acrylic Wi-Fi analyze and acrylic Wi-Fi sniffer



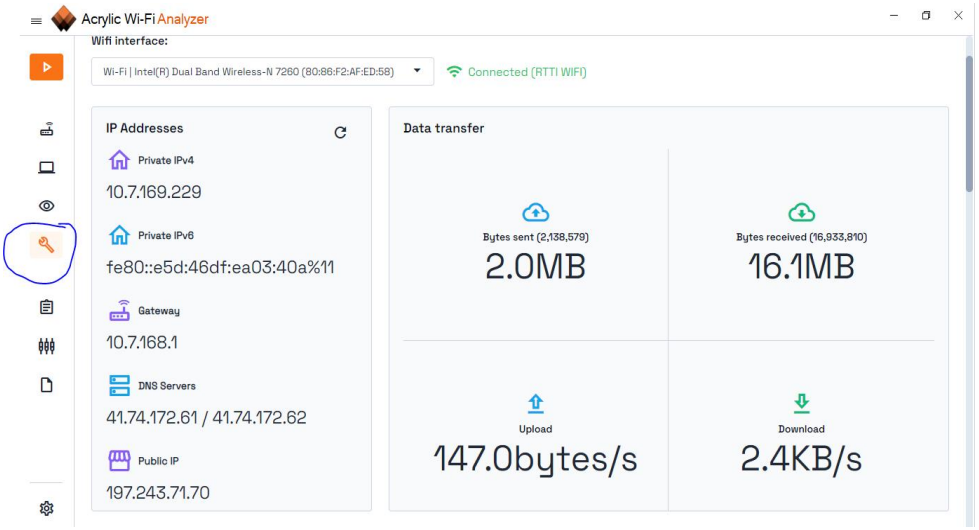




3. Measure Signal Bandwidth

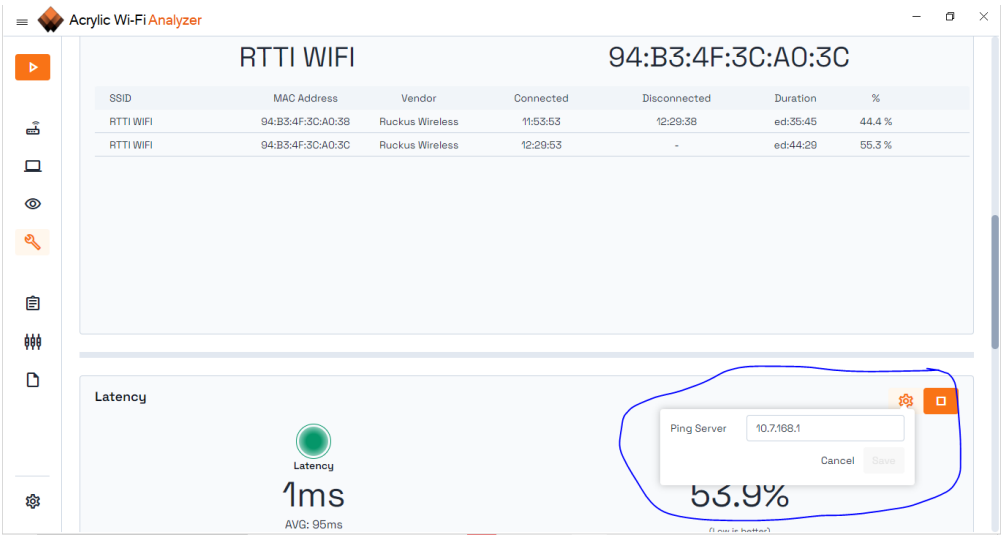
Under setting you can view :

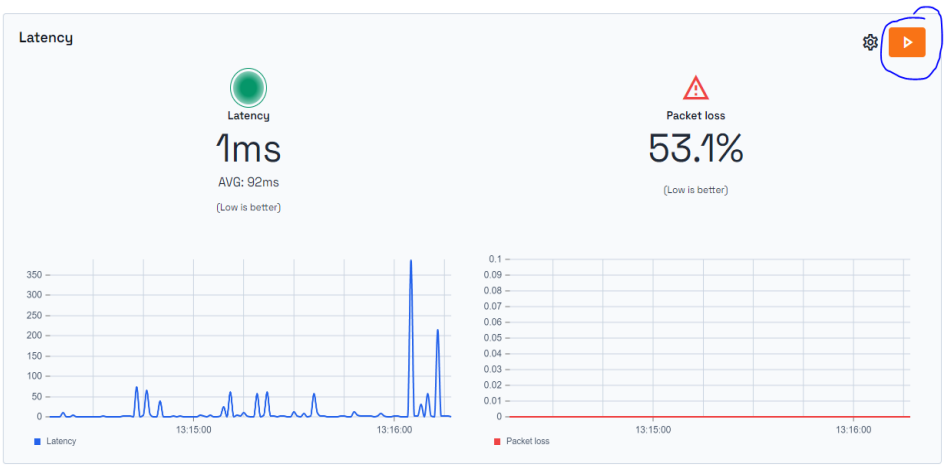
- ✓ Bandwidth in Typically measured in bits per second (bps), kilobits per second (kbps), megabits per second (Mbps), or gigabits per second (Gbps).
- ✓ Name of SSID
- ✓ IP addresss AND gateway
- ✓ MAC address
- ✓ DSN etc.



4. Measure latency and packet loose

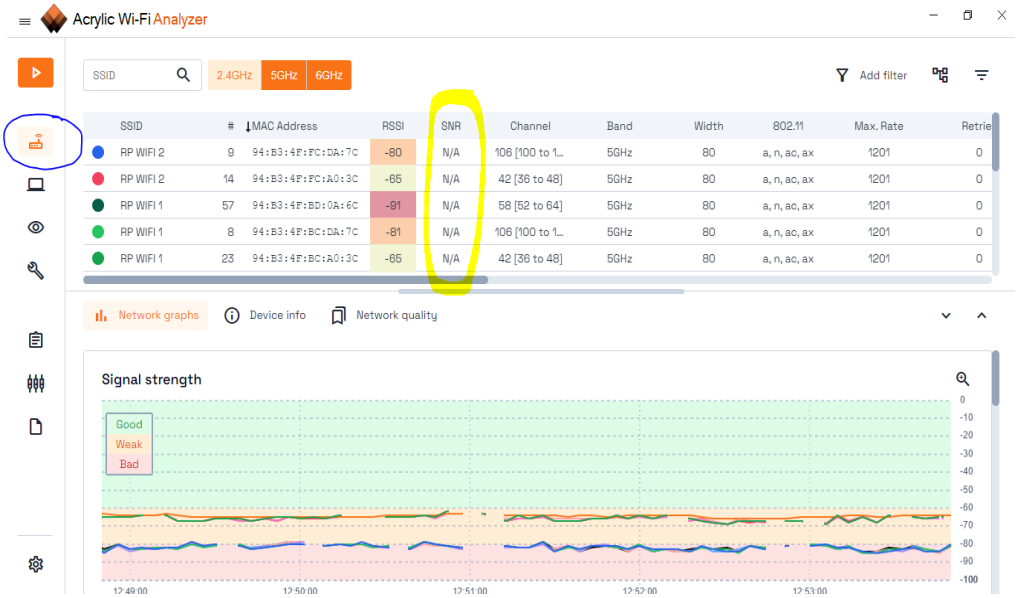
Setting>scroll down > setting>type IP address you wish to measure network latency>save>





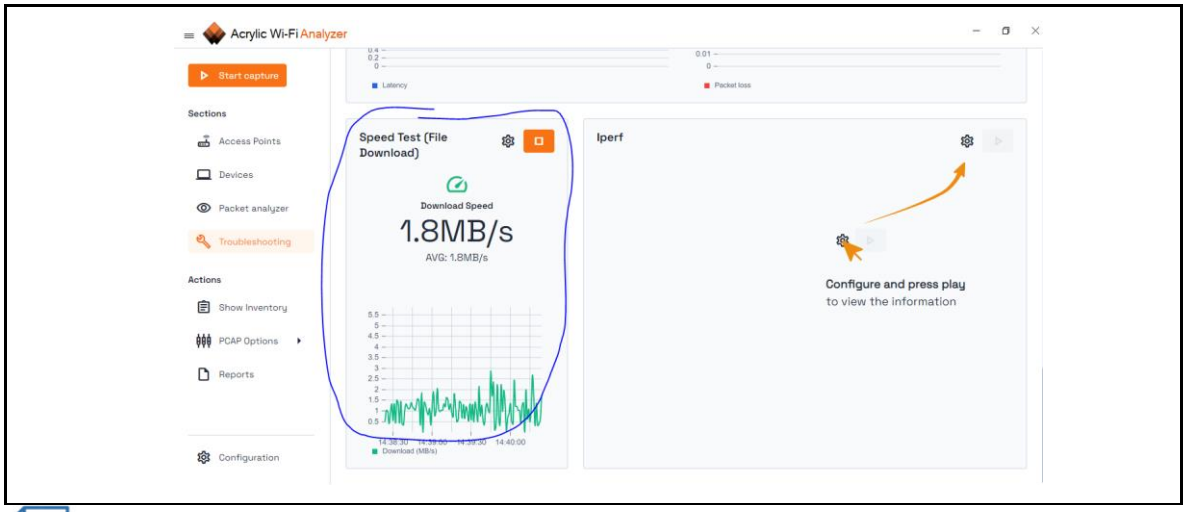
5. Measure Signal to noise Ratio

Under access point you can view Signal to noise Ratio



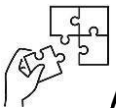
6. Measure Data Throughput

Under troubleshooting you can view the Throughput(speed)



Points to Remember

- Network performance refers to the quality and effectiveness of a network system. It involves evaluating and reviewing the speed, connectivity, reliability, and efficiency of a network.
- Wireless network monitoring metrics are measurements used to assess the performance, reliability, and efficiency of a wireless network
- Key indicators of network performance include bandwidth, latency, throughput, jitter, and error rate. High-performing networks reliably transmit high volumes of data quickly and securely, with minimal delays or errors, improving productivity and user experience.
- Monitoring Tools are software applications or hardware devices used to track and analyze the performance, health, and security of a network or system
- Wireshark is a powerful open-source network protocol analyzer that allows you to capture and inspect data traffic on a network.
- Solar Winds Network Performance Monitor is a commercial, enterprise-grade tool designed to monitor and manage the performance of a network
- Wi-Fi Analyzer is a user-friendly tool that helps monitor and analyze wireless networks by visualizing the signal strength and channel usage of nearby Wi-Fi networks.
- Access Point Controllers are network devices or software solutions designed to manage and control multiple wireless access points (APs) within a network
- When measuring network capacity, you firstly download Acrylic Wi-Fi Analyzer network monitoring tool on the trustfully website.
- Remember to Walk around with your laptop and observe how the RSSI values change as you move closer or farther from the access point (AP).
- Record all collected data and identify patterns



Application of learning 3.1.

As a technician you are requested to measure a public smart city Wi-Fi to find the Signal Strength (Bandwidth and Latency) ,Signal to noise Ratio ,Data throughput, Jitter ,Packet Loss and Re-transmissions and write down the measurement

Indicative content 3.2: Troubleshooting Wireless Network Outdoor.

Duration: 8hrs

Theoretical Activity 3.2.1: Description of Wireless outdoor troubleshooting

Tasks:

1: Answer the following questions:

i. Describe the key factors that can affect wireless network Outdoor performance
ii. Describe the following command :
    a. Ping
    b. Traceroute
    c. netsh wlan show interfaces
    d. IWconfig
    e. Ifconfig

2: Write your findings on paper or flipchart

3: Present your findings in front of the whole class

4: Ask for clarification where necessary

5: Read the key readings 3.2.1

Key readings 3.2.1.: Description of Wireless outdoor troubleshooting

Troubleshoot refers to the process of diagnosing and resolving problems or issues within a system, network, or device. It involves systematic steps to identify the cause of a malfunction and then applying the appropriate fixed

Key factors that can affect wireless network Outdoor performance

Environment Factors

When troubleshooting outdoor wireless networks, environmental factors play a critical role in signal performance and network reliability. Here's how to assess and address these:

✓ **Obstructions**

- **Physical Barriers:** Buildings, trees, and terrain (hills, valleys) can block or weaken the wireless signal.
- **Solution:** Ensure a clear line-of-sight (LoS) between antennas and access points, especially for directional antennas. Consider mounting antennas at higher locations to bypass obstacles.
- **Temporary Obstructions:** Vehicles, construction equipment, or seasonal

foliage can also disrupt signals.

- **Solution:** Regularly inspect the site to account for temporary or movable obstacles and adjust antenna placement if necessary.

✓ **Interference**

- **Electromagnetic Interference (EMI):** Nearby radio towers, power lines, or other wireless networks can create interference.
- **Solution:** Conduct a spectrum analysis to identify interfering frequencies and adjust your network's channel settings to avoid overlap.
- **Device Interference:** Devices like microwaves, Bluetooth, or even security systems in the 2.4 GHz band can interfere with the signal.
- **Solution:** Consider switching to the 5 GHz band if interference is high in the 2.4 GHz band.

✓ **Weather Conditions**

- **Rain and Snow:** Precipitation can absorb and weaken the signal, especially in higher frequency bands like 5 GHz.
- **Solution:** Use weatherproof, outdoor-rated equipment. Consider using lower frequency bands (e.g., 2.4 GHz) for longer-range, weather-resistant connections.
- **Temperature Extremes:** Heat and cold can affect network devices, causing malfunction or signal degradation.
- **Solution:** Install weather-protected enclosures and ensure the equipment is rated for extreme outdoor conditions.
- **Humidity:** High humidity can also affect radio signal propagation.
- **Solution:** Ensure proper ventilation in equipment enclosures to avoid moisture buildup.

✓ **Reflection and Multipath**

- **Reflection:** Signals can reflect off surfaces such as buildings or water bodies, causing signal distortion or multipath interference.
- **Solution:** Use antennas with proper beam forming capabilities to reduce reflection effects and enhance signal focus.
- **Multipath Effects:** Signals taking multiple paths to reach the receiver may interfere with each other, causing a weakened signal.
- **Solution:** Implement MIMO (Multiple Input, Multiple Output) technology to help mitigate multipath interference and improve signal reliability.

✓ **Terrain and Elevation**

- **Terrain Changes:** Hills, slopes, and uneven terrain can obstruct wireless signals or create non-line-of-sight (NLoS) situations.
- **Solution:** Plan the network design considering elevation and use repeaters or additional APs to ensure signal coverage in difficult areas.
- **Signal Loss Over Distance:** Wireless signals weaken over long distances,

particularly outdoors.

- **Solution:** Adjust antenna power levels or use high-gain antennas to extend coverage across long distances.

Diagnosing Commands:

Use diagnostic commands and tools to gather information about the network and troubleshoot connectivity issues.

✓ **Diagnosing commands include:**

- **Ping:** Test connectivity to specific devices or IP addresses.
- **Traceroute:** Identify the path that packets take from source to destination and pinpoint where connectivity issues may occur.
- **Ifconfig**(Linux/macOS)**:**Checks network interfaces and their IP configurations.it can Can help identify misconfigured interfaces or IP conflicts.
- **Iwconfig** (Linux) or **netsh wlan show interfaces** (Windows) to check wireless signal strength and quality.

Practical Activity 3.2.2: Troubleshooting wireless network Outdoor

Task:

1. Read and perform this activity
   Referring to the practical activity 2.3.2, you are requested to troubleshoot the deployed wireless network Outdoor
2. Listen to the instructions given by trainer
3. Follow the demonstrations process of troubleshooting wireless network Outdoor
4. Perform the above activity by following the procedures.
5. Read the key readings 3.2.2 and perform application of learning 3.2

Key readings 3.2.2: Troubleshooting wireless network Outdoor

Troubleshoot refers to the process of diagnosing and resolving problems or issues within a system, network, or device. It involves systematic steps to identify the cause of a malfunction and then applying the appropriate fix**.**

1. **Check Hardware**

✓ **Inspect Wireless Access Points (WAPs)**

- **Physical Condition:** Check for any visible damage to the WAPs, such as cracks, loose mounting, or water damage (especially if the units aren't in proper

weatherproof enclosures).

- **LED Indicators:** Most WAPs have status LEDs that show power, connectivity, and error states. Make sure the WAPs are powered on, and check the lights for any error codes or indications of network issues.
- **Placement and Alignment:** Ensure that WAPs are properly aligned and placed according to the network design. Misalignment can reduce signal strength, especially for directional antennas.
- **Overheating:** Outdoor WAPs are exposed to the elements. Check for signs of overheating (this can occur if they are exposed to direct sunlight without adequate heat protection).

✓ **Antennas**

- **Physical Damage:** Inspect antennas for signs of wear, corrosion, or breakage. Outdoor antennas are prone to environmental damage.
- **Connection:** Ensure antennas are securely connected to the WAP. Loose connections can degrade signal strength or cause intermittent connectivity issues.
- **Alignment:** For directional antennas, alignment is crucial. Verify that they are aimed at the correct angles to ensure optimal signal coverage.

✓ **Cabling**

- **Ethernet and Fiber Optic Cables:** Check for any signs of physical damage to the cables, including cuts, breaks, or fraying. Outdoor environments can be harsh on cables, and rodents or weather conditions may cause damage.
- **Waterproofing:** Ensure that any exposed cable connections (e.g., Ethernet connectors) are properly sealed and waterproofed.
- **Signal Loss:** Test cables for any signal loss or degradation using a cable tester. Damaged cables may introduce latency or packet loss.

✓ **Power Source**

- **Power Over Ethernet (PoE):** For devices powered by PoE, check that the power injectors or PoE-enabled switches are working correctly. Verify that enough power is reaching each WAP.
- **Electrical Power:** If the devices are powered via standard electricity, ensure there are no power outages, and check the condition of the power cables and outlets.
- **UPS (Uninterruptible Power Supply):** If a UPS is being used, make sure it's functioning correctly and hasn't exhausted its battery.

✓ **Mounting and Enclosures**

- **Mounting Stability:** Inspect the poles, brackets, or towers that hold the WAPs and antennas. They should be stable and not swaying or misaligned.

- **Weatherproof Enclosures:** Check if enclosures for network equipment (e.g., WAPs, switches) are intact and properly sealed against moisture, dust, and extreme temperatures. Damaged enclosures can lead to hardware failure.

✓ **Surge Protectors and Grounding**

- **Surge Protection:** Verify that surge protectors are installed correctly to prevent damage from lightning strikes or electrical surges, especially important for outdoor deployments.
- **Grounding:** Ensure that all equipment, including WAPs, antennas, and cabling, is properly grounded to protect against lightning and electrical surges.
- **Switches and Controllers**
- **Port Status:** Check the status of switch ports connected to WAPs. Ensure that all ports are up and functioning, and there are no disconnections.
- **Controller Configuration:** If using a wireless controller, ensure it is functioning and communicating with all WAPs properly. Check for any error logs or alert messages on the controller interface.

✓ **Testing and Diagnostics**

- **Signal Strength Test:** Use a wireless signal strength analyzer (such as a Wi-Fi scanner) to measure signal levels from each WAP. Weak or inconsistent signals could indicate hardware or antenna issues.
- **Replacement Test:** If hardware issues are suspected, temporarily replace or swap out suspect hardware (such as a WAP or cable) to see if performance improves.

Physical Inspection

Antenna Alignment

Check the direction of directional antennas for correct alignment.

Ensure the line-of-sight (LoS) is clear between APs or between APs and clients for optimal signal.

Use alignment tools (e.g., laser pointers or software apps) to fine-tune the direction.

Cable Integrity

✓ Inspect cable connections: Ensure all cables (Ethernet, coaxial, or fiber) are tightly connected and show no signs of wear or corrosion.

✓ Weatherproofing check: Ensure outdoor-rated cables and enclosures are intact and water-resistant to withstand weather conditions.

✓ Look for physical damage: Check for any visible signs of damage like cuts, cracks, or exposed wires. Replace any faulty cables.

Power Issues

✓ Power Supply: Ensure outdoor APs are receiving power from a reliable source,

such as a PoE (Power over Ethernet) injector or a power cable. Verify backup power solutions (e.g., solar, battery) in case of outages.

- ✓ Power Fluctuations: Check for fluctuations or interruptions in the power supply that could affect the performance of the network. Use voltage meters to confirm stable power delivery.
- ✓ Lightning Protection: Ensure there are proper grounding and surge protectors installed to protect the equipment from lightning strikes or electrical surges in outdoor environments.

2. **Check Software**

Firmware Updates

Regularly updating your wireless outdoor access point's firmware is important to get the latest features, bug fixes, and security patches. Here are some tips for updating the firmware:

Check your AP manufacturer's website

Regularly for new firmware versions. Download the latest firmware file for your specific model.

Configuration Review

- Review key settings such as channel selection, bandwidth allocation, and security protocols (e.g., WPA3) to ensure they are properly configured.
- Check that the network is segmented properly (e.g., guest vs. internal networks) and that SSIDs are assigned to the appropriate VLANs.
- Evaluate the transmit power settings for each access point to avoid overlapping coverage and unnecessary interference.

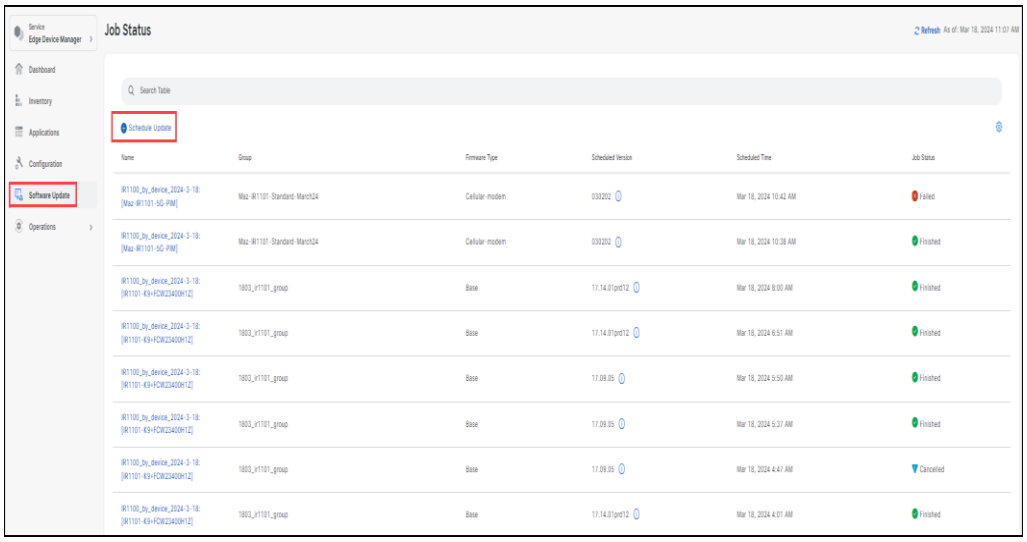
Steps of Troubleshooting wireless network Outdoor

Step 1: Connect proper all suspected device (power cable ,data cable and antennas) as show on the image LED will help to assume that the connection is well done

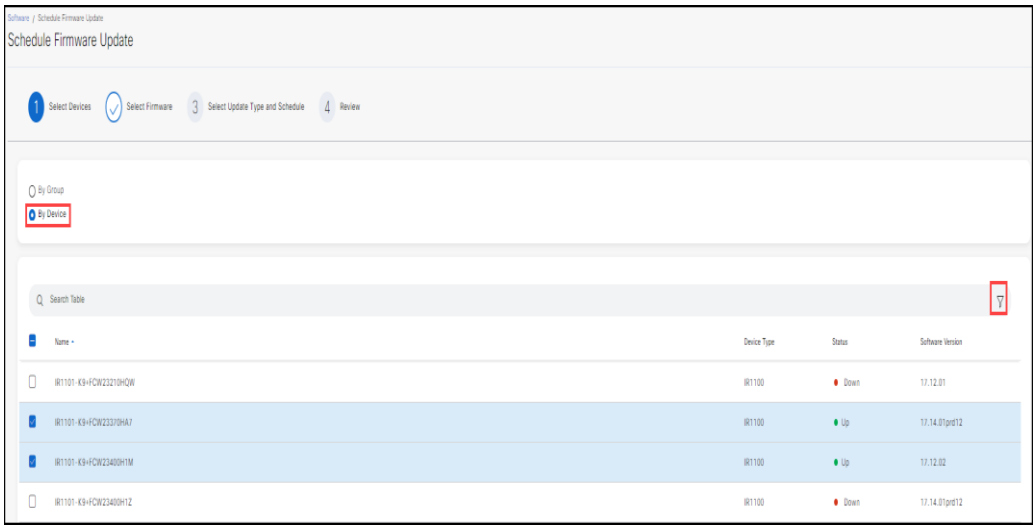
Step 2:Firmware Updates: Regularly check for firmware updates from the manufacturer's website. Download and install any available updates to enhance security and performance.

- ✓ **To update software:**

1. Login in into access point
2. From the left pane, click **Software Update.**
3. On the **Job Status** page, click **Schedule Update**. The Select Devices page opens.



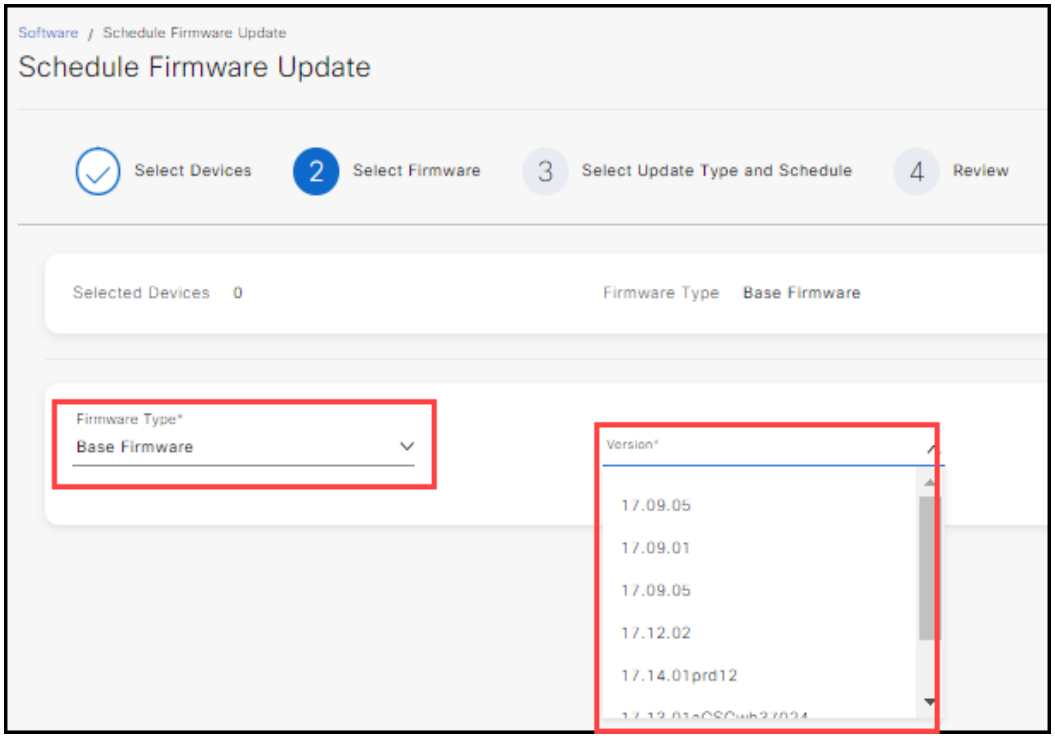
3. Update the firmware either by **group** or **device** as long all the devices are of the same group or device type.



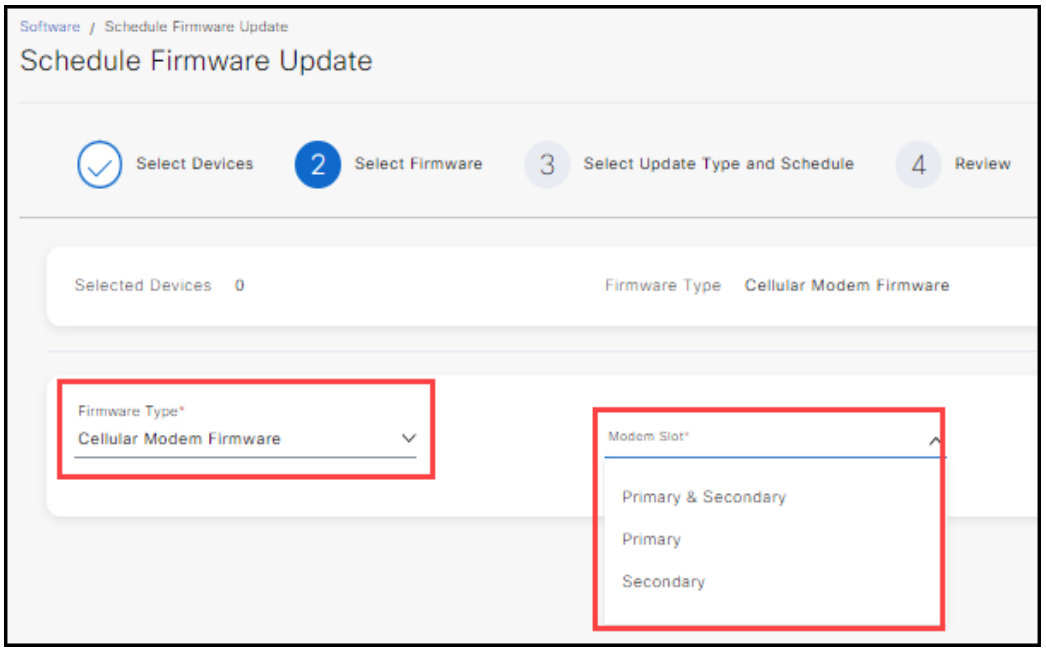
4. Select the **Devices** or **Groups**, and click **Next** to advance to the **Select Firmware** screen. Select only devices/groups of same device type for a single firmware job.
5. In the **Firmware Type** field, select one of the following:
   Base Firmware: Allows you to choose the Firmware Version appropriate for your needs.
   Cellular Modem Firmware: Allows you to choose either **Primary and Secondary, Primary**, or **Secondary** modem slot for either the chassis or expansion module.
   Access Point: (IR829 models only) Allows you to choose the **Firmware Version** appropriate to your needs.

6. Select the appropriate **Firmware Version** (for Base Firmware , Access Point Type) and Modem Slot (for Cellular Modem Firmware).

Base Firmware/Access Point Firmware

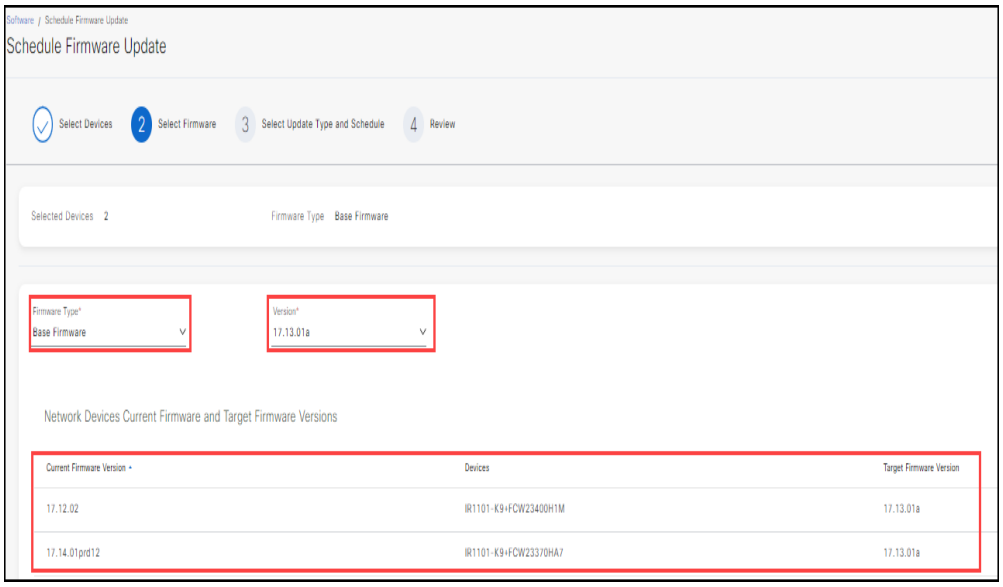


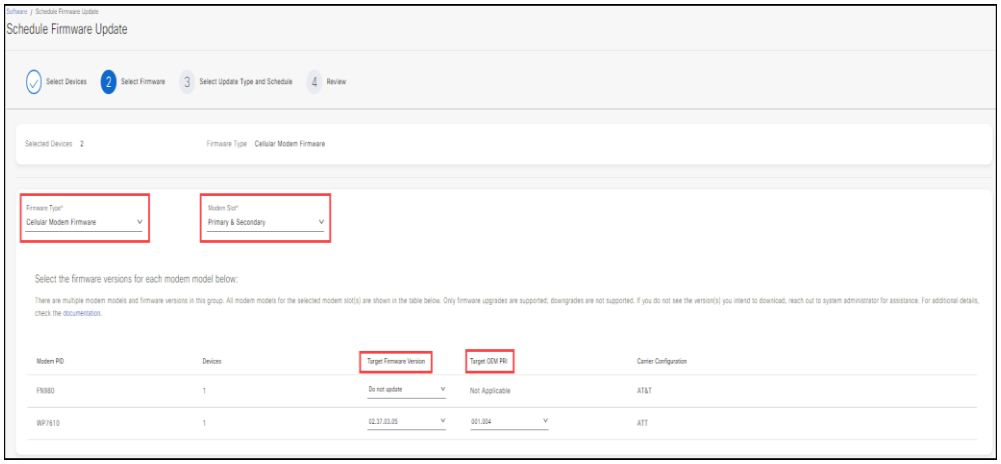
Cellular Modem Firmware



Once you have selected the Base **Firmware/Access Point Firmware** and the **Firmware Version** the screen updates to list the available devices and firmware versions for review.

Firmware Update Screen





7. After configuring the devices (or group), click Next to advance to the Select Update Type and Schedule screen.
8. In the Select **Update Type and Schedule** screen, choose the **Update Type**, either:
   Upload: Upload the firmware to the group (or device), but don't install it.
   Install: Install the firmware to the group (or device).
   Upload and Install: Upload and install the firmware to the group (or device).
9. To run your firmware update, choose either:
   Run Now
   Run Later

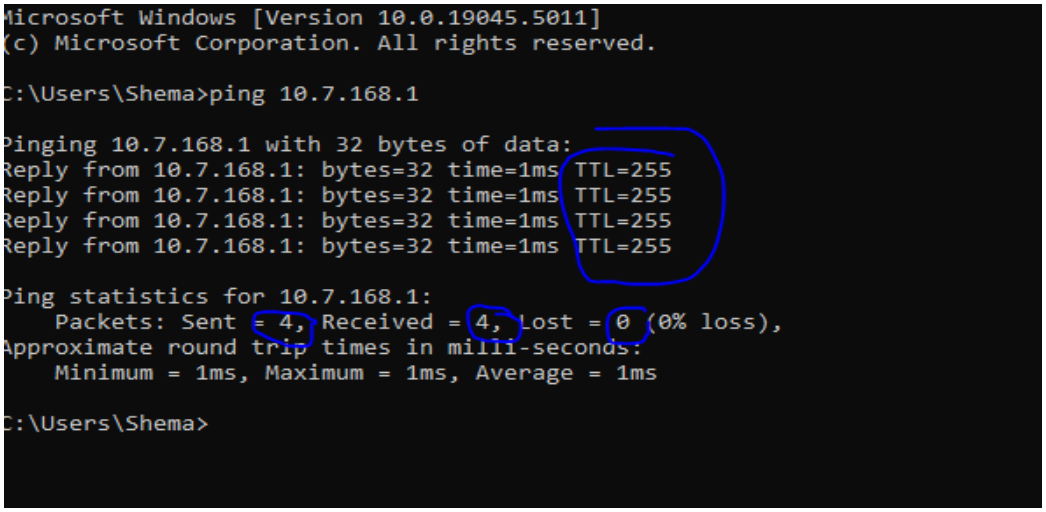
Step 3:Configurations Review: Review the current configurations of each AP. Ensure settings such as SSID, encryption protocols (e.g., WPA3), channel assignments, and bandwidth limits are optimized for your network needs. Document any changes made during this review.

Step 4:Using Diagnosing Commands

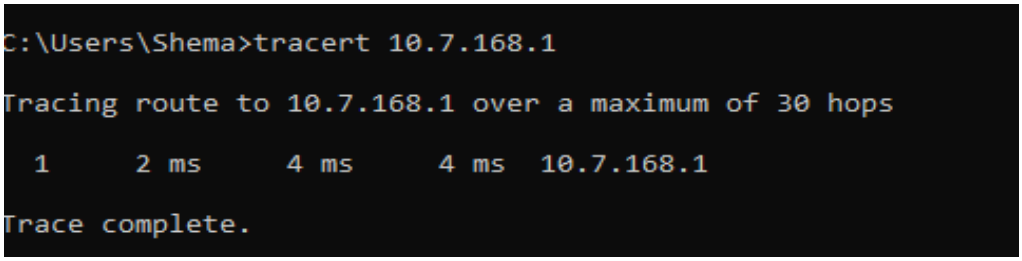
Utilize diagnostic commands to troubleshoot and monitor network

performance:

- **Ping Test**: Use ping commands to test connectivity between the AP and client devices. This helps identify latency issues or packet loss.



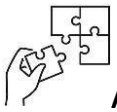
- **Traceroute**: Run traceroute commands to analyze the path data takes through the network, which can help pinpoint where delays or failures occur.



Points to Remember

- Troubleshoot refers to the process of diagnosing and resolving problems or issues within a system, network, or device
- Key factors that can affect wireless network Outdoor performance should include obstructions, interference, weather Conditions, Terrain and Elevation
- Troubleshoot wireless network outdoor include Physical Inspection , Environment Factors, Check Software and Configuration Review
- Use Diagnosing Commands like ping and traceroute, ifconfig, iwconfig or netsh wlan show interfaces to identifier network problem.
- Regularly check for firmware updates from the manufacturer's website.

- Update the firmware either by group or device as long all the devices are of the same group or device type.
  - Select the appropriate Firmware Version (for Base Firmware, Access Point Type) and Modem Slot (for Cellular Modem Firmware).
  - Review the current configurations of each AP. Ensure settings such as SSID, encryption protocols (e.g., WPA3), channel assignments, and bandwidth limits are optimized for your network needs.



Application of learning 3.2.

A remote office is experiencing intermittent connectivity issues with their wireless outdoor access point. Users report slow speeds and frequent disconnections. Troubleshoot the problem, Diagnostic Commands that can be used then provide Possible Solutions Based on Findings

Indicative content 3.3: Upgrading Wireless Network Outdoor.

Duration: 4 hrs

Theoretical Activity 3.3.1: Description of upgrade wireless network outdoor

Tasks:

1: Answer the following questions:

i. Describe the contexts where to upgrade wireless network outdoor.

ii. Describe the important of the following Factors while Upgrading wireless outdoor

a. Coverage and Range

b. Bandwidth and Throughput

c. Interference and Noise

d. Security

e. Scalability

f. Durability and Weather Resistance

g. Power and Connectivity

2: Write your findings on paper or flipchart

3: Present your findings in front of a whole class

4: Ask for clarification where necessary

5: Read the key readings 3.3.1

Key readings 3.3.1.: Description of upgrade wireless network outdoor

1. **Definition**

Upgrade refers to the process of improving or enhancing a system, software, hardware, or infrastructure to a newer, more advanced, or more efficient version. This may involve installing new features, fixing bugs, improving performance, or enhancing security. Upgrading can apply to various contexts, including:

1. **Software:** Installing a new version of an application or operating system that includes updates and improvements.

2. **Hardware:** Replacing or adding components to improve the performance or capabilities of a device (e.g., upgrading RAM in a computer).

3. **Infrastructure:** Enhancing systems like networks or facilities to meet increased demands or improve efficiency.

Upgrading an outdoor wireless network involves considering various factors and following specific steps to ensure a successful transition. Here's a breakdown:

2. Factors of Upgrading:

2.1. Coverage and Range

Assess the current coverage area and determine if there are any dead zones or areas with weak signal strength. Upgrading should aim to improve coverage and extend the range of the network.

2.2. Bandwidth and Throughput

Evaluate the existing network's capacity to handle data traffic. Consider upgrading to equipment that supports higher bandwidth and throughput to accommodate increasing data demands.

2.3. Interference and Noise

Identify sources of interference such as neighboring networks, physical obstacles, or environmental factors like weather conditions. Choose equipment and technologies that minimize interference and ensure reliable connectivity.

2.4. Security: enhance network security by upgrading to equipment with advanced encryption protocols and authentication mechanisms.

Protecting sensitive data and preventing unauthorized access is crucial, especially in outdoor environments where the network may be more vulnerable.

2.5. Scalability

Plan for future growth and expansion by selecting equipment that can

easily scale to accommodate additional users or devices. Scalability is essential for outdoor networks that may need to support larger crowds or new applications over time.

2.6. Durability and Weather Resistance

Choose ruggedized equipment designed to withstand outdoor conditions such as extreme temperatures, moisture, dust, and physical tampering. Ensure that all components are sealed and protected against environmental hazards.

2.7. Power and Connectivity

Ensure adequate power sources and network connectivity for outdoor access points. Consider options such as Power over Ethernet (PoE) for simplified installation and maintenance, especially in remote locations.

Practical Activity 3.3.2: Upgrading wireless network outdoor

Task:

1: Read carefully and perform this task:

Referring to the practical activity 3.2.2, you are requested to upgrade firmware of access point of deployed wireless network outdoor

2: Listen to the instructions given by trainer

3: Follow the demonstration process of upgrading wireless network topology.

4: Perform the activity by following the procedures performed by the trainer.

5: Read the key readings 3.3.2 and perform application of learning 3.3

Key readings 3.3.2.:Upgrading wireless network outdoor

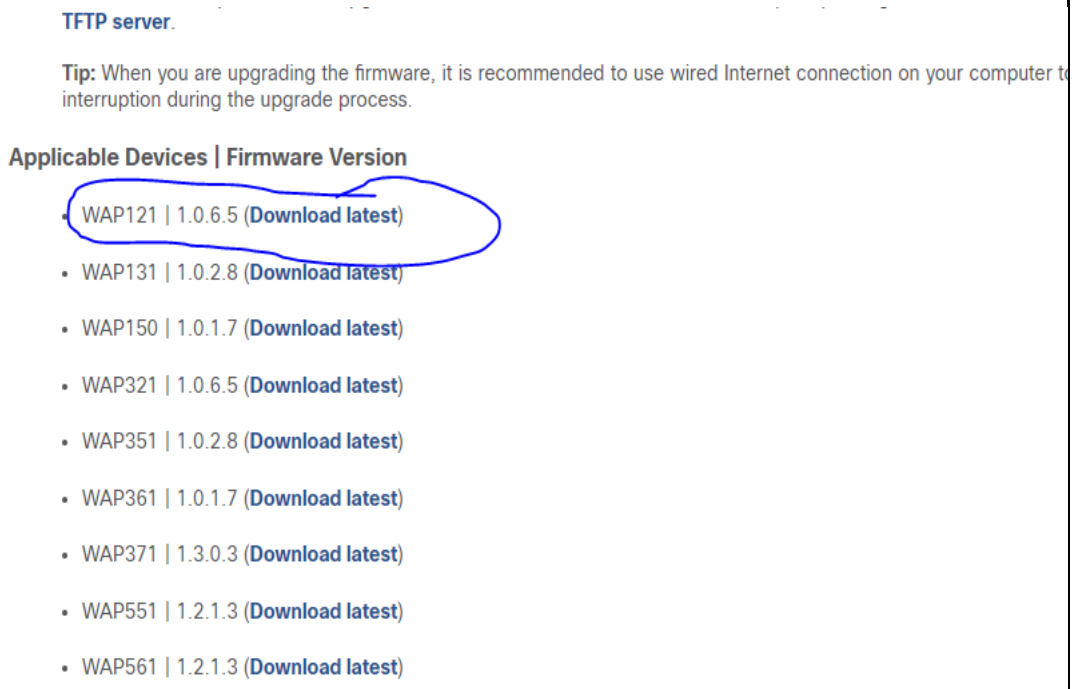
Follow these steps for Upgrading wireless network outdoor

Step 1: Download last version of firmware of cisco website : https://www.cisco.com/c/en/us/support/docs/smb/wireless/cisco-small-business-100-series-wireless-access-points/smb5193-upgrade-firmware-on-wireless-access-point.html

When you are upgrading the firmware, it is recommended to use wired

Internet connection on your computer to avoid interruption during the upgrade process.

Applicable Devices | Firmware Version



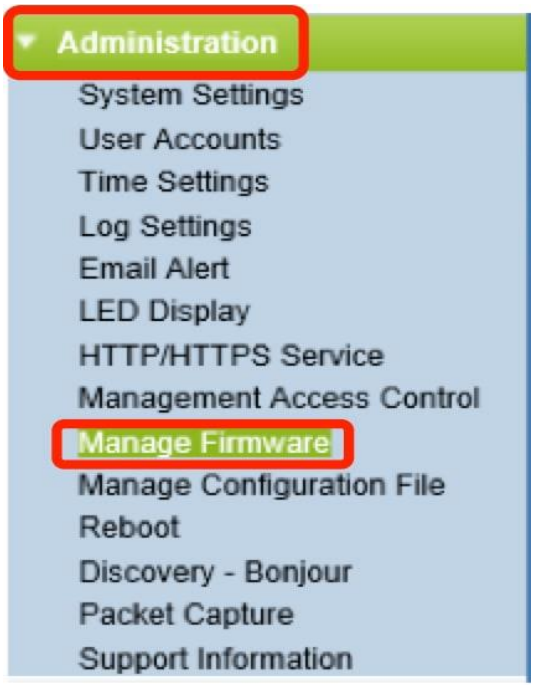
Upgrade Firmware

Before starting the upgrade process, make sure you have downloaded the latest firmware of your device from the Cisco website using the appropriate link above.

Firmware Upgrade through HTTP/HTTPS

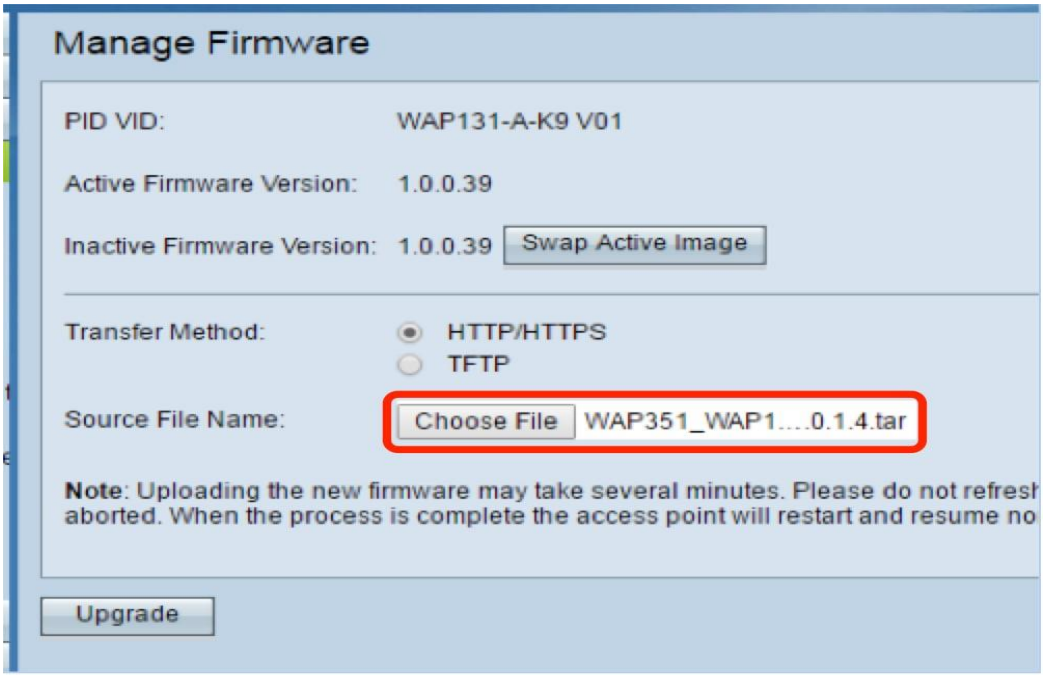
Note: Images used are from the WAP131 as an example.

Step 2: Login to the access point Graphical User Interface (GUI) and choose **Administration > Manage Firmware**.



Step 3: Under the Manage Firmware area, choose the **HTTP/HTTPS** radio button as the Transfer Method.

Note: The Product ID (PID VID) and active and inactive firmware versions appear. When the firmware is upgraded, the previous version is saved as Inactive Firmware Version. These firmware versions are stored on the device so the active firmware can be swapped at any time.

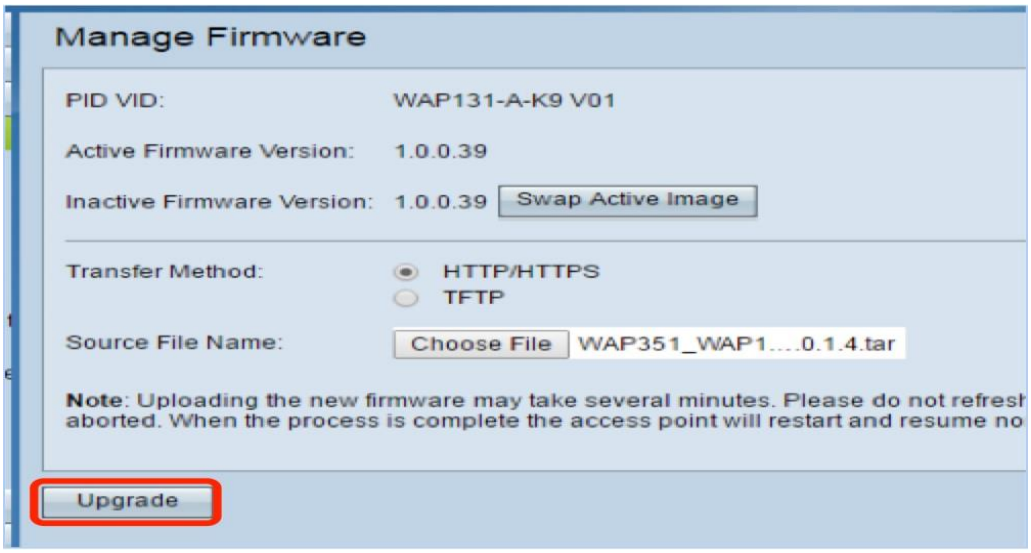


Click **Choose File** and locate the firmware image file you have previously downloaded.

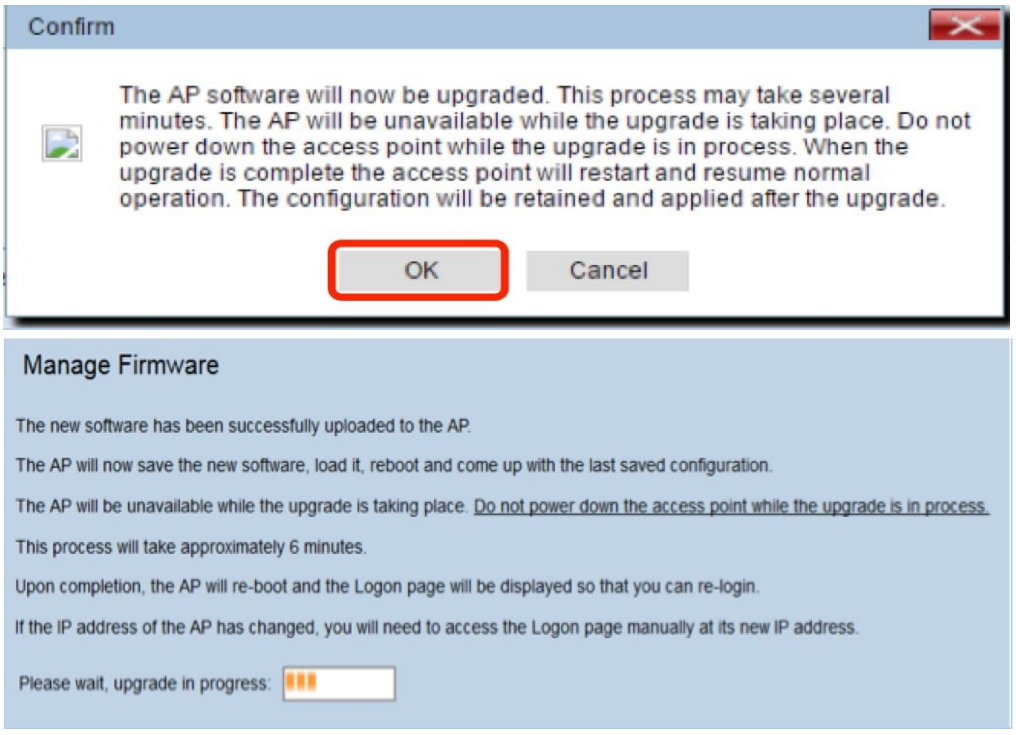
Note: The firmware upgrade file supplied must be a .tar file. Do not attempt to use .bin or other file formats for the upgrade as these types of files do not work. The file name cannot contain the following characters: spaces, and special characters.

Step 4: Upgrade.

Note: Uploading the new firmware may take several minutes. Do not refresh the page or navigate to another page while uploading the new firmware, otherwise, the firmware upload is aborted. Once the process is complete, the WAP restarts and resumes normal operation. In certain cases, you will need to manually refresh the page after the upgrade is completed. If the login page does not appear after six minutes, refresh your web browser.



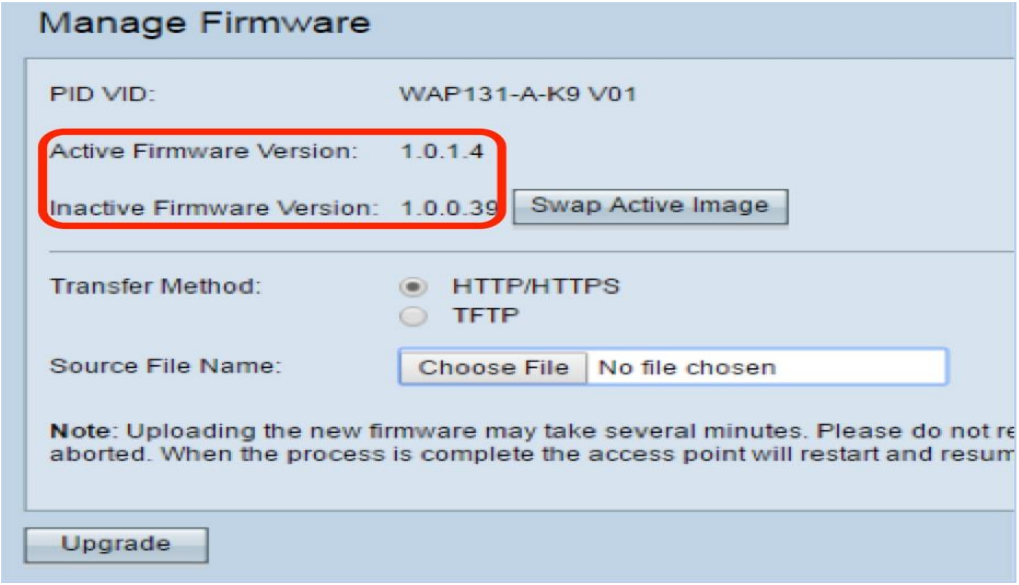
Step 5: Click **OK** to continue.



The progress of the upgrade process will then appear.

Step 6: verify if the firmware upgrade was successful

Log in to the web-based utility and choose **Administration > Manage Firmware.** Under the Manage Firmware area, you will see the active image in the Active Firmware Version.



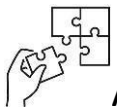
You have now successfully upgraded your firmware through HTTP/HTTPS.

Firmware Upgrade through TFTP

Points to Remember

- Upgrade refers to the process of improving or enhancing a system, software, hardware, or infrastructure to a newer, more advanced, or more efficient version
- Upgrading can be apply to various contexts :
    - ✓ Installing a new version of an application or operating system
    - ✓ Replacing or adding components to improve the performance or capabilities of a device
    - ✓ Enhancing systems like networks or facilities to meet increased demands or improve efficiency.
- Factors of upgrading wireless network outdoor include :
    - ✓ Coverage and Range
    - ✓ Bandwidth and Throughput
    - ✓ Interference and Noise
    - ✓ Security
    - ✓ Scalability
    - ✓ Durability and Weather Resistance
    - ✓ Power and Connectivity

- Firmware files can be downloaded through: Trivial File Transfer Protocol (TFTP) or Hypertext Transfer Protocol/with Secure Sockets (HTTP/HTTPS)
- Download last version of firmware of cisco website
- When you are upgrading the firmware, it is recommended to use wired Internet connection on your computer to avoid interruption during the upgrade process.



Application of learning 3.3.

SXV Community Park hosts events and recreational activities on area of 2 hectare. The existing Wi-Fi network is slow and has limited coverage, causing frustration for visitors who rely on connectivity. you are requested to improve Wi-Fi coverage throughout the park, increase internet speed to support multiple users and provide reliable access for outdoor events

Indicative content 3.4 : Document Wireless Network Outdoor.

Duration: 4 hrs

Theoretical Activity 3.4.1: Description of Technical Reporting and Journal Review

Tasks:

1: Answer the following questions:

i. Describe Technical Reports

ii. Describe a technical journal

2: Write your findings on Paper or flipchart

3: Present your findings in front of a whole class

4: Ask for clarification where necessary

5: Read key readings 3.4.1 in trainee manual

Key readings 3.4.1.: Description of Technical Reporting and Journal Review

Description of Technical Reporting and Journal Review

1. **A technical report**

Definition

A report is a document that presents information in an organized format for a specific audience and purpose. Although summaries of reports may be delivered orally, complete reports are almost always in the form of written documents.

According to the Business Dictionary, a report is a document containing information organized in a narrative, graphic, or tabular form that is prepared on periodic, regular, or as required basis.

Types of reports include memos, minutes, lab reports, book reports, progress reports, justification reports, compliance reports, annual reports, and policies and procedures.

Here are the main sections of the standard report writing format:

- **Title Section:** The title of report is necessary to orient the reader. This includes the name of the author(s) and the date of report preparation.
- **Summary:** There needs to be a summary of the major points, conclusions, and

recommendations. It needs to be short as it is a general overview of the report. Some people will read the summary and only skim the report, so make sure you include all the relevant information.

It would be best to write this last so you will include everything, even the points that might be added at the last minute.

- **Introduction:** The first page of the report needs to have an introduction. You will explain the problem and show the reader why the report is being made. You need to give a definition of terms if you did not include these in the title section, and explain how the details of the report are arranged.
- **Experimental details:** This is the part that you need to state every detail of the experiment, starting from the equipment that you used to the procedure for the test.
- **Results:** This is where you are expected to explain the results that you obtained. You should give clear explanation so that the reader cannot ask themselves any question on your results.
- **Body:** This is the main section of the report. There needs to be several sections, with each having a subtitle. Information is usually arranged in order of importance with the most important information coming first.
- **Conclusion:** This is where everything comes together. Keep this section free of jargon as most people will read the Summary and Conclusion.
- **Recommendations:** This is what needs to be done. In plain English, explain your recommendations, putting them in order of priority.
- **Appendices:** This includes information that the experts in the field will read. It has all the technical details that support your conclusions.

Remember that the information needs to be organized logically with the most important information coming first.

2. Technical Journal

A **technical journal** is a periodical publication that focuses on disseminating scholarly and professional information related to a specific field of technology or applied sciences. These journals are platforms for researchers, engineers, technicians, and professionals to publish original research, technical innovations, case studies, and reviews of emerging technologies. The content in a technical journal is often peer-reviewed to ensure accuracy, credibility, and relevance to the field.

Key Characteristics of a Technical Journal:

✓ **Focus on Specific Fields**:

Technical journals are typically specialized, covering narrow areas such as **network engineering**, **wireless communications**, **artificial intelligence**, **mechanical engineering**, **civil engineering**, **computer science**, or **electronics**. The articles aim to advance knowledge in these fields by presenting cutting-

edge research, technological developments, and practical applications.

- ✓ **Research-Oriented Content**:
  Articles in technical journals present original research, theoretical developments, or practical solutions to industry problems.
  They often include detailed methodologies, technical drawings, schematics, algorithms, experimental results, and data analysis.
- ✓ **Peer-Reviewed**:
  Technical journals are typically **peer-reviewed**, meaning submitted articles are reviewed by experts in the field before publication to ensure the work is of high quality, scientifically sound, and contributes meaningfully to the field.
- ✓ **Detailed and Technical Language**:
  The language used in these journals is often highly technical and assumes that the reader has a background in the subject matter. It includes domain-specific jargon, equations, graphs, and technical terms that are essential to understanding the research.
- ✓ **Structure of Articles**:
  Articles follow a formal structure:
- **Abstract**: A brief summary of the research, its purpose, and findings.
- **Introduction**: Provides background information and the objectives of the research.
- **Methodology**: Details the methods, tools, and techniques used in the study.
- **Results**: Presents the findings or outcomes of the research, often with data or graphical representations.
- **Discussion/Analysis**: Interprets the results and compares them with previous studies or industry standards.
- **Conclusion**: Summarizes the research's contribution to the field and suggests future research areas.
- **References**: Lists all cited works and sources.

- ✓ **Target Audience**:
  The intended audience for technical journals includes **researchers**, **industry professionals**, **engineers**, **academics**, and **students**. These readers rely on technical journals to stay updated on the latest advancements, tools, and methodologies in their fields.
- ✓ **Examples of Technical Journals**:
  Some well-known technical journals include:
- **IEEE Transactions** (published by the Institute of Electrical and Electronics Engineers)
- **ACM Computing Surveys** (published by the Association for Computing Machinery)
- **Journal of Mechanical Engineering**

Wireless Communications and Mobile Computing

Practical Activity 3.4.2: Documenting wireless network Outdoor

Task:

1: Read and perform this activity

You are requested to document the designed wireless network outdoor

2: Listen to the instructions given by trainer
3: Follow the demonstrations of documenting the designed wireless network outdoor
4: Perform the above activity by following the procedures.
5: Read the key readings 3.4.2 and perform application of learning 3.4

Key readings 3.4.2: Documenting wireless network Outdoor

Here is a detailed sample of documentation of wireless network outdoor

Title: Identifying and Resolving Connectivity Issues in xyz school

Authors: John Doe, Jane Smith

Date: November 15, 2024

Summary

This document outlines the troubleshooting process for a wireless outdoor surveillance system experiencing connectivity issues. The investigation involved analyzing network logs, conducting site surveys, and testing hardware components. The root cause of the problem was identified as interference from a nearby Wi-Fi network. Recommendations are provided to mitigate interference and improve system performance.

Introduction

Wireless outdoor surveillance systems have become increasingly popular for security and monitoring purposes. However, these systems can be prone to connectivity issues that can hinder their effectiveness. This document aims to

document the troubleshooting process for a specific surveillance system experiencing intermittent connectivity problems.

Experimental Details

Problem Identification:

- The surveillance system was experiencing frequent disconnections and slow data transfer rates.
- Network logs were analysed to identify any error messages or patterns.

Site Survey:

- A site survey was conducted to assess the wireless environment and identify potential sources of interference.
- The presence of other Wi-Fi networks, microwave ovens, or other electronic devices was noted.

Hardware Testing:

- The surveillance cameras, access points, and other network components were tested for proper functionality.
- Cable connections were inspected for any loose or damaged connections.

Results

Interference Analysis:

- The site survey revealed the presence of a strong Wi-Fi network operating on the same channel as the surveillance system.
- This interference was determined to be the primary cause of the connectivity issues.

Performance Evaluation:

- After identifying the interference, the surveillance system's performance improved significantly.
- Connection stability and data transfer rates increased.

Body

Discussion of Findings:

- The case study demonstrates the importance of conducting thorough site surveys to identify potential sources of interference in wireless networks.
- Interference can significantly impact the performance of wireless devices, leading to connectivity issues and data loss.

Conclusion

The troubleshooting process successfully identified and resolved the connectivity issues affecting the wireless outdoor surveillance system.

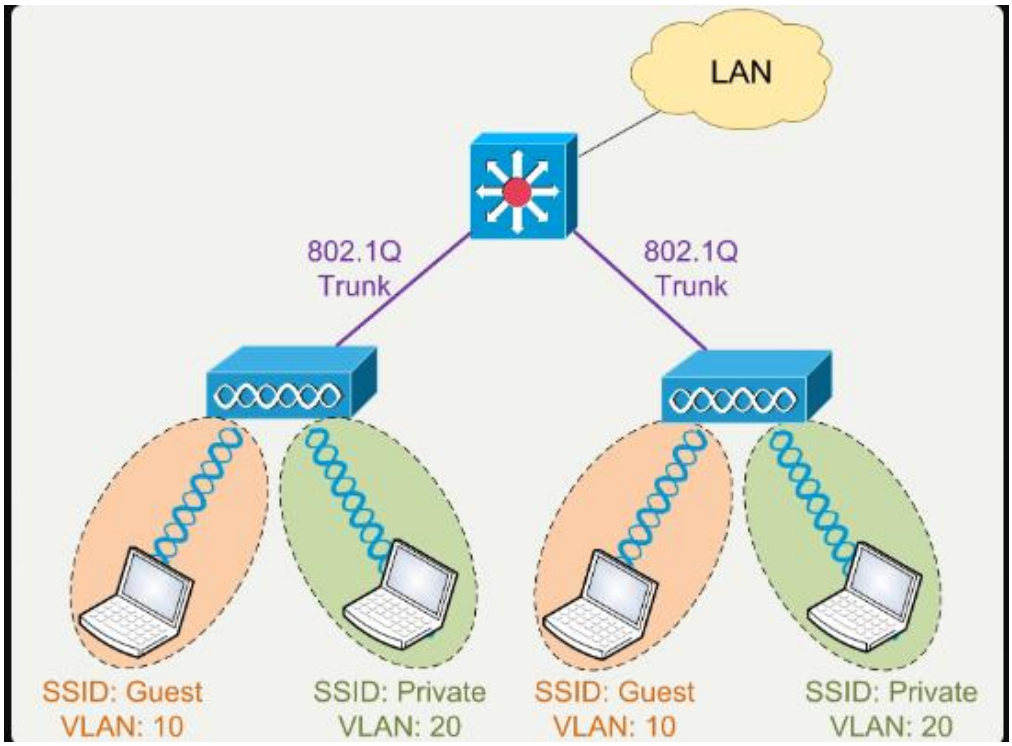
The root cause was determined to be interference from a nearby Wi-Fi network. By addressing the interference, the system's performance was restored to normal levels.

Recommendations

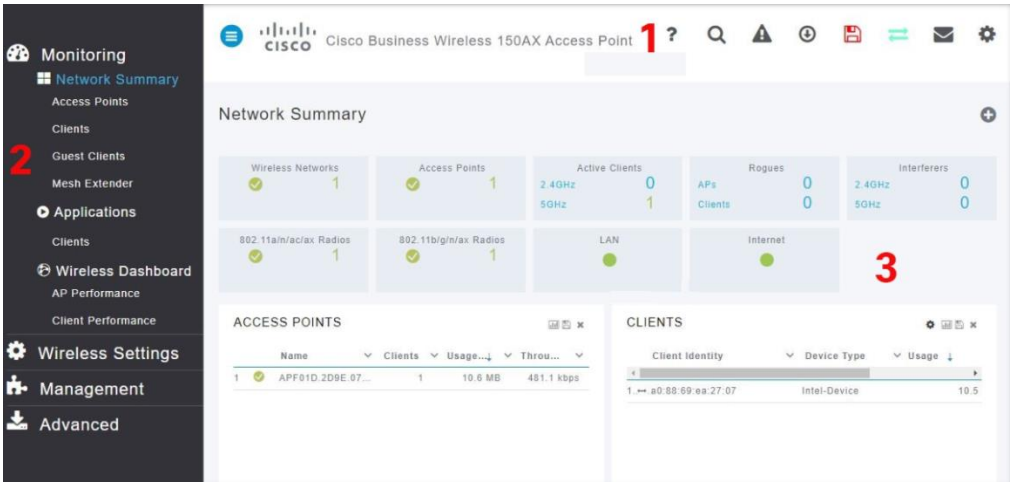
- **Channel Selection:** The surveillance system should be configured to use a wireless channel that is less crowded to minimize interference.
- **Physical Separation:** If possible, the surveillance system should be placed in a location that is physically separated from other wireless devices.
- **Antenna Placement:** Proper antenna placement can help to reduce interference and improve signal strength.
- **Regular Maintenance:** Regular maintenance, including cleaning antennas and checking cable connections, can help to prevent future connectivity problems.

Appendices

New network Topology



Access point Configuration summary

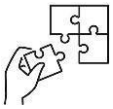


Points to Remember

- A report is a document that presents information in an organized format for a specific audience and purpose
- Types of reports include memos, minutes, lab reports, book reports, progress reports, justification reports, compliance reports, annual reports, and policies and procedures.
- main sections of the standard report writing format is :
    - ✓ Title Section
    - ✓ Summary:
    - ✓ Introduction
    - ✓ Experimental details
    - ✓ Results
    - ✓ Body
    - ✓ Conclusion
    - ✓ Recommendations

- ✓ Appendices

- Remember that the information needs to be organized logically with the most important information coming first.
- The document is generally clear and concise, but some sections could be further streamlined.
- The summary effectively conveys the main points of the document, but it could be slightly more detailed.
- The experimental details section is well-structured, providing a clear overview of the troubleshooting process.
- The results section could be enhanced by providing more specific data and metrics to support the conclusions.



Application of learning 3.4.

As a network technician after installation of wireless network outdoor in XYC Company, you are asked to create an official network documentation to ensure that the company retains all the knowledge that went into creating the network as well as how to maintain and upgrade it.

Learning outcome 3 end assessment

Written assessment

Section A : True or False question

Read the following statement related to wireless network outdoor and answer True if the statement is correct or False if the statement is wrong

1. Signal strength is a critical metric for assessing the performance of an outdoor wireless network.
2. A higher signal-to-noise ratio typically indicates a better quality connection.
3. Data throughput refers to the total amount of data transmitted successfully over a network in a given time.
4. Jitter is the variation in packet delay in a network, which can affect real-time communications.
5. Wireshark is a hardware tool used for monitoring wireless networks.
6. Antenna alignment has no effect on the signal quality of a wireless network.
7. Firmware updates are unnecessary for maintaining optimal network performance.
8. Packet loss can lead to a significant decrease in the quality of service for applications like video streaming.
9. SolarWinds Network Performance is primarily used for analyzing wired networks only.
10. Technical reports should include detailed documentation of network performance metrics.

Section B: Multiple Choice Questions Select the right answer

Circle the letter corresponding the correct answer

1. Which metric indicates the quality of a wireless connection relative to background noise?
   a) Bandwidth
   b) Signal to Noise Ratio
   c) Jitter
   d) Packet Loss
2. What is the primary purpose of a Wi-Fi Analyzer?
   a) To configure routers
   b) To visualize network traffic
   c) To assess and optimize Wi-Fi performance
   d) To upgrade firmware
3. Which of the following is NOT a factor to check when troubleshooting hardware issues in outdoor networks?

a) Antenna alignment
b) Cables integrity
c) Signal strength
d) Software configuration

4. Which of the following tools would you use to monitor data packets in a wireless network?
   a) SolarWinds
   b) Wireshark
   c) NetFlow
   d) PingPlotter
5. What does packet retransmission indicate?
   a) Efficient network performance
   b) High bandwidth usage
   c) Network congestion or errors
   d) Normal operation
6. Which of the following is a common step in upgrading a wireless network?
   a) Disable all access points
   b) Review current configurations
   c) Change the frequency spectrum
   d) Disconnect all users
7. What environmental factor can impact outdoor wireless network performance?
   a) Temperature
   b) Rain and humidity
   c) Obstructions like trees and buildings
   d) All of the above
8. Which command would you use to check connectivity to another device on the network?
   a) traceroute
   b) ipconfig
   c) ping
   d) netstat
9. What type of documentation is essential for maintaining a record of network changes and performance?
   a) User manuals
   b) Technical reports
   c) Installation guides
   d) Marketing materials
10. Which tool can help in identifying and resolving network performance issues?
    a) Wireshark
    b) Word Processor
    c) Spreadsheet software

d) Photo editing software

Section C Match the following terms with their descriptions used in wireless network outdoor and write the letter corresponding to the correct description

Answer	TERM	DESCRIPTION
1.....	**1.** Signal Strength	A. Variation in packet arrival times
2.....	**2.** Packet Loss	B. The effectiveness of data transmission over time
3.....	**3.** Firmware Updates	C. The process of identifying and resolving network issues
4.....	**4.** Wi-Fi Analyzer	D. Tool used to assess wireless network performance
5.....	**5.** Antenna Alignment	E. Loss of data packets during transmission
6.....	**6.** Latency	F. Adjustment for optimal wireless signal reception
7.....	**7.** Data Throughput	G. Regular updates to software controlling hardware
8.....	**8.** Jitter	H. Documentation of ongoing network performance
9.....	**9.** Troubleshooting	I. Time delay in data transmission
10.....	**10.** Technical Journal	J. Measurement of signal quality
		K. Survey that identifies potential signal issues
		M. Review current configurations

Practical assessment

You are part of a network management team responsible for maintaining an outdoor wireless network deployed in a public school. The network is used for public Wi-Fi access, your task is to monitor the network performance, troubleshoot issues, upgrade the system as needed, and document all findings and actions taken.

END

References

Adams, G. (2022, March 18). Effective Upgrading of Wireless Networks. Retrieved from IT Network Guides: www.itnetworkguides.com/upgrading-wireless

Brown, D. (2023, June 25). Troubleshooting Outdoor Wireless Networks. Retrieved from Network Troubleshooting: www.networktroubleshooting.com/outdoor

Brown, S. (2023, June 20). RF Site Survey Best Practices. Retrieved from Network World: www.networkworld.com/rf-site-survey

Doe, J. (2023, October 10). Outdoor Wireless Networks. Retrieved from Network Solutions: www.networksolutions.com/outdoor-wireless

Johnson, A. (2023, September 10). Monitoring Wireless Networks. Retrieved from Network Performance Solutions: www.networkperformancesolutions.com/monitoring

Johnson, E. (2022, August 15). Designing a Public Wi-Fi Network. Retrieved from Wi-Fi Alliance: www.wi-fi.org/public-network-design

Lee, B. (2023, August 5). Understanding Signal Strength and SNR. Retrieved from Wireless Tech Insights: www.wirelesstechinsights.com/signal-strength

Miller, F. (2023, April 30). Analyzing Packet Loss in Wireless Networks. Retrieved from Network Analysis Today: www.networkanalysistoday.com/packet-loss

Roberts, A. (2023, February 8). Weatherproofing Outdoor Equipment. Retrieved from Tech Innovations: www.techinnovations.com/weatherproofing

Smith, C. (2022, July 15). Tools for Monitoring Wi-Fi Performance. Retrieved from Tech Monitoring Hub: www.techmonitoringhub.com/wifi-tools

Smith, J. (2023, September 25). Understanding Wireless Technologies. Retrieved from TechRadar: www.techradar.com/wireless-tech

White, E. (2023, May 20). Firmware Management for Wi-Fi Devices. Retrieved from Cybersecurity Best Practices: www.cybersecuritybestpractices.com/firmware

White, L. (2022, April 18). Interference in Wireless Networks. Retrieved from TechSpot: www.techspot.com/interference

Wilson, J. (2023, December 1). Documenting Wireless Network Changes. Retrieved from IT Documentation Hub: www.itdocumentationhub.com/wireless

Wilson, T. (2023, May 30). Antenna Types Explained. Retrieved from Antenna World: www.antennaworld.com/types

RTB | RWANDA TVET BOARD

October 2024