RQF LEVEL 3

NITLI302

NETWORKING AND INTERNET TECHNOLOGIES

LAN Installation

TRAINEE'S MANUAL

October, 2024

RTB | RWANDA TVET BOARD

LAN INSTALLATION

KOICA Korea International Cooperation Agency

TQUM TVET Quality Management Project

2024

AUTHOR'S NOTE PAGE (COPYRIGHT)

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 Networking and Internet technologies, specifically for the module **" NITLI301: LAN Installation."**

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

NIZEYIMANA Martin

HABIYAMBERE Daniel

Validation

NIYITURAGIYE Vedaste

NDAGIJIMANA Jonathan

Conception, Adaptation and Editorial works

HATEGEKIMANA Olivier

GANZA Jean Francois Regis

HARELIMANA Wilson

NZABIRINDA Aimable

DUKUZIMANA Therese

NIYONKURU Sylvestre

MANIRAKIZA Jean de Dieu

Formatting, Graphics, Illustrations, and infographics

YEONWOO Choe

SUA Lim

SAEM Lee

SOYEON Kim

WONYEONG Jeong

MANIRAKORA Alexis

Financial and Technical support

KOICA through TQUM Project

TABLE OF CONTENT

ACRONYMS

DHCP: Dynamic Host Configuration Protocol

FTP: File Transfer Protocol

HTTP: Hypertext Transfer Protocol

HTTPS: Hypertext Transfer Protocol Secure

IP: Internet Protocol

ISP: Internet Service Provider

LAN: Local Area Network

MAC: Media Access Control

NAT: Network Address Translation

OSI: Open Systems Interconnection (Model)

PAN: Personal Area Network

PoE: Power over Ethernet

RP: Rwanda Polytechnic

RTB: Rwanda TVET Board

TVET: Technical and Vocational Education and Training

TQUM: TVET Quality Management

QoS: Quality of Service

SSH: Secure Shell

SSID: Service Set Identifier (Wi-Fi network name)

TCP: Transmission Control Protocol

UPS: Uninterrupted Power Supply

VLAN: Virtual Local Area Network

VPN: Virtual Private Network

WAN: Wide Area Network

WLAN: Wireless Local Area Network

INTRODUCTION

This trainee's manual includes all the knowledge and skills required in Networking and Internet technologies, specifically for the module of **"LAN Installation".** 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: LAN INSTALLATION

Learning Outcome 1: Plan network installation

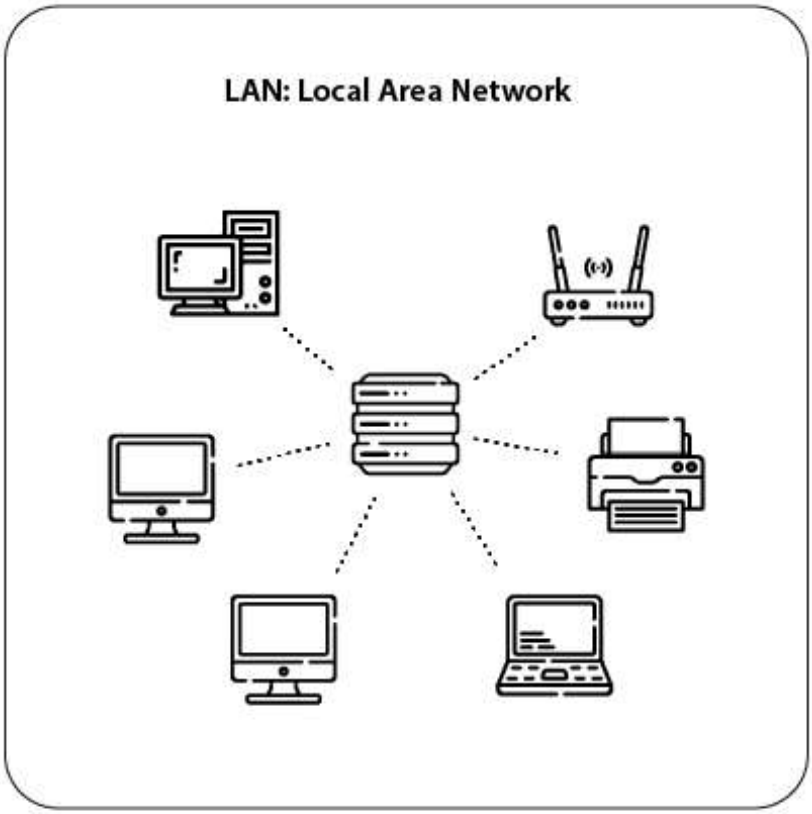
Learning Outcome 2: Perform cabling

Learning Outcome 3: Configure LAN

Learning Outcome 4: Manage network resources

Learning Outcome 5: Test LAN

Learning Outcome 6: Maintain LAN


LAN: Local Area Network

Indicative contents
1.1 Introduction to LAN.
1.2 Identification of LAN installation requirements.
1.3 Designing LAN topology diagram.
1.4 Estimation of LAN installation cost.

Key Competencies for Learning Outcome 1: Plan Network Installation

Knowledge	Skills	Attitudes
• Identification of Local Area Network components • Description of LAN Installation Requirements • Identification of site assessment aspects. • Identification of Local Area network topology diagrams • Identification of cost estimation considerations	• Conducting physical site survey • Selecting LAN topology • Designing a LAN Topology diagram • Estimating cost of LAN installation	• Being Self-motivated • Being Detail-oriented • Having spirit of Creativity • Having spirit of accountability

Duration: 15 hrs

Learning outcome 1 objectives:

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

1. Differentiate correctly types of Local Area Network based on network standards
2. Identify properly key components of Local Area Network based on functionalities
3. Carry out effectively a site survey based on Customer needs
4. Identify properly LAN installation requirements based on site survey findings.
5. Design correctly LAN topology diagram based on LAN design standards.
6. Estimate correctly the cost of LAN installation based on a LAN design and installation requirements.

Resources

Equipment	Tools	Materials
● Computer ● Switch ● Router ● Rack ● Wireless Access point	● Networking toolkit ● Simulation software ● Tape measure ● Distance laser meter	● Network Cables

Indicative content 1.1: Introduction to LAN

Duration: 4 hrs

Theoretical Activity 1.1.1: Describing basic concepts of Local Area Network

Task:

1: Discuss and answer the following questions:

i. Define a local area network.

ii. Describe network topology

iii. Discus on types of physical local area network topologies.

iv. Describe various types of local area networks based on architecture, topology, medium, size or scale and the technology used

v. Explain deeply Key components of LAN.

vi. What is Network installation planning? Describe main phases that complete the network installation planning and their ending results.

2: Present your findings to the trainer and your colleagues.

4: Ask clarifying questions whenever necessary.

5: Read key readings 1.1.1 in trainees manual

Key readings 1.1.1.: INTRODUCTION TO LAN

1. Definition of LAN

A Local Area Network (LAN) is a computer network that interconnects devices within a limited geographical area, such as a home, school, single building or campus.

LANs allow for resource sharing, such as files, printers, and internet connections, enabling users to communicate and collaborate effectively.

2. NETWORK TOPOLOGY

Network topology refers to the arrangement or layout of different elements in a computer network. It describes how devices such as computers, routers, and switches are interconnected and how data flows between them.

- **TYPES OF NETWORK TOPOLOGY**

Network topologies are generally classified into two categories:

- ✓ The physical topology
- ✓ The logical or the signal topology

Physical topology: Refers to the physical layout/arrangement of the devices and cables in a network. Common types include **Bus, Star, Ring, Mesh, Tree, Hybrid Topology**

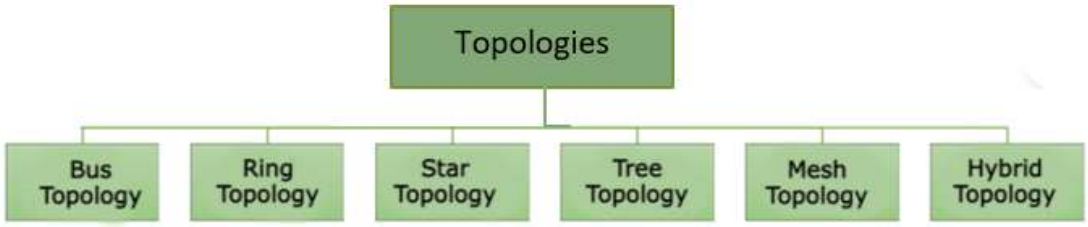
Logical Topology: Refers to the way data flows within a network, regardless of its physical layout. It focuses to logical arrangement of devices and how they communicate with each other, including protocols used for data transmission. Common types logical topology include:

- **Logical Bus Topology**: Data flows along a single path, similar to the physical bus topology, even if the physical layout is different.
- **Logical Ring Topology**: Data flows in a circular pattern, similar to the physical ring topology.
- **Logical Star Topology**: Data flows through a central point, similar to the physical star topology, but the physical connections might be different.

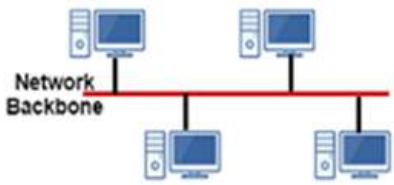
3. Types of physical network topology

The types of physical network topology include bus, ring, star, tree, mesh, and hybrid. Understanding these topologies is crucial for network design, as each type has its own advantages and disadvantages in terms of performance, scalability, and fault tolerance.

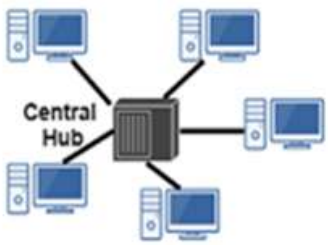
Notes: The choice of physical LAN topology depends on factors like the size of the network, budget, desired performance, and potential for future expansion.



- Bus Topology



- ✓ **Layout**: All devices (nodes) are connected to a single central cable, known as the "bus" or "backbone."
- ✓ **Data Transmission**: Data sent by a device travel along the bus in both directions until it reaches its destination.
- ✓ **Advantages**:
  - Simple and easy to install, especially in small networks.
  - Requires less cabling than other topologies.
  - Cost-effective due to minimal cabling.
- ✓ **Disadvantages**:
  - The entire network can be disrupted if the central cable fails.
  - Difficult to troubleshoot and isolate issues.
  - Limited cable length and number of devices due to signal degradation.
  - Data collisions are common, reducing efficiency.
- ✓ **Use Cases**: Small, temporary, or experimental networks; older LANs.
- Star Topology



- ✓ **Layout:** All devices are connected to a central hub or switch with individual cables. The hub or switch acts as a central point for all data traffic.
- ✓ **Data Transmission**: Data sent from any device is transmitted to the hub or switch, which then forwards it to the intended destination.
- ✓ **Advantages**:
  - Easy to install, manage, and expand.
  - Failure of one cable does not affect the rest of the network.
  - Centralized management and troubleshooting.
  - Reduced chances of data collisions compared to bus topology.
- ✓ **Disadvantages**:
  - Requires more cabling than bus topology, increasing installation costs.

- The central hub or switch is a single point of failure; if it fails, the entire network goes down.

✓ **Use Cases**: Common in modern LANs, especially in home and office networks.

- Ring Topology

✓ **Layout**: Each device is connected to two other devices, forming a circular pathway for data to travel.

✓ **Data Transmission**: Data travels in one direction (unidirectional) or both directions (bidirectional) around the ring until it reaches its destination.

✓ **Advantages**:

- Easy to install and reconfigure.
- Predictable data flow with minimal chances of collisions.
- All devices have equal access to the network.

✓ **Disadvantages**:

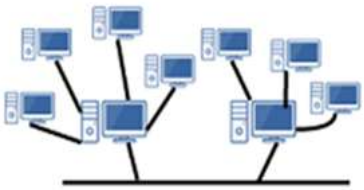
- Failure of a single device or cable can disrupt the entire network.
- Troubleshooting can be difficult.
- Adding or removing devices requires temporarily shutting down the network.

✓ **Use Cases**: Used in certain types of MANs (Metropolitan Area Networks) and for network redundancy in industrial settings.

- Mesh Topology

- ✓ **Layout**: Every device is connected to every other device, creating a web-like structure with multiple paths for data to travel.
- ✓ **Data Transmission**: Data can take any of the available paths to reach its destination, allowing for redundancy.
- ✓ **Advantages**:
  - Highly reliable and fault-tolerant due to multiple redundant paths.
  - High network resilience; if one link fails, data can take an alternative path.
  - Scalable with the ability to add more devices without affecting the network.
- ✓ **Disadvantages**:
  - Expensive and complex to install and maintain due to the large amount of cabling required.
  - Increased costs and complexity as the number of devices grows.
- ✓ **Use Cases**: Used in critical networks where reliability and redundancy are paramount, such as military or financial institutions.

- Tree Topology

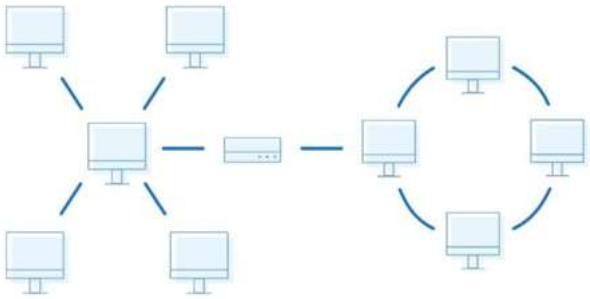


- ✓ **Layout**: A hybrid topology that combines characteristics of star and bus topologies. It consists of groups of star-configured networks connected to a central bus backbone.
- ✓ **Data Transmission**: Data travels from the devices to the central hub or switch and then along the bus backbone.
- ✓ **Advantages**:
  - Hierarchical structure allows for easy management and scalability.
  - Fault isolation is easier in the branches.
  - Supports future expansion of the network.
- ✓ **Disadvantages**:
  - Requires more cabling and configuration than a simple star or bus topology.

- The backbone is a single point of failure; if it fails, entire branches can be affected.

✓ **Use Cases**: Large networks, such as those in schools or large office buildings, where hierarchical organization is beneficial.

- Hybrid Topology



✓ **Layout**: A combination of two or more different types of physical topologies, designed to leverage the strengths of each.

✓ **Data Transmission**: Depends on the specific combination of topologies used.

✓ **Advantages**:

- Flexible and scalable, allowing for tailored network design.
- Can be optimized for specific network requirements and use cases.
- Provides redundancy and fault tolerance where necessary.

✓ **Disadvantages**:

- Complex design and configuration.
- Higher installation and maintenance costs.
- Troubleshooting can be challenging due to the mixed nature of the network.

✓ **Use Cases**: Large, complex networks in enterprises or data centers where different departments or functions have unique network requirements.

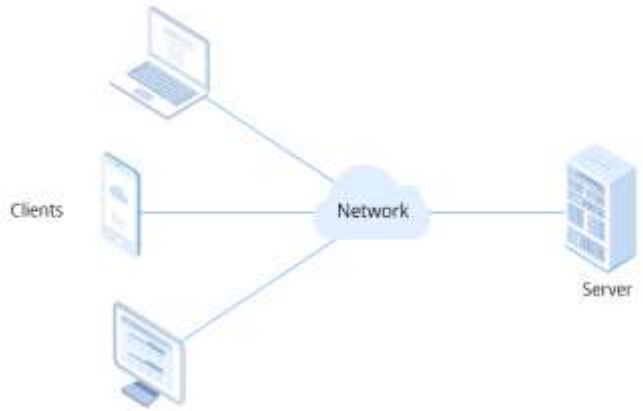
4. **Types of Local Area Network (LAN)**

Local Area Networks (LANs) can be classified based on various criteria, including their architecture, topology, medium, size or scale and the technology used.

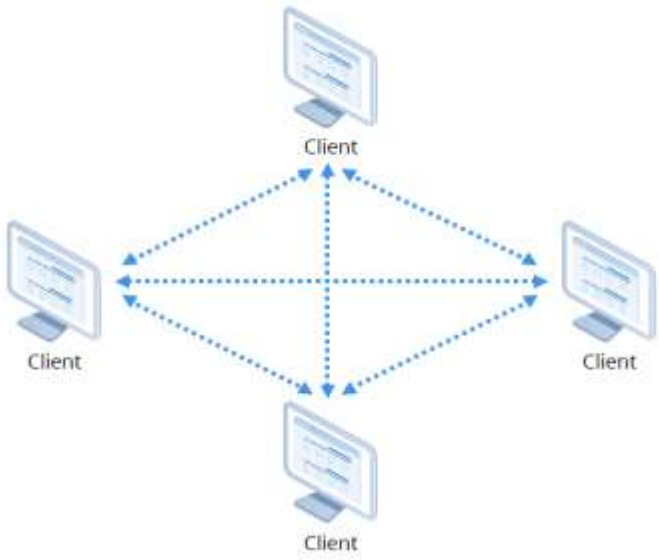
These classifications help in understanding the design, purpose, and functionality of different LAN types, enabling better decision-making when planning and implementing networks.

Here are some common classifications:

- **Classifying by Architecture/ Data sharing method**
  - ✓ **Client-Server LAN:** A Client-Server LAN is a LAN where devices are divided into clients (users) and servers (providers of resources/services).
    - **Advantages:** Centralized control and resource management.
    - **Disadvantages:** Dependency on the server. If the server fails, clients lose access to services.



  - ✓ **Peer-to-Peer (P2P) LAN:** In a peer-to-peer network, All devices are equal and share resources directly with each other without a centralized server.
    - **Advantages:** Simple and cost-effective for small networks.
    - **Disadvantages:** Difficult to manage as the network grows. Less secure than client-server LANs.



- **Classifying by Topology**
  - ✓ **Bus Network:** All devices are connected to a single central cable (the bus). Data is transmitted in both directions along the bus.
    - **Advantages:** Easy to install and requires less cable.
    - **Disadvantages:** Limited cable length and number of stations. A failure in the central cable disrupts the entire network.
  - ✓ **Ring Network:** Devices are connected in a circular configuration, where each device is connected to two other devices, forming a ring.
    - **Advantages:** Data packets travel in one direction, reducing the chance of packet collisions.
    - **Disadvantages:** Failure of a single device can disrupt the entire network.
  - ✓ **Star Network:** All devices are connected to a central hub or switch. The hub acts as a repeater for data flow.
    - **Advantages:** If one link fails, it doesn't affect the rest of the network.
    - **Disadvantages:** The hub is a single point of failure. If it fails, the entire network goes down.
  - ✓ **Mesh Network:** Each device is connected to every other device in the network, providing multiple paths for data to travel.
    - **Advantages:** High redundancy and reliability. If one link fails, data can be rerouted.

- **Disadvantages:** Expensive and complex to install due to the large number of cables and connections.

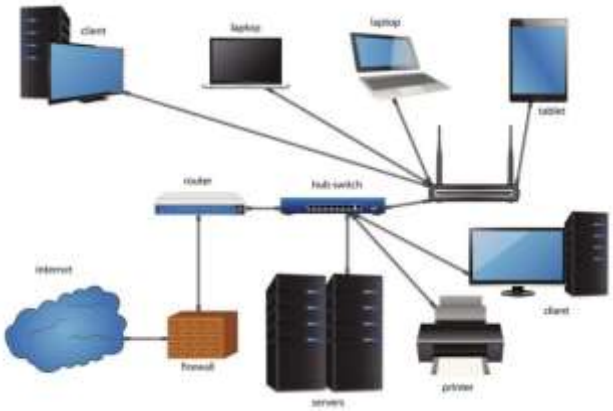
✓ **Hybrid Network:** A combination of two or more topologies (e.g., star-bus, star-ring) to meet specific network needs.

- **Advantages:** Flexible and scalable. Can be tailored to specific requirements.
- **Disadvantages:** Complex to design and manage.

- **Classifying by Transmission medium**

✓ **Wired LAN:** Uses physical cables (e.g., Ethernet) to connect devices.

- **Advantages:** Generally faster and more secure than wireless LANs.
- **Disadvantages:** Limited mobility due to the need for physical connections.



✓ **Wireless LAN (WLAN):** Uses wireless signals (e.g., Wi-Fi) to connect devices.

- **Advantages:** Provides mobility and flexibility. Easier to install in environments where cabling is difficult.
- **Disadvantages: Can be less secure and slower than wired LANs. Susceptible to interference.**

- ✓ **Hybrid LAN:** Combines both wired and wireless connections within the same network.
  - **Advantages:** Integrates the strengths of both wired and wireless networks, offering a balance of performance, reliability, and mobility. Wired connections are used where high performance and stability are needed, while wireless connections provide mobility and ease of access.
  - **Disadvantages:** Requires careful management to ensure seamless integration and security across both types of connections.

- **Classifying by scale/Size and Coverage**

- ✓ **Small Office/Home Office (SOHO) LAN:** A small-scale LAN typically used in a small office or home environment.
  - **Advantages:** Simple and easy to set up. Requires minimal hardware and expertise.

- **Disadvantages:** Limited in scale and features compared to larger LANs.

✓ **Enterprise LAN:** A large-scale LAN used within a single organization, often spanning multiple floors or buildings.

- **Advantages:** Supports a large number of devices and provides centralized management.
- **Disadvantages:** Complex to design, manage, and secure.

- **Classifying by Technology**

✓ **Wired LAN:** Utilizes physical cables to connect devices within the network.

- **Technologies:**

1. **Ethernet:** The most common wired LAN technology, using twisted pair cables (e.g., Cat5e, Cat6) or fiber optics.
2. **Fiber Optic:** High-speed connections using fiber optic cables, often used for backbone connections in larger networks.

- **Characteristics:** Generally, offers higher speeds, lower latency, and more stable connections compared to wireless LANs.

✓ **Wireless LAN (WLAN):** Uses wireless communication technologies to connect devices without physical cables.

- **Technologies:**

1. **Wi-Fi (IEEE 802.11):** The most widely used standard for wireless networking, offering various protocols (e.g., 802.11ac, 802.11ax) for different speeds and ranges.
2. **Bluetooth:** A short-range wireless technology often used for connecting peripherals and devices.
3. **Zigbee:** A low-power wireless standard used for IoT devices and sensor networks.

- **Characteristics:** Provides flexibility and mobility, but may be subject to interference and security concerns.

- ✓ **Token LAN:** An older networking technology where connected devices pass a token to transmit data.
  - **Technologies:**

    Token Ring (IEEE 802.5): A LAN technology that uses token passing for collision-free data transmission.
  - **Characteristics:** Provides predictable performance and avoids collisions but has largely been replaced by Ethernet technologies.
- ✓ **Powerline Networking:** Uses existing electrical wiring to create a network connection.
  - **Technologies:**

    Home Plug: A standard for powerline communication that allows networking over electrical circuits.
  - **Characteristics:** Convenient for extending network coverage without running new cables, but performance can vary based on electrical wiring quality.

5. **Key Components of LAN Architecture**

The architecture of a Local Area Network (LAN) is composed of several key components that work together to enable communication, data transfer, and resource sharing within a localized area, such as an office building, school, or home.

Here are the key architectural components of a LAN:

- **Network Devices/Interconnecting Devices**

Network devices are the hardware components that enable communication between devices in a LAN. Key network devices include:

- ✓ **Switches**: Act as the central point for device connections in a star topology. Switches manage data traffic efficiently by forwarding data only to the intended recipient.
- ✓ **Routers**: Connect different networks and direct data between them. In a LAN, routers are often used to connect the local network to the internet.

- ✓ **Hubs**: Less sophisticated than switches, hubs broadcast incoming data to all connected devices, which can lead to network inefficiencies.
- ✓ **Bridges**: Connect different network segments, filtering traffic to reduce congestion and improve performance.
- ✓ **Access Points (APs)**: Provide wireless connectivity, allowing devices to join the LAN without physical cables.

- **Network Interfaces**

Network interfaces are the points of connection between the network and devices. They can be physical (wired) or wireless. Common types include:

- ✓ **Network Interface Cards (NICs)**: Installed in computers and other devices, NICs enable them to connect to the network via Ethernet cables or wirelessly.
- ✓ **Wireless Adapters**: Allow devices to connect to a wireless LAN (WLAN), using standards like Wi-Fi.

- **Cabling and Connectors**

Cabling and connectors form the physical backbone of a wired LAN, providing the pathways through which data is transmitted.

- ✓ **Twisted-Pair Cables (e.g., Cat5e, Cat6)**: The most common type of cabling used in LANs, twisted-pair cables are cost-effective and support high-speed data transfer.
- ✓ **Fiber Optic Cables**: Used for long-distance and high-speed data transmission, fiber optic cables are immune to electromagnetic interference.
- ✓ **Connectors (e.g., RJ-45, LC, SC)**: Connect cables to network devices. RJ-45 connectors are standard for Ethernet cables, while LC and SC connectors are used for fiber optics.

- **Media**

Media refers to the physical or wireless medium through which data is transmitted in a LAN. This can include:

- ✓ **Wired Media**: Such as twisted-pair cables and fiber optics, providing stable and high-speed connections.
- ✓ **Wireless Media**: Such as radio waves used in Wi-Fi networks, offering flexibility and mobility but with potential interference issues.

- **Network Protocols**

Network protocols are the rules and conventions that govern how data is transmitted and received across the network. They ensure that devices on the network can communicate effectively. Key protocols include:

- ✓ **Ethernet**: The most common LAN protocol, governing how data is framed and transmitted over wired networks.
- ✓ **Wi-Fi (IEEE 802.11)**: The standard for wireless networking, providing guidelines for data transmission over wireless media.
- ✓ **IP (Internet Protocol)**: Governs how data is routed across networks, essential for devices to communicate on a TCP/IP-based LAN.

- **Security Components**

Security components protect the LAN from unauthorized access, threats, and vulnerabilities. They include:

- ✓ **Firewalls**: Control incoming and outgoing network traffic based on predetermined security rules.
- ✓ **Encryption Protocols**: Such as WPA2 for wireless networks, which encrypt data to protect it from eavesdropping.
- ✓ **Authentication Systems**: Ensure that only authorized users and devices can access the network, using methods like passwords, biometric scans, or certificates.

- **Servers and End Devices**

Servers and end devices are the final destinations for data within a LAN. Servers provide resources, services, or applications to clients, while end devices (like computers, printers, and IoT devices) are the tools used by end-users to interact with the network.

- ✓ **Servers**: Centralized systems that manage network resources, host applications, and provide services such as file storage, email, and databases.
- ✓ **Workstations**: End-user devices like desktop computers, laptops, and tablets that connect to the network to access resources.
- ✓ **Printers and Peripheral Devices**: Networked printers, scanners, and other peripherals that multiple users can access.

- **Network Operating Systems (NOS)**

A Network Operating System (NOS) is specialized software that manages network resources and controls communication between devices on the LAN. Examples include:

- ✓ **Windows Server**: Provides file sharing, print services, and other network management features.
- ✓ **Linux-based NOS**: Often used in enterprise environments for web hosting, file servers, and more.

6. Main phases of network installation

Network installation involves several key phases, each building upon the previous one to create a reliable and efficient network. These phases include Initial Assessment and Requirements Gathering, Site Survey, Network Design, Cost Estimation and Budgeting, Implementation Planning, Installation and Configuration, Testing and Validation, Documentation and Handover, and Monitoring and Maintenance.

Each phase has a specific objective and delivers a concrete end result, ensuring that the network meets the organization’s needs and is prepared for long-term operation.

- **Initial Assessment and Requirements Gathering**
  - ✓ **Objective**: Understand the organization's needs, the scope of the network, and specific requirements.

- ✓ **Tasks**:
  - Conduct interviews with stakeholders.
  - Gather information on the number of users, devices, and applications.
  - Determine bandwidth, performance, and security needs.
- ✓ **End Result**: **Requirements Specification Document**
  - This document outlines the network's purpose, scope, user needs, performance requirements, and security considerations.

- **Site Survey**
  - ✓ **Objective**: Physically inspect the installation environment to assess factors like space, infrastructure, and environmental conditions.
  - ✓ **Tasks**:
    - Evaluate physical space for network components.
    - Analyze existing facilities and power availability.
    - Identify potential environmental factors (e.g., interference, temperature).
    - Document site layout, cable routes, and potential obstacles.
  - ✓ **End Result**: **Site Survey Report**
    - This report includes detailed observations of the site, potential challenges, and recommendations for the installation.
- **Network Design**
  - ✓ **Objective**: Develop a detailed design for the network based on gathered requirements and site survey findings.
  - ✓ **Tasks**:
    - Design the network topology (e.g., star, mesh).
    - Specify hardware and software components.
    - Plan IP addressing, subnetting, and VLANs.
    - Develop security protocols and redundancy plans.
  - ✓ **End Result**: **Network Design Documentation**
    - This documentation includes network diagrams, equipment lists, configuration details, security protocols, and redundancy plans.
- **Cost Estimation and Budgeting**

- ✓ **Objective**: Estimate the total cost of the network installation, including hardware, software, labor, and other resources.
- ✓ **Tasks**:
  - Compile costs for equipment, cabling, and installation services.
  - Prepare a budget that aligns with the organization's financial constraints.
  - Consider potential future expenses for scalability and maintenance.
- ✓ **End Result**: **Cost Estimation Report**
  - This report provides a detailed breakdown of the costs associated with the network installation, including a budget plan.

- **Installation and Configuration**
  - ✓ **Objective**: Execute the installation of network hardware and software according to the design and implementation plan.
  - ✓ **Tasks**:
    - Install cabling, racks, and network devices (e.g., switches, routers).
    - Configure devices based on the network design.
    - Implement security measures, including firewalls and access controls.
  - ✓ **End Result**: **Installed and Configured Network**
    - The network hardware is installed and configured according to the design, with all devices operational and secure.
- **Testing and Validation**
  - ✓ **Objective**: Ensure the installed network meets all design specifications and performs as expected.
  - ✓ **Tasks**:
    - Conduct functionality and connectivity tests.
    - Perform performance testing, including bandwidth, latency, and throughput.
    - Verify security measures and redundancy systems.
    - Document test results and resolve any identified issues.
  - ✓ **End Result**: **Test Results and Validation Report**

- This report documents the testing process, results, and any necessary adjustments to ensure the network meets all performance and security criteria.

- **Documentation and Handover**
  - ✓ **Objective**: Provide comprehensive documentation and transition the network to operational status.
  - ✓ **Tasks**:
    - Finalize network documentation, including diagrams, configurations, and test results.
    - Prepare a maintenance plan and training materials for IT staff.
    - Conduct a handover meeting with stakeholders.
    - Ensure the network is fully operational and meets all user requirements.
  - ✓ **End Result**: **Network Handover Package**
    - This package includes all final documentation, maintenance plans, training materials, and a formal handover to the operational team.
- **Monitoring and Maintenance Planning**
  - ✓ **Objective**: Establish ongoing monitoring and maintenance procedures to ensure long-term network performance.
  - ✓ **Tasks**:
    - Set up network monitoring tools and alerts.
    - Develop a maintenance schedule for hardware and software updates.
    - Plan for future network scalability and upgrades.
    - Create procedures for incident response and troubleshooting.
  - ✓ **End Result**: **Monitoring and Maintenance Plan**
    - This plan outlines the ongoing monitoring processes, maintenance schedules, and protocols for handling network issues and future upgrades.

Points to Remember

- A Local Area Network (LAN) is a network that connects computers and devices within a limited area, such as a home, office building, or school campus.
- Network topology refers to the arrangement or layout of different elements in a computer network. It describes how devices such as computers, routers, and switches are interconnected and how data flows between them.
- Local Area Networks (LANs) can be classified based on various criteria, including their architecture, topology, medium, size or scale and the technology used.
- The architecture of a LAN is composed of several essential hardware and software components that work together to enable communication and data transfer. These components include: Network Devices, Nodes (end devices), Cables, ….

Application of learning 1.1.

A new café called "Kigali Brews" wants to provide free Wi-Fi for customers and have a network for their staff to manage orders and inventory.

The café owner decides they need a Local Area Network that connects a few computers, a printer, and provides Wi-Fi for customers.

They need a Network Technician to help them to know key components of LAN. This will help management team to suggest the range of budget that will be needed to buy network components.

Indicative content 1.2: Identification of LAN installation Requirements.

Duration: 4 hrs

Theoretical Activity 1.2.1: Description of essential factors of conducting a LAN installation site survev

Task:

1: Search, discuss and provide the answers for the following questions.

1. Define a site survey
2. What is the primary goal/purpose of conducting a site survey for LAN installation?
3. Discuss key advantages of conducting a site survey before LAN installation?
4. How does the analysis of facilities contribute to the design and implementation of a LAN?
5. Why is analysing network usage important when planning a LAN?
6. Discuss essential factors for Conducting a LAN Installation Site Survey

2: Prepare power point presentation for your findings

3: Ask your trainer for support where it is needed

4: Present your findings to the whole class

5: Ask questions where necessary.

6: For more clarification, read the key readings 1.2.1.

Key readings 1.2.1.: Description of essential factors of conducting a LAN installation site survey

1. Site survey

A site survey is a systematic assessment of a specific location to gather information that is essential for planning and implementing a project.

In the context of LAN (Local Area Network) installation, a site survey involves assessing the installation environment to understand the layout, existing infrastructure, and specific requirements related to network setup.

The survey helps identify potential challenges, determine optimal equipment placement, and ensure that the network design meets the needs.

This process is essential for creating a functional, efficient, and reliable network that supports the intended applications and user demands.

The insights gained from the site survey are used to plan an efficient, reliable, and scalable network installation that meets the organization's needs.

2. The primary goal of conducting a site survey for LAN installation

The primary goal of conducting a site survey for LAN installation is to gather detailed information about the physical environment, existing infrastructure, and specific network requirements of the site. This information is crucial for designing a network that is optimized for the location, ensuring reliable connectivity, efficient performance, and scalability.

3. Key Advantages of Conducting a Site Survey Before LAN Installation

A site survey is a crucial step in the process of planning and installing a Local Area Network (LAN). It provides valuable insights into the physical environment and infrastructure, enabling network engineers to make informed decisions and optimize the network design. Here are some key advantages of conducting a site survey before LAN installation:

- **Optimized Network Design:** A site survey helps identify potential challenges and constraints, allowing the network to be designed to fit the specific physical conditions of the location.
- **Reduced Installation Time and Costs:** A site survey can help anticipate and address potential problems, such as inadequate power outlets or structural obstacles, reducing the time and costs associated with troubleshooting and rework.
- **Improved Network Performance:** A well-planned network layout can minimize cable lengths and avoid interference, leading to better signal quality and performance.

- **Enhanced Security:** A site survey can help identify potential security vulnerabilities, such as areas with weak physical access control or exposure to external interference.
- **Future-Proofing:** A site survey can help identify potential growth areas and plan the network infrastructure accordingly, ensuring that it can accommodate future expansion and changes.

4. Essential Factors for Successful LAN installation Site Surveys

When conducting a LAN site survey, several factors contribute to its success. By focusing on these factors, organizations can conduct successful LAN site surveys that lead to effective network installations, improved performance, and enhanced user satisfaction. Here's a comprehensive description of these factors:

- **Physical Site Survey**

  - ✓ **Objective**: Assess the physical characteristics of the location where the LAN will be installed.
  - ✓ **Key Considerations**:
    - **Building Structure**: Analyze the layout, construction materials, and age of the building to determine how they might affect cabling, signal propagation, and network installation.
    - **Space Availability**: Identify areas for installing network devices such as switches, routers, servers, and access points, as well as where cabling will be run.
    - **Electrical Power**: Ensure adequate and reliable power supply, including backup power solutions like UPS (Uninterruptible Power Supply) systems.
    - **Cooling and Ventilation**: Evaluate the need for proper cooling and ventilation in areas where network equipment, such as server rooms, will be installed.
    - **Access Control**: Consider the security of physical access to critical network infrastructure to prevent unauthorized access.

- **Analysis of Facilities**

- ✓ **Objective**: Assess the existing infrastructure and facilities to determine their suitability for supporting the planned LAN.
- ✓ **Key Considerations**:
  - **Existing Network Infrastructure**: Review any existing network setup, cabling, and equipment to determine if they can be reused or need upgrading.
  - **Cabling Pathways**: Identify and plan the best routes for running network cables, considering factors such as distance, interference, and ease of maintenance.
  - **Availability of Conduits and Cable Trays**: Ensure that there are proper conduits and trays for organizing and protecting network cables.
  - **Mounting Options**: Assess where and how network devices such as switches and access points will be mounted, including wall-mounted racks or ceiling-mounted access points.

- **Network Usage Analysis**

  - ✓ **Objective**: Understand the intended use of the network to ensure that it is designed to meet current and future demands.
  - ✓ **Key Considerations**:
    - **User Requirements**: Identify the number and types of users who will be accessing the network, their locations, and their specific needs (e.g., file sharing, internet access, video conferencing).
    - **Device Density**: Consider the number of devices that will connect to the network, including computers, smartphones, printers, IoT devices, and any other connected devices.
    - **Application Requirements**: Evaluate the types of applications that will run on the network (e.g., VoIP, video streaming, cloud services) and their bandwidth and latency requirements.
    - **Traffic Patterns**: Analyze expected data traffic patterns to determine the need for load balancing, traffic management, and Quality of Service (QoS) configurations.

- **Growth and Scalability**: Plan for future growth by considering how the network might need to expand in terms of users, devices, and applications.

- **Security Requirements**

  ✓ **Objective**: Ensure that the network is secure from potential threats and unauthorized access.

  ✓ **Key Considerations**:

  - **Physical Security**: Implement measures to protect network equipment from physical tampering or theft, including secure server rooms and locked enclosures for switches and routers.
  - **Network Security**: Plan for network security measures such as firewalls, intrusion detection systems (IDS), and secure wireless access protocols (e.g., WPA3 for Wi-Fi).
  - **Access Control**: Define user access policies to restrict who can access certain parts of the network and sensitive data.
  - **Data Protection**: Ensure that data transmitted over the network is protected through encryption and other security protocols.

- **Environmental Factors and Potential challenges**

  ✓ **Objective**: Consider environmental conditions that might impact the network's performance and longevity.

  ✓ **Key Considerations**:

  - **Interference**: Identify potential sources of electromagnetic interference (EMI) that could affect signal quality, especially for wireless networks.
  - **Temperature and Humidity**: Ensure that the installation environment is within the acceptable temperature and humidity ranges for the equipment.
  - **Dust and Contaminants**: Evaluate the presence of dust or other contaminants that could affect network equipment, and consider protective measures like air filters.

- **Documentation and Reporting**

- ✓ **Site Survey Report**: Compile a detailed report that includes all findings, recommendations, and potential challenges. This report should serve as a reference for the installation team.
- ✓ **Network Design Proposal**: Based on the survey, develop a network design proposal that meets the client's needs and addresses any identified challenges.

- **Customer Communication**

  - ✓ **Feedback and Adjustments**: Present the survey findings and proposed design to the client, and make any necessary adjustments based on their feedback.
  - ✓ **Timeline and Budget**: Discuss the timeline for the installation and any budget considerations, ensuring that the client is fully informed and agrees to the plan.

Here's a sample of a LAN installation site survey report that you can use as a template or guide:

LAN Installation Site Survey Report

Date: *August 17, 2024*

Survey Conducted by: *[Your Name/Company Name]*

1. Client Information

- ***Client Name:*** *Greenfield School*
- ***Contact Person:*** *Paul MIHIGO, IT Manager*
- ***Contact Information:*** *Phone: +250- 456-7890 | Email: mihigo@greenfieldschool.edu*

2. Project Overview

- ***Project Name:*** *Greenfield School LAN Installation*
- ***Project Location:*** *123 Greenfield Road, Springfield*
- ***Scope:*** *Installation of a Local Area Network (LAN) to support administrative operations, classrooms, and a computer lab across a four-story school building.*

3. Physical Site Survey

- ***Building Layout:***
  - ✓ ***Structure:*** *Four-story building with three classrooms and one computer lab per floor.*
  - ✓ ***Room Dimensions:*** *Classrooms are approximately 30x20 feet; computer lab is 40x30 feet.*

- ✓ ***Obstacles:*** *Concrete walls between classrooms may impact wireless signal strength.*

4. Analysis of Facilities

- ***Power Supply:***
  - ✓ ***Availability:*** *Power outlets are available in all classrooms, the computer lab, and administrative offices. The server room is equipped with a dedicated power source, including an Uninterruptible Power Supply (UPS) for critical devices.*
- ***Cooling and Ventilation:***
  - ✓ ***Server Room:*** *The server room has adequate cooling with a dedicated air conditioning unit. Temperature and humidity levels are maintained within the optimal range for network equipment.*
  - ✓ ***Classrooms and Computer Lab:*** *The general HVAC system provides sufficient ventilation. However, due to the high density of computers in the lab, additional cooling might be considered during peak usage times.*
- ***Space Allocation:***
  - ✓ ***Server Room:*** *The server room has ample space for the planned network equipment, including racks, switches, and the main router. The layout allows for easy access to all components for maintenance purposes.*
  - ✓ ***Classrooms:*** *Space is available for wall-mounted or ceiling-mounted access points. Lockable cabinets will be installed for securing networking equipment in each classroom.*
  - ✓ ***Cable Management:*** *Existing conduits and cable trays can be utilized for running new cables, ensuring a tidy and organized installation.*

5. Network Usage and Requirements

- ***Current and Future Needs:***
  - ✓ ***Number of Users:*** *Approximately 30 users per classroom, 50 users in the computer lab, and 20 administrative staff.*
  - ✓ ***Application Requirements:*** *High-bandwidth applications expected, including video streaming and interactive learning platforms.*

- ✓ ***Future Expansion:*** *Potential to add 2 more classrooms in the next academic year; design should allow for easy expansion.*

- ***Data and Voice Needs:***
  - ✓ ***Voice Services:*** *VoIP phones required in all classrooms and administrative offices.*
  - ✓ ***Data Services:*** *Wired and wireless connectivity required. Wi-Fi coverage needs to be strong throughout the building, especially in classrooms and labs.*
- ***Security Requirements:***
  - ✓ ***Access Control:*** *Secure access needed for administrative staff; guest network required for visitors.*
  - ✓ ***Surveillance:*** *Security cameras will be connected to the network; coverage needed in hallways and common areas.*
  - ✓ ***Compliance:*** *Network design must comply with educational standards and data protection regulations.*

6. Environmental Factors

- ***Interference:***
  - ✓ ***Potential Issues:*** *Nearby electrical equipment (e.g., elevators) may cause EMI. Wireless signal may be affected by concrete walls.*
  - ✓ ***Mitigation:*** *Use of shielded cabling and strategic placement of access points to minimize interference.*
- ***Weather and Climate:***
  - ✓ ***Outdoor Cabling:*** *No outdoor cabling required. All network components will be installed indoors.*
  - ✓ ***Building Conditions:*** *The building is well-insulated, with no significant climate-related concerns.*

7. Documentation and Reporting

- ***Network Design Proposal:***
  - ✓ ***Wired Network:*** *Cat6 cabling to all classrooms, labs, and administrative offices; centralized switch in the server room.*

- ✓ ***Wireless Network:*** *Deployment of access points on each floor to ensure complete coverage; use of mesh network to enhance signal strength.*
- ✓ ***Security:*** *Installation of a firewall and intrusion prevention system (IPS) in the server room; VLANs to separate staff and student traffic.*

- ***Challenges and Recommendations:***
  - ✓ ***Challenges:*** *Concrete walls may require additional access points for adequate wireless coverage.*
  - ✓ ***Recommendations:*** *Consider using higher-gain antennas for wireless access points. Ensure regular maintenance of the cooling system in the server room.*

8. Customer Communication

- ***Presentation of Findings:***
  - ✓ ***Feedback:*** *Client is concerned about potential wireless signal issues in classrooms. Agreed to add more access points as a precaution.*
  - ✓ ***Adjustments:*** *Revised budget to include additional access points and higher-quality cabling to mitigate potential interference.*
- ***Timeline and Budget:***
  - ✓ ***Estimated Timeline:*** *3 weeks for installation, followed by 1 week of testing and configuration.*
  - ✓ ***Budget:*** *$25,000, including all hardware, installation, and configuration costs.*

Approval and Signatures

Client Representative: _____

Surveyor: _____

Practical Activity 1.2.2.1: Conducting LAN installation site survey

Task:

1: Read the provided copy of scenarios and do task described below:

> Your school intends to install a Local Area Network in the office building, garden, and classroom block. Visit the location described in the scenario, conduct a site survey, and prepare a site survey report that will assist the school in identifying the installation requirements.

2: Visit the location described in the scenario and carry out task 1.2.2 referring to the knowledge gained from Theoretical Activity 1.2.1.

3: Ask for assistance whenever it is needed.

4: In your groups: (1) read key readings 1.2.2 in their manuals, (2) Brainstorm about your findings, (3) refine and produce the perfect site survey report

5: Ask an assistance where it is needed.

6.Submit your site survey report to Trainer.

Key readings 1.2.2.1

Process for LAN installation site survey

Conducting a LAN installation site survey involves a systematic process to ensure that all aspects of the network installation are carefully evaluated. Here's a step-by-step guide to performing a comprehensive LAN installation site survey:

1. Preparation and Planning

Client Consultation:

- ✓ Meet with the client to understand their requirements, including the purpose of the network, number of users, and specific needs like data, voice, and security.

- ✓ Discuss any existing infrastructure and future expansion plans.

- **Gather Existing Documentation:**
  - ✓ Obtain floor plans, network diagrams, and any documentation related to existing infrastructure.
  - ✓ Review any previous network installations or modifications.
- **Assemble Tools and Equipment:**
  - ✓ Prepare necessary tools, such as a laptop, network analyzer, measuring tape, camera, and any specific software needed for the survey.

2. Site Visit and Physical Inspection

- **Evaluate the Physical Layout:**
  - ✓ Walk through the entire site to understand the building's layout, including room dimensions, wall materials, and potential obstacles like doors, windows, and columns.
  - ✓ Identify potential locations for network equipment like switches, routers, access points, and cabling pathways.
- **Infrastructure Assessment:**
  - ✓ Check for existing cabling, power outlets, and network points that could be reused or need upgrading.
  - ✓ Assess the availability and reliability of the power supply, including the need for backup systems like UPS.
  - ✓ Inspect the cooling and ventilation systems in areas like the server room and data centers.

3. Analysis of Facilities

- **Power Supply:**
  - ✓ Confirm the availability of power in all required locations and assess the reliability of the power supply.
  - ✓ Identify the need for additional power outlets, dedicated circuits, or backup power systems.
- **Cooling and Ventilation:**
  - ✓ Evaluate the cooling and ventilation in critical areas, ensuring that server

rooms and areas with high equipment density have adequate cooling to prevent overheating.

- **Space Allocation:**
  - ✓ Ensure there is sufficient space for all network equipment, including racks, servers, and patch panels.
  - ✓ Evaluate cable management options, such as conduits, cable trays, and pathways.

4. Assessment of Network Usage and Requirements

- **Determine Network Requirements:**
  - ✓ Identify the number of users, devices, and types of applications that will run on the network.
  - ✓ Assess bandwidth requirements for both wired and wireless networks, considering current and future needs.
- **Voice and Data Needs:**
  - ✓ Determine the need for voice services, such as VoIP, and ensure the network can support these services.
  - ✓ Evaluate the need for wired versus wireless connections and plan for adequate Wi-Fi coverage.
- **Security Requirements:**
  - ✓ Identify access control needs, both physical and digital, to ensure network security.
  - ✓ Consider the need for surveillance systems, firewalls, and intrusion prevention systems (IPS).

5. Environmental Factors

- **Interference and Obstructions:**
  - ✓ Identify potential sources of interference, such as electrical equipment or thick walls, which could affect network performance.
  - ✓ Plan for the placement of access points and cabling to minimize interference and ensure strong signal coverage.
- **Weather and Climate Considerations:**

- ✓ Assess any environmental factors that might impact the installation, such as outdoor cabling, exposure to weather, and temperature control.

6. Documentation and Reporting

- **Compile Findings:**
  - ✓ Document all observations, measurements, and assessments made during the site survey.
  - ✓ Create a detailed site survey report that includes floor plans, network diagrams, photos, and notes.
- **Network Design Proposal:**
  - ✓ Develop a network design proposal based on the survey findings, addressing all client requirements and identified challenges.
  - ✓ Include recommendations for equipment, cabling, access points, and security measures.

7. Client Review and Feedback

- **Present the Survey Report:**
  - ✓ Share the site survey report and network design proposal with the client, explaining the rationale behind each recommendation.
  - ✓ Discuss any potential challenges and proposed solutions.
- **Gather Feedback:**
  - ✓ Listen to the client's feedback and make necessary adjustments to the network design or installation plan.
  - ✓ Finalize the design and obtain client approval before proceeding with the installation.

Here's a sample LAN Installation Site Survey Report focused specifically on the school garden and playground areas:

LAN Installation Site Survey Report

Date: *August 17, 2024*

Survey Conducted by: *[Your Name/Company Name]*

1. **Client Information**

- ***Client Name:*** *Kigali-B Secondary School*
- ***Contact Person:*** *Mrs. GAJU Annette, Principal*
- ***Contact Information:*** *Phone: +250 723-4567 | Email: gajuanne@kigalibsecondary.edu*

2. Project Overview

- ***Project Name:*** *Kigali-B Secondary School LAN Installation for Outdoor Areas*
- ***Project Location:*** *NYARUGENGE District*
- ***Scope:*** *Design and installation of a Local Area Network (LAN) to provide Wi-Fi coverage in the school garden and playground areas.*

3. Physical Site Survey

- ***Outdoor Area Layout:***
  - ✓ ***School Garden:***
    - ***Size:*** *Approximately 100x80 feet.*
    - ***Usage:*** *Outdoor learning sessions, student gatherings, and events.*
    - ***Obstacles:*** *Trees and shrubbery that may interfere with signal strength.*
    - ***Existing Structures:*** *Benches, a small pavilion, and garden sheds where equipment can be mounted.*
  - ✓ ***Playground:***
    - ***Size:*** *Approximately 150x100 feet.*
    - ***Usage:*** *Recreational activities during breaks and physical education classes.*
    - ***Obstacles:*** *Play structures and open space with no existing shelters.*
    - ***Existing Structures:*** *Fencing and light poles that can serve as mounting points for equipment.*
- ***Infrastructure Assessment:***
  - ✓ ***Existing Cabling:*** *No existing cabling in the garden or playground. New Cat6 outdoor-rated cabling will need to be installed.*
  - ✓ ***Power Supply:*** *Limited power supply in the garden and playground. Power*

will need to be extended from nearby buildings to support the network equipment.

- ✓ ***Environmental Conditions:*** *Both areas are fully exposed to weather conditions, requiring durable, weatherproof equipment.*

4. Network Usage and Requirements

- ***Current and Future Needs:***
  - ✓ ***Number of Users:*** *The garden and playground areas need to support up to 100 students simultaneously, primarily for outdoor classes, recreational activities, and Wi-Fi access during breaks.*
  - ✓ ***Application Requirements:*** *Reliable Wi-Fi coverage for accessing online educational resources, video streaming for outdoor lessons, and general internet browsing during free time.*
  - ✓ ***Future Expansion:*** *The network should allow for additional access points if the outdoor areas are expanded or usage increases.*
- ***Data and Voice Needs:***
  - ✓ ***Data Services:*** *Wi-Fi coverage is required throughout both the garden and playground areas, with sufficient bandwidth to handle multiple simultaneous connections.*
  - ✓ ***Voice Services:*** *No VoIP services required in these areas.*
- ***Security Requirements:***
  - ✓ ***Access Control:*** *Secure access to the network is required to prevent unauthorized use. The outdoor network should be isolated from the internal school network.*
  - ✓ ***Surveillance:*** *Security cameras will be connected to monitor both the garden and playground, with footage stored on a secure server.*
  - ✓ ***Compliance:*** *The outdoor network must comply with the same security and data protection regulations as the internal network.*

5. Environmental Factors

- ***Interference and Obstructions:***
  - ✓ ***Potential Issues:*** *Trees, shrubs, and playground equipment may cause*

signal reflection and attenuation. Weather conditions, such as rain and wind, may also impact signal stability.

- ✓ ***Mitigation:*** *Use of higher-gain antennas and strategic placement of weatherproof access points on existing structures, such as light poles and garden pavilions, to ensure robust coverage.*

- ***Weather and Climate Considerations:***
  - ✓ ***Outdoor Coverage:*** *Wi-Fi coverage is required in all weather conditions. Weatherproof access points and enclosures will be used to protect equipment from the elements.*
  - ✓ ***Environmental Durability:*** *Equipment must be able to withstand temperature fluctuations, moisture, and UV exposure. All cabling will be outdoor-rated and properly insulated.*

6. Documentation and Reporting

- ***Network Design Proposal:***
  - ✓ ***Wired Network:*** *Outdoor-rated Cat6 cabling will be installed to connect access points in the garden and playground to the main network. Cabling will be routed through existing conduits where possible and buried underground when necessary.*
  - ✓ ***Wireless Network:*** *Dual-band, weatherproof access points will be strategically placed in the garden and playground to ensure complete coverage. Access points will be mounted on existing structures such as light poles and garden pavilions.*
  - ✓ ***Security:*** *A separate VLAN will be established for the outdoor network, with strict access controls and monitoring to prevent unauthorized use. The network will be integrated with the school's existing security systems, including cameras.*
- ***Challenges and Recommendations:***
  - ✓ ***Challenges:*** *The outdoor environment presents challenges related to weather conditions and potential interference from natural and man-made obstacles. Limited existing power infrastructure will require careful planning to extend power to necessary locations.*

- ✓ ***Recommendations:*** *Use outdoor-rated, weatherproof equipment and ensure proper installation to protect against environmental factors. Extend power lines from nearby buildings, and consider solar-powered backup options for critical access points.*

- ***Photographs****:*
  - ✓ *Photo 1: Ceiling space above the main corridor showing available space for cable runs.*
  - ✓ *Photo 2: The server room with current network equipment and available outlets.*
  - ✓ *Photo 3: The metal filing cabinet near the conference room that may interfere with wireless signals.*
- ***Measurement Data****:*
  - ✓ *Server room to farthest workstation: 60 meters.*
  - ✓ *Distance between central wireless access points: 20 meters.*

7. Client Communication

- ***Presentation of Findings:***
  - ✓ ***Feedback:*** *The school administration expressed concerns about the durability of outdoor equipment and the potential impact on the school's landscape. Reassurances were provided regarding the use of discreet, weatherproof equipment and minimal disruption to the garden and playground areas.*
  - ✓ ***Adjustments:*** *Adjusted the report to include additional protective measures for equipment and explored options for solar-powered solutions to reduce reliance on the existing power grid.*

Approval and Signatures

Client Representative: _____

Surveyor: _____

Notes: After the site survey is completed and the network site survey report is created, the next logical step is to move into the network design phase.

Points to Remember

Conducting a LAN installation site survey is a critical step in ensuring that the network is designed and implemented effectively. Here are tasks to be performed before conducting a network installation site survey:

- Define Objectives and Requirements
  - ✓ Identify Goals
  - ✓ Gather User Requirements
- Assemble a Survey Team
  - ✓ Select Team Members
  - ✓ Assign Roles
- Prepare Survey Tools
  - ✓ Gather Equipment

Practical Activity 1.2.2.2: Determining LAN installation requirements

Task:

1: Obtain a copy of the LAN installation site survey report from Practical Activity 1.2.2.1 and proceed to complete Task 1.2.2.2 as detailed below.

> Analyse the survey data from LAN installation site survey report prepared in Practical Activity 1.2.2.1. Based on your analysis, identify all types of LAN installation requirements and provide clear specifications. Finally, compile a comprehensive network installation requirements document to facilitate a smoother installation process and ensure more accurate cost estimates.

2: Observe and engage in the demonstration of the key considerations for determining LAN installation requirements. Ask questions and participate in discussions to deepen your understanding of the process.

3: Individually complete the Task 1.2.2.2 by applying the knowledge and insights gained from Step 3

4: Seek assistance from the trainer when needed to ensure successful completion of the task.

5: Sit in your small groups and (1) read key readings 1.2.2.2 in trainee manual, (2) Discuss about your findings, (3) and produce perfect equipment list.

6: Ask for assistance where it is needed.

7.Submit your network design Document to trainer.

8: Read key readings 1.2 in your manual for further understanding.

Key readings 1.2.2.2

1. Essential LAN Hardware Requirements

The topic of Essential LAN Hardware Requirements focuses on the critical components necessary for building a robust Local Area Network (LAN). It covers the various devices and elements that form the backbone of any LAN, including Interconnecting Devices, Access Devices, Security Devices, End Devices, Connectors, and Media. Each of these components plays a vital role in ensuring seamless communication, connectivity, and security within the network.

- **Interconnecting Devices**
  - ✓ **Switches**
    - **Purpose:** Serve as the central point for connecting multiple devices within the LAN, enabling data exchange between them.
    - **Types:**
      - **Managed Switches:** Offer advanced configuration, monitoring, and control.
      - **Unmanaged Switches:** Plug-and-play devices with no configuration required.
    - **Features:** Port density, PoE (Power over Ethernet) support, and data transfer speeds.
  - ✓ **Routers**
    - **Purpose:** Connect the LAN to external networks (e.g., the Internet) and route traffic between them.
    - **Features:** Routing capabilities, firewall functions, NAT (Network Address

Translation), and VPN support.

- ✓ **Hubs**
  - **Purpose:** Basic device for connecting multiple Ethernet devices, operating at the physical layer (Layer 1).
  - **Note:** Hubs are largely obsolete, replaced by more efficient switches.

- **Access Devices**
  - ✓ **Wireless Access Points (WAPs)**
    - **Purpose:** Provide wireless connectivity to devices within the LAN.
    - **Features:** Support for different Wi-Fi standards (e.g., 802.11ac, 802.11ax), dual-band or tri-band operation, and coverage area.
    - **Deployment:** Ceiling-mounted or wall-mounted for optimal coverage.
  - ✓ **Network Interface Cards (NICs)**
    - **Purpose:** Enable devices like computers, printers, and servers to connect to the network, either wired or wirelessly.
    - **Types:**
      - **Wired NICs:** Ethernet-based connections.
      - **Wireless NICs:** Wi-Fi-based connections.

- **Security Devices**
  - ✓ **Firewalls**
    - **Purpose:** Protect the LAN by controlling incoming and outgoing network traffic based on security rules.
    - **Types:**
      - **Hardware Firewalls:** Standalone devices or integrated into routers.
      - **Features:** Intrusion detection/prevention, VPN support, and advanced threat protection.
  - ✓ **Intrusion Detection Systems (IDS) / Intrusion Prevention Systems (IPS)**
    - **Purpose:** Monitor network traffic for suspicious activity (IDS) and take action to block threats (IPS).
    - **Features:** Signature-based detection, anomaly detection, and real-time alerts.

- ✓ **Access Control Devices**
  - **Purpose:** Control physical access to network infrastructure, ensuring that only authorized personnel can interact with critical network devices.
  - **Types:** Biometric scanners, keycard readers, and secure enclosures.

- **End Devices**
  - ✓ **Computers (Desktops, Laptops)**
    - **Purpose:** Primary devices used by end-users to access network resources.
    - **Connectivity:** Wired (Ethernet) or Wireless (Wi-Fi).
  - ✓ **Printers and Scanners**
    - **Purpose:** Networked devices for printing and scanning documents.
    - **Types:** Multifunction devices that may also include faxing capabilities.
  - ✓ **VoIP Phones**
    - **Purpose:** Enable voice communication over the LAN using IP protocols.
    - **Features:** Support for HD voice, video calls, and integration with other communication systems.
  - ✓ **IP Cameras**
    - **Purpose:** Provide security surveillance by capturing video over the network.
    - **Features:** High-definition video, night vision, and motion detection.
- **Connectors**
  - ✓ **RJ45 Connectors**
    - **Purpose:** Standard connector for Ethernet cables used in wired networking.
    - **Compatibility:** Cat5e, Cat6, and Cat6a cables.
  - ✓ **LC/SC Connectors**
    - **Purpose:** Connect fiber optic cables for high-speed data transmission.
    - **Types:** LC (Lucent Connector), SC (Subscriber Connector).
  - ✓ **BNC Connectors**
    - **Purpose:** Used in coaxial cable connections, primarily in older or specialized network setups.
- **Media**
  - ✓ **Twisted-Pair Cables**

- **Purpose:** Commonly used for Ethernet connections within the LAN.
- **Types:**
  - **Cat5e:** Supports up to 1 Gbps.
  - **Cat6:** Supports up to 10 Gbps at shorter distances.
  - **Cat6a:** Enhanced version of Cat6 for better performance.
- **Shielding:** Unshielded (UTP) and Shielded (STP) options.

✓ **Fiber Optic Cables**

- **Purpose:** Used for high-speed and long-distance data transmission.
- **Types:**
  - **Single-mode Fiber:** Long-distance, high-speed transmission.
  - **Multi-mode Fiber:** Shorter distances, often used within buildings.
- **Advantages:** Immune to electromagnetic interference and capable of higher bandwidths.

✓ **Coaxial Cables**

- **Purpose:** Used in older network setups, primarily for cable TV and some broadband connections.
- **Components:** Central conductor, insulating layer, shielding, and outer jacket.

2. Process for determining LAN installation requirements

Determining the LAN installation requirements is a crucial step in ensuring a successful network setup. This process typically involves assessing various factors to meet both the technical and business needs of the organization. After completing a LAN installation site survey, the following tasks were undertaken to determine the necessary LAN installation requirements.

- **Analysis of Site Survey Data(report)**

✓ **Site Layout and Topography**: Review the physical layout of the site, including room dimensions, building materials, and any obstacles that might affect network performance (e.g., thick walls, metal structures, or large open areas).

✓ **Existing Infrastructure**: Identify existing network infrastructure that can be utilized or will need to be upgraded. This includes current cabling, network devices, power sources, and any legacy systems.

- ✓ **Environmental Conditions**: Consider environmental factors such as temperature, humidity, and electromagnetic interference that could impact the performance and reliability of the network.

- **Identification of Specific Network Requirements**
  - ✓ **Coverage Areas**: Determine the specific areas that need network coverage, such as classrooms, offices, common areas, and any outdoor spaces (e.g., the school garden). This will guide the placement of access points, cabling, and other network components.
  - ✓ **Bandwidth and Performance Needs**: Based on the site survey and user needs analysis, estimate the required bandwidth to support activities such as video streaming, file sharing, and real-time collaboration. This will influence the choice of network equipment and cabling.
  - ✓ **Network Topology**: Decide on the optimal network topology based on the site layout and coverage requirements. Common topologies include star, mesh, or a hybrid approach, depending on the need for redundancy and ease of expansion.
  - ✓ **Device and Equipment Placement**: Plan the placement of network devices such as routers, switches, and access points. This includes identifying optimal locations for signal strength, coverage, and ease of maintenance.
  - ✓ **Power Requirements**: Assess power needs for all network equipment, including the potential need for Power over Ethernet (PoE) to simplify cabling and installation, especially in hard-to-reach areas.
  - ✓ **Redundancy and Failover**: Consider the need for redundancy in critical network components (e.g., switches, routers) to ensure network reliability and minimize downtime.
- **Security Considerations**
  - ✓ **Physical Security**: Identify any physical security requirements for network devices, especially in areas that are easily accessible to unauthorized individuals. This could involve securing devices in locked cabinets or enclosures.
  - ✓ **Network Segmentation**: Plan the segmentation of the network to create separate VLANs (Virtual Local Area Networks) for different user groups (e.g., students,

teachers, administration) to enhance security and manage traffic more effectively.

- ✓ **Access Control and Authentication**: Define the methods for controlling access to the network, such as implementing role-based access controls, setting up secure authentication mechanisms (e.g., WPA3 for Wi-Fi), and integrating with existing user directories.

- **Equipment Specification and Selection**
  - ✓ **Network Devices**: Based on the analysis, specify the types and quantities of network devices needed, such as routers, switches, wireless access points, and firewalls. This should include considerations for scalability and future upgrades.
  - ✓ **Cabling and Connectivity**: Determine the types of cabling required (e.g., Cat6, Cat6a, or fiber optic) based on the performance needs and distances between network components. Consider using structured cabling systems to support future expansion.
  - ✓ **Power and Backup Solutions**: Specify any power backup solutions required, such as uninterruptible power supplies (UPS) or redundant power supplies for critical network components.
- **Documentation and Reporting**
  - ✓ **Network Design Documentation**: Create a detailed network design document that outlines all the components, their placement, and the rationale behind the decisions. This document serves as a blueprint for the installation team and a reference for future maintenance and upgrades.
  - ✓ **Stakeholder Review**: Share the documented requirements and design with stakeholders (e.g., school administration, IT department) for feedback and approval before proceeding to the cost estimation phase.

Notes: The Next step should be Cost Estimation: you will be needed to Use the documented requirements to develop a detailed cost estimate for equipment, installation, and ongoing maintenance.

Points to Remember

- Determining the LAN installation requirements is a crucial step in ensuring a successful network setup. This process typically involves assessing various factors to meet both the technical and business needs of the organization.
- After completing a LAN installation site survey, the following tasks were undertaken to determine the necessary LAN installation requirements.
    - ✓ Analysis of site survey data
    - ✓ Identification of Specific Network and security Requirements
    - ✓ Equipment Specification and Selection
    - ✓ Documentation and Reporting

Application of learning 1.2.

MGS Grand Hotel, is a luxury hotel chain located at Muhanga District, a hotel is opening a new branch in the beautiful city of Gisenyi. To provide excellent service, the hotel needs a strong and dependable Local Area Network (LAN) to support their operations and give guests smooth Internet access.

A Hotel want to hire a network technician to analyze the situation and the survey report provided here above, and based on the analysis, determine and provide a list of required networking equipment (switches, routers, access points), cables, and other materials to facilitate a smoother installation process and ensure more accurate cost estimates.

The building overview and Site Survey Report are provided here below:

Building Overview:

- **Type:** Multi-story hotel building
- **Floors:** 7 floors
- **Key Areas:**
    - ✓ **Office Spaces:** Located on the 2nd and 3rd floors, these offices require high-speed wired connectivity for business operations.

- ✓ **Conference Rooms:** Situated on the 4th floor, these rooms need robust wireless connectivity to support meetings, presentations, and video conferences.
- ✓ **Guest Rooms:** Spanning the 5th to 7th floors, guest rooms require both wired and wireless access for personal devices and entertainment systems.
- ✓ **Lobby and Reception Area:** Requires strong wireless coverage to manage a high volume of guest devices and to support hotel operations.
- ✓ **Restaurant and Lounge:** Located on the ground floor, this area needs wireless access for guest convenience and mobile point-of-sale systems.

Site Survey Report: MGS Grand Hotel

1. Introduction

- **Objective:** This report documents the findings from the site survey conducted at MGS Grand Hotel, with the aim of preparing for the installation of a LAN that supports both wired and wireless connectivity across all key areas of the hotel.
- **Scope:** The survey covered all floors of the hotel, focusing on the office spaces, conference rooms, guest rooms, lobby, and common areas.

2. Building Layout and Infrastructure

- **Floor Overview:**
  - ✓ **Ground Floor:** Houses the lobby, reception, restaurant, and lounge. High-density wireless coverage is essential.
  - ✓ **2nd & 3rd Floors:** Dedicated office spaces requiring reliable wired connections for desktops, printers, and network-attached storage.
  - ✓ **4th Floor:** Contains conference rooms needing wireless connectivity for business events, as well as some wired connections for AV equipment.
  - ✓ **5th to 7th Floors:** Guest rooms require both wired and wireless options for personal and entertainment use.
- **Existing Infrastructure:**
  - ✓ **Cabling:** No existing cabling. New Ethernet and fiber optic cables will need to be installed throughout the building.
  - ✓ **Power:** Adequate power outlets are available, but additional power strips and possibly some new circuits may be required in the server room and conference areas.
  - ✓ **Cooling:** Adequate cooling exists in most areas, though the server room may require an additional cooling unit to maintain optimal temperatures.

3. Networking Requirements

- **Wired Connectivity:**
  - ✓ **Office Spaces:** Cat6 Ethernet cabling to all workstations, printers, and network devices. A dedicated network switch for each floor with sufficient ports.

- ✓ **Conference Rooms:** Wired connections for AV equipment, plus additional Ethernet ports for presenters.
- ✓ **Guest Rooms:** Ethernet ports near the desks in each room for wired Internet access.

- **Wireless Coverage:**
  - ✓ **Lobby and Reception:** High-density access points (APs) to handle a large number of simultaneous connections.
  - ✓ **Conference Rooms:** Enterprise-grade APs to ensure uninterrupted connectivity during meetings.
  - ✓ **Guest Rooms:** APs installed in hallways with careful planning to avoid interference and dead zones.
  - ✓ **Restaurant and Lounge:** Wireless access points that provide coverage throughout the area.

4. Environmental and Security Considerations

- **Interference:** Thick walls and reinforced concrete between floors may attenuate wireless signals. AP placement will be crucial, and signal boosters may be necessary in some areas.

- **Security:** Implementation of VLANs to separate guest traffic from office and management traffic. WPA3 encryption for wireless networks, along with a firewall and intrusion detection systems.

Indicative content 1.3: Designing LAN Topologies Diagram

Duration: 4 hrs

Theoretical Activity 1.3.1: Description criteria of selecting suitable network topology for network installation

Tasks:

1: Reflecting to the revision and ask question where is necessary.

2: Discuss and answer the following questions

a) Describe criteria of selecting suitable network topology for network installation.
b) Discuss about the activities involved in the network design phase.
c) Describe the result of the network design phase?

3: Write your answers on flipchart/paper.

4: Discuss on the provided answers and choose correct answers

5: Listen attentively, take notes and ask questions where is needed

6: Read the key reading 1.3.1 in the trainee's manual.

Key readings 1.3.1.:

1. Criteria to select a network topology suitable for network installation

After the site survey is completed and the network site survey report is created, the next logical step is to move into the network design phase.

The network design phase builds upon the findings from the site survey, translating them into a detailed blueprint for the network. This design will outline the layout, configuration, and specifications for the network infrastructure, including aspects such as network topology, equipment selection, cabling, and security measures.

When selecting a network topology for a LAN installation, several criteria should be considered to ensure that the chosen topology meets the network's performance, scalability, and reliability requirements. Selecting the right topology requires balancing these criteria based on the specific needs and constraints of the network environment.

Here are the key selection criteria:

- **Scalability**:
  - ✓ The chosen topology should easily accommodate future network growth. Consider how simple it is to add new devices or segments to the network without causing significant disruptions or requiring extensive reconfiguration.
- **Performance and Speed**:
  - ✓ The topology should support the required data transfer rates and ensure efficient traffic management. This includes considering factors like latency, bandwidth, and the potential for network congestion.
- **Reliability and Fault Tolerance**:
  - ✓ A reliable topology should have minimal downtime and offer redundancy to ensure continuous network availability in case of a device or connection failure. For example, a mesh topology provides multiple paths for data, reducing the risk of network failure.
- **Cost**:
  - ✓ The cost of implementing and maintaining the topology is a significant factor. This includes the initial setup cost, the cost of network devices, cabling, and any potential future upgrades. More complex topologies like mesh may offer higher reliability but are also more expensive to implement. A simple topology, like a star, might be easier to implement and manage than a more complex one, like a hybrid or mesh topology.
- **Security:**
  - ✓ The topology should support the network's security requirements, including the ability to control access to different parts of the network and protect data integrity. For instance, a star topology allows for central control and monitoring, which can enhance security.

- **Network Size and Layout**:
    - ✓ The physical layout of the network and the number of devices it needs to support play a crucial role. For example, a bus topology might be suitable for a small network in a single office, while a star topology could be better for a larger, multi-floor building.

Notes: Compatibility with Existing Infrastructure, is another crucial factor to consider in case there is an existing network. The chosen topology should be compatible with any existing network infrastructure or devices. This consideration helps in reducing the cost and complexity of integration.

Here are three scenarios with a suitable network topology chosen for each, along with the reasoning behind the choice:

Scenario 1: Small Office for a Startup

***Details**:*

- *A startup with a single office space housing 15 employees.*
- *The company is budget-conscious but plans to expand to 25 employees within a year.*
- *The network will primarily support internet access, file sharing, and VoIP communications.*
- *The office layout is simple, with all workstations in one open area.*

Chosen Topology**: **Star Topology

***Reasons**:*

- ***Scalability**: A star topology allows easy expansion as the company grows. New devices can be added to the central switch or hub without affecting the existing network.*
- ***Cost**: Star topology is cost-effective for a small office. It requires minimal cabling and the cost of a central switch is manageable.*
- ***Ease of Management**: With all devices connected to a central hub, the network is easy to monitor and troubleshoot, which is ideal for a small company without a dedicated IT team.*

- ***Performance**: The topology supports the required performance for internet access, file sharing, and VoIP by ensuring that data travels directly between devices and the central hub.*

Scenario 2: University Campus

***Details**:*

- *A university with multiple buildings, including administrative offices, classrooms, laboratories, and dormitories.*
- *The network needs to support thousands of devices, including computers, printers, and mobile devices.*
- *There are requirements for high-speed internet, internal data sharing, and robust security measures.*
- *The network must be reliable with minimal downtime, as it supports critical academic and administrative functions.*

Chosen Topology**: **Tree Topology

***Reasons**:*

- ***Scalability**: The tree topology is well-suited for a large campus environment. It can connect multiple star networks, allowing each building or floor to have its own star topology connected to a larger backbone network.*
- ***Network Layout**: The hierarchical structure of the tree topology mirrors the physical layout of the campus, making it easier to manage different segments of the network.*
- ***Reliability**: The topology offers a balance between cost and fault tolerance. If a segment fails, it doesn't necessarily bring down the entire network, especially if redundancy is built into critical parts of the hierarchy.*
- ***Security**: Different segments of the network can be isolated or secured independently, which is crucial for managing access across various departments with different security requirements.*

Scenario 3: School Campus with Administration Block, Garden, Classroom Block, and Computer Lab

***Details**:*

- *A school campus consists of an administration block, a classroom block with four classrooms, a computer lab, and an outdoor garden area.*

- *The network needs to support administrative tasks, classroom activities, and computer lab usage, including internet access, internal file sharing, and educational software.*
- *The computer lab requires high-speed connections for multiple devices, while the garden area has minimal connectivity needs (e.g., outdoor Wi-Fi for students).*
- *The school plans to expand its network in the future by adding more classrooms and possibly another lab.*

***Chosen Topology**: **Hybrid Topology (Star-Tree Combination):** The garden area might require a simple star topology for outdoor Wi-Fi, while (administration, classroom, and lab) uses a more structured tree topology.*

***Reasons**:*

- ***Scalability**: The hybrid topology, combining star and tree structures, allows the school to easily expand the network as more classrooms or labs are added. Each block (administration, classroom, and lab) can operate on its own star topology, connected to a central backbone.*
- ***Network Layout**: The tree structure connects the administration block, classroom block, and computer lab, reflecting the physical layout of the campus. Each classroom and the lab can operate on individual star networks, ensuring that each area has dedicated and efficient connectivity.*
- ***Performance**: The computer lab, which requires high bandwidth, can have a dedicated star topology within the hybrid design. This ensures that the lab has direct, high-speed connections to the central network without interference from other areas.*
- ***Cost and Flexibility**: The hybrid topology provides a cost-effective solution by using a combination of topologies that suit different areas of the school. For instance, the garden area might only require a simple star topology for outdoor Wi-Fi, while the classroom block uses a more structured tree topology.*

2. Activities involved in Network Design Phase

The network design phase is a critical step following the completion of the network site survey and the creation of the site survey report. This phase involves translating the insights

gathered during the site survey into a comprehensive network design that will guide the installation and configuration of the network. Here's a detailed breakdown of the activities typically involved in the network design phase:

- **Review and Analysis of Site Survey Data**
  - ✓ **Site Layout and Requirements:** Re-examine the site survey data, including floor plans, topography, and environmental factors, to ensure that the design will accommodate the physical characteristics of the site.
  - ✓ **Existing Infrastructure:** Analyze any existing network infrastructure that can be integrated into the new design, such as cabling, network devices, and power sources. Identify components that require upgrading or replacement.
- **Defining Network Objectives**
  - ✓ **User Needs and Application Requirements:** Based on user needs analysis, define the objectives for the network, such as supporting specific applications (e.g., video conferencing, VoIP), providing high-speed internet access, and Consider future growth and potential technology upgrades.
- **Designing the Network Topology**
  - ✓ **Topology Selection:** Choose the most suitable network topology based on the site layout, performance needs, and redundancy requirements. Common topologies include star, mesh, tree, or a hybrid approach.
  - ✓ **Logical and Physical Design:** Develop both the logical design (how data flows through the network) and the physical design (the physical placement of devices and cabling). This includes creating diagrams that illustrate the network's structure.
- **Device and Equipment Specification**
  - ✓ **Network Devices:** Specify the types and models of network devices required, such as routers, switches, wireless access points, and firewalls. Consider the need for high-availability features like load balancing and failover.
  - ✓ **Cabling and Media:** Determine the types of cabling and media (e.g., Cat6, Cat6a, fiber optic) needed based on distance, data rate, and environmental factors. Include structured cabling systems for better organization and scalability.

- ✓ **Power Requirements:** Assess the power needs for all network components, including PoE (Power over Ethernet) for devices like access points and IP cameras. Plan for backup power solutions like UPS (Uninterruptible Power Supply) systems.

- **Security Design**
  - ✓ **Physical Security:** Plan for the physical security of network equipment, particularly in areas accessible to unauthorized individuals. This may include secure mounting, locked cabinets, or tamper-proof enclosures.
  - ✓ **Network Segmentation:** Design the network to include segmentation, such as VLANs, to isolate different traffic types (e.g., guest Wi-Fi, internal communications) and enhance security.
  - ✓ **Access Control and Authentication:** Define the authentication and access control mechanisms, including secure Wi-Fi authentication (e.g., WPA3), role-based access control (RBAC), and integration with identity management systems.
- **Documentation and Design Validation**
  - ✓ **Network Design Documentation:** Create detailed documentation (Network Design Document) that outlines the entire network design, including diagrams, equipment lists, and configuration settings. This serves as a blueprint for installation and future maintenance.
  - ✓ **Stakeholder Review:** Present the design to stakeholders, such as the IT team, school administration, or management, for review and feedback. Make necessary adjustments based on their input.
  - ✓ **Validation:** Perform a design validation to ensure that the proposed network meets all requirements and objectives. This may involve simulations, proof-of-concept testing, or consulting with network specialists.

3. Result of the network design phase

The end result of the network design phase is a comprehensive **Network Design Document**. This document serves as the blueprint for the network installation and includes the following key elements:

- **Detailed Network Design Diagrams**

- ✓ **Logical Design:** Diagrams showing how data flows through the network, including the network topology (e.g., star, mesh) and the relationships between different network segments.
- ✓ **Physical Design:** Diagrams illustrating the physical placement of network devices (e.g., routers, switches, access points), cabling routes, and power sources within the site.

- **Equipment and Materials List**

  - ✓ **Device Specifications:** A list of all network devices needed, including types, models, and quantities of routers, switches, access points, firewalls, and other hardware.
  - ✓ **Cabling Requirements:** Specifications for the types and lengths of cables (e.g., Cat6, Cat6a, fiber optic) and any connectors or adapters required.
  - ✓ **Power Solutions:** Details on power requirements, including any PoE (Power over Ethernet) needs, UPS (Uninterruptible Power Supply) systems, and redundant power supplies.

- **Design Validation and Stakeholder Approval**

  - ✓ **Design Validation Results:** Any results from simulations, proof-of-concept testing, or consultations that validate the design's effectiveness in meeting the network's objectives.
  - ✓ **Stakeholder Feedback:** Documentation of any feedback from stakeholders (e.g., IT team, management) and any adjustments made to the design based on that feedback.

Practical Activity 1.3.2: Designing LAN Topology Diagram

Task:

1: Listen attentively as trainer explaining the differences between a topology diagram and a network diagram, take key notes and ask question where is necessary

2: Observe the image of one LAN topology shown by trainer and perform the following task:

a) Name type of topology illustrated from a picture?

b) Observe careful the physical structure of your computer lab, choose the best LAN topology that can match with its structure. Draw the best topology for your computer Lab/ shown image.

3: Follow attentively as trainer demonstrating how to design a network topology diagram and ask for clarification whenever necessary.

4: Individually carry out the Task 1.3.2.b by applying what you learned from the trainer's demonstration.

5: while working on activity ask for clarification and assistance whenever necessary.

6: Repeat the activity until the topology is fully completed

7: Perform the application of learning 1.3 as home work

Key readings 1.3.2

Network diagram:
One of the first things you should do before setting up a complex network is creating a network diagram so you'll know how everything will work together.

The diagram provides a visual representation of a network architecture.

Conversely, when a network doesn't work properly, this type of diagram can aid in pinpointing issues.

Difference between topology diagram from network diagram.
A **topology diagram** visually represents the arrangement and interconnections of different components within a network, illustrating how devices such as computers, routers, and switches are organized and communicate with each other.
In contrast, a **network diagram** provides a more detailed view that includes the physical or logical connections between devices, often incorporating elements like IP addresses, network protocols, and bandwidth information.

While topology diagram focuses on the physical layout and structure of the network, whether it's a star, mesh, bus, or ring topology, A network diagram combines both logical and physical topologies to provide a comprehensive view of how a network operates.

Network diagram can be created using specialized software or drawn by hand. The diagram shows the physical and logical connections between different devices and nodes in a network. The physical connections refer to the actual cables, switches, and routers that connect the devices. The logical connections refer to the way the data flows between the devices.

This training manual focused on designing network diagram instead of network topology, because

Importance of Network Diagrams

Network diagrams play a crucial role in designing and managing computer networks. They help network administrators to:

- Understand the network topology.
- Identify the location of different devices and nodes.
- Visualize the flow of data between different components of the network.
- Plan for future expansion.
- Troubleshoot network issues quickly.

The network diagram is an essential tool for network administrators, as it helps them to understand the network's structure, identify potential issues, and plan for future growth. By visualizing the network topology, network administrators can quickly identify bottlenecks and other issues that may be affecting network performance.

Without a network diagram, network administrators would have a difficult time managing and troubleshooting the network. The diagram provides a clear and concise overview of the network, making it easier to identify potential issues and plan for future growth.

Types of Network Diagrams

There are different types of network diagrams used for different purposes. The most common types of network diagrams are:

Physical Network Diagrams: Physical network diagrams show the physical connections between devices and nodes in a network. They include details such as the type of cable used, the length of the cable, and the location of the devices.

Logical Network Diagrams: Logical network diagrams show the logical connections between devices and nodes in a network. They include details such as IP addresses, subnets, and routing protocols.

Basic Components of a Network Diagram

Before drawing a network diagram, it's essential to understand the basic components of a network diagram.

Nodes and Devices

Nodes and devices refer to the various components of a network, such as routers, switches, hubs, servers, and workstations. These components are represented by different shapes in a network diagram.

Connections and Links

Connections and links refer to the physical or logical connections between different components of the network. These connections are represented by lines in a network diagram.

Network Topologies

Network topologies refer to the different ways in which nodes and devices in a network are connected. The most common network topologies are star, mesh, ring, and bus.

Steps to Draw a Network Diagram

Now that we understand the basic components of network diagrams, let's explore the steps to draw a network diagram.

Define the Scope and Purpose

The first step in drawing a network diagram is to define the scope and purpose of the diagram. What components of the network do you want to include in the diagram? What is the purpose of the diagram?

Gather Information and Data

Once you have defined the scope and purpose of the diagram, you need to gather information and data about the network components. You can use network discovery tools, such as NMAP and LANsurveyor, to collect information automatically.

Choose the Right Layout/topology

Choosing the right layout for the network diagram is essential. Different layouts work better for different network topologies. Some of the most common layouts are hierarchical, circular, and mesh.

Add Nodes and Devices

After choosing the layout, you can start adding nodes and devices to the diagram. Pick the right shapes and icons for each component of the network.

Connect Nodes with Links

Once you have added all the components, connect them with appropriate links and connections. Use different types of lines and arrows to represent different types of connections.

Label and Annotate the Diagram

Finally, label and annotate the diagram with relevant information, such as IP addresses, device names, and connection types. Use a professional font and size for all the text.

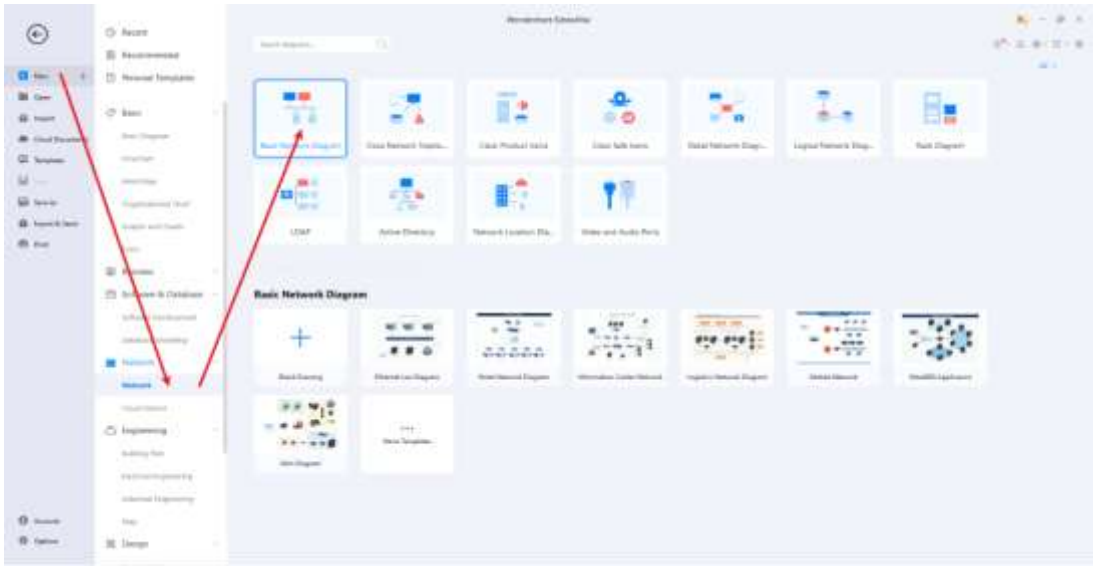
How to Draw a LAN Diagram in EdrawMax

EdrawMax is a simple, all-around diagram tool that allows you to create LAN network diagrams and other types of diagrams without stress. It contains symbols such as mainframe, terminal, cloud, firewall, comm-link, printer, switch, server, router, bridge, and hub. LAN network diagrams comprise symbols that make visualizing several types of LAN networks easier.

There are several ways to draw a LAN network diagram.

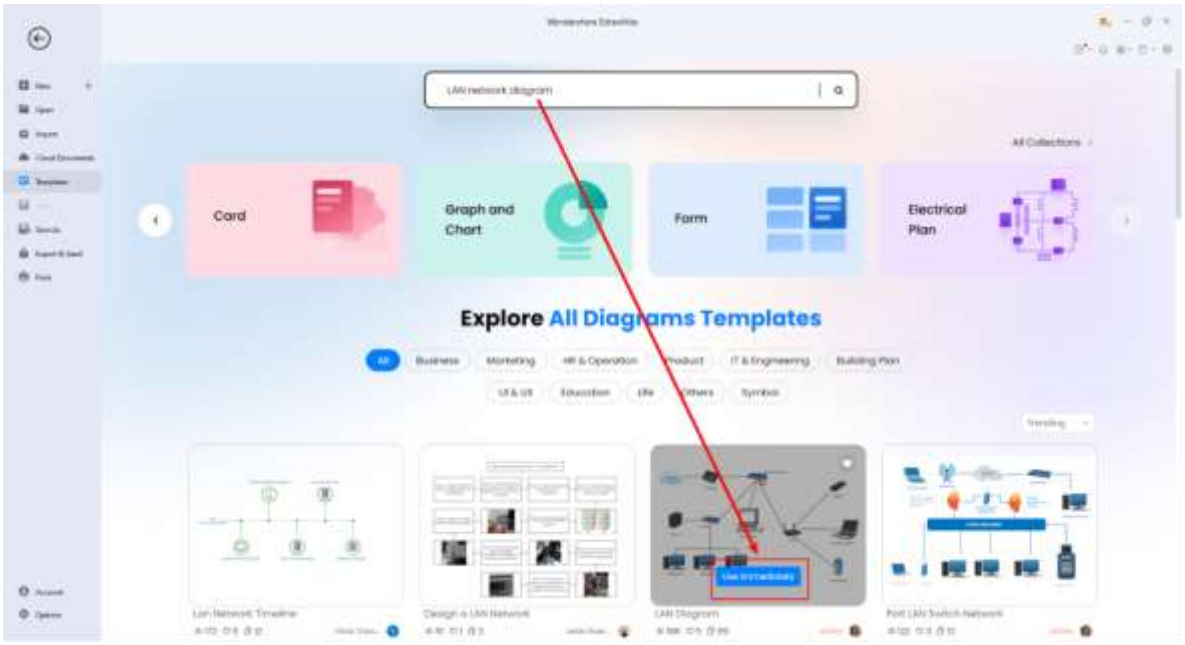
Step 1: Open EdrawMax and Login

The very first step that you need to follow is to install EdrawMax in your system. Go to EdrawMax Download and download the LAN network diagram software depending upon your operating system. If you need remote collaboration with your office team, head to EdrawMax Online and log in using your registered email address.



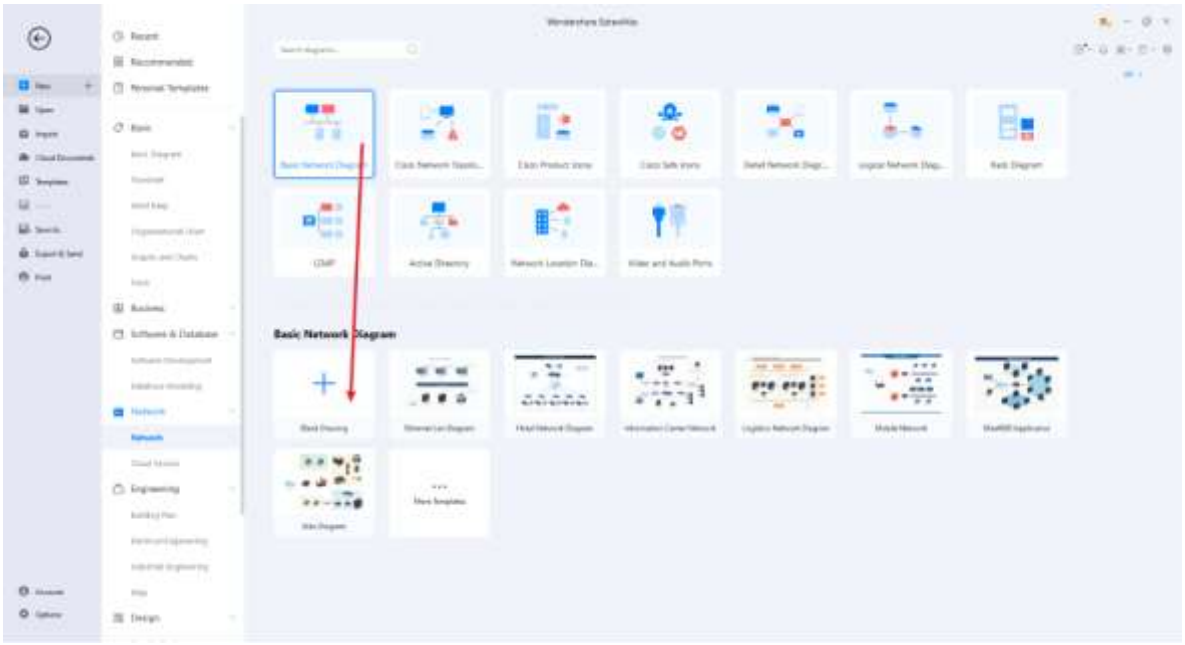
Step 2: Select a Template

After launching, the Home screen opens by default. Head to the Template bar and search for LAN Network Diagrams in the search box. Select the template you like and click Use Immediately to open it in a new window for customization.



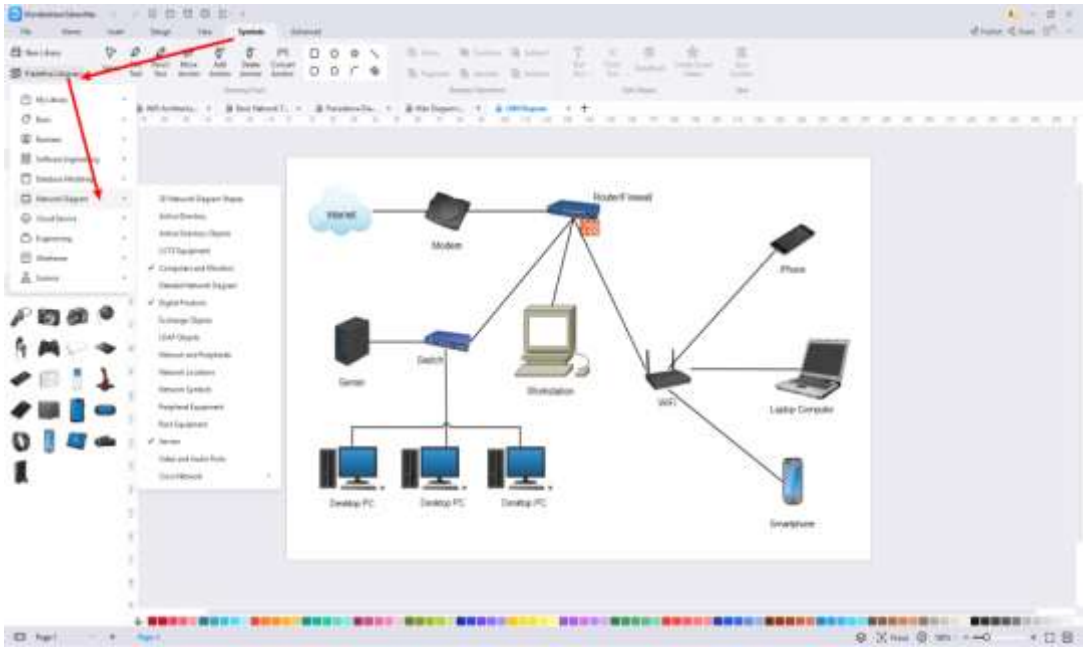
Step 3: Create From Scratch

From the EdrawMax homepage, you will find the '+' sign that takes you right to the canvas board, from where you can start designing the LAN network diagram from scratch. Coupled with your technical expertise, you can use a wide range of symbols to draw a detailed LAN network diagram.



Step 4: Select Symbols

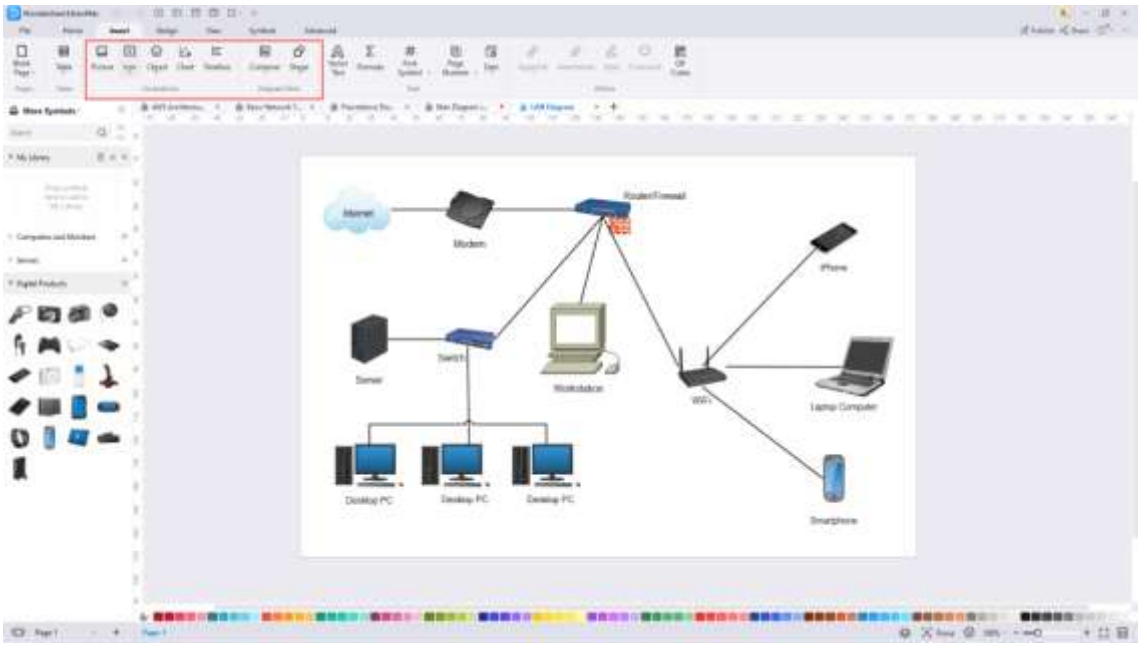
EdrawMax includes a large number of symbol libraries. If you can't locate the symbols you need, you can easily import some images/icons or build your own shape and save it as a symbol for later use. Simply go to the 'Symbols' part of EdrawMax and select the 'Predefined Symbol' section from the top toolbar. Hundreds of symbol categories are accessible for you to utilize and incorporate into your LAN network diagram.



Step 5: Add Components

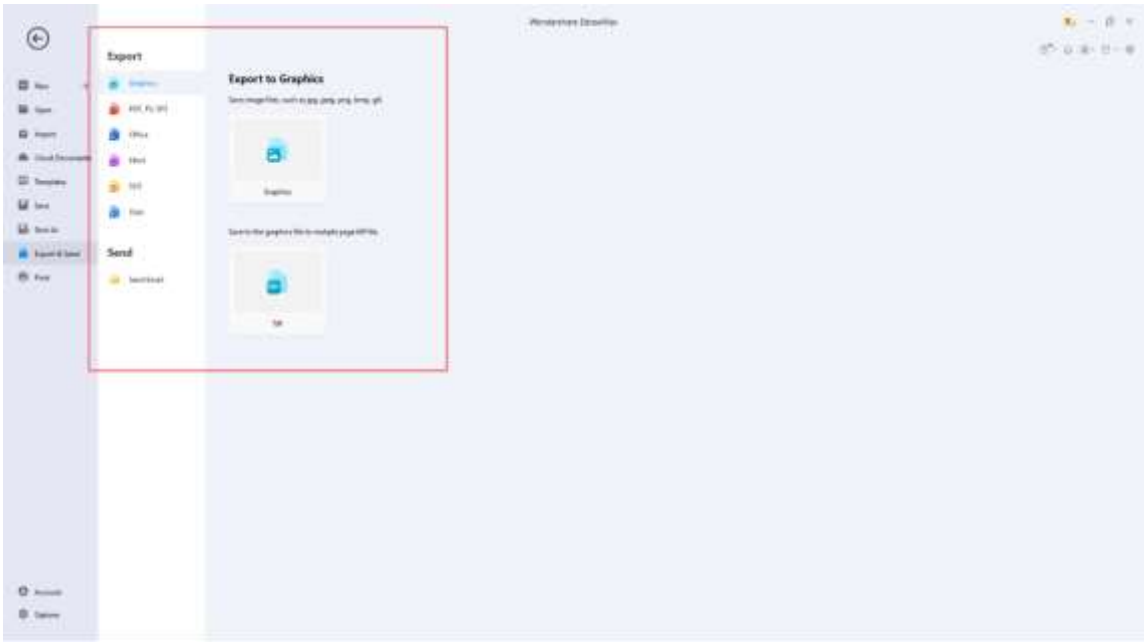
After you have sketched out the basic pieces, you may customize the typefaces, colors, and other details by selecting the right or top menu to make your LAN network design

more visually appealing.



Step 6: Finalizing the Plan

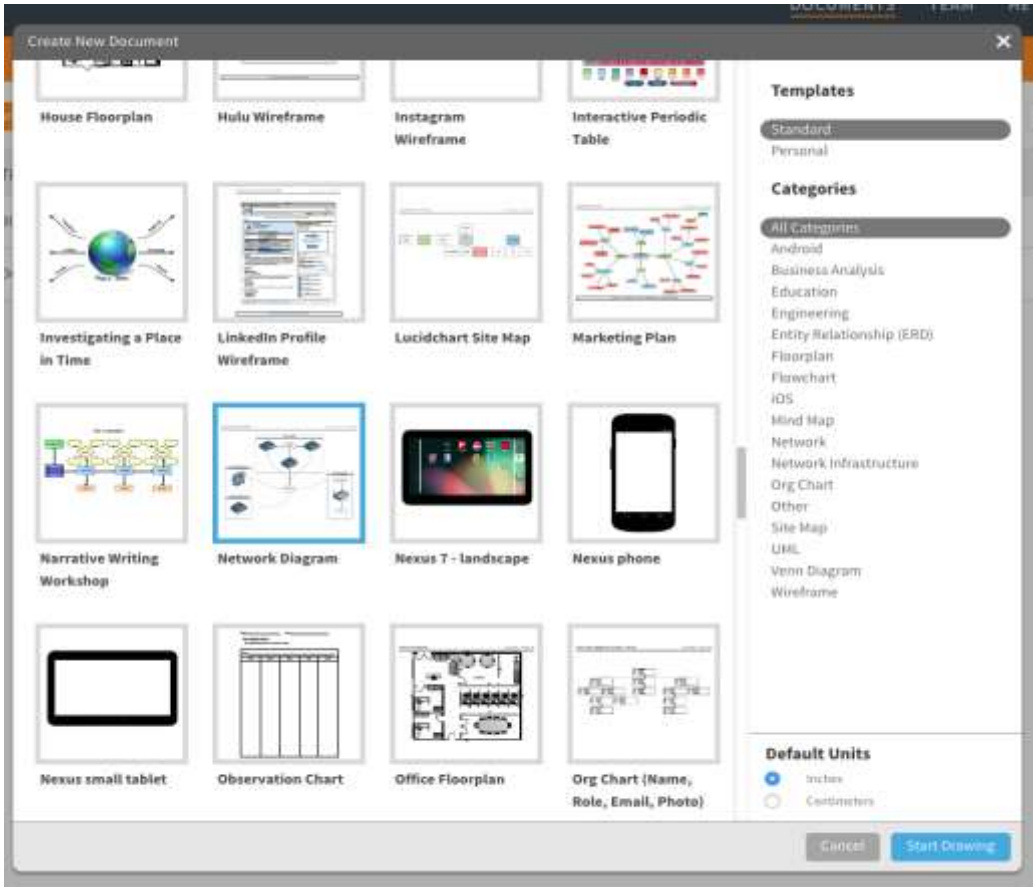
Once your LAN network diagram is ready, you can collaborate with your team to consider their opinion using the Cloud-base files. EdrawMax allows up to 100M free cloud storage. It is not a complicated process to create a LAN network diagram in EdrawMax. You can take a template and continue customizing it to suit whatever design you want.



Create a network diagram using LucidChart

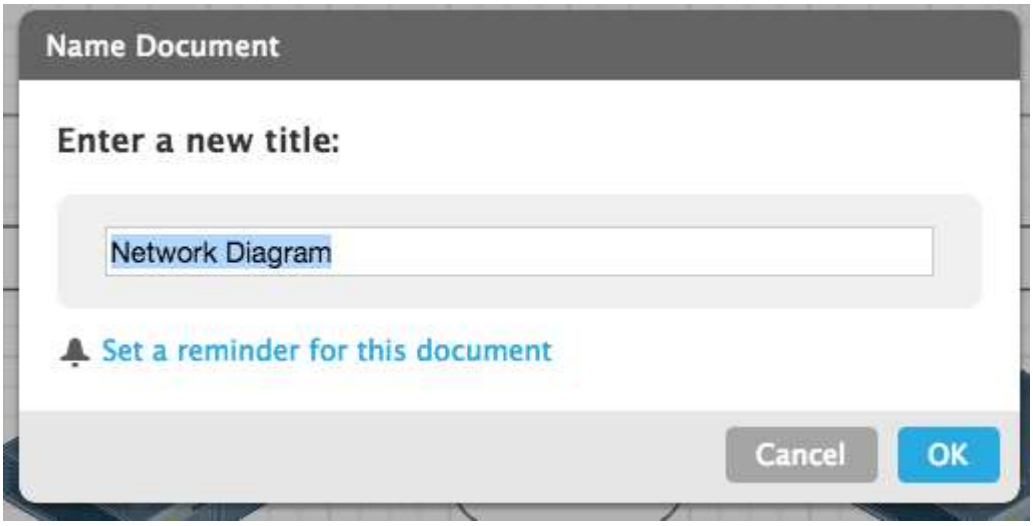
Step 1 Select a network diagram template

In the Documents section, click on the orange +Document button and double-click on the Network Diagram template.



2. Name the network diagram

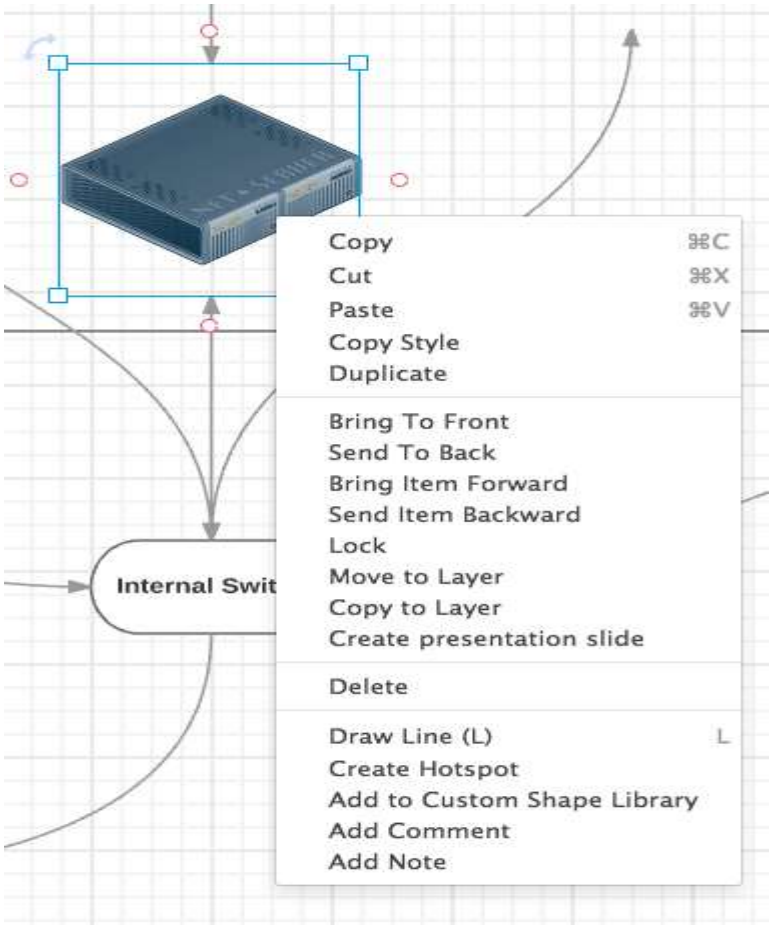
Click on the Network Diagram header in the top left corner of the screen. A pop-up screen opens, type the name of your diagram in the text box and click OK. The name of your network diagram appears in the top left corner of the screen.



3. Remove existing elements that you don't need on your diagram

A template is just a starting point, but if there are any elements on the network diagram template that you won't be using, remove them now. Click on the item and then right-click on the mouse. Menu options will appear on the screen, select Delete.

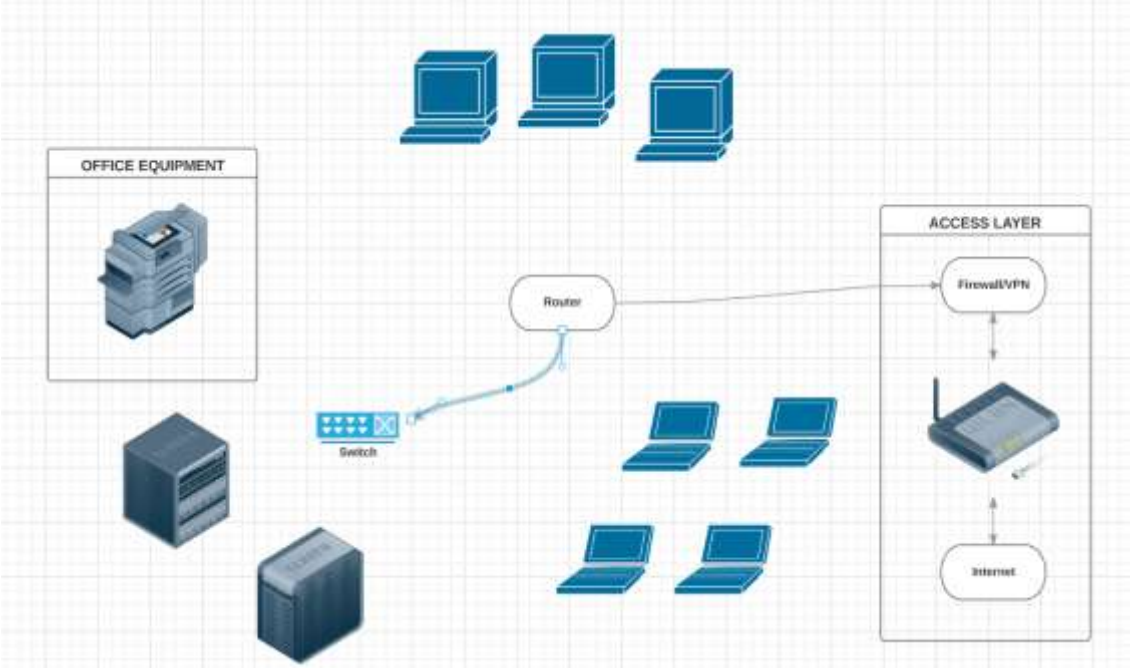
Tip: You can also hit the Delete button on your keyboard.



4. Add network components to the diagram

In the left column of the screen, you'll notice a plethora of computer-related icons. You can choose from our options, standard icons, Cisco (basic and extended), network, electronics, audio equipment, and Bing images. There are a lot of options, so you may want to enter the name of the network device you're looking for in the search box at the top of the left column. You can also scroll through the images/icons. When you see one you like, click on it and drag it to the screen.

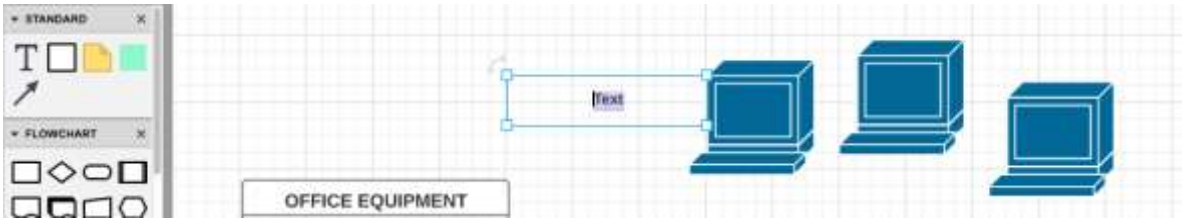
(Note: We've used a variety of icons/images to demonstrate all the options available. For consistency, you may want to use icons from the same set.)



5. Name the items in your network diagram

Before you start drawing network connections, let's name the items added to the diagram. As you can see, you can group entities by drawing squares around them. Here's how to add text and draw squares.

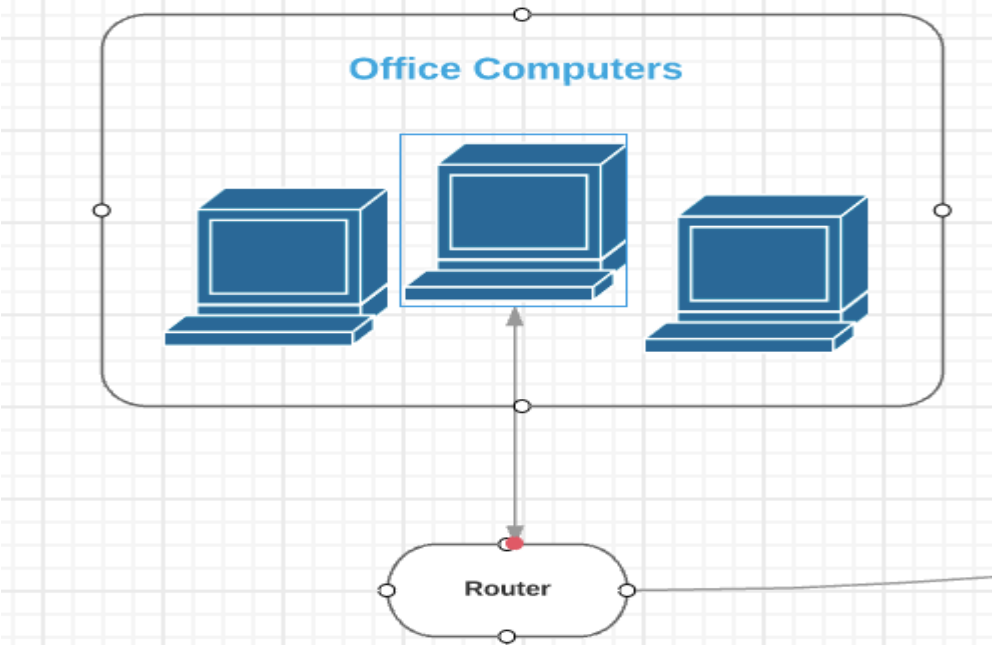
Add text: To add text to the diagram, scroll through the left column and look for the heading Standard (you'll see a T, a square, arrow, note, and a colored box). Click on the T and drag it to the place on the diagram where you want to add text. Type in the text and use the menu options for color, font, size, bold, etc. to customize it.



Group items using containers: In the left column, scroll to Containers. Choose the shape you want to draw around a group of items on the diagram, click on it and drag it to where you want it placed on the diagram. Click it to see the squares in the corners signaling that you can resize the box. Click a corner and drag it to make the container bigger or smaller. Use the background grid as a guide for alignment and sizing.

6. Draw connections between components

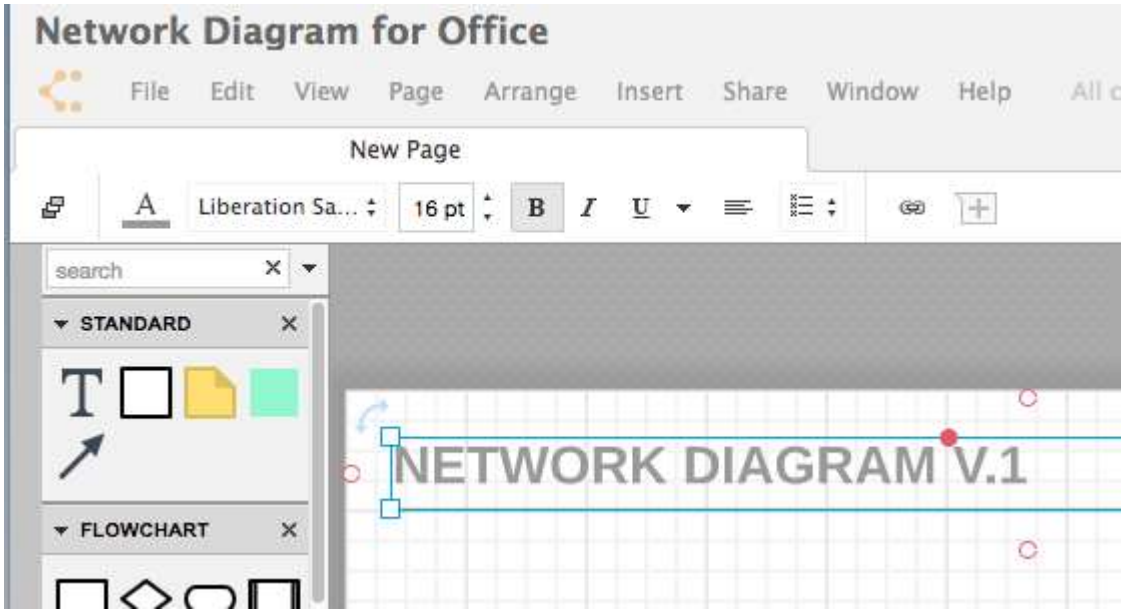
Double-click on any component and then click and hold one of the orange circles, and drag the line to the appropriate symbol. Continue to draw all the connections on the network diagram.



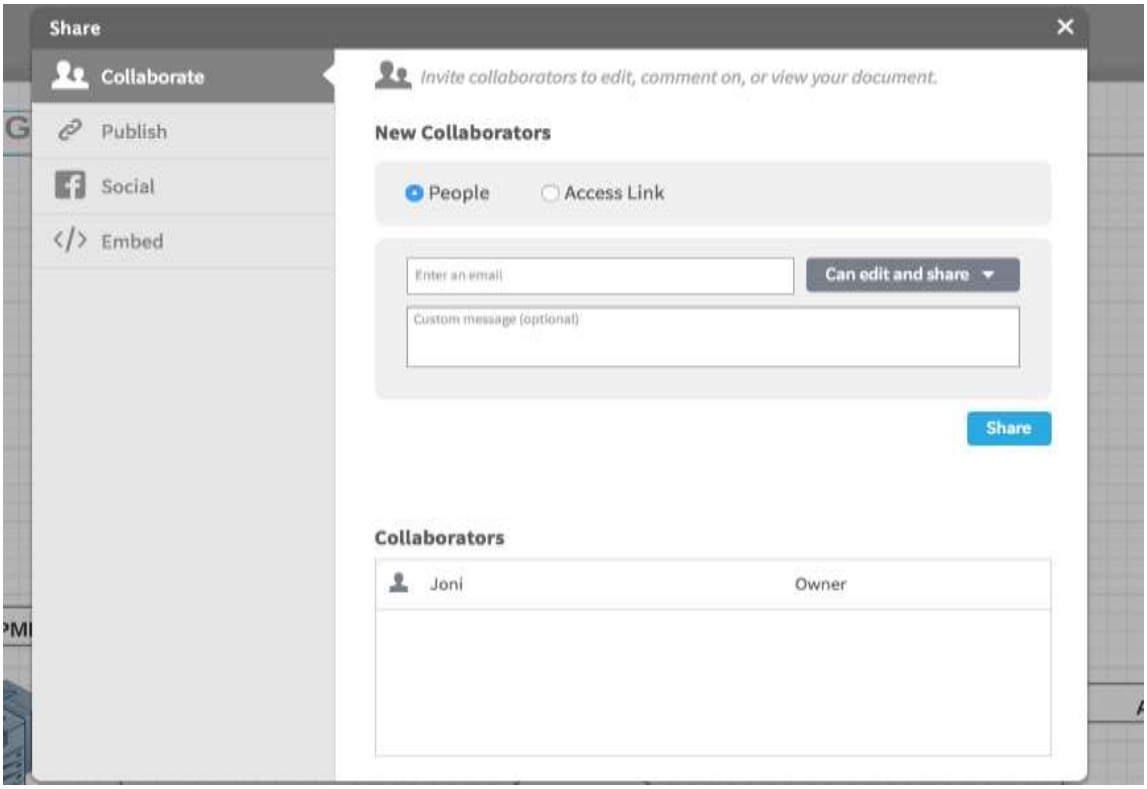
Tip: You can adjust the arrow style by clicking on it. Next, click the arrow icon in the menu bar and choose one of the two other styles. To change the style of all the arrows, choose Select All from the Edit menu and then click on the style you prefer.

7. Add a title and share your network diagram

The title at the top of your network diagram grid is the same as what you named the file. If you want to change the name on the actual diagram, double-click the diagram title and type in a new name. If you'd like to adjust the font and type size, use the shortcut keys in the menu bar at the top of the screen.



You can easily share your network diagram with others either via email, web link, social media (Facebook, Twitter, Google+, and LinkedIn), or embed it on a website. Click the blue Share button in the top right corner of the screen and a pop-up will appear. Choose how you'd like to share your diagram and enter the appropriate information.



When you add collaborators, you can give them permission to work on the diagram and have discussions with them using the chat feature (the yellow quote icon in the top right corner of the screen).

Points to Remember

- Factors Influencing Topology Design
  - ✓ **Scalability:** The ability to easily add or remove devices without disrupting the network is crucial. Star and mesh topologies generally offer better scalability.
  - ✓ **Cost:** The budget for cabling, switches, and other hardware can influence the choice of topology. Bus and star topologies are often less expensive to set up than mesh.
  - ✓ **Performance:** The expected load on the network and the types of applications being used can impact performance. For example, a star topology may handle high traffic better due to the central switching.
  - ✓ **Reliability:** The need for fault tolerance and redundancy can dictate the choice of topology. Mesh networks are highly reliable but require more resources.
  - ✓ **Ease of Installation and Maintenance:** Some topologies are easier to install and manage than others, which can be a significant consideration for organizations with limited IT resources.

Application of learning 1.3.

At Muhanga District is a small technology consulting firm named "MUHTCF company" that has recently moved into a new office space. The firm has 10 employees who primarily work on desktop computers and occasionally use laptops and mobile devices for meetings and remote work. The company relies heavily on digital collaboration, file sharing, and printing, making a reliable and efficient Local Area Network (LAN) essential for their operations.

The company needs Network Technician:

- ✓ Create a detailed network topology diagram that illustrates how devices will be connected
- ✓ Decide on the types of devices needed and their specifications based on performance requirements.
- ✓ Finally create document including network topology diagram, and needed devices with their specifications

Indicative content 1.4: Estimation of LAN Installation Cost.

Duration: 3 hrs

Theoretical Activity 1.4.1: Description LAN installation cost estimation

Tasks:

1: Follow trainer and ask questions for clarification if any.

2: Answer the following questions:

a) List advantages of making cost estimation before LAN installation.

b) What key documents are necessary for an accurate cost estimation of LAN installation?

3: Observe proforma invoice of items and define the use/role of proforma invoice in general and in cost estimation.

5: Check whether all LAN installation requirements are in proforma invoice/market survey.

6: Present your findings to trainer and ask for an assistance if any.

7: Read key readings 1.4.1 in trainees manual about Identifying needs for efficiently estimating LAN

Key readings 1.4.1.:

1. **LAN installation cost estimation** refers specifically to the expenses associated with the physical setup and deployment of a Local Area Network (LAN). This includes costs for hardware such as routers, switches, and cabling, as well as labor costs for technicians to install and configure the network.
2. **Advantages for estimating LAN installation cost before installation**

Making cost estimation before LAN installation offers several advantages:

- **Budget Planning:** It helps organizations allocate the right budget for the project, ensuring that funds are available for all necessary components and services.

- **Resource Allocation:** By understanding the costs involved, businesses can effectively allocate resources, including personnel and equipment, to avoid shortages or overages.
- **Avoiding Unexpected Expenses: A** detailed cost estimation can highlight potential hidden costs, allowing for better preparation and reducing the chances of unexpected financial burdens during installation.
- **Informed Decision-Making:** Accurate cost estimates enable stakeholders to make informed decisions regarding the scope of the project, including whether to proceed, scale back, or seek alternative solutions.
- **Vendor Negotiation:** With a clear understanding of costs, organizations can negotiate better deals with suppliers and service providers, potentially leading to cost savings.
- **Timeline Management:** Estimating costs can help in creating a realistic timeline for the project, ensuring that financial constraints do not lead to delays.
- **Risk Management:** Identifying potential financial risks upfront allows for the development of mitigation strategies, leading to smoother project execution.

3. Essential documents you should avail for Cost estimation

To achieve an accurate LAN installation cost estimation, several key documents are needed:

- **Network Design Document:** This outlines the proposed layout of the LAN, including device locations, cabling routes, and the overall architecture (e.g., star, mesh).
- **Equipment List:** A detailed list of all required hardware, such as routers, switches, access points, and cables, along with specifications for each item.
- **Site Survey Report:** Insights from a physical assessment of the installation site, including existing infrastructure, potential obstacles, and environmental considerations.
- **Labor Cost Estimates:** Documentation that includes labor rates for technicians and engineers involved in the installation and configuration processes.
- **Project Scope Document:** A clear definition of the project scope, detailing the specific tasks and deliverables expected during the installation.

- **Vendor Quotes:** Price estimates from suppliers for equipment, materials, and any third-party services required for the installation.
- **Maintenance and Support Agreements:** Any existing or proposed agreements that outline ongoing support costs, which can impact overall budget considerations.
- **Timeline and Milestones:** A project timeline that includes key milestones and deadlines, helping to align costs with the expected duration of the installation.

Steps for cost Estimation

1. **Define Network Requirements**:
    - ✓ List network devices and their specifications.
    - ✓ Determine the number of users and devices per area.
2. **Plan the Network Layout**:
    - ✓ Revise a network diagram showing the physical and logical layout.
    - ✓ Identify key network segments and device placements.
3. **Gather Quotes**:
    - ✓ Request quotes from vendors for hardware and software.
    - ✓ Compare prices and select cost-effective options.
4. **Calculate Total Costs**:
    - ✓ Sum up hardware, software, labor, and other components.
    - ✓ Include a contingency budget.
5. **Review and Adjust**:
    - ✓ Review estimates with stakeholders and adjust based on feedback.
    - ✓ Ensure estimates meet technical requirements and budget constraints.

Example Cost Breakdown

1. **Cabling**:
    - ✓ Cat6 cable: $0.20 per foot
    - ✓ Total length required: 1000 feet
    - ✓ Cost: $200
2. **Switches**:
    - ✓ Managed switch (24 ports): $300 each

- ✓ Number of switches: 2
- ✓ Cost: $600

3. **Routers**:
   - ✓ Router: $150 each
   - ✓ Number of routers: 1
   - ✓ Cost: $150
4. **Access Points**:
   - ✓ Access point: $100 each
   - ✓ Number of access points: 4
   - ✓ Cost: $400
5. **Labor**:
   - ✓ Installation: $75 per hour
   - ✓ Number of hours: 20
   - ✓ Cost: $1500
6. **Network Management Software**:
   - ✓ Software: $500
   - ✓ Licensing: $100 per year
   - ✓ Initial Cost: $500

Total Estimated Cost

- Equipment: $200 (Cabling) + $600 (Switches) + $150 (Router) + $400 (Access Points) = $1350
- Labor: $1500
- Software: $500
- **Total Initial Cost**: $3350

Practical Activity 1.4.2: Estimating LAN installation cost

Task:

1: Follow demonstration of how to make cost estimation using Microsoft Office (Word/excel) and as questions where is possible.
2: Individually do the following task:

By using site survey report that have been completed in Practical Activity 1.2.2. As a network technician make a LAN installation cost estimation for your school.

3: Read a copy of proforma invoice of the needed items provided by trainer

4: Read copy of requirements document that you have prepared at Practical Activity 1.2.2

5: By using MS Office (Excel, word), Draft cost estimation basing on instructions given at **step 2** of **Practical activity 1.4.2.**

6: Presentation your work to trainer and ask question if any.

7: Repeat the task until a perfect cost estimation is achieved.

8: Submit Cost Estimate Report/Cost Estimation Document to the trainer

9: Read key readings 1.4.2 in trainees manual for further understanding.

Key readings 1.4.2

Estimating LAN installation cost

To estimate the cost of a LAN (Local Area Network) installation, several factors need to be considered. Here are the primary components and steps to estimate the cost:

1. **Site Survey and Planning**:
   - ✓ Conduct a site survey to determine the layout and requirements.
   - ✓ Create a detailed plan including the number of workstations, servers, switches, routers, and other network devices.
2. **Equipment Costs**:
   - ✓ **Cabling**: Cost of Ethernet cables (Cat5e, Cat6, or Cat7).

- ✓ **Switches**: Managed or unmanaged switches depending on the network size and requirements.
- ✓ **Routers**: Based on the network size and internet connection type.
- ✓ **Access Points**: For wireless LANs (WLANs).
- ✓ **Network Interface Cards (NICs)**: For devices without built-in network capability.
- ✓ **Patch Panels and Racks**: For organizing and managing cables.
- ✓ **Other Hardware**: Firewalls, power supplies, backup systems, etc.

3. **Labor Costs**:
   - ✓ **Installation**: Charges for technicians to install and configure the network.
   - ✓ **Testing and Troubleshooting**: Ensuring everything is working correctly.
   - ✓ **Maintenance and Support**: Ongoing costs for network support and troubleshooting.
4. **Software and Licensing**:
   - ✓ **Network Management Software**: For monitoring and managing the network.
   - ✓ **Licensing Fees**: For software and hardware that require licenses.
5. **Additional Costs**:
   - ✓ **Upgrades**: Future-proofing by planning for upgrades.
   - ✓ **Training**: Training staff to use and maintain the network.

Example Cost Breakdown

1. **Cabling**:
   - ✓ Cat6 cable: $0.20 per foot

- ✓ Total length required: 1000 feet
- ✓ Cost: $200

2. **Switches**:
   - ✓ Managed switch (24 ports): $300 each
   - ✓ Number of switches: 2
   - ✓ Cost: $600
3. **Routers**:
   - ✓ Router: $150 each
   - ✓ Number of routers: 1
   - ✓ Cost: $150
4. **Access Points**:
   - ✓ Access point: $100 each
   - ✓ Number of access points: 4
   - ✓ Cost: $400
5. **Labor**:
   - ✓ Installation: $75 per hour
   - ✓ Number of hours: 20
   - ✓ Cost: $1500
6. **Network Management Software**:
   - ✓ Software: $500
   - ✓ Licensing: $100 per year
   - ✓ Initial Cost: $500

Total Estimated Cost

- Equipment: $200 (Cabling) + $600 (Switches) + $150 (Router) + $400 (Access Points) = $1350
- Labor: $1500
- Software: $500
- **Total Initial Cost**: $3350

This is a simplified example. The actual cost can vary significantly based on the size and complexity of the network, local labor rates, and specific requirements. Always get detailed quotes from suppliers and contractors before proceeding.

Points to Remember

Steps to Follow for Estimation

1. **Define Network Requirements**:
   - ✓ List all the network devices and their specifications.
   - ✓ Determine the number of users and devices per area.
2. **Plan the Network Layout**:
   - ✓ Create a network diagram showing the physical and logical layout.
   - ✓ Identify key network segments and the placement of switches, routers, and access points.
3. **Gather Quotes and Prices**:
   - ✓ Request quotes from vendors for the required hardware and software.
   - ✓ Compare prices and select the most cost-effective options.
4. **Calculate Total Costs**:
   - ✓ Sum up the costs of hardware, software, labor, and other components.
   - ✓ Include a contingency budget for unexpected expenses.
5. **Review and Adjust**:
   - ✓ Review the estimate with stakeholders and adjust based on feedback.
   - ✓ Ensure the estimate meets both the technical requirements and budget constraints.

Application of learning 1.4.

LAN Installation Cost Estimation for MUGISHA Grand Hotel

With the network design phase completed for MUGISHA Grand Hotel, the next step involves estimating the costs associated with the installation of the Local Area Network (LAN). This cost estimation covers all essential components, including networking equipment, cabling, labor, and additional resources necessary to implement the designed network across the hotel's seven floors.

The hotel wants to hire a network technician:

To prepare cost estimation for their proposed LAN.

Learning outcome 1 end assessment

Written assessment

PART I: Choose the correct answers

Question 1

Which of the following is NOT a common network topology?

A. Star **B.** Ring **C.** Bus **D.** Cloud

Question 2

What device connects multiple devices within a network?

A. Router **B.** Switch **C.** Hub **D.** Modem

Question 3

The physical arrangement of network devices and cables is referred to as:

A. Network topology **B.** IP addressing **C.** Network layout **D.** Cabling infrastructure

PART II: Answer by true for correct statement and False for incorrect statement

i. A router is used to connect multiple devices within the same network.
ii. A star topology is the most common network topology.
iii. A hub is a more efficient network device than a switch
iv. Ethernet cables are used for wired network connections.
v. IP addresses are assigned to identify devices on a network.
vi. A firewall is a hardware or software device that protects a network from unauthorized access.
vii. A network interface card (NIC) is a hardware component that enables a device to connect to a network.
viii. A bus topology is more reliable than a star topology.
ix. Power over Ethernet (PoE) allows for the transmission of data and power over a single cable.
x. Wireless networks are always less secure than wired networks.

Practical assessment

GTech is a growing software development company located in GASABO District. The company's daily activities include software development, online meetings, and large file transfers.

Employees frequently encounter slow internet speeds, dropped connections during video conferences, and difficulty accessing shared files on the server.

To address these challenges and support their anticipated growth, GTech decided to invest in a properly planned and designed LAN for their office space.

As Network Technician, you have been hired by the company to plan and design a Local Area Network (LAN) for the office space.

Upon completing the planning and design phase, you will present the network design and Estimation of LAN installation costs to Company management Team. You will also provide detailed documentation to ensure smooth implementation and maintenance of the network.

END

References

1. Ashikuzzaman.Md. (December 28, 2023). Components of Local Area Network (LAN). LIS Education Network, page 3. https://www.lisedunetwork.com/components-of-local-area-network-lan/
2. Geeksforgeeks .Types-of-network-topology. (06 Sep, 2024). geeksforgeeks, Page 1.
3. https://www.geeksforgeeks.org/types-of-network-topology/
4. Inc., L. S. (2024). How to Draw a Network Diagram. *lucidchart*, Page 1-3. https://www.lucidchart.com/pages/network-diagram/how-to-draw-a-network-diagram
5. Paradigm, V. (2024). How to Create Network Diagram?https://www.visual-paradigm.com/tutorials/how-to-create-network-diagram/. *visual-paradigm-tutorials*, Page 1-2. https://www.visual-paradigm.com/tutorials/how-to-create-network-diagram/

Indicative contents
2.1. Identification of materials, Tools and equipment.
2.2·Trunking of LAN Cables
2.3 Mounting of LAN Equipment
2.4 Connecting LAN Devices

Key Competencies for Learning Outcome 2: Perform cabling

Knowledge	Skills	Attitudes
• Description of Materials and equipment used in LAN installation • Identification of the best routes of cables • Description of the mounting safety	• Selecting the right Material, tool and equipment for LAN installation • Mounting LAN equipment • Network labelling • Cable terminating • Cable patching	• Being Self-motivated • Being Detail-oriented • Having spirit of Creativity • Having Accountability

Duration: 15 hrs

Learning outcome 2 objectives:

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

1. Select properly tools, materials and equipment based on LAN requirements
2. Conduct appropriately piping (Trunking) according to LAN Design
3. Mount properly the LAN equipment basing on LAN design.
4. Connect properly LAN devices basing on LAN design

Resources

Equipment	Tools	Materials
• Brackets • Patch panel • Switch • Router • PPE • Rack Mount	• Glue gun • Networking Toolkit • Drilling Tools • Fixing Tool • Pliers • Crimping tool • Cable tester • Cable trunking tools	• Network cables (cat 6) • Connectors (RJ45) • Cables Ties • Cables clips • Pipes • Cable segregation strips (Separators) • Cable trunks

Indicative content 2.1: Identification of Materials, Tools and Equipment of Physical LAN installation

Duration: 3 hrs

Theoretical Activity 2.1.1: Description Materials, Tools and Equipment for physical LAN installation

Tasks:

1: Provide answers to the following questions.

1. Define the term cabling in context of Networking
2. Differentiate the following three terms tool, material and equipment as used in networking.
3. Describe essential tools, materials and equipment needed in LAN installation.

2: Present your findings to the whole class.

3: Ask any clarifications to the trainer

4: Read key readings 2.1.1 in Trainee's manuals.

Key readings 2.1.1.:

1. Network Cabling

Cabling refers to the physical medium that connects devices in a network, enabling communication between them. It involves the installation of cables and related hardware to create a network infrastructure that facilitates the transmission of data, voice, and video signals.

2. Difference between the term tool, material and equipment.

In the context of Information and Communication Technology (ICT), the terms "tool," "material," and "equipment" have distinct meanings:

- **Tool:** A tool is a handheld device or software application that used to perform the specific task or function.

Examples:

- ✓ **Physical:** Screwdrivers, crimping tools, cable testers.
- ✓ **Software:** Network analyzers, diagnostic utilities, code editors.

- **Material:** Materials are the consumable items or substances used in the creation, maintenance, or operation of ICT systems.

Examples:

- ✓ **Physical:** Cables, connectors, thermal paste, solder.
- ✓ **Digital:** Data files, software code, digital certificates.

- **Equipment:** Equipment refers to larger, often more complex devices or machinery that are used to perform specific ICT functions or tasks.

Examples:

- ✓ **Physical:** Servers, routers, switches, computers.
- ✓ **Infrastructure:** Racks, cooling systems, power supplies.

3. Essential tools, materials and equipment needed during network installation

When undertaking a network installation, having the right tools, materials, and equipment is crucial for ensuring a successful, efficient, and reliable network setup.

Below is a detailed overview of the essential tools, materials, and equipment needed for network installation.

- **Tools**
  - ✓ **Cutting tool (Wire cutters and Utility Knives)**

Cutting tools are essential for preparing network cables by cutting them to the desired length. These tools ensure clean cuts without damaging the internal wires.

- **Cable Cutters:** Specially designed to cut through network cables cleanly without damaging the internal conductors. They are used to cut cables such as twisted pair (Cat5e, Cat6) and coaxial cables.
- **Utility Knives:** Used for precision cutting of cable jackets, removing excess material from around the connectors, or cutting through other materials like cable sheathing.

✓ **Stripping tools**

Wire Strippers: Used to strip the insulation from network cables without damaging the internal conductors. This tool is critical for preparing cables for termination.

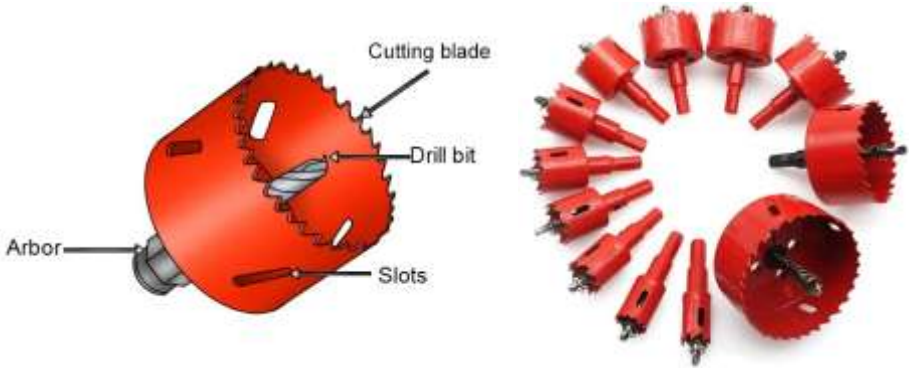
✓ **Drilling Tools**

Drilling tools are used to create holes in walls, floors, or ceilings for running cables or installing network hardware like wall plates and access points

- **Electric Drills:** Corded or cordless electric drills are used to create holes in various materials such as drywall, wood, and concrete for running network cables or mounting equipment.

- **Drill Bits:** Specialized hard electric drill bits, such as spade bits or masonry bits, are used depending on the material being drilled.

- For network installations, hole saw bits are often used to create larger openings for cables and conduits.



✓ **Punching tool**

A **punch down tool** is used for inserting wire into insulation-displacement connectors on punch down blocks, patch panels, Keystone jack, and surface mount boxes.

✓ **Crimping tools**

Crimping tools are devices used to crimp, or squeeze, connectors onto the ends of wires or cables.

✓ **Testing tools**

Testing tools are used to verify the integrity and performance of network cables and connections. They help identify any faults, incorrect wiring, or signal loss, ensuring that the network is installed correctly and functions reliably.

- **Cable Testers:** Used to test the continuity, wiring configuration, and signal strength of network cables. They can detect open circuits, shorts, miswiring, and split pairs, ensuring that the cables are correctly terminated and free from faults.

- **Network Analysers:** Advanced tools that test the performance of the network, including speed, signal strength, and data transfer rates. They can diagnose issues such as latency, packet loss, and network congestion.



- Tone Generators and Probes: Used to trace and identify cables within a bundle or across different locations, helping technicians locate specific cables quickly during installation or troubleshooting

- **Materials**
  - ✓ **LAN Cables**

A network cable is a physical medium used to connect and transmit data between computers, servers, routers, switches, and other network devices within a computer network.

Types of Network cable

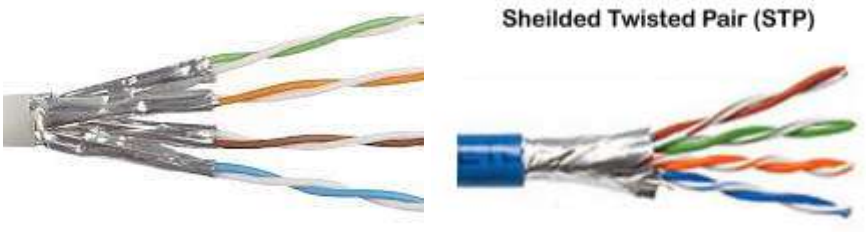
There are several types of LAN cables, each suited for different networking needs and environments:

- Twisted pair cable
- Coaxial cable
- Fiber Optic cable

A. **Twisted pair or Copper twisted pair**: The most common type of LAN cable used today, especially for Ethernet networks. Twisted pair cables consist of pairs of insulated copper wires twisted together to reduce electromagnetic interference. Commonly used for Ethernet networking to connect computers, switches, and routers.

The two main types of twisted pair cables are:

- **Shielded Twisted Pair (STP):** A twisted pair cable with an additional shielding layer to protect against electromagnetic interference. STP cables are used in environments with high interference or where higher data integrity is required.



- **Unshielded Twisted Pair (UTP):** The most commonly used twisted pair cable, typically seen in Cat5e, Cat6, and Cat6a cables. UTP cables are used for Ethernet connections and are suitable for most standard network se

The twisted-pair Ethernet cable comes in different categories including:

Cat5e cable, Cat6 cable, Cat6a cable, Cat7 cable and Cat8 cable

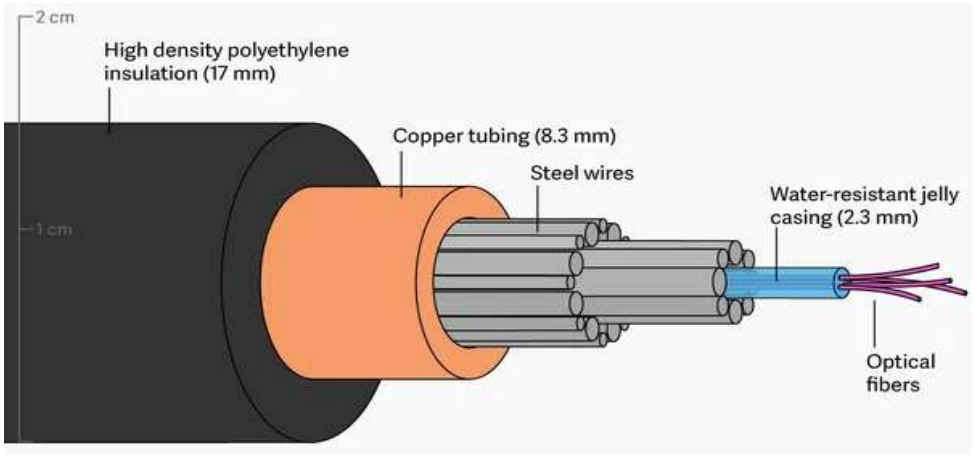
Notes: Cat6 and Cat6a cables are capable of higher data transfer rates than Cat5e.

B. **Coaxial cable**

Coaxial cables are an older type of LAN cable that consists of a central conductor, insulating layer, metallic shield, and outer insulating layer.

Nowadays it used for cable television, internet connections, and some types of network installations.

C. **Fiber optic cables** are faster and more efficient at transmitting network signals. Consist of thin strands of glass or plastic fibers that transmit data as light signals. These cables are faster, more reliable, and carry larger bandwidth than the copper wire can handle. Used for high-speed and long-distance data transmission, often in backbone networks and data centers. All those makes fiber optic cables to be generally more expensive than traditional Ethernet cables.



D. **Management cable**

A management cable, also known as a console cable or rollover cable, is a specific type of cable used to connect a computer to the console port of a network device, such as a router, switch, or firewall.

This connection allows for direct management and configuration of the device, typically through a terminal emulation program. Management cables are essential for network administrators to set up/configure, monitor and troubleshoot network device.

These cables are commonly used in data centers, server rooms, and other IT environments where multiple devices need to be controlled and configured centrally.

There are different types of management cables based on the connector types used. Here are some common types:

- **RS-232 Serial Cable:**

  Connector Types: DB9 (9-pin D-sub) or DB25 (25-pin D-sub) connectors on one end, RJ-45 connector on the other end.

- **USB to Serial Cable:**

  Connector Types: USB Type-A connector on one end, DB9 or DB25 connector on the other end, RJ-45 connector might be present in some models for networking devices.

- **USB to RJ-45 Console Cable:**

  Connector Types: USB Type-A connector on one end, RJ-45 connector on the other end.

- **Ethernet to Serial Console Cable:**

  Connector Types: RJ-45 connector on both ends, with built-in serial-to-Ethernet conversion.

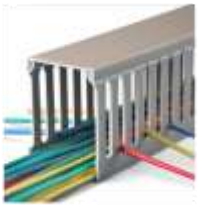
- **Ethernet to USB Console Cable:**

  Connector Types: RJ-45 connector on one end, USB Type-A connector on the other end.

✓ **Trunking**

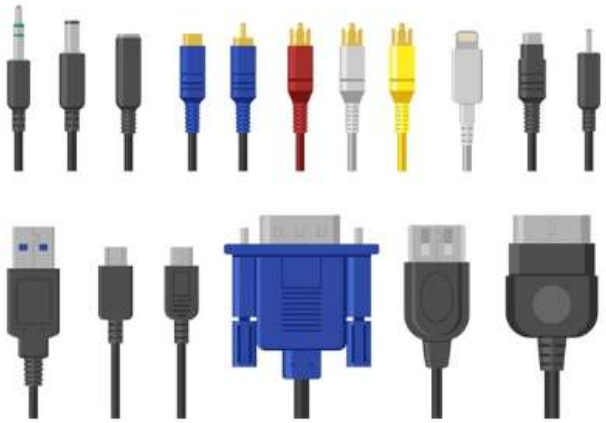
In cable management, trunking refers to enclosed pathways or conduits used to organize, protect, and manage cables. These pathways are often called trunking channels.

The purpose of cables trunking is to keeps cables organized, reduces physical damage, and enhances the aesthetic and safety of the installation environment.



✓ **A cable connector**

Connector is the component that you attach to the end of a cable so that it can plug into a port or an interface a device. Including USB connector, Ethernet connector etc.



✓ **Cable Ties**

Cable ties, also known as zip ties or wire ties, are versatile fastening devices used for bundling and organizing wires, cables, and other objects.

✓ **Cable clips**

A cable clip is a device that manages wires and cables and secures them to a fixed point on a surface, like a wall, ceiling or floor.

- ✓ **Cable Sockets**

Cable Socket is typically a wall-mounted or surface-mounted device with multiple ports designed for Ethernet cables. The types of network sockets based on their installation method and physical placement like **Wall plugs/wall plates and surface mount socket**

- ✓ **Cable coupler:**

Cable Coupler is a small, portable device used to connect two Ethernet cables together, effectively extending the length of the cables.

- ✓ **Nails**

Nails in networking used in cable mounting by fixing cable clips or wall plugs

- ✓ **Junction boxes**

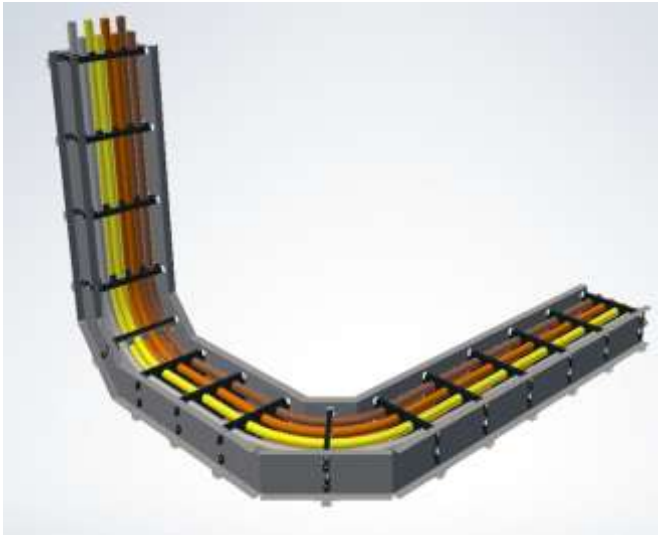
Junction box is for joining two Ethernet CAT5E cables with each other without any usage of couplers and connectors.

- ✓ **Elbow or Tee**

In the context of network cabling, "elbow" and "tee" can refer to types of cable management accessories used to route and organize cables.

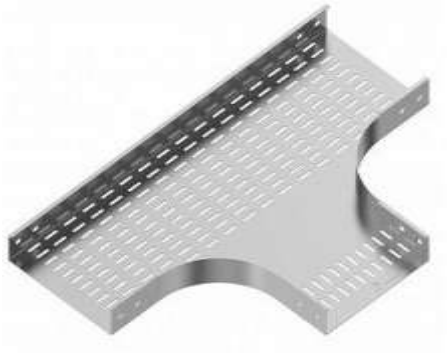
- **Elbow**

This is used to guide network cables around corners or bends. It helps to maintain the proper bend radius and prevent damage to the cables, ensuring that the signal integrity is maintained.



- **Tee**

This accessory is used to split a bundle of cables into two separate directions. It's useful when you need to branch off cables to different locations while keeping them organized and protected.



✓ **Insulating tape**

Insulating tape used to insulate electrical wires and other materials that conduct electricity. Insulating tape offers even more advantages. After a cable has been stripped, an insulating tape protects the stripped part of the cable.

Insulating tape is also a suitable solution when cables need to be bundled.



- **Equipment**

LAN equipment, refers to the various devices and components that are required to establish and maintain a functional network. The choice of LAN equipment depends on the specific requirements of the network, including size, scale, intended use, and security needs.

LAN equipment typically includes the following categories:

✓ **Interconnecting Devices**

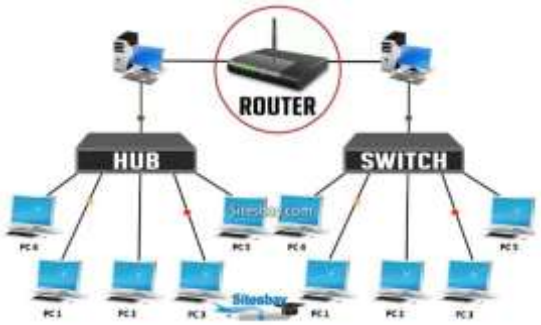
These devices involve in connecting different segments of a LAN and ensuring smooth communication between devices.

- **Switches**: These are the backbone of a LAN. Switches connect multiple devices on the same network within a building or campus. They operate at Layer 2 (Data Link) of the OSI model and use MAC addresses to forward data to the correct destination.

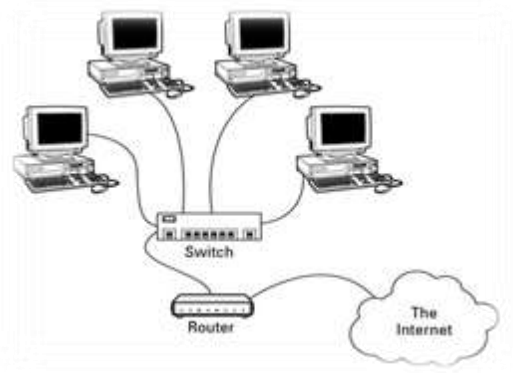
A network switch connects devices within a network (often a local area network, or LAN*) and forwards data packets to and from those devices.

- **Routers**: Routers are used to connect different networks, often between a LAN and a WAN (Wide Area Network) or the internet. They operate at Layer 3 (Network) of the OSI model, using IP addresses to route data packets between networks.

The router acts as a gatekeeper between the LAN and the Internet. It uses the Internet IP address itself and then provides computers on the LAN with their own IP addresses, which can't be seen outside of the LAN.



Also may act as a gateway that passes data between one or more local area networks (LANs). Routers use the Internet Protocol (IP) to send IP packets containing data and IP addresses of sending and destination devices located on separate local area networks.



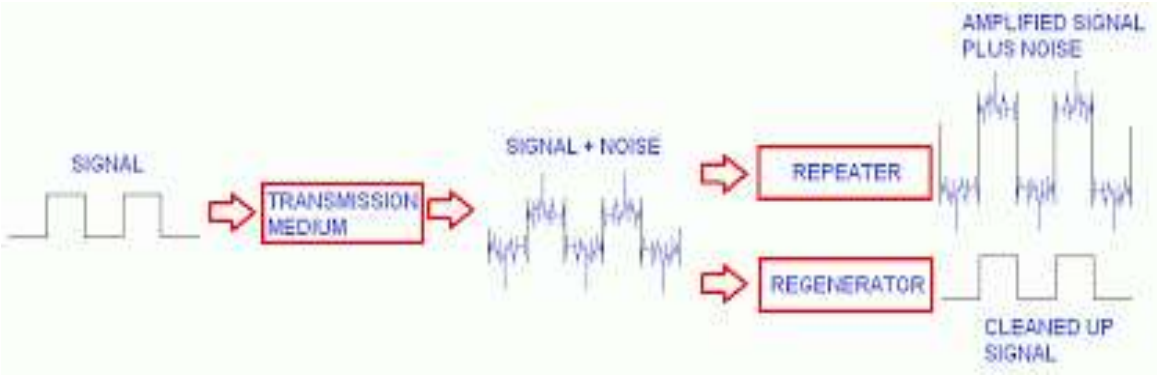
- **Hubs**: Hubs are simple devices that connect multiple Ethernet devices, making them act as a single network segment. Unlike switches, hubs broadcast data to all connected devices, regardless of the destination.
- **Bridges**: Bridges connect two or more LAN segments, filtering traffic and reducing network collisions. They operate at Layer 2 and are used to extend networks or segment them for better performance.
- **Repeater** A repeater is a network device that retransmits a received signal with more power and to an extended geographical or topological network boundary than what would be capable with the original signal.

✓ **Regenerator**

In networking, a regenerator, also known as a signal regenerator or data regenerator, is a device used to amplify and retime digital signals as they travel along a communication channel.

The primary purpose of a regenerator is to restore the quality of the signal, especially in long-distance transmissions where the signal might have attenuated (weakened) or suffered from distortion.

The repeater amplifies the signal including the noise. The regenerator removes the noise so it's a more useful device.



✓ **Access Devices**

These devices provide connectivity to end-user devices and are typically used in scenarios where wireless access is needed.

- **Access Points (APs)**: These devices allow wireless devices to connect to a wired network using Wi-Fi. Access points are essential for creating wireless networks and are often used in environments where cabling is impractical.
- **Range Extenders**: Also known as repeaters, these devices extend the coverage area of a wireless network by receiving the existing signal and retransmitting it.

✓ **Security Devices**

Security devices are essential for protecting the LAN from internal and external threats.

- **Firewalls**: Firewalls are used to protect networks by controlling incoming and outgoing network traffic based on predetermined security rules. They can be hardware-based or software-based.
- **Intrusion Detection and Prevention Systems (IDPS)**: These devices monitor network traffic for suspicious activity and potential threats. An IDS (Intrusion Detection System) alerts network administrator, while an IPS (Intrusion Prevention System) can take action to prevent the threat.
- **VPN (Virtual Private Network) Appliances**: VPNs provide secure remote access to a LAN over the internet. VPN appliances are dedicated hardware devices that handle encryption, authentication, and other VPN-related tasks.

✓ **End Devices**

End devices are the computers, printers, and other devices that users interact with.

- **Computers**: Desktop computers, laptops, and workstations are common end devices in a LAN. They require network interface cards (NICs) to connect to the network.
- **Printers and Scanners**: These peripherals are often network-enabled, allowing multiple users to share them across the LAN.
- **IP Phones**: These devices are used in VoIP (Voice over Internet Protocol) networks, allowing voice communication over the LAN and the internet.

✓ **Connectors and Media**

These components are essential for physical network connections.

- **Ethernet Cables**: Twisted pair cables (Cat5e, Cat6, Cat6a, etc.) are the most common type of cabling used in LANs. They connect devices to switches, routers, and other network equipment.
- **Fiber Optic Cables**: Fiber optic cables are used for high-speed connections and longer distances. They are less susceptible to electromagnetic interference than copper cables.
- **RJ45 Connectors**: These connectors are used with twisted pair Ethernet cables. They are standard in most LAN installations for connecting network cables to NICs, switches, and routers.

✓ **Other Essential Components**

These components support the operation and management of a LAN.

- **Patch Panels**: Patch panels organize and manage Ethernet cable connections. They are typically mounted on racks and serve as a central point for network cable management.

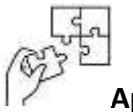
A patch panel in a local area network (LAN) is a mounted hardware assembly that contains ports that are used to connect and manage incoming and outgoing LAN cables.

- **Racks and Cabinets**: These are used to house network equipment such as switches, routers, servers, and patch panels. They help with organization, airflow, and security.

- **Power Over Ethernet (PoE) Injectors and Switches**: PoE technology allows network cables to carry electrical power, eliminating the need for separate power supplies for devices like IP cameras and access points.
- **UPS (Uninterruptible Power Supply)**: UPS devices provide backup power in case of a power outage, ensuring that critical network devices remain operational.

Points to Remember

1. **Networking materials:** Typically refers to the physical materials used to set up and maintain a computer network.
2. **Networking Tools:** Are specialized equipment that is used to install, configure, and troubleshoot network equipment.
3. **Networking equipment:** Refers to the hardware devices that are used to connect and manage a computer network**.**



Application of learning 2.1.

X School, a TVET institution, plans to expand its internet connection from the Administration Block to the Computer Lab. The lab is equipped to accommodate 30 desktop computers, 10 - 15 laptops, and one printer for the teacher. The network will provide wired access for all desktop computers and Wi-Fi coverage for the 10-15 laptops that students may use during lab sessions. The Administration Block, which is 20 meters away from the Computer Lab, already has an existing internet connection that needs to be extended to the lab and the administration block requires a wireless network to feed 15 staff and 4 visitors as addition.

As an IT Technician, you need to analyze the network design document and select the appropriate tools, materials, and equipment for installing the Local Area Network (LAN). After selection, categorize them into tools, materials, or equipment.

Indicative content 2.2: Trunking of LAN Cables

Duration: 4 hrs

Theoretical Activity 2.2.1: Description of the LAN Cable Trunking

Tasks:

1: Answer the following questions:

1. Define is mean cable installation method
2. Describe types of cable installation methods
3. Discuss about cable trunking materials
4. Describe essential cable trunking tools and protective equipments

2: Present your findings to the whole Class.

3: Ask any clarifications to the trainer

4: Read key readings 2.2.1 in Trainee's manuals.

Key readings 2.2.1.:

1. Types of Cable Installation Method

Cable Installation Methods refer to the various techniques and processes used to lay, secure, and protect cables that transmit data, power, or signals.

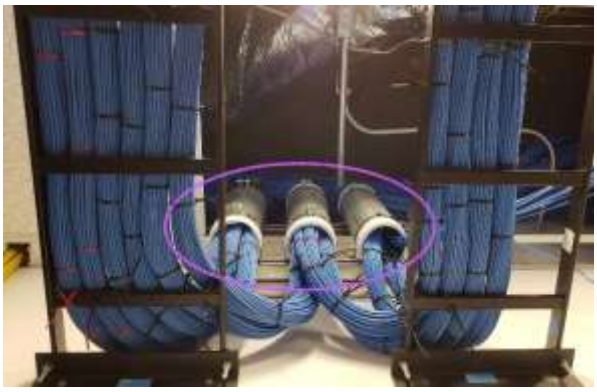
These methods are chosen based on the type of cable, the environment, cost, and specific requirements of the installation site. The goal is minimizing potential damage and interference.

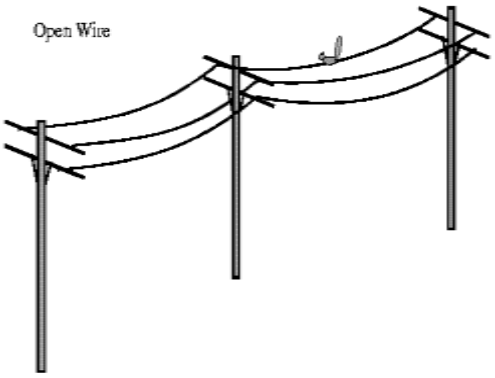
In this overview, we will discuss specific network cable installation methods including: Open-Wire, Aerial, Above-Ground Conduits, Underground, Underwater, Built-In, and Semi Built-In. Each method has its unique features, advantages, and challenges.

2. Types of Cable Installation Method

Here are key types of Cable Installation Method:

- **Open-Wire Installation (Surface wiring)**
  A method where cables are installed without any protective covering, sometimes cables suspended on poles or towers.





  - ✓ **Advantages:**
    - **Cost-Effective:** Minimal materials and labor required compared to other methods.
    - **Ease of Access:** Cables are easy to access for maintenance and repairs.

  - ✓ **Challenges:**
    - **Limited Protection:** Cables are exposed to environmental factors like wind, rain, and temperature changes, which can degrade them over time.
    - **Interference:** Susceptible to electromagnetic interference (EMI) and signal loss due to exposure.

  - ✓ **Use Cases:**
    Common in rural areas for telecommunication lines or temporary installations where long-term durability is not critical.

- **Aerial Installation**

Aerial installation involves suspending cables between poles or towers. This method is widely used for outdoor network connections, especially in areas where ground installations are impractical.

- ✓ **Advantages:**
  - **Quick and Cost-Effective:** Less expensive than underground installations since it avoids the need for trenching or boring.
  - **Easy Maintenance:** Cables are easily accessible for repairs or upgrades, reducing downtime.

- ✓ **Challenges:**
  - **Environmental Exposure:** Cables are exposed to weather conditions, which can affect durability and performance.
  - **Aesthetic and Safety Concerns:** Visible cables may not be suitable for all environments, and there is a risk of damage from falling trees, vehicles, or vandalism.
- ✓ **Use Cases:**
  Ideal for connecting buildings in rural or suburban areas, along roadways, or where ground installation is not feasible.

- **Above-Ground Conduits**

Cables are run through protective tubing or piping that is mounted above the ground. These conduits provide some degree of protection from environmental factors and physical damage.

Above-ground conduit installation involves running cables through protective tubes or conduits that are mounted on surfaces like walls or poles.

- ✓ **Advantages:**
  - **Moderate Protection:** Conduits shield cables from physical damage, moisture, and direct sunlight.
  - **Organized and Neat:** Provides a clean and organized appearance while protecting cables.

- ✓ **Challenges:**
  - **Installation Complexity:** Requires careful planning and installation, particularly in complex environments.
  - **Visibility:** Conduits are visible, which may not be suitable for aesthetically sensitive areas.
- ✓ **Use Cases:**
  Suitable for industrial environments or temporary installations where frequent access to cables is needed.

- **Underground Installation**

Underground installation involves burying cables directly into the ground/below the earth's surface.

This method provides excellent protection against environmental factors and physical damage, making it suitable for long-term and high-reliability installations.

- ✓ **Advantages:**
  - **Maximum Protection:** Cables are protected from environmental exposure, physical damage, and vandalism.
  - **Aesthetic Appeal:** Cables are completely hidden from view, maintaining a clean and uncluttered environment.

- ✓ **Challenges:**
  - **High Installation Cost:** Requires significant labor and equipment for trenching, boring, or plowing.
  - **Maintenance Difficulty:** Accessing cables for repairs or upgrades can be difficult and costly.

- ✓ **Use Cases:**
  Ideal for connecting buildings on a campus, in urban areas, data centers where space is limited, or in environments where cable protection is critical.

- **Underwater Installation**

  Underwater cable installation involves laying Cables on the seabed or underwater environments such as lakes and rivers to connect locations separated by bodies of water.

  This method is commonly used for intercontinental communication networks and connecting islands or offshore facilities.

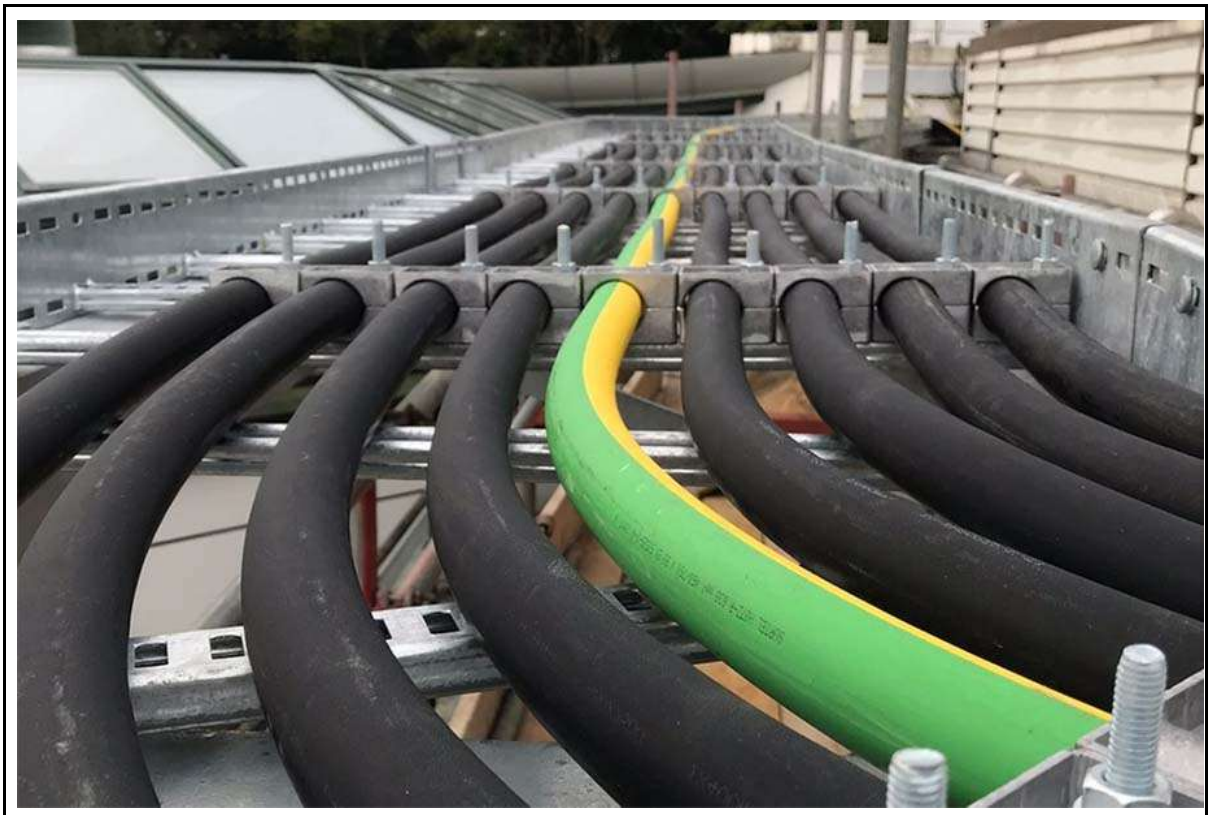
- ✓ **Advantages:**
  - **Long-Distance Capabilities:** Enables high-capacity, long-distance connections across oceans or lakes.
  - **Protected Pathways:** Cables are less likely to be tampered with due to their underwater location.

- ✓ **Challenges:**
  - **Complex Installation and Maintenance:** Requires specialized equipment and expertise for installation and maintenance, making it highly expensive.
  - **Environmental Challenges:** Exposure to underwater currents, marine life, and corrosion can affect cable longevity.

- ✓ **Use Cases:**
  Used for submarine communications cables and underwater power transmission. Used also for undersea fiber optic cables that connect continents, islands, and offshore platforms.

- **Built-In Installation**

Built-in installation refers to embedding cables directly into building structures, such as within walls, floors, or ceilings, during construction.



- ✓ **Advantages:**
  - **Aesthetic Integration:** Cables are completely hidden, providing a seamless appearance in modern buildings.
  - **Protected Installation:** Provides protection from physical damage and environmental exposure.

- ✓ **Challenges:**
- **Lack of Flexibility:** Once cables are embedded, it can be challenging and costly to make changes or repairs.
- **Requires Planning:** Must be integrated into the building design from the outset, requiring coordination with other construction trades.

- ✓ **Use Cases:**
  Common in new construction projects and renovations to create a clean and organized appearance.

- **Semi Built-In Installation**

Semi built-in installation combines aspects of built-in and exposed installations. Cables are partially integrated into a structure, often using surface-mounted conduits or decorative elements to conceal them.

- ✓ **Advantages:**
  - **Flexibility:** Easier to modify or expand compared to fully built-in installations.
  - **Aesthetic Improvement:** Cables are mostly hidden, providing a cleaner look while allowing access points.

- ✓ **Challenges:**
  - **Limited Protection:** Provides less protection than fully built-in methods but more than fully exposed methods.
  - **Requires Planning and Coordination:** Needs to be carefully planned during construction or renovation.

- ✓ **Use Cases:**
  Ideal for renovations, buildings that require a mix of aesthetics and future flexibility, or environments where frequent updates to the network are anticipated.

3. Cable Trunking Materials

Cable trunking is a method used to protect, organize, and manage cables in network installations. It involves enclosing cables within a protective conduit or casing, often referred to as a trunking system. This provides protection against physical damage, environmental factors, and interference. Here are some common materials used for cable trunking in network installations:

- **Plastic Trunking**

Plastic trunking, made from materials like as PVC (Polyvinyl Chloride), ABS (Acrylonitrile Butadiene Styrene), or polypropylene, is one of the most widely used options for cable management.

Advantages

- It is relatively inexpensive compared to other materials, which makes it an economical choice for large-scale installations.
- It is easy to cut, shape, and install, which reduce labor costs and quick adjustments on-site.
- It is resistant to moisture, chemicals, and corrosion which reduces the risk of electrical shocks or short circuits in electrical installations.
- Provides good protection against environmental factors.

Disadvantages

- It has Limited heat resistance, means can melt or deform at high temperatures, which limits its use in environments with high heat exposure
- Less durable compared to metal trunking.

Applications: Ideal for residential buildings, office environments, schools, and other where cost and ease of installation are priorities and it is applied for both data and power cables.

- **Wood Trunking**

Wood trunking is a traditional material for cable management, used primarily for its attractive appeal in specific environments. While not as common today, it is still used in certain settings where the natural look of wood is desired.



Advantages:

- Attractive in appearance and can integrate smoothly with interior design.
- Can be painted or finished to complement interior design.
- Provides a natural and warm look.
- Can be customized and finished to match specific design requirements.

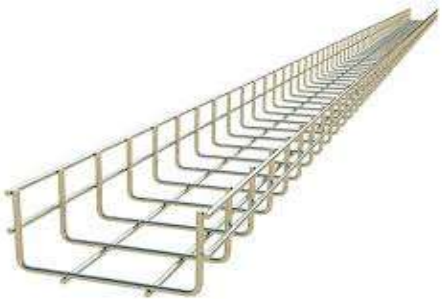
Disadvantages:

- Vulnerable to damage from moisture, insects, and decay.
- Requires regular maintenance and treatment.
- Not suitable for environments with high humidity or risk of fire.

Applications: Suitable for residential homes and heritage buildings where beauty and design are important, such as in historic buildings, offices, and homes.

- **Metal Trunking (Steel or Aluminum)**

Metal trunking, typically made from steel or aluminum, provides a high level of protection for cables. It is used in environments where durability and resistance to physical damage are paramount.




✓ Advantages:

- It has high mechanical strength.
- It has excellent fire resistance, does not burn or melt.

- It provides high degree of electromagnetic shielding, protecting sensitive data cables from interference.
- It has a long service life and is resistant to wear and tear

✓ Disadvantages

- More expensive than plastic options.
- Heavier and more challenging to install, often requiring specialized tools and labor.
- Requires grounding to provide additional electrical safety.

✓ **Application:**
Ideal for industrial environments, data centers, and areas where high durability and protection are required.

4. Cable trunking tools

To install cable trunking effectively, you'll need a range of tools. Here are some common tools used in cable trunking installations:

- **Basic Tools**

✓ **Measuring Tape:** To measure the length of trunking needed and ensure accurate cuts.

✓ **Utility Knife:** To cut the trunking material, especially for plastic trunking.

✓ **Hacksaw:** To cut through metal or thick plastic trunking.

✓ Screwdrivers: To secure trunking covers and fixings.

- ✓ Drill: To create holes for screws and anchors when mounting trunking to walls or ceilings.

- ✓ Level: To ensure the trunking is installed straight and level.

- ✓ **Cable Trunking Cutter:** To make clean, precise cuts in plastic trunking.

- **Safety Equipment**
- ✓ **Safety Glasses: To** protect eyes from debris when cutting or drilling. Protective eyewear.

- ✓ **Gloves:** To protect hands from sharp edges and tools. Durable work gloves.

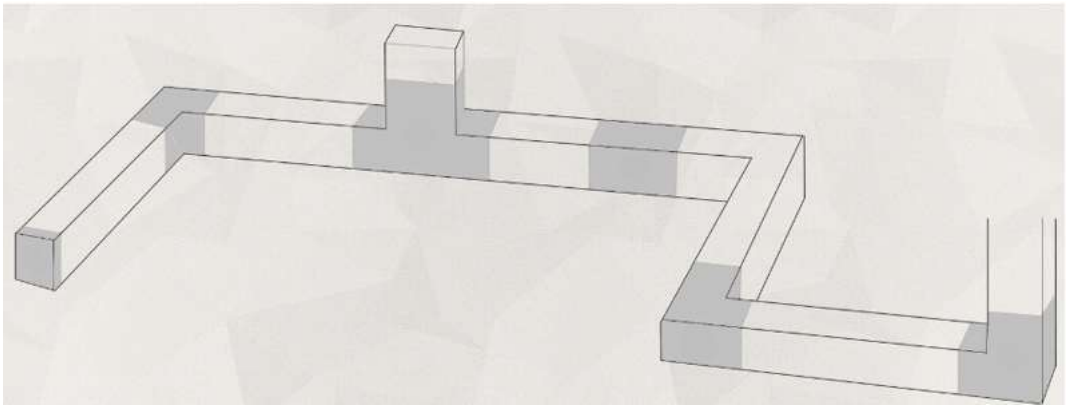
- ✓ **Dust Mask:** To protect from inhaling dust when cutting or drilling. A mask that covers the nose and mouth.

Practical Activity 2.2.2.1: Installing the cable trunking

Task:

1: Read the given task:

The provided image illustrates the cable route planned for a trunking system to safeguard LAN cables. As a Network Technician, you are tasked with implementing this design by installing the trunking system accordingly.



2: Follow the trainer's demonstration and ask clarifying questions if needed.

3: Perform the given task basing on what trainer demonstrated.

4: While installing, ask for assistance where is needed

5: Present your work to trainer.

6: Read key readings 2.2.2.1 in trainee's manual

Key readings 2.2.2.1

INSTALLATION OF TRUNKING FOR LAN CABLES:

Cable trunking is a system used to organize, route, and protect electrical and data cables within a building or infrastructure.

Cable trunking helps keep cables secure, reduces clutter, minimizes the risk of damage, and improves the safety and aesthetics of a space by preventing exposed wires. It ensures that your network cables are organized, protected, and easily maintainable.

STEP-BY-STEP GUIDE TO INSTALLING TRUNKING FOR LAN CABLES:

Notes: Here are two possible situations, the first is when site survey is Already conducted, survey report elaborated, and network design Created (as completed in Learning outcome one). The second is when installation environment not evaluated.

Here is a **step-by-step guide to installing trunking** for LAN cables where installation environment not previously evaluated:

Step 1: Planning the Installation

- **Assess the Environment:**
  - ✓ Start by evaluating the physical layout of the area where the trunking will be installed.
  - ✓ Identify the locations of network devices, identify key areas where network devices will be located (e.g., workstations, switches, routers), power sources, and any potential obstacles.
- Determine the best routes for the trunking, Consider the shortest and most efficient paths while avoiding obstacles and minimizing cable bends.

Step2: Selecting the Right Materials and Necessary tools

- ✓ **Size:** Choose trunking with enough capacity for the number of LAN cables and allowing for future growth.
- ✓ **Material:**
  - ✓ **PVC Trunking:** Common for indoor applications (offices, schools).
  - ✓ **Metal Trunking:** Suitable for heavy-duty or industrial environments.
- ✓ **Accessories:** Get appropriate connectors (e.g., bends, joints, end caps) for corners or intersections.
- ✓ **Compartments:** Consider trunking with dividers, if you need to route power and data cables separately.
- ✓ **Tools:** Gather all necessary tools including:
  - Saw or trunking cutter
  - Drill and appropriate drill bits
  - Screws and wall plugs
  - Screwdriver
  - Level
  - Measuring tape

- Pencil or marker
- Cable ties or clips

Step 3: Marking and Measuring the Path

- **Measure the Trunking Path:** Use a measuring tape to measure the distance of the planned trunking route, ensure you have enough trunking material and add a little extra to account for any adjustments.
- **Mark the Mounting Points:**
  - ✓ Use a pencil or marker to indicate where the trunking will be mounted, ensuring alignment along the path.
  - ✓ Mark the spots where you'll need to drill holes for screws, especially for long runs of trunking.

Step 4: Cutting and Fitting Trunking

- **Marking:** Use a pencil or marker to mark the cutting points on the trunking based on your measurements.
- **Cutting:** Cut the trunking to the required lengths using a saw or trunking cutter. Ensure the cuts are clean and smooth to prevent damage to the cables.

Step 5: Installing the Trunking

- **Drill Mounting Holes:**
  - ✓ Drill holes along the marked path where the trunking will be mounted.
  - ✓ Use wall plugs for a firm anchor if attaching trunking to plasterboard, drywall, or masonry.
- **Mount the Trunking:**
  - ✓ Secure the trunking to the wall, ceiling, or floor with screws, making sure it is level and aligned along the entire path.
  - ✓ Attach trunking connectors (e.g., elbows, tees) at joints and corners to create a continuous route.

Step 6: Pulling and Laying LAN Cables (this topic discussed in details in next Practical 2.2.2.2)

- **Bundle and Insert Cables:**
  - Lay the cables inside the trunking, ensuring they are loosely arranged to prevent overcrowding.

- Ensure that cables are not kinked or bent beyond the recommended bend radius (especially for Cat 5e, Cat 6 cables).

- **Separate Power and Data Cables:**
  - If running both power and data cables in the same trunking, use internal dividers or separate trunking to avoid interference. Ensures that LAN cables in the trunking are placed at least 12-18 inches away from electrical cables to avoid electromagnetic interference (EMI).

Step 7: Securing the Trunking Cover

- Once all the trunking sections are in place, install the cover plates. These plates help protect the cables and give the installation a finished appearance. Align the cover plates with the trunking sections and secure them using the provided screws or clips.

Step 8: Labeling and Documentation

- **Label the Trunking Sections:**
  - ✓ Use labels to identify the cables within each section of the trunking. This is particularly useful for future maintenance or network upgrades.
- **Update Network Documentation:**
  - ✓ Document the trunking layout, including where cables are routed and any critical connection points. This will assist in future troubleshooting or modifications.

Step 9. Maintenance and Upkeep

- **Periodic Inspections:**
  - ✓ Regularly inspect the trunking system to ensure it remains intact and free from damage. Check for loose covers or damaged sections.
- **Add New Cables:**
  - ✓ When adding new cables, open the trunking carefully, lay the new cables, and re-secure the cover.

TRUNKING ACCESSORIES AND COMMON TRUNKING BENDS

Trunking accessories are components used to enhance or support the installation, organization, and management of trunking systems. They help ensure smooth routing of cables, allow for changes in direction of the trunking system.

Here are the common trunking accessories:

1. Couplers

- Used to connect two lengths of trunking together, ensuring a continuous path for cables.

2. Bends (Internal and External)

- **Internal Bend:** Allows trunking to change direction around an inside corner (e.g., along the corner of a room).
- **External Bend:** Enables the trunking to route around an outside corner (e.g., the outer edge of a wall).

3. Tees and Crosses

- **Tee Junction:** Divides the trunking into two or more directions at a right angle.
- **Cross Junction:** Allows cables to be routed in four directions, forming a cross intersection.

4. End Caps

- Used to close off the end of a trunking run to protect cables from external damage and prevent dirt or debris from entering.

5. Dividers

- Internal barriers used to separate different types of cables (e.g., power and data) within the same trunking to reduce electromagnetic interference (EMI).

6. Trunking Clips/Clamps

- Secure the trunking to walls, floors, or ceilings, ensuring it remains in place and organized during and after installation.

7. Cable Retainers

- Installed inside trunking to hold cables securely in place, preventing them from moving or becoming disorganized.

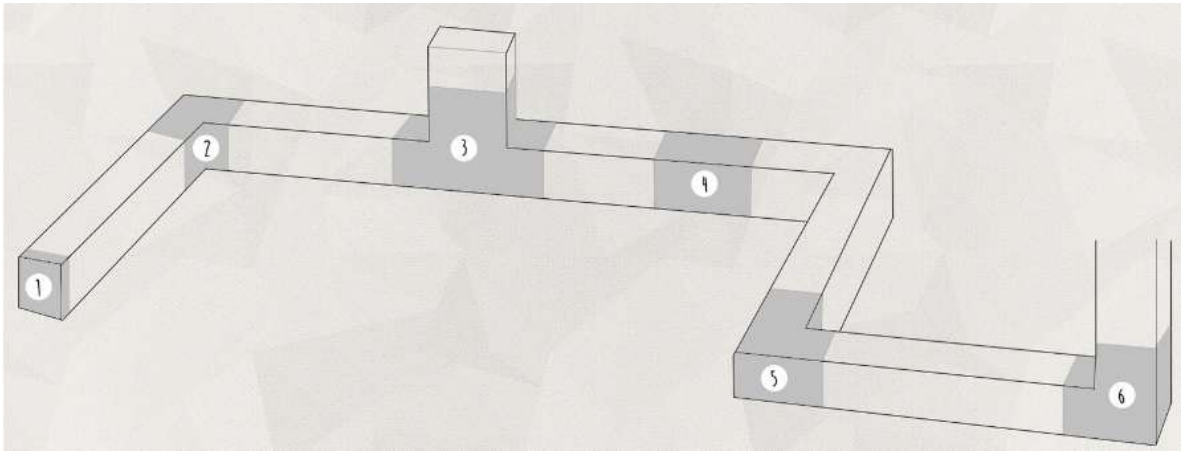
8. Joints

- Flexible or rigid joints that allow the trunking to bend or adjust for non-linear routes or irregular surfaces.

9. Reducers: Used to connect trunking of different sizes, allowing for a smooth transition between larger and smaller trunking sections.

10. Cable Entry Boxes

- Allow cables to exit or enter the trunking at specific points, providing a neat and protected connection for devices or network points.



1: END CAP: Used to close off trunking runs

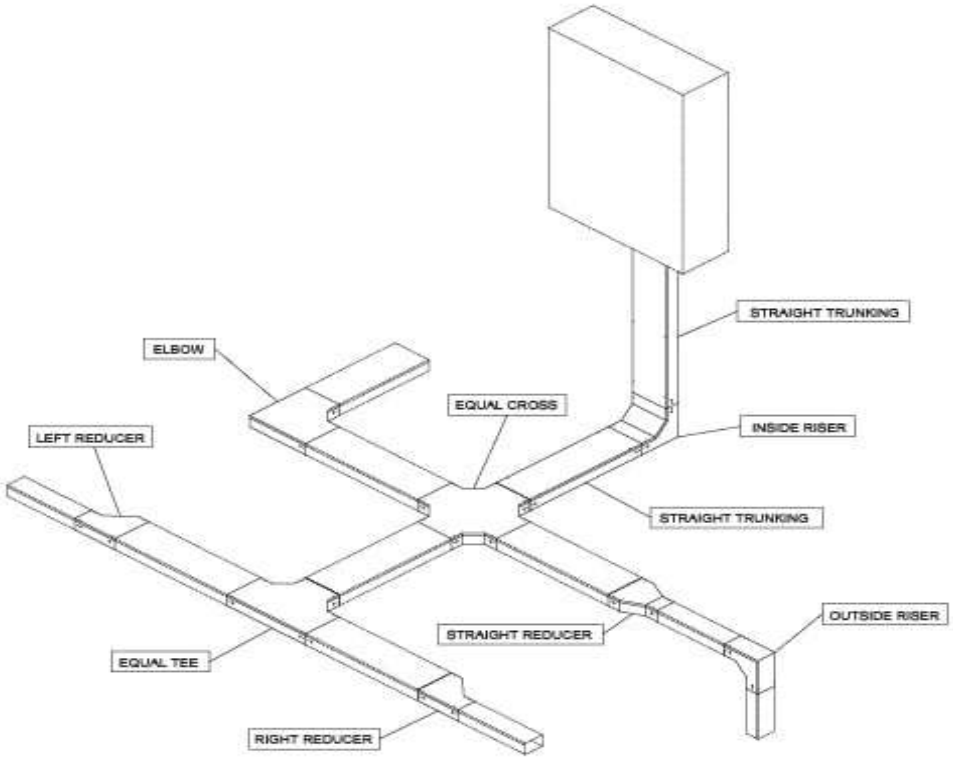
2: INTERNAL ANGLE: used to turn 90^0 corners inside a room

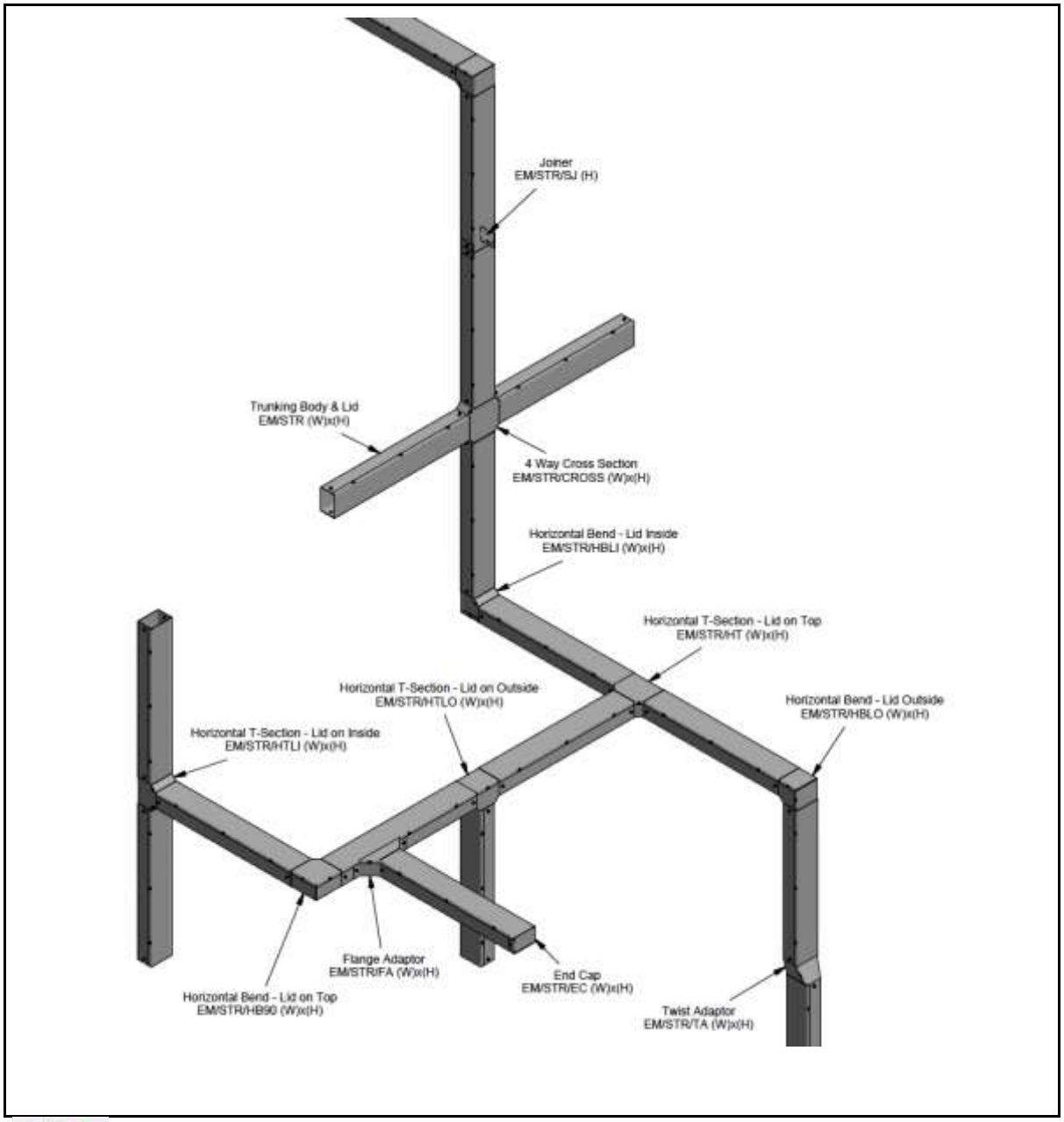
3: FLAT T: Used to create a secondary Channel at 90^0 Angle

4: Coupler: Used to connect longer pieces of trunking

5: External angle: Used to turn 90^0 corners outside

6: Flat 90^0 : Used to change direction of straight trunking run by 90 Angle





Practical Activity 2.2.2.2: Applying cable laying and pulling methods

Task:

1: Read the given task:

Referring to Practical Activity 2.2.2.1, install the cables in the trunking system that was set up during that activity.

2: Follow the trainer's demonstration and ask clarifying questions if needed.

3: Perform the given task basing on what trainer demonstrated.

4: While installing, ask for assistance where is needed

5: Presents your work to trainer.

6: Repeat the activity individually until you achieve the perfect output.

7: Read key readings 2.2.2.2 in trainee's manual

Key readings 2.2.2.2

After installing the trunking, means once the trunking (the pathway or conduit system for the cables) is in place, the next action is to pull the network cables through this trunking system.

CABLE PULLING VS. CABLE LAYING

- **Cable Laying**: This term is more broadly used to describe the overall process of placing and positioning cables in a network installation. It includes pulling the cables through pathways and positioning them correctly in open areas, under floors, above ceilings, or along walls. "Cable laying" generally refers to the entire process of installing cables, including planning, routing, and physically placing the cables in conduits or trays.

  In short **Cable Laying** is the overall process of installing and positioning network cables, which includes steps like planning, measuring, pulling, securing, terminating, and testing the cables.

- **Cable Pulling**: This is the process of physically pulling or guiding the network cables through the pathways provided by the trunking system, conduits, or other cable management systems. The term "cable pulling" specifically refers to the action of pulling cables from one end to another through these pathways, using tools like cable pullers, fish tapes, or pulling ropes.

  In short **Cable Pulling** specifically refers to the part of the cable laying process where cables are physically pulled through the pathways (trunking, conduits, etc.) that have been installed.

  Notes: Cable laying is the overarching process of installing cables, while **cable pulling** is a specific task within cable lying process. Cable pulling refers to the act of physically drawing or pulling cables through conduits or ducts.

Order of actions that take place in Cabling (cables Installation)

1. **Trunking Installation**: The trunking system is installed first to create a structured pathway for the cables. This could include cable trays, conduits, or plastic trunking systems that run along walls, ceilings, or floors.

2. **Cable Pulling**: After the trunking or conduits are in place, the next step is to **pull the cables** through these pathways. This step requires careful handling to avoid damaging the cables, ensuring they are not overstressed, kinked, or bent beyond their bend radius.
3. **Cable Securing and Organizing**: Once the cables are pulled through the trunking or conduits, they are secured in place using cable ties or clamps to prevent movement, maintain organization, and ensure they remain neatly routed.
4. **Cable Termination and Testing**: Finally, the pulled cables are terminated with appropriate connectors, labeled, and tested to ensure they meet network performance standards and are correctly installed.

CABLE LAYING PROCESS

Once cable trunking is installed, the next step in the LAN installation process is the actual **cable laying**. This involves placing the network cables inside the trunking system to ensure they are organized, protected, and properly routed throughout the building. Here's a step-by-step guide to the cable laying process after trunking:

Step 1. Preparation and Planning

- **Review the Network Layout:** Before beginning the cable laying process, review the detailed network design plan that outlines the routes the cables will take through the trunking. Ensure that all trunking pathways are correctly installed according to the layout.
- **Gather Necessary Tools and Equipment:** Ensure you have all the necessary tools, such as cable pullers, fish tape, cable ties, labeling tags, and termination tools, ready and accessible.

Step 2. Cable Measurement and Cutting

- **Measure Cable Lengths:** Measure the required lengths of each cable run based on the network design plan. Make sure to account for additional slack to accommodate any adjustments or future maintenance.
- **Cut the Cables:** Cut the cables to the appropriate lengths. It is advisable to cut slightly longer than the measured length to allow for termination and connection flexibility.

Step 3. Cable Pulling Through Trunking

- **Start from the Patch Panel or Switch Location:** Begin laying the cable from the central distribution point, such as the network switch or patch panel, to ensure proper connection and termination later.
- **Use Cable Pullers or Fish Tape:** Use a cable puller or fish tape to guide the cable through the trunking. Insert the cable puller into the trunking, attach the cable securely to the puller, and then carefully pull the cable through the trunking system.
- **Avoid Over-Bending and Kinking:**

Ensure the cable is pulled smoothly without exceeding the recommended bend radius to prevent damage or signal loss. Avoid kinking the cable, as this can impair performance.

Step 4. Organizing and Securing the Cables

- **Route Cables Neatly Within Trunking:** Lay the cables neatly within the trunking, keeping them organized and separated as needed. For instance, separate power and data cables to prevent electromagnetic interference (EMI).
- **Secure Cables Inside the Trunking:** Use cable ties or Velcro straps to bundle cables together securely, but not too tightly, to avoid crushing the cables and affecting their performance.

Step 5. Connecting and Terminating Cables

- **Terminate the Cables:** Terminate the cables at both ends with appropriate connectors (e.g., RJ45 connectors for Ethernet cables). Make sure that terminations are done correctly to avoid issues such as signal loss or network failure.
- **Connect to Patch Panels and Network Devices:** Connect the terminated cables to patch panels, network switches, routers, or other network devices as specified in the network design plan. Ensure connections are secure and match the labeling scheme used in the planning phase.

Step 6. Labeling and Documentation

- **Label Each Cable Run:** Use labeling tags or markers to label each cable run clearly. Include information such as the cable type, destination, and source to facilitate future troubleshooting and maintenance.
- **Update Network Documentation:** Update the network documentation to reflect the actual cable runs, terminations, and connections. This documentation is critical for future reference and any network modifications.

GENERAL METHODS OF CABLE LAYING

Cable laying methods refer to the techniques and procedures used to install cables in various environments for different applications. The choice of method depends on factors such as the environment (indoor or outdoor), type of cable, safety requirements, cost considerations, and the need for future accessibility and maintenance, and the specific requirements of the project.

Below, we discuss different cable laying methods, considerations, and best practices.

- **Direct Buried laying Method:** Cables are buried directly in the ground without additional protective conduits.

  - ✓ **Advantages:** Cost-effective and straightforward.
  - ✓ **Disadvantages:**
    - Difficult to repair and maintain.
    - Vulnerable to ground movements and digging.
  - ✓ **Applications**: Suitable for outdoor environments where cables need to be hidden and protected from surface interference, such as in urban and rural areas for power distribution and telecommunications.
- **Conduit Laying Method:** Cables are laid inside protective conduits or ducts, which are buried underground or run along the surface.

- ✓ **Advantages**:
  - Conduits provide additional protection against mechanical damage, moisture, and chemical exposure.
  - Protects cables from environmental hazards.
  - Easier to maintain and replace cables.
  - Easier to upgrade or replace cables without the need to dig trenches.
- ✓ **Disadvantages**:
  - Higher installation cost due to the cost of conduits and the need for precise installation.
- ✓ **Applications**: Common in both indoor and outdoor environments, including industrial facilities, commercial buildings, and residential areas.

- **Trunking Laying Method:** Cables are laid inside trunking systems, which are surface-mounted enclosures usually made of plastic or metal.

- ✓ **Advantages**:
  - Provides an organized way to route cables.
  - Trunking can be easily opened for adding or removing cables.
  - Easy to install and modify.

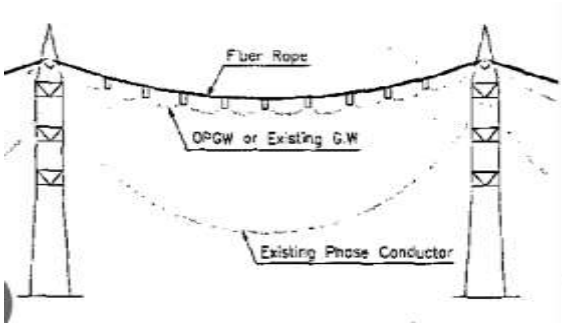
- Protects cables from physical damage.

✓ **Disadvantages**:

- May not provide adequate protection against fire or water damage.
- Can be visually intrusive in some settings.

✓ **Applications**: Commonly used in indoor environments such as offices, commercial buildings, and industrial settings.

- **Aerial Laying Method:** Cables are suspended in the air using poles or towers.



✓ **Applications**: Typically used for power transmission and telecommunications in both urban and rural settings.

✓ **Characteristics**:

- Requires poles, towers, or other supporting structures.
- Suitable for crossing rivers, roads, or other obstacles.

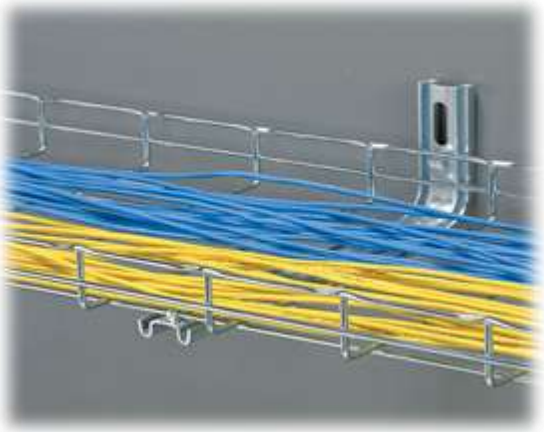
✓ **Advantages**:

- Cost-effective for long distances where trenching is impractical.
- Easy to access for maintenance and repair.

✓ **Disadvantages**:

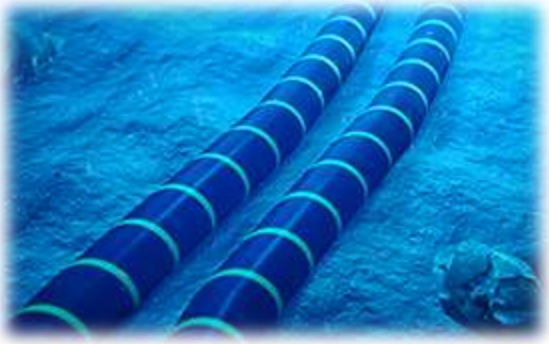
- Exposed to environmental hazards like wind, ice, and lightning.
- Vulnerable to physical damage from trees, vehicles, and vandalism.

- **Cable Tray Laying Method:** Cables are laid on cable trays that are installed on walls, ceilings, or floors.



- ✓ **Advantages**:
  - Easy to install, modify, and maintain.
  - Provides good cable management and ventilation.
- ✓ **Disadvantages**:
  - Limited protection against fire and physical damage.
  - Requires careful planning to avoid overcrowding and excessive weight.
- ✓ **Applications**: Commonly used in data centers, industrial facilities, and commercial buildings.

- **Underwater Laying Method**: Cables are laid underwater in oceans, rivers, or lakes, often buried in seabed or laid on the seabed with protective coverings.




- ✓ **Characteristics**:
  - Requires specialized techniques and equipment for underwater installation.
  - Cables are designed to withstand high pressure and corrosion.
- ✓ **Advantages**:
  - Provides secure communication and power transmission routes across water bodies.
  - Protected from most physical and environmental hazards.
- ✓ **Disadvantages**:
  - High installation and maintenance costs.
  - Difficult to repair and maintain.
- ✓ **Applications**: Used for submarine communication cables, intercontinental and coastal networks, and underwater power transmission.

- **Built-In and Semi Built-In laying Methods**

✓ **Built-In Method**: Cables are integrated into the building's structure, such as inside walls, floors, or ceilings.

Advantages:

- Aesthetically pleasing and secure.
- Provides protection against tampering and environmental damage.

Disadvantages:

- Costly and time-consuming to install.
- Challenging to modify or repair.
- Difficult to access for maintenance

Applications: Ideal for new construction projects where cables can be concealed for aesthetic and safety purposes.

✓ **Semi Built-In Method**: Cables are partially concealed within channels or ducts mounted on walls, floors, or ceilings.

- **Characteristics**:
  - Provides good protection while maintaining accessibility.
  - Easier to modify and maintain than fully built-in systems.

- **Advantages**:
  - Flexible and easier to install.
  - Allows for future upgrades or repairs.
- **Disadvantages**:
  - Less aesthetically pleasing than built-in methods.
  - May not provide full protection in all environments.
- **Applications**: Suitable for both new constructions and retrofits, providing protection and concealment while allowing easier access than fully built-in methods.

CABLE PULLING

As mentioned early, Cable pulling is a critical aspect of cable installation that involves the physical process of drawing cables through conduits, ducts, cable trays, or other pathways.

- **Equipment and Tools required in Cable pulling**

✓ **Cable Pulling Machines:** Mechanical devices that provide the necessary force to pull cables through long or complex routes.

✓ **Fish Tape:** A flexible, flat steel tape used to guide cables through conduits.

✓ **Cable Lubricants:** Special lubricants that reduce friction and make it easier to pull cables through tight spaces.

- ✓ **Cable Rollers and Guides:** Devices that help guide and support cables during the pulling process to prevent damage.




- ✓ **Pulling Grips:** Attachments used to securely grip the cable during pulling.



- **Pulling Process**
  - ✓ **Initial Feed:** Begin by feeding the fish tape or pulling rope through the conduit or duct. Attach the pulling grip to the cable end and secure it to the fish tape or rope.
  - ✓ **Lubrication:** Apply cable lubricant generously to the cable as it is fed into the conduit to minimize friction.
  - ✓ **Controlled Pulling:** Start the pulling process slowly, maintaining a steady and controlled pace. Monitor the tension using a tension meter to ensure it does not exceed the cable's maximum rating.
  - ✓ **Communication:** Maintain clear communication between the pulling team at both ends of the route to coordinate efforts and address any issues immediately.
- **Cable pulling Methods and Techniques**
  - ✓ **Manual Pulling:** Suitable for short distances and smaller cables; involves manually pulling the cable through the conduit or tray.
  - ✓ **Mechanical Pulling:** Uses cable pulling machines for longer distances, larger cables, or more complex routes.
  - ✓ **Blow or Air-Assisted Pulling:**

Utilizes compressed air to blow lightweight cables through ducts or conduits, commonly used in fiber optic installations.

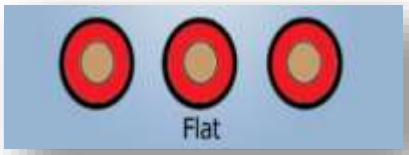
- **Safety Considerations during Cable pulling**
  - ✓ **Personal Protective Equipment (PPE):** Ensure that all personnel involved in cable pulling wear appropriate PPE, such as gloves, safety glasses, and helmets.
  - ✓ **Load Monitoring:** Use tension meters to monitor the pulling force and prevent exceeding the cable's maximum tension rating.
  - ✓ **Communication:** Maintain clear communication among team members to coordinate efforts and respond to any issues promptly.

CABLE LAYING ARRANGEMENT

After the process of cable pulling, where cables are physically pulled through conduits, trays, or along pathways to their designated locations, the next step is the cable laying arrangement. This step involves organizing, securing, and positioning the cables in a manner that ensures optimal performance, safety, and ease of maintenance.

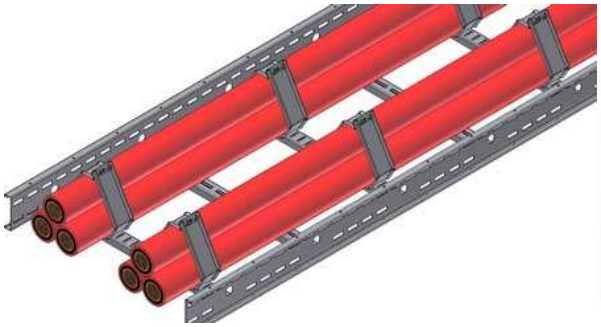
Cable laying arrangement: Cable laying arrangement refers to the specific setup of cables during cables installation.

Types Cable Arrangement



- **Trefoil Arrangement**: Three single-core cables are laid in a triangular formation, using trefoil clamps to maintain their position.
  - ✓ **Installation Steps**:

    0. **Positioning**: Place the three cables in a triangular layout to ensure that each cable is equally spaced from the others.
    1. **Securing**: Use trefoil clamps at regular intervals to hold the cables in place. This prevents movement and ensures that the formation is maintained over the entire length.
    2. **Alignment**: Ensure the cables are aligned correctly, and check that the clamp positions do not cause any unnecessary stress on the cables.



  - ✓ **Flat Formation Arrangement**: Single-core cables are laid side-by-side in a flat, linear formation.
    - **Installation Steps**:
      1. **Laying Out**: Lay the cables parallel to each other on a flat surface, such as a cable tray or support system.
      2. **Spacing and Separation**: Maintain adequate spacing between the cables to allow for heat dissipation and avoid cross-interference.
      3. **Securing**: Use cable ties, straps, or clamps to secure the cables in place at regular intervals, ensuring they remain in a flat formation.

- **Benefits of cable arrangement**

  - ✓ **Organized Layout**: Ensures a neat and organized installation, making it easier to manage and identify cables.
  - ✓ **Efficient Use of Space**: Allows for efficient use of available space, especially in data centers or industrial environments where numerous cables are installed.
  - ✓ **Segregation of different Cable Types:** Separating power cables from data and communication cables is important to prevent interference, where electromagnetic interference (EMI) can affect data transmission quality.
  - ✓ **Ease of Maintenance**: Cables laid in a flat formation are easier to access, identify, and service.
  - ✓ **Cable Spacing:** Maintain adequate spacing between cables to allow for proper ventilation and heat dissipation.

- **Factors Affecting cable Arrangement/ Key Considerations for Cable Laying Arrangement**

  - ✓ **Cable Type:** The type of cable (e.g., power, communication, control) will influence the appropriate arrangement.
  - ✓ **Voltage Level:** Higher voltage levels may require more specific arrangements to minimize interference and ensure safety.
  - ✓ **Environmental Conditions:** Factors like temperature, humidity, and soil conditions can affect cable behavior and require specific arrangements.
  - ✓ **Safety Regulations:** Adherence to local safety regulations and standards is essential for proper cable laying.

CABLES SEGREGATION

Cable segregation is the practice of separating different types of cables to prevent interference and ensure safety. This is particularly important in electrical installations

where power cables, data cables, and other types of cables are run together.

No matter what method is used for laying, cables must be segregate taking into account, cables with different voltage levels and/or different functions must not be laid at the same physical support, must be separated.

Segregation of cables must be done in accordance with standards and regulations, and must consider the following situations:

- ✓ Power cables (by voltage level);
- ✓ Control cables;
- ✓ Communication cables.

Factors Affecting Cable Segregation

- **Cable Type:** The type of cable (e.g., power, data, control) will determine the specific segregation requirements.
- **Voltage:** Higher voltage cables may require greater separation distances.
- **Frequency:** The frequency of the electrical signals can also influence segregation requirements.
- **Local Regulations:** Building codes and electrical standards will provide specific guidelines for cable segregation in a particular region.

Why is Cable Segregation Important?

1. **Electromagnetic Interference (EMI):** Power cables can generate electromagnetic fields that can interfere with data cables, leading to signal degradation or even data loss. Segregation helps to minimize this interference.
2. **Safety:** Incorrectly routed cables can pose a safety hazard. For example, if a power cable is accidentally cut or damaged, it can cause electrical shock or fire. Segregation reduces the risk of such accidents.
3. **Compliance:** Many electrical codes and standards require specific cable segregation practices to ensure safety and reliability.

Points to Remember

- **Cable trunking process**

✓ Evaluate the installation area to determine the best routes for cable trunking and laying and Identify locations for network devices, such as switches, routers, and access points.

✓ Create/Design a detailed plan for the cable trunking layout, including the placement of trunking, cable routes, and outlet locations. And Decide on the type and quantity of cables needed

✓ Collect all necessary materials, including cable trunking, Ethernet cables, connectors, mounting hardware, and tools (e.g., cable cutters, drills, measuring tape). Cut cables according to the taken measurements.

✓ Take measurements from cable route plan (Network layout floor plan).

✓ Cut Trunking according to the taken measurements.

✓ Mount the Trunking to the walls or ceilings using brackets or screws and Leave openings for cable entry and exit points as needed.

✓ Label the trunking to indicate the type of cables that will run through them or their destination.

✓ Cut the cables to the required lengths based on the layout.

✓ Carefully lay the cables inside the installed trunking, ensuring they are organized and not twisted or kinked.

✓ Use cable separators (segregation strip) to keep different types of cables organized within the trunking.

Application of learning 2.2.

X School, a TVET institution, plans to expand its internet connection from the Administration Block to the Computer Lab. The lab is equipped to accommodate 30 desktop computers, 10 - 15 laptops, and one printer for the teacher. The network will provide wired access for all desktop computers and Wi-Fi coverage for the 10-15 laptops that students may use during lab sessions. The Administration Block, which is 20 meters away from the Computer Lab, already has an existing internet connection that needs to be extended to the lab and the administration block requires a wireless network to feed 15 staff and 4 visitors as addition.

In the initial phase, the IT team conducted a site survey for the LAN installation, developed a network design, and assembled the necessary tools, materials, and equipment.

For the next phase, the school needs to hire a specialized cabling company to complete the installation, which includes cable trunking, pulling, and laying.

Indicative content 2.3: Mounting of LAN Equipment

Duration: 5 hrs

Theoretical Activity 2.3.1: Description of mounting of LAN equipment

Tasks:

1: Discuss on the following questions:

i. What is Mounting?
ii. Which network equipment needs to be mounted?
iii. Provide the importance of mounting network equipment.
iv. Describe different mounting options available for LAN equipment
v. Discuss about major mounting Components
vi. Describe different mounting safety

2: Engage with the trainer during the discussions.

3: Present your findings to the class

6: Ask clarifying questions if needed

7: Read key readings 2.3.1 in the trainee manual for further learning.

Key readings 2.3.1.:

Mounting of LAN Equipment

1. Mounting

In network installation, **mounting** is the process of securely attaching or fixing network equipment, such as switches, routers, patch panels, servers, and other hardware, to wall, rack, cabinet, ceilings or other surface.

This helps to organize the equipment in a structured and accessible manner, ensuring stability, airflow for cooling, and easy access for maintenance and troubleshooting. Proper mounting also reduces the risk of damage, improves cable management

2. Types of network device that can be mounted

The network devices that are commonly mounted includes:

- ✓ Switches
- ✓ Routers
- ✓ Access Points
- ✓ Firewalls
- ✓ servers

Notes: These devices are often mounted in network racks or cabinets to provide centralized management and organization of network connections. This helps to keep the network organized and easy to troubleshoot.

3. Importance of Mounting LAN equipment

- Helps to keep the network devices organized
- Provide centralized management and organization of network connections
- Mounted equipment is less likely to be accidentally knocked over or damaged.
- Mounted equipment is more difficult to steal or tamper with.
- Mounted equipment makes it easier to keep cables neat and organized.
- Mounted equipment allows for better air circulation, which helps to keep it cool and prevent overheating.
- Mounted equipment is often easier to access for maintenance and troubleshooting.

4. Different mounting options available for LAN equipment

When setting up LAN equipment, different mounting options are available depending on the type of equipment, installation environment, and functional requirements

The choice of mounting option depends on the equipment type, space constraints, environmental conditions, and network requirements.

Here are the common mounting options available for LAN equipment:

- **Rack-Mounting**

  Rack-mounting involves placing network equipment in standardized racks. These racks come in different forms:

  - ✓ **Floor-Mounted Racks**: Larger racks installed on the floor, typically used for housing servers, switches, and other large equipment in data centers or network rooms.

- ✓ **Wall-Mounted Racks**: Smaller racks attached to walls, suitable for limited spaces, often used in smaller networks to hold switches and patch panels.

- **Wall-Mounting**

  Wall-mounting involves directly attaching network devices like switches, access points, or cameras to the wall using brackets or mounting kits.

- **Ceiling-Mounting**

  Ceiling-mounting is used to install devices like wireless access points, cameras, or speakers onto the ceiling, optimizing space and coverage


- **Pole-Mounting**

Pole-mounting is used to attach devices such as outdoor cameras, antennas, or access points to poles, often found in outdoor or industrial settings.


- **Cabinet Mounting**

Cabinet mounting involves placing network equipment inside enclosed cabinets for protection from dust, unauthorized access, and environmental conditions, often used for servers or sensitive electronics. Cabinets can be floor or wall-mounted.

- **Major Mounting Components**

  ✓ **Panel**

  A mounting panel, also known as a patch panel, is a physical device that organizes and centralizes network connections within a structured cabling system.

Patch panels provide several benefits for network management and organization:

- **Centralized Connectivity:** They provide a central location for managing and connecting network cables, making it easier to track and troubleshoot network issues.
- **Improved Cable Management:** They organize and arrange network cables, reducing clutter and improving airflow within network racks or cabinets.
- **Flexible Connectivity:** They allow for easy rearrangements of network connections without the need to rewire individual devices.
- **Easy Labeling and Identification**: Ports on patch panels can be labeled, making it easier to identify and trace network connections.

- **Protection Against Cable Damage:** They protect network cables from damage and wear and tear caused by frequent movement or disconnections.
- **Standardized Interface:** They provide a standardized interface for connecting different types of network devices using patch cables.

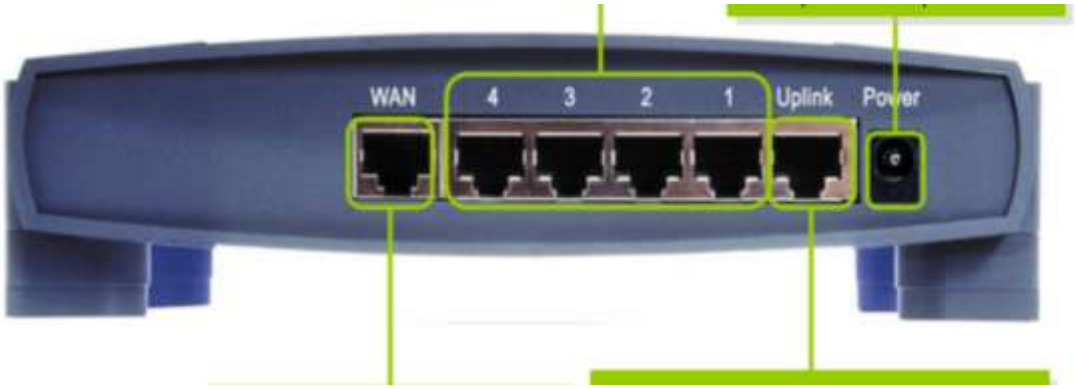
✓ **Back panel**

The back panel is typically the side of a device that contains the ports, connectors, and other external interfaces. It is used to connect the device to external devices, power sources, and networks.

In contrast to the front of panel, which houses LEDs, status indicators, and other user-facing elements.

Here are some pictures illustrating the differences between the front and back of panel in networking:

Picture: *Front Panel of a router*



Picture: Back panel of router

- **Mounting Base:**

A mounting base is a physical component that provides a stable and secure foundation for attaching network devices to a wall, rack, or other surface.

- **Rear**

The term "rear" in network equipment mounting typically refers to the back or posterior side of a network device where various ports, connectors, and other external interfaces are located.

5. Mounting Safety in LAN installation

Mounting Safety in LAN installation refers to the practices and precautions taken to ensure the safe and secure installation of network hardware, cables, and support structures.

It includes the following key aspects:

1. **Proper Mounting Equipment**: Using the correct mounts, brackets, and anchors that can safely support the weight and size of network devices like switches, routers, and racks.
2. **Securing Cables and Connections**: Ensuring that all cables are properly fastened and managed to prevent damage, tripping hazards, or signal degradation due to stress or bending.
3. **Load Management**: Ensuring that racks or mounting brackets are not overloaded with equipment beyond their capacity, which could lead to failure or collapse.
4. **Grounding and Bonding**: Ensuring proper electrical grounding to protect equipment and personnel from electric shocks, and bonding metal structures to prevent static build-up.
5. **Environmental Considerations**: Taking into account factors such as humidity, temperature, and dust, which can affect both equipment and personnel safety, ensuring the installation is in a suitable and secure location.
6. **Personal Protective Equipment (PPE)**: Ensuring that installers wear appropriate safety gear, such as safety glasses, gloves, and appropriate footwear.

6. Application of Mounting Standards

Mounting can be applied in various locations and scenarios within a LAN installation.

Here are key areas where mounting is commonly applied:

- **Network Rooms (Server Rooms/Closets)**

  - ✓ **Racks and Cabinets**: Mounting is widely used in network or server rooms where racks or cabinets hold multiple network devices such as switches, routers, firewalls, and servers. These racks are typically floor-mounted or wall-mounted to maximize space and organize devices.
  - ✓ **Patch Panels**: Patch panels are mounted in racks to organize and manage connections between the backbone network and individual devices.

- **Office Spaces/ Homes and Small Businesses**

  - ✓ **Wall-Mounted Routers and Modems**: In residential setups or small businesses, network devices such as routers, modems, or small switches are often mounted on walls to reduce clutter and provide central access points for network connectivity.

- ✓ **Ceiling or Wall-Mounted Wi-Fi Extenders/ Wireless Access Points**: In larger homes, office or buildings, Wi-Fi extenders can be mounted on ceilings or walls to boost signal strength in areas that experience weak connectivity.

- **Data Centers**

  - ✓ **Rack-Mounted Servers and Storage:** In data centers Servers, storage units, network switches, and power management systems (PDUs and UPS units) are typically mounted in floor-standing racks to allow for maximum scalability, proper airflow, and easy cable management.
  - ✓ **Cable Trays and Ladder Racks**: To organize the large number of network and power cables, overhead cable trays or ladder racks are used to mount and route cables in a structured and safe manner.

- **Public and Commercial Buildings**

  - ✓ **Security Devices**: In public areas such as retail stores, airports, or hospitals, surveillance cameras, motion sensors, and other security devices are mounted on walls or ceilings to monitor critical areas and ensure safety.

- **Outdoor Environments**

  - ✓ **Outdoor Wireless Access Points**: In campuses, parks, or other outdoor environments, wireless access points and antennas are mounted on poles, walls, or rooftops to provide wide area network coverage.
  - ✓ **Surveillance Cameras**: In outdoor environments, security cameras may be mounted on building exteriors, poles, or even trees to monitor the surroundings and provide security coverage.

- **Conference and Meeting Rooms**

  - ✓ **Audio-Visual (AV) Equipment**: In conference rooms, projectors, monitors, or speakers may be mounted to support network-connected AV systems. These mounts help conserve space and keep the room tidy for meetings.

- **Healthcare Facilities**

  - ✓ **Wall-Mounted Medical Equipment**: In hospitals or clinics, network-connected medical devices like patient monitors, RFID systems, and nurse call systems are mounted on walls or beds to provide immediate access while maintaining a clean and organized environment.

Practical Activity 2.3.2: Mounting LAN Equipment

Task:

1: Observe the trainer while identifying the necessary tools for the mounting process, take notes and ask questions as needed.

2: Proceed to the workshop and complete the task outlined below:

At your school, new network switches need to be installed in a central location within the staff room to ensure easy access for staff members' connections. Head to the NIT Workshop and complete the following tasks:

i. Mount rackmount on the wall or stands.
ii. Fix switch and patch panel onto mounted Rack.
iii. Mount the router directly on the wall
iv. Mount an access point on the ceiling of the workshop.
v. Finally mount the Antenna or access point on the pole outside of the workshop

3: Gather/collect all necessary tools and Materials needed during mounting process

4: Select the appropriate mounting location

5: Observe the trainer as mounting the rack on the wall and how to fix switch and patch panel into rackmount take notes and ask questions as needed.

6: Individually repeat the task of mounting the rack and securing the switch and patch panel into the rack mount.

7: Request assistance whenever necessary.

8: Observe the demonstration carefully and take notes on the process of mounting the access point on the ceiling.

9: Individually repeat the task of Mounting an access point on the ceiling of the workshop

10: Ask for assistance where is needed

11: Ask trainees to read key readings 2.3.2 in the trainee manual

Key readings 2.3.2

NECESSARY TOOLS FOR MOUNTING NETWORK DEVICES

Here's a list of necessary tools you might need while Mounting network devices

1. **Rack Screws and Cage Nuts**: Essential for securing devices to rack rails.
2. **Screwdrivers**:
    - ✓ **Phillips Head Screwdriver**
    - ✓ **Flathead Screwdriver**
3. **Wrenches or Nut Drivers**: For tightening bolts and nuts associated with mounting hardware.
4. **Rack Mounting Brackets and Rails**: used to house servers, routers, switches, and other hardware devices in a compact, organized manner.
   Some equipment requires specific brackets or rails provided by the manufacturer in rackmount kit.
5. **Level**: To ensure devices are mounted evenly and to maintain an organized rack.
6. **Label Maker or Labels**: For labeling cables, ports, and devices to keep track of connections.
7. **Flashlight or Headlamp**: Useful in dimly lit rack environments.
8. **Power Drill or Screw Gun**: May be needed for installing racks or drilling mounting holes.
9. **Measuring Tape**: For precise placement and to ensure equipment fits in the designated space.
10. **Documentation Materials**:
    - ✓ **Notepad and Pen**: For taking notes during installation.
    - ✓ **Installation Manuals**: Manufacturer's guides for specific equipment.

RACK-MOUNTING

Mounting a rack for LAN equipment is essential for organizing and securing your networking gear. Here’s a step-by-step guide to help you through the process:

1. **Planning and Preparation**
   - **Assess Requirements:** Determine the equipment needed, such as switches, routers, patch panels, and servers.
   - **Select a Rack:** Choose an appropriate rack or cabinet that fits your equipment and allows for future expansion.
   - **Gather Tools:** Ensure you have all necessary tools, including screwdrivers, power drills, cable ties, and mounting brackets.
2. **Choosing a Location**
   - **Find a Suitable Spot:** Select a location that provides optimal access, ventilation, and proximity to power sources and network connections.
   - **Check Floor and Wall Structure:** Ensure the floor or wall can support the weight of the rack and equipment. For wall-mounted racks, locate studs for secure mounting.
3. **Rack Assembly and Placement**
   - **Assemble the Rack:** Follow the manufacturer's instructions to assemble the rack if it's not pre-assembled.
   - **Position the Rack:** Place the rack in an optimal location with sufficient space for ventilation and access to power sources.
4. **Mounting Equipment**
   - **Install Rails and Brackets:** Attach the mounting rails and brackets to the rack according to the equipment specifications.
   - **Mount Patch Panels:** Start by mounting patch panels at the top of the rack for easier cable management.
   - **Install Network Switches and Routers:** Securely mount switches and routers below the patch panels, ensuring they are accessible for cable connections.
   - **Mount Servers:** If applicable, mount servers in the rack using appropriate rails and brackets.

WALL-MOUNTING

Mounting LAN devices on the wall is a practical solution for small spaces or when a full-sized rack is not necessary. Here's a step-by-step guide to help you through the process:

1. **Planning and Preparation**
   - **Assess Requirements:** Identify the equipment that will be wall-mounted, such as switches, patch panels, and routers.
   - **Select a Wall-Mount Rack or Bracket:** Choose a suitable wall-mount rack or bracket that fits your equipment and supports the required weight.
   - **Gather Tools:** Ensure you have all necessary tools, including a drill, screwdrivers, level, measuring tape, and mounting hardware.
2. **Choosing a Location**

- **Find a Suitable Spot:** Select a location that is easily accessible, has adequate ventilation, and is close to power sources and network connections.
- **Check Wall Structure:** Ensure the wall can support the weight of the equipment. For heavy equipment, it's best to mount on studs or use appropriate wall anchors.

3. **Marking and Drilling**
   - **Measure and Mark:** Use a measuring tape and level to mark the positions for the mounting holes on the wall.
   - **Drill Holes:** Drill holes at the marked positions, ensuring they are the correct size for the mounting hardware.
4. **Mounting the Bracket or Enclosure**
   - **Attach the Bracket or Enclosure:** Secure the wall-mount bracket or enclosure to the wall using screws and anchors. Ensure it is level and firmly attached.
   - **Double-Check Stability:** Ensure the bracket or enclosure is securely mounted and can support the weight of the equipment.
5. **Mounting Equipment**
   - **Install Patch Panels:** Start by mounting patch panels at the top of the bracket or enclosure for easier cable management.
   - **Mount Network Switches and Routers:** Securely mount switches and routers below the patch panels, ensuring they are accessible for cable connections.
   - **Install Wireless Access Points (WAPs):** If mounting WAPs, attach them to the bracket or enclosure according to the manufacturer's instructions.
   - **Mount Additional Devices:** Securely attach any additional devices, such as cameras or network sensors, to the bracket or enclosure.

CEILING-MOUNTING

Mounting LAN equipment on the ceiling can be a great way to optimize network coverage and save space, especially for wireless access points (WAPs) and surveillance cameras. Here's a detailed step-by-step guide to help you through the process:

1. **Planning and Preparation**
   - **Assess Requirements:** Identify the equipment that will be ceiling-mounted, such as wireless access points, cameras, or other network devices.
   - **Select Mounting Hardware:** Choose appropriate ceiling-mount brackets, enclosures, or mounts that fit your equipment and support the required weight.
   - **Gather Tools:** Ensure you have all necessary tools, including a drill, screwdrivers, measuring tape, level, and mounting hardware.
2. **Choosing a Location**

- **Find a Suitable Spot:** Select a location that provides optimal coverage and is accessible for maintenance. Ensure it is close to power sources and network connections if necessary.
- **Check Ceiling Structure:** Ensure the ceiling can support the weight of the equipment. For heavy equipment, it's best to mount on ceiling joists or use appropriate anchors.

3. **Marking and Drilling**
   - **Measure and Mark:** Use a measuring tape and level to mark the positions for the mounting holes on the ceiling.
   - **Drill Holes:** Drill holes at the marked positions, ensuring they are the correct size for the mounting hardware.
4. **Mounting the Bracket or Enclosure**
   - **Attach the Bracket or Enclosure:** Secure the ceiling-mount bracket or enclosure to the ceiling using screws and anchors. Ensure it is level and firmly attached.
   - **Double-Check Stability:** Ensure the bracket or enclosure is securely mounted and can support the weight of the equipment.
5. **Mounting Equipment**
   - **Install Wireless Access Points (WAPs):** If mounting WAPs, attach them to the bracket or enclosure according to the manufacturer's instructions.
   - **Mount Cameras or Other Devices:** Securely attach any additional devices, such as cameras or network sensors, to the bracket or enclosure.

POLE-MOUNTING

Mounting LAN equipment on a pole is a practical solution for extending network coverage in outdoor or large indoor areas. Here's a detailed step-by-step guide to help you through the process:

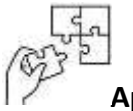
1. **Planning and Preparation**
   - **Assess Requirements:** Identify the specific equipment to be pole-mounted, such as wireless access points (WAPs), cameras, or antennas.
   - **Select Mounting Hardware:** Choose appropriate pole-mount brackets, clamps, or enclosures that fit your equipment and can support its weight.
   - **Gather Tools:** Ensure you have all necessary tools, including wrenches, screwdrivers, measuring tape, level, and any mounting hardware provided with the equipment.
2. **Choosing a Location**
   - **Find a Suitable Spot:** Select a pole that provides optimal coverage and is accessible for maintenance. Ensure it is close to power sources and network connections if necessary.

- **Check Pole Structure:** Ensure the pole is sturdy and can support the weight of the equipment. For new installations, consider using a durable pole made of materials like steel or aluminum.

3. **Marking and Preparing the Pole**
   - **Measure and Mark:** Use a measuring tape and level to mark the positions for the mounting brackets on the pole.
   - **Clean the Pole:** Ensure the pole surface is clean and free of debris to ensure a secure attachment.
4. **Mounting the Bracket or Clamp**
   - **Attach the Bracket or Clamp:** Secure the pole-mount bracket or clamp to the pole using the provided hardware. Tighten the bolts or screws to ensure the bracket is firmly attached.
   - **Double-Check Stability:** Ensure the bracket or clamp is securely mounted and can support the weight of the equipment.
5. **Mounting Equipment**
   - **Install Wireless Access Points (WAPs):** If mounting WAPs, attach them to the bracket or clamp according to the manufacturer's instructions.
   - **Mount Cameras or Antennas:** Securely attach any additional devices, such as cameras or antennas, to the bracket or clamp.
   - **Adjust Position:** Adjust the position and angle of the equipment to ensure optimal coverage and performance.

Points to Remember

- **Step-by-step guide to mount a network switch in a small office:**
  - ✓ Gather the necessary tools and materials:
  - ✓ Choose the mounting location:
  - ✓ Marking and Drilling Holes
  - ✓ Attach the mounting brackets
  - ✓ Mount the equipment



Application of learning 2.3.

X School, a TVET institution, is expanding its internet connection from the Administration Block to the Computer Lab. In the initial phase, the IT team conducted a site survey for the LAN installation, developed a network design. In the second phase, XY cabling company completed cable trunking, pulling, and laying. In the third phase, DT company completed network equipment mounting.

The last phase, the school needs to hire a specialized company to Label, Terminate and apply network cable Patching where is necessary.

Indicative content 2.4: Connecting LAN Devices

Duration: 3 hrs

Theoretical Activity 2.4.1: Describing labelling in LAN installation

Tasks:

1: Engage in the discussion about labelling and its importance in network management and performance.

2: Observe the trainer as is demonstrating tools used for labelling.

3: Form small groups, then read key reading 2.4.1 in the trainee's manual and discuss the Types of Labels, Labelling Standards, and Labelling Schemes.

4: Participate in the activity and seek clarification if they encounter any uncertainties.

5: Present your findings to the class

6: Listen attentively as the trainer providing expert view take notes and ask clarifying questions if needed.

7: Ask questions if you have any.

Key readings 2.4.1.:

Labelling involves identifying and categorizing network components, such as cables, ports, devices, and rooms, to provide a clear and understandable structure.

Proper labelling helps network administrators quickly identify and trace cables, devices, and connections within the network infrastructure.

What to Label:

1. **Cables**: Each cable should be labeled at both ends to indicate its origin and destination.
2. **Ports**: Network ports on switches, routers, patch panels, and wall plates should be labeled to show their connection points.
3. **Devices**: Network devices such as servers, switches, routers, and access points should have labels indicating their function and network segment.

4. **Patch Panels**: Each port on a patch panel should be labeled to show the corresponding device or wall plate it connects to.
5. **Racks and Cabinets**: Label racks and cabinets to indicate the equipment contained and its function within the network

TYPES OF CABLE LABELS

The common types of cable labels are:

1. Wrap-Around Cable Labels:

These labels wrap around the cable, creating a secure fit. They are durable and can withstand various environmental conditions.

It is ideal for labeling network cables in environments where durability is required, such as data centers.

2. Flag Cable Labels:

These labels form a flag around the cable, providing additional space for more detailed information.

It is commonly used for cables requiring extensive identification, such as fiber optic cables or cables with multiple conductors.

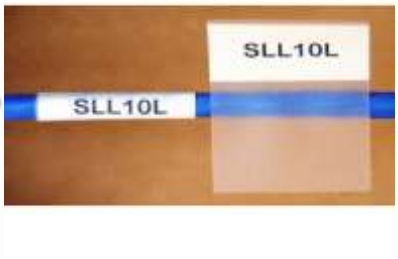



3. Self-Laminating Cable Labels:

These are made of a printable area covered by a clear protective laminate that wraps around the cable.

It is suitable for cables exposed to harsh conditions, such as moisture or chemicals, as the laminate provides extra protection.





4. Heat Shrink Tube Labels

Heat-shrinkable tubes that are printed with identification information and then shrunk to fit tightly around the cable.

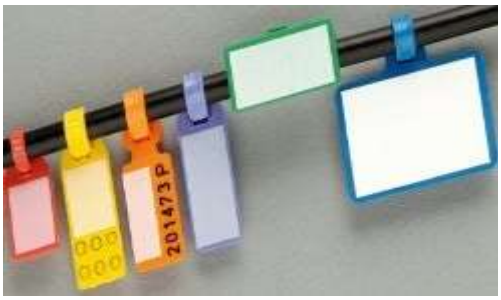
It is ideal for environments where the label needs to be tamper-resistant or exposed to extreme conditions.

5.Cable Tags: Often made from durable materials like PVC or metal, these tags are attached to cables using ties or clips and are suitable for harsh environments.

6. Write-On Cable Labels

These labels have a writable surface, allowing for manual labeling with a pen or marker.

It is convenient for quick identification or when customization is needed on-site.




7. Color-Coded Cable Labels

Labels that use color-coding for quick visual identification.

It is often used in environments where cables need to be grouped by function, such as in large network installations.



Importance of Labelling in LANs

- Clear labeling helps network administrators quickly identify and locate specific components, reducing troubleshooting time and minimizing downtime.
- Proper labeling helps keep the network organized, making it easier to identify cables, ports, and devices.
- When network issues arise, labeled cables and ports allow for quicker identification and resolution of problems.
- Regular maintenance and upgrades are simpler when components are clearly labeled.
- Labeling aids in creating accurate network documentation, which is essential for future reference and planning.

TYPES OF LABELLING

There are several types of labelling used in LAN installations, each serving a different purpose depending on the network components they are attached to. These labels ensure

that network components can be easily identified and managed during maintenance, troubleshooting, or upgrades.

Here's different types of labelling in LAN environments:

1. Cable Labels:

Identify individual network cables and trace them from one connection point to another.

- **Common Uses**:
  - ✓ Label both ends of cables to show their connection points (e.g., from patch panel to device).
  - ✓ Differentiate between data cables, power cables, fiber optic cables, etc.
- **Label Types**:
  - ✓ **Wrap-around Labels**: Adhesive labels wrapped around the cable, typically with clear text or color-coding.
  - ✓ **Heat-Shrink Labels**: Labels that shrink when heated, ensuring a tight fit around the cable.
  - ✓ **Flag Labels**: These stick out like flags from the cable, offering more surface area for information.
- **Example**: "D-101-SW1-01" (Data cable from Room 101 to Switch 1, Port 1).

2. Patch Panel Labels

Identify the ports on patch panels that connect network cables to other devices or rooms.

- **Common Uses**:
  - ✓ Ensure proper connection tracking between patch panels and connected devices.
  - ✓ Help technicians quickly locate specific connections during troubleshooting.
- **Label Types**:
  - ✓ **Port Labels**: Stickers placed directly next to each port, often indicating port number or destination.
  - ✓ **Pre-numbered Strips**: A strip across the top or bottom of the panel with port numbers for easy identification.
- **Example**: "PP1-P12" (Patch Panel 1, Port 12).

3. Device Labels

Identify network hardware such as switches, routers, firewalls, and other LAN devices.

- **Common Uses**:
  - ✓ Label devices with key information like IP address, device name, function, or MAC address.
  - ✓ Aid in inventory management and troubleshooting.
- **Label Types**:
  - ✓ **Adhesive Labels**: Durable and often laminated labels placed on the device's exterior.
  - ✓ **Asset Tags**: Barcoded or QR-coded labels used for tracking and asset management.
- **Example**: "Switch-01-SRV1" (Switch 01 in Server Room 1).

4. Port and Outlet Labels

Identify network access points like wall outlets or floor boxes where devices connect to the network.

- **Common Uses**:
  - ✓ Indicate the connection to the patch panel or switch for easier troubleshooting.
  - ✓ Identify the purpose of each port (e.g., data, voice, or power).
- **Label Types**:
  - ✓ **Faceplate Labels**: Stickers or engravings on the wall outlets indicating port number and connection.
  - ✓ **Modular Labels**: Inserts that can be easily updated or replaced as needed.
- **Example**: "W-201-PP1-05" (Wall outlet in Room 201 connected to Patch Panel 1, Port 5).

5. Rack Labels

Identify racks or enclosures used to house network equipment like servers, switches, and patch panels.

- **Common Uses**:
  - ✓ Label racks to indicate the type of equipment or function (e.g., data rack, voice rack).

- ✓ Help in organizing large server rooms or data centers.

- **Label Types**:
  - ✓ **Rack Unit Labels**: Numbered stickers placed alongside each unit space to identify device placement.
  - ✓ **Rack ID Labels**: Larger labels identifying the entire rack or section.
- **Example**: "Rack-03-Server" (Rack 03 housing servers).

6. Room or Area Labels

Identify rooms, cabinets, or enclosures where network equipment or cabling is located.

- **Common Uses**:
  - ✓ Label specific rooms like server rooms, network closets, or telecommunications enclosures.
  - ✓ Help technicians navigate large installations with multiple network areas.
- **Label Types**:
  - ✓ **Room Number Labels**: Clear labels placed on the door or entry point to identify specific network rooms.
  - ✓ **Enclosure Labels**: Labels for enclosed cabinets or telecom closets.
- **Example**: "SRV-RM-2F" (Server Room on the 2nd floor).

Practical Activity 2.4.2: Labelling the LAN installation

Task:

1: Introduce the activity by reviewing some key points from Theoretical Activity 2.4.1.

Your school is a growing school that has new local area network installed. The office consists of multiple departments, including DOS, BURSAR, and SECRETARY each with its own set of devices (laptop, printer, server). The school has decided to implement a clear labeling system to facilitate easy management and troubleshooting of the network.

As network technician go in your workshop, build a network similar to the scenario and perform the following task:

a. Lebel (All network cables connecting devices to the switch, Ports on the switch, Wireless access point and Devices in each department (laptops, printers, servers).
b. Finally Document the setup by creating a network diagram that reflects the labeling scheme.

2: Work collaboratively within your assigned teams to complete the tasks related to their specific department, and do the following:

- ✓ Discuss and create a labeling scheme that fits the scenario.
- ✓ Create and apply their labels to the appropriate devices and cables.
- ✓ Fill out the network diagram and inventory list based on their labeling.

3: Ask for assistance where is needed

4: Presents your labeling scheme, the labels they created, and your network diagram, explaining your choices and any challenges you encountered.

5: Listen attentively as the trainer explains and ask clarifying questions if needed

6: Read key readings 2.4.2 in the trainee manual.

Key readings 2.4.2

How to Label

1. **Label Maker**: Use a label maker with durable, easy-to-read labels. Ensure the labels are resistant to wear and tear.
2. **Color Coding**: Implement a color-coding scheme for different types of cables (e.g., blue for data, yellow for voice, red for power).
3. **Numbering System**: Use a consistent numbering system for cables and ports, starting from one end of the network and moving sequentially.
4. **Clear Descriptions**: Labels should include clear descriptions such as "Server Room to Office 101" or "Switch 1 Port 24".
5. **Double-Check**: Double-check labels for accuracy before finalizing the installation.

Labeling Best Practices

1. **Plan Ahead**: Plan your labeling system before starting the installation to ensure consistency.

2. **Be Consistent**: Maintain consistency in labeling format and terminology throughout the network.
3. **Use Quality Labels**: Invest in high-quality labels that won't fade or peel over time.
4. **Document the System**: Create a detailed document of your labeling system, including a map of the network and a legend for any color codes or abbreviations used.
5. **Regular Updates**: Update labels and documentation whenever changes are made to the network.

Examples of Labels

1. **Cable Label**:
   - ✓ "SW1-P01 to SR1-01" (Switch 1, Port 1 to Server Room 1, Port 1)
2. **Port Label**:
   - ✓ "Patch Panel A, Port 1 to Office 101"
3. **Device Label**:
   - ✓ "Main Router, Floor 1"
4. **Rack Label**:
   - ✓ "Rack 1: Core Switches"
5. **Wall Plate Label**:
   - ✓ "WP-101-A" (Wall Plate in Room 101, Jack A)

Theoretical Activity 2.4.3: Describing cable terminating and patching in LAN installation

Tasks:

1: Listen attentively to the introduction and take notes on key points

2: Observe the presentation of the tools and materials used for cable termination and patching, take notes and ask questions to enhance your understanding of each item's purpose and use.

3: Collaborate in your small groups, read and discuss on cable termination and patching from key reading 2.4.3 in your manual and share insights.

4: Ask questions and seek clarification if needed for a better understanding.

5: Note dawn key points from their findings.

6: Present your findings to the class.

7: Ask questions and seek clarification if needed.

Key readings 2.4.3.:

CABLE TERMINATING AND PATCHING

Cable terminating and patching are crucial steps in LAN (Local Area Network) installation. Proper techniques ensure network reliability and performance. Here's a detailed description of both processes:

- **Cable Terminating**

Cable terminating involves attaching connectors to the ends of network cables, allowing them to be plugged into devices, patch panels, or wall jacks.

Tools and Materials

1. **Cables**: Typically Cat5e, Cat6, Cat6a, or Cat7.
2. **RJ45 Connectors**: Common connectors for Ethernet cables.
3. **Crimping Tool**: Used to attach the RJ45 connectors to the cable.
4. **Cable Stripper**: Strips the outer insulation of the cable without damaging the inner wires.
5. **Punch Down Tool**: For terminating cables into keystone jacks or patch panels.
6. **Cable Tester**: Ensures the cable is terminated correctly and is functional.

Steps

1. **Strip the Cable**: Use the cable stripper to remove about 1 inch (2.5 cm) of the outer jacket, exposing the twisted pairs.
2. **Untwist and Arrange Wires**: Untwist the wire pairs and arrange them in the correct order according to the T568A or T568B wiring standard.
3. **Cut Wires to Length**: Trim the wires to ensure they are even and will fit into the RJ45 connector.

4. **Insert Wires into RJ45 Connector**: Push the wires into the connector, ensuring each wire is in the correct slot.
5. **Crimp the Connector**: Use the crimping tool to secure the connector onto the cable.
6. **Test the Cable**: Use a cable tester to verify proper termination and connectivity.

- **Cable Patching**

Cable patching involves connecting devices to the network using patch cables, which are short Ethernet cables, typically from a patch panel to a switch or from a wall jack to a device.

Tools and Materials

1. **Patch Cables**: Pre-made or custom Ethernet cables of varying lengths.
2. **Patch Panels**: Centralized panels where cables are terminated and organized.
3. **Network Switches**: Devices that connect multiple devices on a network.
4. **Cable Management Accessories**: Such as cable ties, Velcro straps, and management panels to keep cables organized.

Steps

1. **Plan the Layout**: Determine the path and length of each patch cable.
2. **Select Patch Cables**: Choose the appropriate length and category of patch cables.
3. **Connect Patch Cables**: Plug one end of the patch cable into the patch panel and the other end into the switch port or device.
4. **Organize Cables**: Use cable management accessories to keep the cables neat and avoid tangling.
5. **Label Connections**: Label both ends of the patch cable for easy identification and future troubleshooting.
6. **Test Connectivity**: Ensure that each patched connection is working correctly by testing connectivity.

Best Practices

1. **Use Quality Components**: Ensure all cables, connectors, and patch panels are of high quality to avoid connectivity issues.

2. **Follow Standards**: Adhere to T568A or T568B wiring standards for consistency.
3. **Maintain Cable Integrity**: Avoid bending or twisting cables excessively to prevent damage.
4. **Keep Cables Organized**: Use proper cable management techniques to maintain an orderly setup.
5. **Document Connections**: Keep detailed documentation of all terminations and patch connections for future reference and troubleshooting.

Examples

- **Terminating a Cat6 Cable**:
  - ✓ Strip the cable, arrange the wires according to T568B, insert into the RJ45 connector, and crimp securely.
- **Patching in a Data Center**:
  - ✓ Connect patch cables from a patch panel to switch ports, ensuring cables are neatly managed and labeled, and test each connection for network access.

Practical Activity 2.4.4: Cable terminating and patching in LAN installation

Task:

1: Wear the PPE and perform the task described below:

As Network Technician, go workshop and patch cables to Patch panel that you have been installed at Practical activity 2.3.2. Secondary, terminate another end of cable with connectors (RJ-45 and RJ-11) to allows devices like computers, printers, and phones to connect to the network.

2: List out the tools/Instrument, Material and equipment required in Cable terminating and patching.

3: Gather all necessary tools and Materials needed during cable termination and patching process

4: Observe the step-by-step demonstration carefully and take notes on how to apply patching at one end of the cable and termination at the other end.

5: Work independently to complete task 2.4.4, utilizing the skills and knowledge they gained from step 4.

6: Actively seek help and guidance when necessary while working on their tasks.

7: Practice the task repeatedly until they reach a satisfactory level

8: Read key readings 2.4.4 in the trainee manual.

Key readings 2.4.4

CABLE TERMINATING

Performing cable terminating and patching in a LAN installation involves several detailed steps to ensure a reliable and efficient network. Here's a comprehensive guide on how to perform these tasks:

Tools and Materials

1. **Cables**: Cat5e, Cat6, Cat6a, or Cat7.
2. **RJ45 Connectors**: Standard connectors for Ethernet cables.
3. **Crimping Tool**: For securing RJ45 connectors to the cable.
4. **Cable Stripper**: To remove the outer insulation of the cable.
5. **Punch Down Tool**: For terminating cables into keystone jacks or patch panels.
6. **Cable Tester**: To verify the termination and connectivity of the cables.

Steps to Terminate an Ethernet Cable

1. **Strip the Cable**:
   - ✓ Use the cable stripper to remove about 1 inch (2.5 cm) of the outer jacket, exposing the inner twisted pairs of wires.
2. **Untwist and Arrange Wires**:
   - ✓ Untwist the wire pairs and arrange them according to either the T568A or T568B wiring standard. T568B is more common in the U.S.
   - ✓ The order for T568B is:
     - Pin 1: White/Orange
     - Pin 2: Orange
     - Pin 3: White/Green
     - Pin 4: Blue
     - Pin 5: White/Blue
     - Pin 6: Green
     - Pin 7: White/Brown
     - Pin 8: Brown
3. **Cut Wires to Length**:
   - ✓ Ensure the wires are even and cut them to fit into the RJ45 connector properly.
4. **Insert Wires into RJ45 Connector**:
   - ✓ Push the wires into the connector, ensuring each wire is in the correct slot. The wires should reach the end of the connector.

5. **Crimp the Connector**:
    - ✓ Use the crimping tool to secure the connector onto the cable. This process also connects the metal contacts within the connector to the wires.
6. **Test the Cable**:
    - ✓ Use a cable tester to verify that the cable is terminated correctly and is functional.

CABLE PATCHING

Tools and Materials

1. **Patch Cables**: Short Ethernet cables.
2. **Patch Panels**: Panels where cables are terminated and organized.
3. **Network Switches**: Devices that connect multiple devices on a network.
4. **Cable Management Accessories**: Cable ties, Velcro straps, and management panels.

Steps to Patch Cables in a LAN

1. **Plan the Layout**:
    - ✓ Determine the path and length of each patch cable. Identify the ports on the patch panel and switch that will be connected.
2. **Select Patch Cables**:
    - ✓ Choose the appropriate length and category of patch cables. Ensure they are suitable for the network's speed and bandwidth requirements.
3. **Connect Patch Cables**:
    - ✓ Plug one end of the patch cable into the appropriate port on the patch panel and the other end into the corresponding port on the switch or device.
4. **Organize Cables**:
    - ✓ Use cable management accessories to keep the cables neat and avoid tangling. Ensure that cables are routed cleanly and do not obstruct access to other components.
5. **Label Connections**:
    - ✓ Label both ends of the patch cable for easy identification and future troubleshooting. Labels should include information such as the source and destination of the connection.
6. **Test Connectivity**:
    - ✓ Ensure that each patched connection is working correctly by testing the connectivity and functionality of the network devices.

Example Scenario

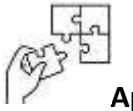
1. **Terminating a Cat6 Cable**:
    - ✓ You have a Cat6 cable that needs to be terminated with an RJ45 connector. Strip the cable, arrange the wires in the T568B order, insert them into the connector, and crimp securely. Test with a cable tester to confirm functionality.
2. **Patching in an Office Network**:
    - ✓ Connect patch cables from the patch panel in the network closet to the ports on the network switch. Ensure cables are neatly organized and labeled. Test each connection to confirm network access.

Best Practices

1. **Use Quality Components**: Ensure all cables, connectors, and patch panels are of high quality.
2. **Follow Standards**: Adhere to T568A or T568B wiring standards for consistency.
3. **Maintain Cable Integrity**: Avoid bending or twisting cables excessively.
4. **Keep Cables Organized**: Use proper cable management techniques.
5. **Document Connections**: Keep detailed documentation of all terminations and patch connections for future reference.

Points to Remember

- **Importance of Labeling:**
  Proper labeling helps keep the network organized, making it easier to identify cables, ports, and devices. When network issues arise, labeled cables and ports allow for quicker identification and resolution of problems,……..
- The network equipments that are necessarily to label include: Cables, Ports, Devices, Patch Panels, Racks and Cabinets
- **Cable Terminating:** Cable terminating involves attaching connectors to the ends of network cables, allowing them to be plugged into devices, patch panels, or wall jacks.
- **Cable Patching:** Cable patching involves connecting devices to the network using patch cables, which are short Ethernet cables, typically from a patch panel to a switch or from a wall jack to a device



Application of learning 2.4

A new educational institution, KK University, is being established. The institution requires a robust network infrastructure to connect classrooms, administrative offices, a library, and a computer lab. The IT team assesses the building layout and determines the number of classrooms, offices, and common areas that need network access.
They decide to install Ethernet drops in each classroom, office, and common area, as well as a central network closet for the main equipment.
Institution planned the work in two batch. First **Batch No.1** has dealt by running Bulk Cat6 cables from the central network closet to each classroom, office, and common area. And cables are pulled through walls and ceilings to reach designated locations.

They want to hire a Network Technician to complete Batch **No.2** of the following Job specifications:

- ✓ Terminating cables with RJ-45 connectors and install into wall outlets, at each classroom and office.
- ✓ Patching Short patch cables used to connect the ports on the patch panel to network switches located in the network closet.

Learning outcome 2 end assessment

Written assessment

PART I: Match each statement on the left with the correct term or tool on the right.

No	Functions	Tool
1…….	1. Conducts a site survey to assess the layout	A. Frequent disconnects and slowdowns
2…….	2. Used to organize and protect network cables	B. Crimping tool
3…….	3. Tests Ethernet cables for proper connections	C. Troubleshooting ease
4…….	4. Terminating Ethernet cables with these connectors	D. Network documentation
5…….	5. Helps in keeping cables organized and labeled	E. RJ45 connectors
6……	6. Plan for this to handle additional devices and traffic	F. Future scalability
7……	7. Detailed layout for future maintenance	G. Cable management tools
8……	8. Tool used to terminate Ethernet cables	H. Site survey
9……	9. Main benefit of labeling cables	I. Cable trays and conduits
10…..	10. Common issue with poorly organized cabling	J. Cable tester

PART II: Fill in the Blank with the appropriate term:

1. The first step in performing cabling for a LAN is conducting a _____ survey.
2. Cable _____ and conduits are used to organize and protect network cables.
3. A _____ tester is used to ensure proper connections and functionality of terminated Ethernet cables.
4. Ethernet cables are terminated with _____ connectors.
5. Using _____ tools such as zip ties and cable labels helps in keeping cables organized.
6. Planning for future _____ ensures the network can handle additional devices and increased traffic.
7. Creating a detailed cabling layout _____ helps in future maintenance and troubleshooting.

8. A _____ tool is used to terminate Ethernet cables with RJ45 connectors.
9. Labeling cables makes _____ easier by providing clear identification.
10. A poorly organized cabling system can lead to frequent _____ and network slowdowns.

PART III: Answer by true for correct statement and False for incorrect statement

1. Conducting a site survey is an optional step when performing cabling for a LAN.
2. It is important to choose Ethernet cables based on the required bandwidth and distance.
3. Cable trays and conduits help in organizing and protecting network cables.
4. Terminating Ethernet cables with RJ45 connectors requires the use of a soldering iron.
5. Cable testers are used to ensure proper connections and functionality of terminated Ethernet cables.
6. Labeling cables during the cabling process makes troubleshooting easier.
7. Creating a detailed cabling layout document is unnecessary for future maintenance.
8. Planning for future scalability is important to ensure the network can handle additional devices and increased traffic.
9. Installing cable trays and conduits can prevent physical damage to network cables.
10. A poorly organized cabling system can lead to frequent disconnects and network slowdowns.
11. Running Ethernet cables through exposed areas without protection is a best practice.
12. Using cable management tools such as zip ties and cable labels is important for keeping cables organized.
13. It is not necessary to test each Ethernet cable after terminating it.
14. A well-organized cabling layout does not affect network performance.
15. Documenting the cabling layout helps ensure that future maintenance and troubleshooting are easier.

Practical assessment

The Luxe Stay Hotel, is a mid-sized hotel chain, located at Kigali, NYARUGENGE District. The Hotel provides accommodations with a Gym or fitness center, free private parking, Swimming pool, Vacation Homes and other services related to Guesthouses.

The Hotel is upgrading its network infrastructure to provide guests with high-speed internet access, better connectivity for staff operations, and enhanced security systems. The existing network setup is outdated, causing frequent disruptions and slow internet speeds, which have led to guest complaints and operational inefficiencies.

The IT team has planned to complete the task in two phases. The first phase addressed network planning and effective network design. Now, it's time for the second phase, which will focus on all aspects of cabling.

Luxe Stay Hotel has decided to hire a professional network cabling company to execute the installation by implementing cabling based on the design ensuring minimal disruption to hotel operations.

END

References

Inc, T.-S. T. (April 2024). A Guide to the Different Types of Cable Labeling. Tri Star Technologies, Page 1. https://tri-star-technologies.com/blog/a-guide-to-the-different-types-of-cable-labeling/

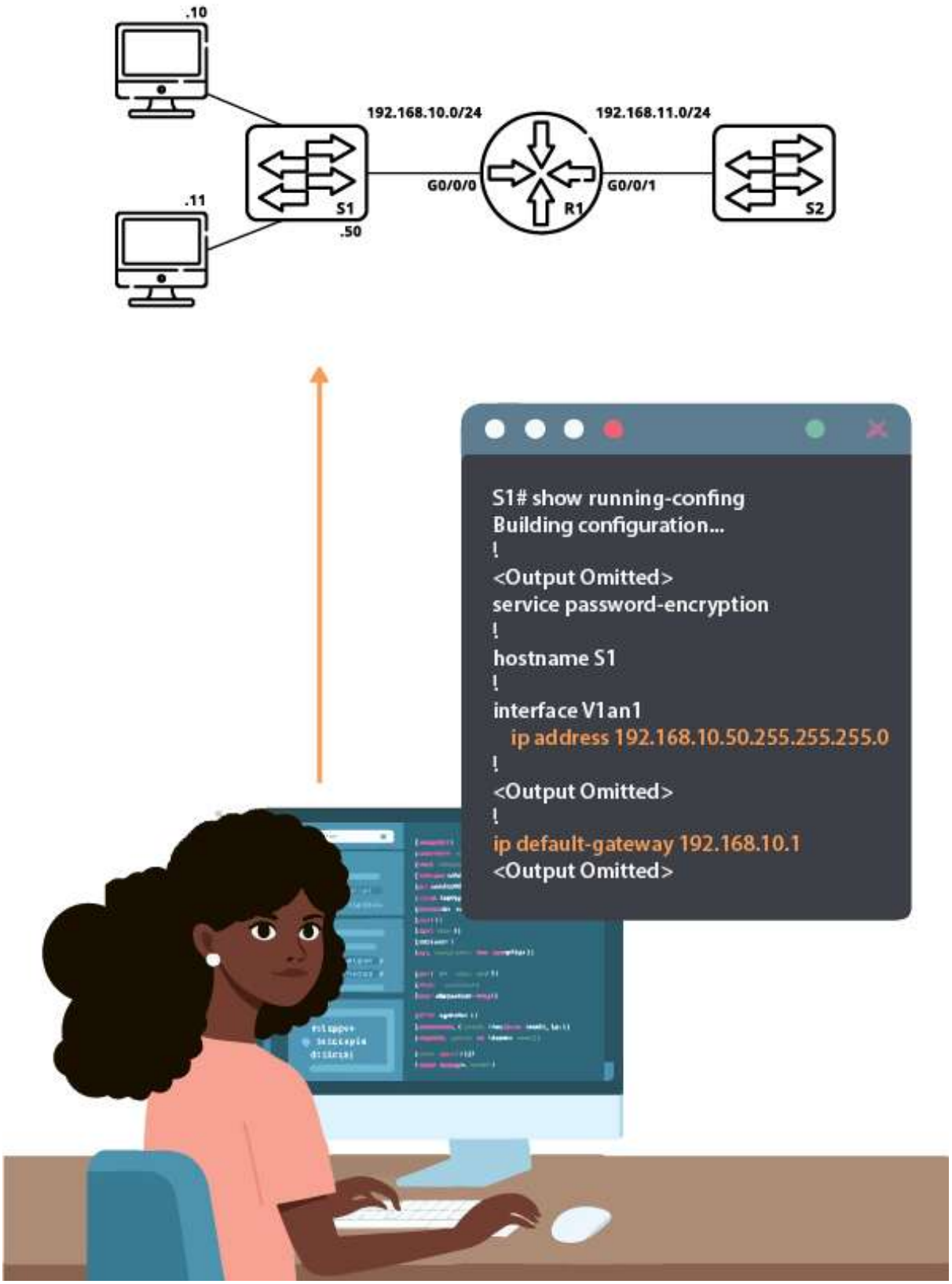
Mill, L. (2024). Cable Labelling. Caledonian, Page 1. http://www.caledoniancable.com/English/download/cable%20labelling%20systems/cable%20labelling%20systems.pdf

Organizer, C. (2024). Cable Labels & Printers. Cable Organizer, Page 1. https://www.cableorganizer.com/categories/cable-identification/

CMW, G. V. (15 March 2023). A Step-by-Step Guide To Installing Slotted Trunking. Cable Management Warehouse, Page

https://www.cmwltd.co.uk/blog/cable-management-containment/a-step-by-step-guide-to-installing-galvanised-trunking?srsltid=AfmBOorPN1nIcPhoJVLCmE3Xza9aWRjqeitVGR77_bOyiQ5g_JKHymq0

Oulu, K. (2024, 01 01). Cable Trunking System Installation and Operation Manual. Retrieved from meka.eu: https://meka.eu/wp-content/uploads/2023/01/Instal-Installation-and-Operation-Manual-Meka-1.pdf


.10
.11
S1
.50
192.168.10.0/24
G0/0/0
R1
192.168.11.0/24
G0/0/1
S2
S1# show running-confing
Building configuration...
!
<Output Omitted>
service password-encryption
!
hostname S1
!
interface V1an1
ip address 192.168.10.50.255.255.255.0
!
<Output Omitted>
!
ip default-gateway 192.168.10.1
<Output Omitted>

Indicative contents
3.1 Performing Basic IOS Configuration.
3.2 Configuration IP Address
3.3 Configuration Routing Protocols

Key Competencies for Learning Outcome 3: Configure LAN

Knowledge	Skills	Attitudes
● Description of IOS Configurations ● Description of routing protocols	● Configuring the networking devices	● Having an innovative spirit. ● Being Creative Person ● Having critical thinking

Duration: 15 hrs

Learning outcome 3 objectives:

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

1. Perform correctly basic IOS configurations based on LAN requirement
2. Configured correctly IP addresses based on LAN topology
3. Configure properly Routing protocols according to the LAN topology

Resources

Equipment	Tools	Materials
● Switch ● Router ● Computer	● Simulation software ● Tera term ● Putty ● winSCP	● Internet bundles ● Network cables

Indicative content 3.1: Performing Basic IOS Configuration

Duration: 6 hrs

Theoretical Activity 3.1.1: Description of the Basic IOS Configuration

Tasks:

1: Listen attentively to the explanation of IOS and its significance in networking, take notes and prepare to ask questions if they need further clarification.

2: Observe the presentation of Cisco devices and ask questions to enhance your understanding of how these devices operate with IOS.

3: Read key readings 3.1.1 in trainee's manual and discuss about methods of accessing a Cisco device, User Modes in IOS during router configuration

4: Participate in the discussion and seek clarification whenever they encounter uncertainties during the activity.

5: Listen carefully to the explanation of basic configuration commands and note down the key points for future reference.

6: Ask questions to clarify any doubts or seek further understanding

7: Read key readings 3.1.1 in trainee's manual about basic configuration commands

Key readings 3.1.1.:

Describing the Basic IOS Configuration

- **IOS Navigation Modes**

Cisco IOS software allows us to control the Cisco device on which it runs. IOS software contains several commands to configure and control Cisco devices. Not all these commands are the same. Some commands only provide information while others allow us to configure and control a particular feature, or a specific area of the device, or the entire device.

Based on how IOS commands affect the device, they are organised into the modes. An IOS mode is a group of commands that are used to configure similar features or to control a particular area of the device. An IOS mode is also known as the **IOS access mode** or the **IOS commands mode.**

There are five IOS modes: - user **EXEC** mode, privileged **EXEC** mode, global configuration mode, setup mode, and **ROM** Monitor mode.

The first three modes are used to view current settings and configure new settings or modify existing settings. The next two modes are used to set up the initial device configuration and troubleshoot the device in an emergency, respectively. Let's understand each mode in detail:

- **User EXEC Mode**

This is the first mode of the IOS. No matter how a user accesses the IOS, the IOS always places the user in this mode. If configured, the IOS prompts the user to enter the password to access this mode.

This mode has very limited commands that allow the user to view statistics and perform basic troubleshooting. This mode does not allow the user to change any of the settings. This mode is the starting (or entry) point of the IOS. Other modes of the IOS can only be accessed through this mode.

- **Privileged EXEC Mode**

This is the second mode of the IOS. This mode can be accessed only from the *user exec* mode by executing the **enable** command. Since the **enable** command is used to access this mode, this mode is also known as the **enable mode**.

To close this mode or to return into the *user exec* mode, use the **exit** command or the **end** command.

As the name suggests, this mode includes privileged or powerful commands. This mode is usually used for the following purposes: -

- ✓ To view, save and erase device configuration

- ✓ To take the backup of the current device configuration
- ✓ To restore the configuration from backup
- ✓ To install a new IOS image file
- ✓ To debug or troubleshoot the device
- ✓ To restart or reload the device

Although this mode allows the user to manage device configuration and IOS image files, it does not allow the user to change the device configuration. A user can change device configuration only from the *configuration mode*.

- **Global configuration mode**

As the name suggests, this mode includes the commands that are used to configure the device. From this mode, a user can not only configure new settings but can also change, update or delete existing settings.

To enter this mode, use the **'configure terminal'** command from the *privileged-exec* mode. To exit from this mode, you can use the **'end'** or the **'exit'** commands. You can also press the **CTRL + Z** key combinations.

- **Setup Mode**

When we power-on the IOS operated device, the IOS looks for the device configuration. If it does not find a valid configuration, it places the user in this mode. This mode allows the user to configure the initial device configuration.

This mode presents a text-based wizard that asks questions about initial settings in the sequence. Based on the answers provided by the user, the IOS automatically builds the initial configuration.

- **ROMMON Mode**

During the boot process, the IOS image file is loaded into the RAM. If the IOS image file is missing or corrupt, the device automatically enters this mode. This mode allows the user to troubleshoot the IOS.

In this mode, the user can select a different IOS image file to boot the device or load a new IOS image file from the TFTP server.

Cisco IOS navigation modes.

The following table lists commands that are used to navigate the different modes of the IOS.

Mode	Prompt	Command to enter	Command to exit
User EXEC	Router >	Default mode after booting. Login with the password, if configured.	Use the exit command
Privileged EXEC	Router #	Use the **enable** command from the *user exec mode*	Use the exit or end command
Global Configuration	Router(config)#	Use the **'configure terminal'** command from the *privileged exec mode*	Use the exit command
Interface Configuration	Router(config-if) #	Use the **'interface type number'** command from the *global configuration mode*	Use the exit command to return in global configuration mode
Sub-Interface Configuration	Router (config-sub if)	Use the **'interface type *sub interface number*'** command from the *global configuration mode* or the *interface configure mode*.	Use the **exit** command to return in the previous mode. Use the **end** command to return in the *privileged exec mode*.

Setup	Parameter [Parameter value]:	After booting, the IOS automatically starts this mode, if it does not detect the running configuration.	Press **CTRL+C** to abort. Type **Yes** to save the configuration, or **No** to exit without saving when asked at the end of the setup program.
ROMMON	ROMMON>	Starts automatically if functional IOS is missing. To start manually, Press the **CTRL + C** key during the first 60 seconds of the booting process	Use the **exit** command.

IOS Configuration Modes

Cisco IOS (Internetwork Operating System) is a proprietary operating system that runs on most Cisco Systems routers and switches.

The IOS provides the interface for interaction with the hardware components and provides various configuration modes for better management and control over the network devices. Each mode provides a different set of commands. Below are some of the common configuration modes:

User EXEC Mode: This is the first level of access. Here you can perform basic tests and check system information.

Privileged EXEC Mode: This mode allows you to access all device commands, such as those used for configuration and management, and includes access to global configuration mode. You can usually access it by entering the "enable" command in the user EXEC mode.

Global Configuration Mode: This mode allows changes to the system configuration. You can enter this mode from privileged EXEC mode by using the "configure terminal" command.

Interface Configuration Mode: This is used to configure interfaces. You can access it from the global configuration mode. To configure an interface, you need to specify the interface you want to configure. For example, the "interface fast Ethernet 0/0" command.

Sub-interface Configuration Mode: Similar to interface configuration, but for virtual interfaces, not physical ones. You can create a subinterface from the interface configuration mode.

Line Configuration Mode: This mode is used to configure console, SSH, Telnet, AUX etc. You can enter this mode using the "line" command from the global configuration mode.

Router Configuration Mode: This mode is used to configure routing protocols such as RIP, OSPF, EIGRP etc. You can enter this mode by typing "router" followed by the routing protocol you wish to configure.

VLAN Configuration Mode: This mode is used to configure VLANs (Virtual Local Area Networks). It can be accessed by typing "vlan" followed by the VLAN number in the global configuration mode.

- **HOST NAME**

In the context of Cisco IOS (Internetwork Operating System), the "hostname" is a command used to set the device's name, which is essentially its identifier. This is helpful when you're managing multiple devices, as it allows you to easily differentiate between them.

Here is how to set the hostname on a Cisco IOS device:

1. Access the device's command-line interface (CLI). This usually requires using a console cable to connect to the device physically or connecting via Telnet or SSH.

2. Enter **"enable"** mode. This is done by typing the command **enable** at the command prompt, then pressing **Enter**. You might be asked for a password.

3. Now, to change the hostname, you need to go into the global configuration mode. Type **configure terminal** (or **conf t** for short) and press Enter.

4. Now you can change the hostname by typing the **hostname** command followed by the desired name. For example, if you wanted to change the hostname to **"CiscoRouter",** you would type **hostname CiscoRouter.**

4. Press **Enter** to apply the change. The prompt should immediately reflect the new hostname.

5. To save the changes permanently, type **write memory** or **copy running-config startup-config** and press Enter.

If you don't save the configuration, the changes will be lost when the device is rebooted. Remember that the hostname should be unique within your network to avoid confusion and potential connectivity issues

- **Banner message**

A banner is a message presented to a user who is using the Cisco switch. Based on the type of banner you configured for use, the message will be shown to users of Cisco switch. Cisco IOS routers support a number of banners, such as:

- ✓ **MOTD banner:** When users connect to the router, the "Message Of The Day (MOTD)" banner is presented.
- ✓ **Login banner:** The login banner is displayed right before the authentication prompt.
- ✓ **Exec banner:** The Exec banner appears before the user sees the exec prompt.
- ✓ **Incoming banner:** These banners are displayed for users who connect through reverse telnet.

Steps to configure banners through CLI.

1. Login to the device using SSH / TELNET and go to enable mode.

2. Go into the config mode.

   Router**# configure terminal**

   Enter configuration commands, one per line. End with CNTL/Z.

   Router(config)#

3. Use below command to configure banner for required banner types (motd / login / exec)

   Router(config)#**banner motd #Unauthorised access to this device is prohibited!** #

4. Exit config mode

   Router(config)#**exit**

   Router#

5. Copy the running configuration into startup configuration using the below command:

   Router# **write memory**

   Building configuration... [OK]

   Router#

Reload Device

The Cisco **"reload"** command is used on almost all IOS Cisco networking devices (routers, switches etc) to restart (or reboot) the appliance.

As we have said above, the basic usage of this command is to reload the IOS operating system of the router or switch. Its the same as rebooting a computer.

If the current running configuration is modified and not saved to flash, the device prompts you to save the configuration.

The following example shows how to immediately reload a Cisco device:

CiscoRouter# **reload**

Another useful trick to know is to verify first the stored IOS image on the device before reloading:

CiscoRouter# **reload /verify**

The above will first perform a signature verification and file integrity check on the stored bootflash image file before reloading the appliance. After the verification is done the system will ask you again if you want to reboot the device.

CiscoRouter# **reload [text specifying the reason]**

e.g CiscoRouter# **reload testing of Access Control List**
The above specifies the reason of reloading the system.

How to schedule a reload

Now this is the useful practical application of the reload command we have mentioned at the beginning.

By scheduling a reload at some specified time in the future allows the administrator to make critical changes to the configuration that might drop connectivity or have some other traffic implications.

If something unexpected happens after the configuration change, the device will reboot by itself in let's say 2 minutes from now thus restoring the previous state of the network.
Let's see how reload scheduling works:
There are two keywords that you can specify for reload scheduling:
reload at [specific date and time]
reload in [minutes]
Examples:
CiscoRouter# **reload at 14:00**
The above will reload the router at 2:00pm in the current date.
CiscoRouter# **reload at 14:00 jan 10**
The above will reload the router at 2:00pm on January 10.

- **Configure port**

In Cisco's Internetwork Operating System (IOS), the process for configuring a port depends on the type of port you want to configure (e.g., an Ethernet port, a serial port, etc.) and what you want to configure on that port (e.g., IP address, speed, duplex mode, etc.).

Here's an example of how you can configure an Ethernet port:

Here's a breakdown of what each line does:

- ✓ **configure terminal** or **conf t** for short, enters global configuration mode.
- ✓ **interface FastEthernet 0/1** selects the port you want to configure. Change "FastEthernet 0/1" to the appropriate interface name for your device.
- ✓ **ip address 192.168.1.1 255.255.255.0** sets the IP address and subnet mask for the interface. Replace "192.168.1.1 255.255.255.0" with the desired IP address and subnet mask.
- ✓ **no shutdown** activates the interface. By default, many interfaces are administratively down, so you must use this command to activate them.
- ✓ **exit** returns to the previous mode.
- ✓ **wr** or **write** saves the configuration changes. If you don't save the changes, they will be lost when the device is restarted.

Remember that actual commands might vary based on the type of interface and what specific configurations you want to apply. Always refer to the appropriate documentation or online resources for more information.

The above commands should be entered in the CLI (Command Line Interface) of the IOS device.

Practical Activity 3.1.2: Configuring Basic IOS

Task:

1: Pay attention to the introduction and prepare to complete the assigned task as described.

Suppose, you are a network administrator responsible for a small business with 10 employees. The business is currently using a wireless network, but you are concerned about security.

You have decided to implement a wired LAN and configure strong passwords for all network devices to protect the network from unauthorized access.

2: Identify and gather the necessary tools needed for the activity.

3: Listen carefully to the guidance and actively participate by repeating the activity as instructed by the trainer.

4: Repeat the activity individually until you achieve a perfect result.

5: Read key reading 3.1.2 attentively to gain a deeper understanding of the topic.

Key readings 3.1.2

- **Configure IOS passwords**
  - ✓ **Secret password**

Enable secret password – this command serves the same purpose as the enable password command, but with one major difference – the configured password is stored in encrypted form. The following command is used to configure the enable secret password:

- **DEVICE (config)** *enable secret PASSWORD*

The entire configuration process:

Router>configure terminal

Enter configuration commands, one per line. End with CNTL/Z.

Router(config)#enable password cisco123

Router(config)#end

Router#write memory

Building configuration...

[OK]

Router#show running-config | include enable password

enable password cisco123

Router#

- ✓ **Line Password**

When you initially connect to a device, you are in user EXEC mode. This mode is secured using the console.

To secure user EXEC mode access, enter line console configuration mode using the **line console 0** global configuration command, as shown in the example. The zero is used to represent the first (and in most cases the only) console interface. Next, specify the user EXEC mode password using the **password** password command. Finally, enable user EXEC access using the **login** command.

The entire configuration process:

Router>configure terminal

Enter configuration commands, one per line. End with CNTL/Z.

Router(config)#line console 0

Router(config-line)#password cisco123

Router(config-line)#login

Router(config-line)#exit

Router(config)#line vty 0 15

Router(config-line)#password cisco123

Router(config-line)#login

Router(config-line)#exit

Router(config)#end

Router#write memory

Building configuration...

[OK]

Router#

- ✓ **Enable password**

Enable password – you can configure an IOS device to require a password before entering the privileged exec mode. This can prevent an unauthorized user from entering the global configuration mode and changing the configuration of the device. Note that the configured password is stored in the device configuration in clear-text. The enable password is set using the following command:

DEVICE (config) *enable password PASSWORD*

The entire configuration process:

Router>configure terminal

Enter configuration commands, one per line. End with CNTL/Z.

Router(config)#enable password cisco123

Router(config)#end

Router#write memory

Building configuration...

[OK]

Router#

- ✓ **Auxiliary Password**

Sure, I can walk you through the process of configuring the Auxiliary (AUX) port password on a Cisco IOS device. The AUX port is usually used for out-of-band management and can also serve as a backup interface for dial-up connectivity.

Here are the steps:

1. Access your Cisco IOS device through the console port or through an SSH/Telnet session.

2. Once connected, you will enter into user EXEC mode, represented by the **>** prompt. You need to go into privileged EXEC mode (Enable mode) by using the **enable** command. It will change your prompt to **#**.

Router> enable

3.Next, you need to go into global configuration mode. You do this using the configure terminal command.

Router# configure terminal

4. Now you're in global configuration mode and you can start configuring the AUX port. First, go into line configuration mode for the AUX port. This is usually line aux 0 for most routers, but it could be different if your router supports multiple AUX lines.

Router(config)# line aux 0

5. Now you can set the password for the AUX port using the password command followed by the desired password.

Router(config-line) # password YourPassword

6. Also, you need to ensure that the password will be asked for when connecting to the AUX port. You can do this using the login command.

Router(config-line) # login

7. Exit back to the privileged EXEC mode by typing exit twice.

Router(config-line) # exit Router(config)# exit

8. Finally, save your running configuration to startup configuration (so that your changes persist after a reboot) with the copy running-config startup-config command.

Router# copy running-config startup-config

Replace YourPassword with the password you want to set. Remember, to secure your device properly, use strong passwords and do not expose the AUX port unnecessarily**.**

The entire configuration process:

Router>configure terminal

Enter configuration commands, one per line. End with CNTL/Z.

Router(config)#line aux 0

Router(config-line)#password cisco123

Router(config-line)#login

Router(config-line)#exit

Router(config)#end

Router#write memory

Building configuration...

[OK]

Router#

- **SSH password**

Telnet simplifies remote device access, but it is not secure. Data contained within a Telnet packet is transmitted unencrypted. For this reason, it is highly recommended to enable Secure Shell (SSH) on devices for secure remote access.

It is possible to configure a Cisco device to support SSH using the following six steps:

Step 1. Configure a unique device hostname. A device must have a unique hostname other than the default.

Step 2. Configure the IP domain name. Configure the IP domain name of the network by using the global configuration mode command **ip domain name** *name*. In the example, router R1 is configured in the span.com domain. This information is used along with the bit value specified in the **crypto key generate rsa general-keys modulus** command to create an encryption key

Step 3. Generate a key to encrypt SSH traffic. SSH encrypts traffic between source and destination. However, to do so, a unique authentication key must be generated by using the global configuration command **crypto key generate rsa general-keys modulus** bits. The modulus bits determine the size of the key and can be configured from 360 bits to 2048 bits. The larger the bit value, the more secure the key. However, larger bit values also take longer to encrypt and decrypt information. The minimum recommended modulus length is 1024 bits.

Step 4. Verify or create a local database entry. Create a local database username entry using the **username** global configuration command. In the example, the parameter **secret** is used so that the password will be encrypted using MD5.

Step 5. Authenticate against the local database. Use the **login local** line configuration command to authenticate the vty line against the local database.

Step 6. Enable vty inbound SSH sessions. By default, no input session is allowed on vty lines. You can specify multiple input protocols including Telnet and SSH using the **transport input {ssh| telnet}** command.

The entire configuration process

Router>configure terminal

Enter configuration commands, one per line. End with CNTL/Z.

Router(config)#ip ssh version 2

Router(config)#crypto key generate rsa

[OK] (elapsed time was 9 seconds)

Router(config)#username admin password cisco123

Router(config)#end

Router#write memory

Building configuration...

[OK]

Router#

- **Save configuration**

Where Configuration Files are Stored

A Cisco device needs to use the configuration file to do its work. Cisco devices have random-access memory (RAM) to store data from the configuration file while Cisco IOS is using it, but the RAM loses its contents when the device loses power. In order to load all configuration data back after the device loses power, Cisco use several types of more permanent memory.

The following list explains the four main types of memory found in Cisco switches or Cisco routers, as well as the most common use of each type:

RAM — RAM is used by a Cisco device for working storage. The running configuration file is stored

ROM — Read-only memory (ROM) stores a bootstrap program that is loaded when the switch first powers on. This program finds the full Cisco IOS image and loads it into RAM.

Flash memory — This memory can be either inside the device or on a removable memory card. Flash memory stores fully functional Cisco IOS images and is the default location where the switch gets its Cisco IOS at boot time. Flash memory also can be used to store other files, including backup copies of configuration files.

NVRAM — Nonvolatile RAM (NVRAM) stores the initial or startup configuration file that is used when the Cisco device is powered on or reloaded.

Points to Remember

- **User EXEC Mode:** This is the first level of access. Here you can perform basic tests and check system information.
- **Privileged EXEC Mode:** This mode allows you to access all device commands, such as those used for configuration and management
- **Global Configuration Mode:** This mode allows changes to the system configuration.
- **Interface Configuration Mode:** This is used to configure interfaces.
- **Sub-interface Configuration Mode:** Similar to interface configuration, but for virtual interfaces, not physical ones.
- **Line Configuration Mode:** This mode is used to configure console, SSH, Telnet, AUX etc

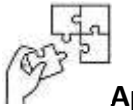
- The Necessary commands to configure passwords in Cisco devices.

The entire configuration process to configure secret password:

```
Router>configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#enable password cisco123
Router(config)#end
Router#write memory
Building configuration...
[OK]
Router#show running-config | include enable password
```

enable password cisco123

Router#



Application of learning 3.1.

You are the network administrator for a small office that has recently set up a new network. The office has a Cisco router (Router1) and a Cisco switch (Switch1). The office requires the following configurations:

1. The router should have a hostname of "Router1".
2. It should have a management IP address of `192.168.1.1` with a subnet mask of `255.255.255.0`.
3. The router needs to be accessible via console and SSH, with secure passwords configured.

Indicative content 3.2: Configuration of IP Address

Duration: 2 hrs

Theoretical Activity 3.2.1: Description of IP Address configuration

Tasks:

1: Engage in the discussion, share your thoughts and insights on the questions presented.

i. Define an IP Address.

ii. What are the functions of an IP Address in LAN installation?

iii. Provide an example of an IP Address.

iv. Name two ways to assign an IP Address to network devices.

2: Read key reading 3.2.1 attentively to gain a deeper understanding of the topic.

3: Ask questions to clarify any doubts or seek further understanding

Key readings 3.2.1.:

1. IP Address

An IP address (Internet Protocol address) is a unique numerical label assigned to each device connected to a computer network that uses the Internet Protocol for communication.

It serves two main functions:

- **Network interface identification:** An IP address identifies a specific interface on a device, allowing it to communicate with other devices on the same network.
- **Location addressing:** An IP address provides a location address that identifies the device on the internet, enabling it to send and receive data from other devices on the internet.

IP addresses are typically represented in a dotted-decimal format, consisting of four numbers separated by periods, each number ranging from 0 to 255. For example, **192.168.1.1** is a valid IP address.

2. Two main ways to configure IP settings:

- **Static**

Sure, to configure an IP address statically on a Cisco device, you generally need to go into the configuration mode of the device. This process assumes that you are using a Cisco IOS-based device. Here is a simple step-by-step guide to configuring a static IP address:

1. Connect to the device via the console cable, SSH, or Telnet.

2. Login using your credentials.

3. Enter **"enable"** mode

Router>enable

4. You'll then be asked for a password, if one is set. After entering the password, you will be in privileged EXEC mode (the prompt changes to **Router#**).

5. Enter global configuration mode:

Router#configure terminal

The prompt changes to **Router(config)#.**

6. Go into interface configuration mode for the interface you want to configure, for example, FastEthernet 0/0:

Router(config)#interface FastEthernet 0/0

The prompt changes to Router(config-if)#.

7. Assign the IP address and subnet mask:

Router(config-if) #ip address 192.168.1.1 255.255.255.0

Replace **192.168.1.1** with the IP address you want to assign and **255.255.255.0** with the appropriate subnet mask.

8. Enable the interface:

Router(config-if)#no shutdown

9. Exit back to global configuration mode:

Router(config-if)#exit

10. Save your configuration:

Router(config)#do write memory

Remember to replace Router with the name of your device, and replace FastEthernet 0/0, **192.168.1.1**, and **255.255.255.0** with the appropriate interface name and IP address details for your situation. You should also ensure that the IP address and subnet mask match your network's address plan.

- **Dynamic**

Configuring an IP address dynamically on a Cisco device involves using the Dynamic Host Configuration Protocol (DHCP).

DHCP can be used to automatically assign IP addresses, subnet masks, default gateways, and other IP parameters to devices on the network.

Practical Activity 3.2.2: Configuring Static IP Address.

Task:

1: Proceed to the computer lab and work individually to configure the static IP Address, applying the knowledge gained from activity 3.1.2

Individually, referring to the previous activity 3.1.2, you are asked to go to the computer lab and configure the static IP Address to ensure that clients on the network can communicate effectively.

2: Navigate to the network installed in Task 3.1.2 or open the simulated network in the lab as instructed.

3: Configure the IP Address on the router interface, ensuring they apply the correct settings as learned in previous activities.

4: Configure the IP Address on the client devices, ensuring that they complete the task accurately.

5: Read the key readings 3.2.2 for more Information.

Key readings 3.2.2

An IP address (internet protocol address) acts as a unique identifier for a device that connects to the internet. Computers use IP addresses to locate and talk to each other on the internet, much the same way people use phone numbers to locate and talk to one another on the telephone.

When a static IP address is necessary

Because static IP addresses are not used as commonly now, it is important to note when using a static IP address is necessary.

Businesses will mostly use static IP addresses if they are hosting servers and websites which require a high uptime percentage, use voice over IP (VoIP), or have employees that work from home often.

If employees want to remotely access their device from home, an IP address that changes may require the employee to know the new address. Using a remote access application and a static IP address, an employee could always access their computer with that same address.

How static IP addresses work

Because static IP addresses are not the default provided by most ISP companies, if an individual or organisation wants one, they first have to call their ISP and ask to assign their device such as a router for example -- a static IP address.

Once the device is set up with a new and unchanging IP address, they will have to restart their device once. Computers or other devices behind the router will use the same IP address. Once the IP address is in place, it doesn't require any steps to manage, since it doesn't change.

There is a limit to the number of static IP addresses available, however, meaning requesting a static IP address will often cost money. IPv6 is an idea to get around this issue.

IPv6 lengthens IP addresses from 32 bits to 128 bits (16 bytes) and increases the number of available IP addresses significantly, making static IP addresses easier and less expensive to obtain and maintain.

Pros and cons of static IP addresses

Because they aren't used as often, it may be difficult to see where **static IP addresses** have advantages. However, a static IP address can have advantages such as:

- Businesses that rely on IP addresses for mail, FTP and web servers can have one, unchanging address.
- Static IP addresses are preferred for hosting voice over IP, VPNs and games.
- They can be more stable in the case of an interruption in connectivity -- meaning packet exchanges won't be lost.
- They allow for file servers to have faster file uploads and downloads.
- A static IP will make it easier for any geolocation services to access where a device is.
- Static IPs are better for remote access to a computer.
- A static IP address-enabled device does not need the device to send renewal requests.
- Static IP addresses can be simpler for network administrators to maintain considering running servers.
- And it is easier for administrators to track internet traffic, assigning access to users based on IP address.

Disadvantages of static IP address include some reasons why it isn’t used as often today, such as:

- It limits the amount of IP addresses. A static IP address assigned to a device or website is occupied until otherwise noted, even when the device is off and not in use.
- Most people do not need a static IP address now.
- Because the IP address is constant and cannot easily be changed, a static IP address is more susceptible to hackers or follow-up attacks.
- It can be complicated to set up a static IP manually.
- It may be difficult to transfer server settings from a static IP device to a new one if the original device becomes obsolete.
- Devices with a static IP are easier to track.

The steps to configure DHCP on a Cisco router:

1. Enter global configuration mode

2. Define the DHCP pool name:

3. Define the network for DHCP service

4.Specify the default gateway

5.(Optional) Specify the DNS server

6.(Optional) Specify the lease duration

7.Exit DHCP configuration mode

Router> enable

Router# configure terminal

Router(config)# ip dhcp pool DHCP_POOL

Replace DHCP_POOL with the name of your DHCP pool.

Router(dhcp-config) # network NETWORK SUBNET

Replace **NETWORK** with the network address and **SUBNET** with the subnet mask.

Router(dhcp-config) # default-router GATEWAY_IP

Replace **GATEWAY_I**P with the IP address of the default gateway.

Router(dhcp-config) # dns-server DNS_IP

Replace DNS_IP with the IP address of the DNS server.

Router(dhcp-config) # lease DAYS HOURS MINUTES

Replace **DAYS, HOURS,** and **MINUTES** with the desired lease duration.

Router(dhcp-config) # exit

Router# copy running-config startup-config

Points to Remember

- **Configure the IP Address on a computer.**

  To configure an IP address on a computer, you will need to know the IP address, subnet mask, and default gateway. You can usually get this information from your network administrator or internet service provider (ISP).
- **Once you have the necessary information, you can follow these steps to configure your IP address:**
  - ✓ Open the Network and Sharing Center.
  - ✓ Click Change adapter settings in the left-hand pane.
  - ✓ Right-click on the network adapter that you want to configure and select Properties.
  - ✓ Double-click on Internet Protocol Version 4 (TCP/IPv4).
  - ✓ Select Use the following IP address and enter the IP address, subnet mask, and default gateway.

- ✓ Click OK to save your changes.

You may need to restart your computer for the changes to take effect.

- **Here are some additional tips for configuring IP addresses:**
  - ✓ Make sure that the IP address you choose is within the subnet range of your network.
  - ✓ Avoid using the IP address 192.168.0.1, as this is typically reserved for the router.
  - ✓ If you are unsure about how to configure your IP address, contact your network administrator or ISP for assistance.
- To configure a static IP address, you will need to know the following information:
  - ✓ IP address
  - ✓ Subnet mask
  - ✓ Default gateway
  - ✓ DNS server addresses
- You can usually get this information from your network administrator or internet service provider (ISP).
- Once you have the necessary information, you can follow these steps to configure a static IP address on your computer:
  - ✓ Open the Settings app.
  - ✓ Click Network and internet.
  - ✓ Click Wi-Fi or Ethernet, depending on your connection type.
  - ✓ Click Manage known networks.
  - ✓ Click the network that you want to configure and then click Properties.
  - ✓ Click Edit IP assignment.
  - ✓ Select Manual and then enter the following information:
    - IP address
    - Subnet mask
    - Default gateway
    - DNS server addresses
  - ✓ Click Save.

Application of learning 3.2.

ABC Primary School is a well-established educational institution located in a vibrant community in Rwanda.

The school has several network printers strategically placed in administrative offices and classrooms. These printers are essential for producing lesson materials, administrative documents, and student assignments. However, the school faced challenges with printing reliability due to dynamic IP addresses assigned to the printers by the DHCP server. When the printers received new IP addresses, it caused confusion among staff, resulting in printing errors and delays.

As network Technician, set a static IP address for the school's network printer to ensure that teachers and administrative staff can consistently access it for printing documents.

Indicative content 3.3: Configuration of Routing Protocols

Duration: 7 hrs

Theoretical Activity 3.3.1: Description of Routing Protocols

Tasks:

1: Answer the following questions:

- ✓ What are routing protocols?
- ✓ Give Importance of Routing Protocols in networking

2: Participate actively in the discussion regarding the given questions.

3: Prepare and deliver presentations to the class, share your findings and insights from the activity.

4: listen to the expert insights being shared and Ask questions to clarify any doubts

5: Listen attentively to the explanation of the types of routing protocols and take notes to enhance their understanding of the topic.

6: Read key readings 3.3.1 in trainee's manual

Key readings 3.3.1.:

➔ **Configuring Routing Protocols**

❖ **Introduction to Routing Protocols**

Routers to communicate between source & destination are called by routing protocols. the routing protocol does not move information sources to a destination, but only updates routing table information.

Routing protocols are sets of rules used by routers to determine the most efficient path for forwarding packets across network nodes. In other words, they dictate how routers communicate with each other, disseminating information that enables them to select routes between any two nodes on a computer network.

There are many types of routing protocols, but they can broadly be divided into two categories:

1. **Interior Gateway Protocols (IGPs):** These are used within a single autonomous system (AS), which is a network or group of networks under common administration. Examples of IGPs include:
    - ✓ **Routing Information Protocol (RIP):** This is a distance-vector protocol that uses hop count as a routing metric. It has a maximum network diameter of 15 hops. RIP is an old protocol and is not commonly used today in large networks due to its limitations.
    - ✓ **Open Shortest Path First (OSPF):** This is a link-state routing protocol that organizes networks into areas and uses the Dijkstra algorithm to find the shortest path to each network. It's widely used in large enterprise networks.
    - ✓ **Enhanced Interior Gateway Routing Protocol (EIGRP):** EIGRP is a Cisco proprietary protocol that incorporates features of both link-state and distance-vector protocols.
2. **Exterior Gateway Protocols (EGPs):** These are used to exchange routing information between autonomous systems. An example is:
    - ✓ **Border Gateway Protocol (BGP):** This is a complex protocol that routers use to maintain a map of the internet. BGP provides the backbone of the internet, allowing data packets to traverse multiple networks from their source to their destination.

All these protocols make use of different algorithms and metrics to find the most efficient path for routing packets.

Routing protocols also exchange information about the state of the networks they're connected to, which allows them to respond to changes in the network's structure and to route around any areas of the network that might be down or congested.

- **Static routing protocol**

Routers forward packets using either route information from route table entries that you manually configure or the route information that is calculated using dynamic routing algorithms.

Static routes, which define explicit paths between two routers, cannot be automatically updated; you must manually reconfigure static routes when network changes occur. Static routes use less bandwidth than dynamic routes. No CPU cycles are used to calculate and analyse routing updates.

You can supplement dynamic routes with static routes where appropriate. You can redistribute static routes into dynamic routing algorithms but you cannot redistribute routing information calculated by dynamic routing algorithms into the static routing table.

You should use static routes in environments where network traffic is predictable and where the network design is simple. You should not use static routes in large, constantly changing networks because static routes cannot react to network changes. Most networks use dynamic routes to communicate between routers but may have one or two static routes configured for special cases.

Static routes are also useful for specifying a gateway of last resort (a default router to which all unbootable packets are sent).

- **Standard**

The system automatically inserts routing entries into the routing table for networks that are directly connected to the system. Manual entries are necessary in those cases where there is an additional router which is to be accessed via a specific network. Routes for networks that are not directly connected and that are inserted to the routing table via a command or a configuration file, are called static routes.

To add a standard static route, proceed as follows:

1. On the **Standard Static Routes** tab click **New Static Route**.

2. The **Add Static Route** dialog box opens.

3. Make the following settings:

Route type: The following route types are available:

- ✓ **Interface route:** Packets are sent out on a particular interface. This is useful in two cases. First, for routing on dynamic interfaces PPP because in this case the IP address of the gateway is unknown. Second, for defining a default route having a gateway located outside the directly connected networks.
- ✓ **Gateway route:** Packets are sent to a particular host (gateway).
- ✓ **Blackhole route:** Packets are discarded silently. This is useful in connection with OSPF or other dynamic adaptive routing protocols to avoid routing loops, route flapping, and the like.

Network: Select the destination networks of data packets Sophos UTM must intercept.

Interface: Select the interface through which the data packets will leave Sophos UTM (only available if you selected **Interface Route** as route type).

Gateway: Select the gateway/router to which Sophos UTM will forward data packets (only available if you selected **Gateway Route** as route type).

Comment (optional): Add a description or other information.

3. Optionally, make the following advanced setting:

Metric: Enter a metric value which can be an integer from 0 to 4294967295 with a default of 5. The metric value is used to distinguish and prioritise routes to the same destination. A lower metric value is preferred over a higher metric value. IPsec routes automatically have the metric 0.

4. Click **Save**.

The new route appears on the **Standard Static Route** list.

5. Enable the route.

Click the toggle switch to activate the route.

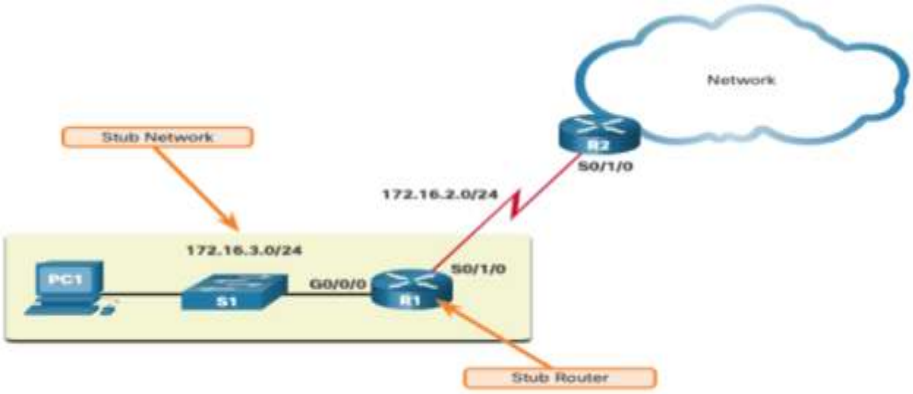
To either edit or delete a route, click the corresponding buttons.

- **Default**

A default route is a static route that matches all packets. A single default route represents any network that is not in the routing table.

Routers commonly use default routes that are either configured locally or learned from another router. The default route is used as the Gateway of Last Resort.

Default static routes are commonly used when connecting an edge router to a service provider network, or a stub router (a router with only one upstream neighbor router).



The figure shows a typical default static route scenario.

IPv4 Default Static Route: The command syntax for an IPv4 default static route is similar to any other IPv4 static route, except that the network address is 0.0.0.0 and the subnet mask is 0.0.0.0. The 0.0.0.0 0.0.0.0 in the route will match any network address.

Note: An IPv4 default static route is commonly referred to as a quad-zero route.

The basic command syntax for an IPv4 default static route is as follows:

Router(config)# ip route 0.0.0.0 0.0.0.0 {ip-address | exit-intf}

R1(config)# ip route 0.0.0.0 0.0.0.0 172.16.2.2

The **show ip route static** command output from R1 displays the contents of the static routes in the routing table.

Summary

A static summary route is used to minimize the number of static routes in the routing table and lessen the administrative overhead that may impact the memory usage of the routers.

Using a static summary route efficiently manages a large number of static routes in the routing table, which lessens the probability of errors occurring.

Multiple static routes can be replaced by a single static summary route, given that those routes have a common prefix length. Configuring a static summary route is just the same as how we configure a static route.

Route Summarization

The process of advertising multiple sets of addresses as a single address with a less specific and shorter subnet mask is how we simply define Route Summarization. Classless InterDomain Routing (CIDR) is synonymous with Supernetting and is a form of route summarization. CIDR overlooks the limitation of classful boundaries and allows summarization with subnet masks that are smaller than the default classful subnet masks.

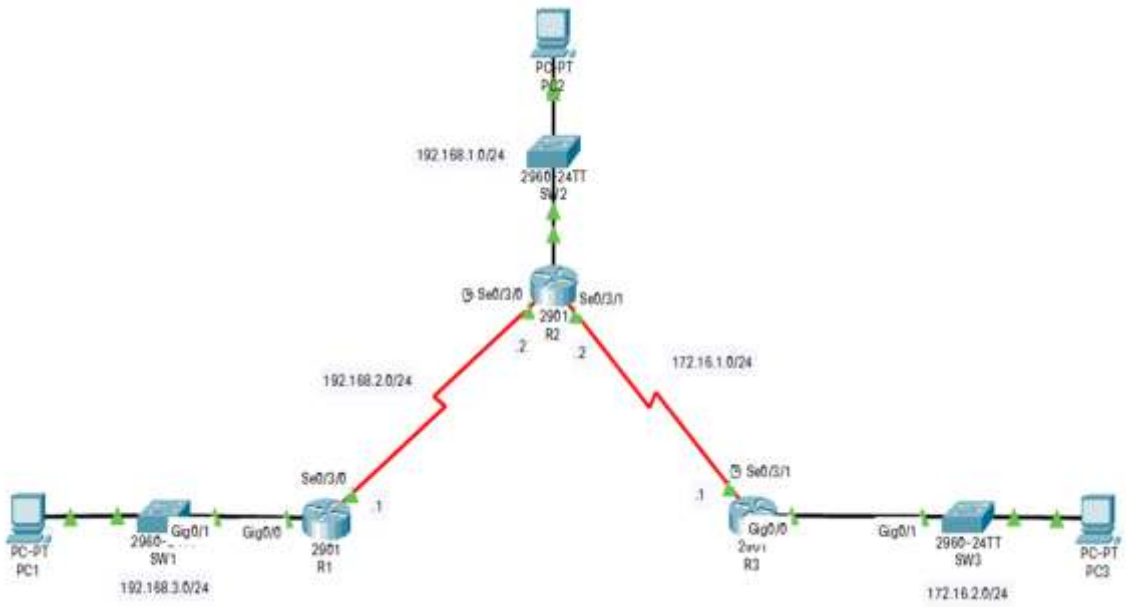
This type of summarization helps to reduce the number of routes in the routing table, minimizing route updates, reduces memory and CPU utilization, and faster routing table lookups.

Summary of Static Route Calculation

Let us consider the diagram below as an example to deeply understand how the summary static route does its calculation. We configure static routes individually on the routers already.

Keep in mind that multiple static routes can be summarized into a single static route if the following conditions are met:

- ✓ The destination networks are in a contiguous range and can be summarized into a single network address.
- ✓ All of the multiple static routes use the same exit interface or next-hop IP address



The following output below shows the static routing table entries for R3. The following output displays the routing information, the routing table static route entries, of R3. Notice that it has three static routes in contiguous ranges that can be summarized because the destination network shares the same two first octets, 192.168.

R3# show ip route static | begin Gateway

Gateway of last resort is not set

192.168.0.0/24 is subnetted, 3 subnets

192.168.1.0 is directly connected, Serial0/3/1

192.168.2.0 is directly connected, Serial0/3/1

192.168.3.0 is directly connected, Serial0/3/1

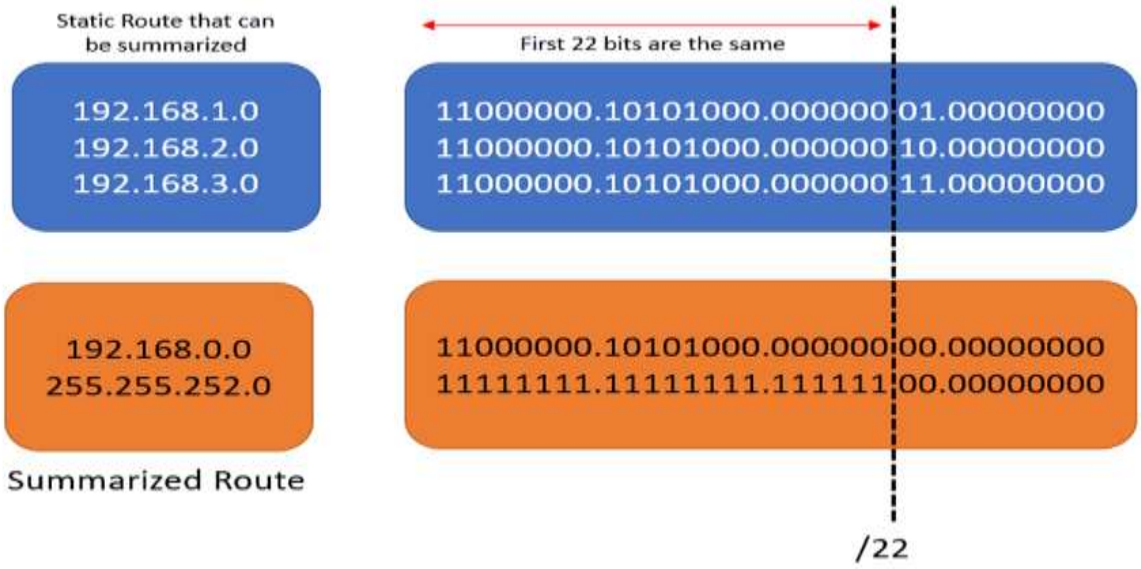
Here are the steps in how to calculate the networks for route summarization:

1. Write out the network addresses to be summarised in binary.

2. Next, let's find the subnet mask for summarization. We'll start with the far left bit, going to the right, finding all the bits that match until we reach the unmatching column. This signifies the summary boundary.

3.Count the number of far-left matching bits. In our example, it is 22. This number identifies the subnet mask, in slash notation, for the summarised route. We have a /22 or a 255.255.252.0 in dotted decimal form.

4. To find the network address for summarization, copy the matching 22 bits and add all 0 bits to the end to make 32 bits.



Summary Static Route Configuration

In our example, we have the three routes configured individually. To summarise them, we need to issue the **'no'** command to remove the individual routes. Then, we enter the summarised route. We can optionally configure the next-hop address as well.

Here, we can use any subnet mask as long as it covers the required network. We can use a /16, 255.255.0.0, or 255.255.252, which is more granular.

R3(config)# no ip route 192.168.1.0 255.255.255.0 s0/3/1

R3(config)# no ip route 192.168.2.0 255.255.255.0 s0/3/1

R3(config)# no ip route 192.168.3.0 255.255.255.0 s0/3/1

R3(config)# ip route 192.168.0.0 255.255.252.0 s0/3/1

We can verify the routing information by checking the output of configuring a static route using the '**show ip route static'** command.

R3# show ip route static | begin Gateway

Gateway of last resort is not set

192.168.0.0/22 is subnetted, 1 subnets

192.168.0.0 is directly connected, Serial0/3/1

NOTE
We can have route summarization for the static and dynamic routing protocol.

- **Floating**

Another type of static route is a floating static route. Floating static routes are static routes that are used to provide a backup path to a primary static or dynamic route. The floating static route is only used when the primary route is not available.

To accomplish this, the floating static route is configured with a higher administrative distance than the primary route. The administrative distance represents the trustworthiness of a route. If multiple paths to the destination exist, the router will choose the path with the lowest administrative distance.

By default, static routes have an administrative distance of 1, making them preferable to routes learned from dynamic routing protocols.

The administrative distance of a static route can be increased to make the route less desirable than that of another static route or a route learned through a dynamic routing protocol. In this way, the static route "floats" and is not used when the route with the better administrative distance is active.

The commands to configure default and floating IP default routes are as follows:

R1(config)# ip route 0.0.0.0 0.0.0.0 172.16.2.2

R1(config)# ip route 0.0.0.0 0.0.0.0 10.10.10.2 5

The **show ip route** and **show ipv6 route** output verifies that the default routes to R2 are installed in the routing table. Note that the IPv4 floating static route to R3 is not present in the routing table.

- **Dynamic routing protocols.**

Dynamic routing protocols are used by routers to automatically share information about the reachability and status of remote networks. Dynamic routing protocols perform several activities, including network discovery and maintaining routing tables.

A routing protocol is a set of processes, algorithms, and messages that are used to exchange routing information and populate the routing table with the choice of best paths.

The purpose of dynamic routing protocols includes the following:

- Discovery of remote networks
- Maintaining up-to-date routing information
- Choosing the best path to destination networks
- Ability to find a new best path if the current path is no longer available

RIP version 2.

The Routing Information Protocol, version 2 (RIPv2) is an enhanced version of RIP that includes support for important routing features such as class-less addressing and variable-length subnet masks.

Configuring RIPv2 is a pretty straightforward process. Only three steps are required:

1. enabling RIP by using the *router rip* global configuration command
2. instructing the router to use RIPv2 by typing the *version 2* command
3. telling RIP which networks to advertise by using one or more *network* commands.

The first two commands are easy to comprehend, but the last command requires a little bit more thought. With the *network* command you specify which interfaces will participate in the routing process. This command takes a classful network as a parameter and enables RIP on the corresponding interfaces.Let's configure our sample network to use RIP.

Router R1 and R2 have directly connected subnets. We want to include these subnets in the RIP routing process. To do that, we first need to enable RIP on both routers and then advertise these subnets using the network command.

On router R1, in the global configuration mode, enter the *router rip* command to enable RIP. In the RIP configuration mode, change the version of the protocol to 2 by using the *version 2* command. Next, use the *network 10.0.0.0* command to include the Fa0/1 interface on the router R1 in the routing process. Remember, the *network* command takes a classful network number as a parameter, so in this case every interface that has an IP address that begins with 10 will be included in the RIP process (IP addresses that begins with 10 are, by default, the class A addresses and have the default subnet mask of 255.0.0.0). For instance, if another interface on the router had the IP address of 10.1.0.1 it would also be included in the routing process with the network command. You also need to include the link between the two routers in the RIP routing process. This is done by adding another *network* statement, network 172.16.0.0.

So, the configuration on R1 should look like this:

R1(config)#router rip

R1(config-router)#version 2

R1(config-router)#network 10.0.0.0

R1(config-router)#network 172.16.0.0

The configuration on R2 looks similar, but with different network number for the directly connected subnet:

R2(config)#router rip

R2(config-router)#version 2

R2(config-router)#network 192.168.0.0

R2(config-router)#network 172.16.0.0

You can verify that router R1 has a route to R2's directly connected subnet by typing the *show ip route* command

- **OSPF version 2.**

Open Shortest Path First Version 2 (OSPFv2) is a link-state routing protocol that uses link-state advertisements (LSAs) to update neighboring routers about a router's interfaces. Each router maintains an identical area-topology database to determine the shortest path to any neighboring router.

Below are some key details and characteristics of OSPF version 2:

1. Link-state Routing Protocol: OSPF is a link-state routing protocol. This means each router in the network maintains a detailed database of the network's topology. It uses this information to calculate the shortest path to each node using Dijkstra's algorithm.

2. Areas and Hierarchical Design: In OSPF, a large network can be divided into smaller sections known as areas. This hierarchical design helps limit network traffic, reduce routing

table size and improve network performance. Area 0, also known as the backbone area, interconnects all other areas in the OSPF network.

3. Route Cost Metric: OSPF uses a cost metric to determine the shortest path between nodes. The cost is usually determined by the link bandwidth; however, it can be manually configured.

4. Fast Convergence: OSPF networks quickly adapt to changes or failures in the network. When a change occurs, the new information is flooded out to all routers in the network or area, and each router independently recalculates routes.

5. Authentication: OSPF supports authentication between routers. This can help increase the security of the routing information.

6. Equal-Cost Multipath (ECMP): OSPF supports multiple equal-cost routes to the same destination. Traffic can be balanced across these routes.

7. Types of OSPF routers: There are several types of routers in an OSPF environment: Internal routers, Area Border Routers (ABRs), and Autonomous system boundary routers (ASBRs).

8. Neighbour Discovery: OSPF uses Hello packets to discover OSPF neighbours and establish neighbour adjacencies. This forms the basis of the OSPF communication.

9. Scalability: OSPF is highly scalable and can be used in both small and large network environments.

10. Support for CIDR and VLSM: OSPF supports Classless Inter-Domain Routing (CIDR) and Variable Length Subnet Masking (VLSM)

Practical Activity 3.3.2.: Configuring the static routing protocols

Task:

1: Listen carefully to the explanation of static routing protocols and prepare to engage in the following activity.

You have two routers, Router A and Router B, connected to each other. Router A is also connected to a LAN, and Router B is connected to a WAN. You want to configure static routing so that devices on the LAN can access the WAN.

2: Configure a static route for the WAN network, on Router A.

3: Configure a static route for the LAN network, on Router B.

4: Verify that the static routes are configured correctly

5: Read key readings 3.3.2. in their trainees

Key readings 3.2.2.1

The Steps to configure the static routing

On Router A, configure a static route for the WAN network. For example, if the WAN network is 192.168.1.0/24, you would use the following command:

ip route 192.168.1.0 255.255.255.0 192.168.0.2

The first argument to the **ip route** command is the destination network, the second argument is the subnet mask, and the third argument is the next hop address. The next hop address is the IP address of Router B.

On Router B, configure a static route for the LAN network. For example, if the LAN network is 192.168.0.0/24, you would use the following command:

ip route 192.168.0.0 255.255.255.0 192.168.0.1

The next hop address is the IP address of Router A.

Verify that the static routes are configured correctly. On each router, you can use the following command to display the routing table:

netstat -rn

Once you have configured the static routes, devices on the LAN will be able to access the WAN.

Static Routing Vs Dynamic Routing

Static Routing is a manual process and all routes in the Routing table of all the connecting Routers between Source and Destination are manually configured by the Network Administrator.

Static Routing is often used on point-to-point links to Stub Routers or as a backup link to routes provided by a dynamic routing protocol.

Dynamic Routing is achieved by configuring a Routing Protocol such as RIPv2 or OSPF on each Router and new routes or broken routes are automatically shared between the Routers who dynamically update their Routing tables without requiring intervention from the Network Administrator.

The following table shows the main differences between Static Vs Dynamic Routing:

Static Routing	Dynamic Routing
Configured manually by the administrator	Automatically created by a Routing Protocol.
Easy to configure.	More complex to configure (many configuration options, you must know what you are doing).
Best for small networks	Best for medium to large networks.
Provide limited path redundancy and failover.	Provide very good path redundancy, load balancing and failover.
Routes do not react to network changes.	Routes change and react with network changes (e.g when a link goes down).
Low resource usage on Router devices.	High resource usage on Router devices (must have enough memory to hold the routing table).

Does not use complex algorithms.	Dynamic routing uses complex routing algorithms.
Better network security.	Lower network security (unless proper security is implemented, such as routing authentication etc).
Great interoperability between router vendors.	Routing interoperability between vendors is challenging.

Points to Remember

Practical Activity 3.3.2: Configuring the Dynamic routing protocols

Task:

1: Listen carefully to the explanation of Dynamic routing protocols and prepare to engage in the following activity.

You have a network with multiple routers. You want the routers to automatically learn about the network topology and exchange routing information with each other. This will allow the routers to find the best path to any destination network.

2: List out procedures and formulas to be used to perform the given tasks 3.3.3.2 and choose a dynamic routing protocol to use

3: Referring to procedures and formulas provided on task 2, Perform the given tasks (Configure the dynamic routing protocol on all of the routers in the network)

4: Present your work to the trainer to Verify that the dynamic routes are configured correctly

5: Read key readings 3.3.2. in their trainees

6: Perform the task provided in application of learning 3.3.

Key readings 3.3.2

To configure dynamic routing using RIP v2, you will need to follow these steps:

Enable RIP v2 on all of the routers in your network. To do this, use the following command:

" router rip version 2 "

This will enable RIP v2 on the router.

Specify the networks that you want the router to advertise. To do this, use the following command:

" network <network_address> <subnet_mask> "

For example, to advertise the network 192.168.0.0/24, you would use the following command:

" network 192.168.0.0 255.255.255.0 "

Verify that RIP v2 is working correctly. To do this, you can use the following command:

" show ip route "

This will display the routing table on the router. The routing table should show the routes that the router has learned from RIP v2.

Here is an example of how to configure RIP v2 on two routers:

Configure RIP v2 on Router A

router rip

version 2

network 192.168.0.0 255.255.255.0

Configure RIP v2 on Router B

router rip

version 2

network 192.168.1.0 255.255.255.0

Once you have configured RIP v2 on both routers, they will start to exchange routing information with each other. After a few seconds, the routing tables on both routers will show the routes that they have learned from RIP v2.

You can use the show ip route command to verify that RIP v2 is working correctly:

Show the routing table on Router A

show ip route

Show the routing table on Router B

show ip route

The routing tables should show the routes to the 192.168.0.0/24 and 192.168.1.0/24 networks, respectively.

Once RIP v2 is configured, devices on the LAN will be able to access the WAN and other subnets on the network.

To configure dynamic routing using OSPF version 2, you will need to follow these steps:

1. Enable OSPF version 2 on all of the routers in your network. To do this, use the following command:
   - router ospf
2. Specify the OSPF process ID. This is a unique identifier for the OSPF routing process. To do this, use the following command:
   - router-id <router_id>

   The router ID can be any IP address on the router.
3. Specify the OSPF area ID. This is an identifier for the OSPF area that the router belongs to. To do this, use the following command:

- area <area_id>

All of the routers in the same OSPF area must have the same area ID.

4. Specify the networks that you want the router to advertise. To do this, use the following command:
   - network <network_address> <subnet_mask>

For example, to advertise the network 192.168.0.0/24, you would use the following command:

- network 192.168.0.0 255.255.255.0

5. Verify that OSPF version 2 is working correctly. To do this, you can use the following command:
   - show ip ospf neighbor

This will display a list of the OSPF neighbors that the router has learned about.

Here is an example of how to configure OSPF version 2 on two routers:

```
# Configure OSPF version 2 on Router A
router ospf
router-id 192.168.0.1
area 0
network 192.168.0.0 255.255.255.0
# Configure OSPF version 2 on Router B
router ospf
router-id 192.168.1.1
area 0
network 192.168.1.0 255.255.255.0
```

Once you have configured OSPF version 2 on both routers, they will start to exchange routing information with each other.

After a few seconds, the routing tables on both routers will show the routes that they have learned from OSPF version 2.

You can use the show ip route command to verify that OSPF version 2

Show the routing table on Router A

show ip route

Show the routing table on Router B

show ip route

The routing tables should show the routes to the 192.168.0.0/24 and 192.168.1.0/24 networks, respectively.

Once OSPF version 2 is configured, devices on the LAN will be able to access the WAN and other subnets on the network.

Here are some additional tips for configuring OSPF version 2:

- Use different area IDs for different parts of your network. This will help to reduce the amount of routing traffic that is generated.
- Use different router IDs for each router in your network. This will help to prevent routing loops.
- Use the passive-interface command to disable OSPF on interfaces that you do not want to participate in OSPF routing.
- Use the redistribute command to redistribute routes from other routing protocols into OSPF.

OSPF version 2 is a powerful routing protocol that can be used to create scalable and reliable networks.

✓ **when you might use each routing protocol:**

RIP v2:

A. Small networks (less than 50 routers)
B. Networks with simple topologies
C. Networks where convergence time is not a critical factor

OSPF v2:

A. Large networks (more than 50 routers)
B. Networks with complex topologies
C. Networks where convergence time is a critical factor

D. Networks with multiple paths to the same destination (OSPF v2 can load balance traffic across multiple paths)

The Difference between RIP version 2 and OSPF version 2.

RIP v2 and OSPF v2 are both dynamic routing protocols that are used to route traffic between networks.

RIP v2 is a distance-vector routing protocol. This means that it uses the hop count to determine the best path to a destination network. The hop count is the number of routers that a packet must pass through to reach its destination.

OSPF v2 is a link-state routing protocol. This means that it uses the topology of the network to determine the best path to a destination network.

The comparison of RIP v2 and OSPF v2

Feature	**RIP v2**	**OSPF v2**
Protocol type	Distance-vector	Link-state
Maximum hop count	15	Infinite
Convergence time	Slow	Fast
Scalability	Limited	High
Authentication	Optional	Mandatory
Support for load balancing	No	Yes

Points to Remember

- **Steps to configure the static routing**

✓ **On Router A, configure a static route for the WAN network.** For example, if the WAN network is 192.168.1.0/24, you would use the following command:

ip route 192.168.1.0 255.255.255.0 192.168.0.2

The first argument to the ip route command is the destination network, the second argument is the subnet mask, and the third argument is the next hop address. The next hop address is the IP address of Router B.

- ✓ **On Router B, configure a static route for the LAN network.** For example, if the LAN network is 192.168.0.0/24, you would use the following command:

  ip route 192.168.0.0 255.255.255.0 192.168.0.1

  The next hop address is the IP address of Router A.

- ✓ **Verify that the static routes are configured correctly.** On each router, you can use the following command to display the routing table:

  netstat -rn

  Once you have configured the static routes, devices on the LAN will be able to access the WAN.

- **The steps to configure dynamic routing using RIP v2**:

- ✓ Enable RIP v2 on all of the routers in your network. To do this, use the following command:

Specify the networks that you want the router to advertise. To do this, use the following command:

" network <network_address> <subnet_mask> "

For example, to advertise the network 192.168.0.0/24, you would use the following command:

" network 192.168.0.0 255.255.255.0 "

- ✓ Verify that RIP v2 is working correctly. To do this, you can use the following command:

" show ip route "

This will display the routing table on the router. The routing table should show the routes that the router has learned from RIP v2.

Here is an example of how to configure RIP v2 on two routers:

 # Configure RIP v2 on Router A
router rip
version 2
network 192.168.0.0 255.255.255.0

 # Configure RIP v2 on Router B
router rip
version 2
network 192.168.1.0 255.255.255.0

Once you have configured RIP v2 on both routers, they will start to exchange routing information with each other.

After a few seconds, the routing tables on both routers will show the routes that they have learned from RIP v2.

You can use the **show ip route** command to verify that RIP v2 is working correctly:
Show the routing table on Router A
show ip route

Show the routing table on Router B
show ip route

The routing tables should show the routes to the 192.168.0.0/24 and 192.168.1.0/24 networks, respectively.

Once RIP v2 is configured, devices on the LAN will be able to access the WAN and other subn ets on the network.

Application of learning 3.3.

D&H LTD have two buildings in Kigali city, Block 1 has R_A and Block 2 has R-B, those are routers connected to each other. Router A is also connected to a LAN, and Router B is connected to the other side of LAN. They want to configure routing protocols so that buildings on the LAN can access the WAN.

Learning outcome 3 end assessment

Written assessment

Question One:

Item No.	Command	Description
1…….	configure terminal	A. Specifies the networks to be included in RIP routing
2…….	hostname <name>	B. Enters router configuration mode for RIP
3…….	copy running-config startup-config	C. Advertises a network in OSPF
4……..	show running-config	D. Enters router configuration mode for OSPF
5…….	interface GigabitEthernet 0/1	E. Displays the OSPF routing table
6……..	ip address <address> <subnet mask>	F. Assigns a hostname to the device
7……..	no shutdown	G. Enables an interface that has been administratively shut down
8…….	show ip interface brief	H. Removes the IP address configuration from an interface
9…….	ip default-gateway <gateway address>	I. Displays a brief summary of the IP addresses assigned to all interfaces
10……	no ip address	J. Enters interface configuration mode for a specific interface
11…….	router ospf <process-id>	K. Configures a default gateway
12…….	network <network address> <wildcard mask> area <area-id>	L. Saves the running configuration to the startup configuration
13……	show ip route ospf	M. Enters global configuration mode

14……	router rip	N. Displays the current running configuration
15……	network <network address>	O. Assigns an IP address and subnet mask to an interface

Question Two.

Performing Basic IOS Configuration

1. **Which command is used to enter global configuration mode in Cisco IOS?**

   A) enable
   B) configure terminal
   C) interface
   D) exit

2. **What command is used to set the hostname of a Cisco device?**

   A) hostname <name>
   B) set hostname <name>
   C) device-name <name>
   D) configure hostname <name>

3. **How do you save the configuration changes on a Cisco device?**

   A) write
   B) save
   C) copy running-config startup-config
   D) config save

4. **Which command displays the current configuration on a Cisco device?**

   A) show configuration
   B) show running-config
   C) display config
   D) show config

5. **What is the command to enter interface configuration mode for interface GigabitEthernet0/1?**

   A) interface GigabitEthernet 0/1
   B) int GigabitEthernet 0/1
   C) interface G0/1
   D) int G0/1

Configuration IP Address

6. **Which command is used to assign an IP address to an interface?**

   A) ip address <address> <subnet mask>
   B) set ip <address> <subnet mask>
   C) address <address> <subnet mask>
   D) config ip <address> <subnet mask>

7. **How do you enable an interface after assigning an IP address?**

   A) enable interface
   B) activate interface
   C) no shutdown
   D) interface up

8. **What command displays the IP address assigned to all interfaces on a Cisco device?**A) show ip address

   B) show ip interface brief
   C) display ip interface
   D) show interface ip

9. **Which command is used to configure a default gateway on a Cisco device?**

   A) ip default-gateway <gateway address>
   B) set default-gateway <gateway address>
   C) config gateway <gateway address>
   D) default-gateway <gateway address>

10. **How do you remove an IP address configuration from an interface?**

    A) no ip address
    B) delete ip address
    C) remove ip address
    D) clear ip address

Configuration Routing Protocols

11. **Which command is used to enter router configuration mode for OSPF?**

    A) router ospf
    B) router-config ospf
    C) config router ospf
    D) router ospf <process-id>

12. **How do you advertise a network in OSPF?**

A) network <network address> <wildcard mask> area <area-id>
B) advertise network <network address> <wildcard mask> area <area-id>
C) ospf network <network address> <wildcard mask> area <area-id>
D) set ospf network <network address> <wildcard mask> area <area-id>

13. **Which command is used to view the OSPF routing table?**

A) show ip ospf routes
B) show ospf routes
C) show ip route ospf
D) display ospf route

14. **What command is used to enable RIP routing protocol?**

A) router rip
B) router-config rip
C) enable rip
D) config router rip

15. **How do you specify the networks to be included in RIP routing?**

A) network <network address>
B) advertise <network address>
C) rip network <network address>
D) set rip network <network address>

Practical assessment

The Kigali Employment Service Center (KESC) is a mid-sized institution managed by the City of Kigali, situated in the Nyarugenge district, Kimisagara sector. Due to a significant increase in clients, KESC is in the process of opening a new branch in Kicukiro District. This expansion is intended to improve its services and extend its reach to more clients in the region.

The new branch has an installed LAN that is not yet configured. The IT department is tasked with configuring the Local Area Network (LAN) to ensure seamless communication, efficient data transfer, and secure operations. The network must support various departments, including administration, development, and support, while providing secure and efficient connectivity.

To achieve this, KESC needs to:

- Perform basic IOS configuration on their Cisco switches and routers.
- Configure IP addresses for all network devices.
- Set up routing protocols to enable efficient data routing between different network segments.

The IT team will adopt a structured approach to configure the LAN, beginning with basic IOS configuration, followed by assigning IP addresses, and finally configuring routing protocols.

END

References

You can use the Link provided to give practical LABS to the trainees:

https://www.freeccnaworkbook.com/workbooks/ccna

Anderson, M. C. (2018). LAN Configuration and Optimization: A Step-by-Step Guide. Network Management Quarterly, 22(4), 55-71.

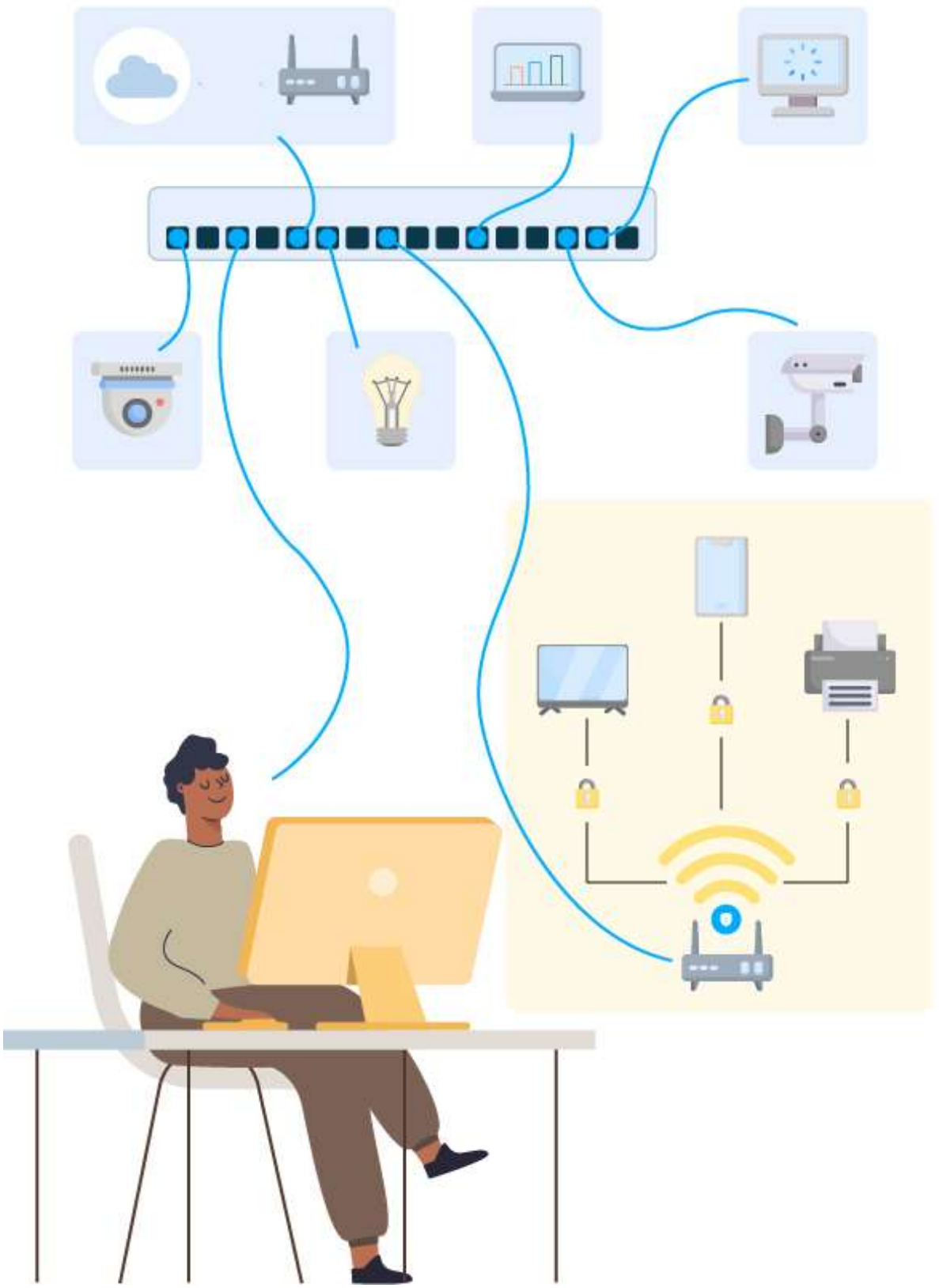
ARWD. (2023). Different Types of LAN. *thewifispecialist*, Page 1.Ashikuzzaman.Md. (December 28, 2023). Components of Local Area Network (LAN). *LIS EDUCATION NETWORK*, 3.

CMW, G. V. (15 March 2023). A Step-by-Step Guide To Installing Slotted Trunking. *Cable Management Warehouse*, Page 1.

How to create a network diagram/. (2024). *miro*, Page 1.

https://www.teamwavelength.com/download/Datasheets/rackmt.pdf. (2024). DATASHEET AND OPERATING GUIDE. *teamwavelength*, Page 1.

Inc, T.-S. T. (April 2024). A Guide to the Different Types of Cable Labeling. *Tri Star Technologies*, Page 1.



Indicative contents
4.1 Management of Files
4.2 Management of Network Printer
4.3 Management of Network Visual Equipment

Key Competencies for Learning Outcome 4: Manage Network Resources

Knowledge	Skills	Attitudes
• Description of network resources that can be shared • Description of the importance of utilizing shared network resources. • Inventory of all existing network resources including hardware and connectivity • Identification of where resource sharing is applied • Description of basic design and structure of networks.	• Sharing network resources over a network • Assigning access permission to network users • Securing network resource by avoiding unauthorized users	• Having Teamwork spirit • Having spirit of perseverance • Being a critical thinker • Being analytical and details oriented

Duration: 5 hrs

Learning outcome 4 objectives:

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

1. Manage appropriately Files based on LAN requirements
2. Share properly Network printers according to the LAN requirements
3. Share properly Network visual equipment (projector and screens) based on LAN requirements

Resources

Equipment	Tools	Materials
• Computer • Switch • Router • Firewalls • Rack • UPS devices • Hubs	• Networking toolkit • Simulation tools	• Network cables • Internet bundles

Indicative content 4.1: Management of Files

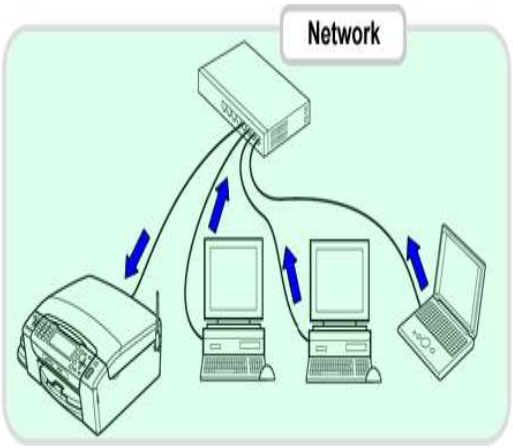
Duration: 3 hrs

Theoretical Activity 4.1.1: Description of Management of files

Tasks:

1: Answer the following questions:

Observe the following images and answer the following questions in groups:



i. What do you see on figure A & B?

ii. what is file and folder sharing?

iii. what are the permission that can be given while sharing file/folder on network?

iv. 4.What is the importance of sharing resources on network?

v. 5.What do think can be challenges of sharing files over network?

2: Present your work to trainer and class

3: Ask any clarifications to the trainer

4: Read key readings 4.1.1 in trainee manual

Key readings 4.1.1.:

Files and folder sharing

Definition: File sharing is the practice of distributing or sharing or providing access to digital media, such as files and folder, electronic devices, computer programs and other network resources.

File sharing is an essential aspect of our daily lives, enabling us to exchange information, collaborate on projects, and access documents and media across different devices and locations.

File sharing affects our personal lives, workplaces, and societies as a whole, presenting both benefits and challenges.

File sharing is one among key advantage gained by users that are at the same network.

These shared resources can significantly enhance productivity, collaboration, and resource utilization within a networked environment. By sharing resources effectively, organizations and individuals can streamline workflows, optimize resource allocation, and reduce costs.

Advantages of using shared files

Here are the key reasons why shared files are important:

Collaboration: Shared files enable multiple users to work collaboratively on the same document, spreadsheet, presentation, or project.

This collaborative environment promotes teamwork and enhances productivity by allowing real-time contributions and feedback from team members, regardless of their physical location.

Version Control: Shared file systems often include versioning capabilities, ensuring that changes are tracked over time. This feature prevents confusion and allows users to revert to previous versions if necessary, maintaining the integrity of the content.

Increased Efficiency: Sharing files electronically reduces the time and effort required to distribute information. Users can instantly share documents without the need for physical media, leading to faster decision-making processes and improved efficiency in communication.

Centralized Information: Shared files help centralize important information, making it easily accessible to authorized users. This centralization streamlines information management, ensuring that everyone is working with the most up-to-date and accurate data.

Reduced Paper Usage: By transitioning from physical documents to shared electronic files, organizations can significantly reduce their paper usage. This not only saves resources but also contributes to environmental conservation efforts.

Enhanced Security: Many shared file systems offer advanced security features, including encryption, access controls, and authentication mechanisms. These measures help protect sensitive information, ensuring that only authorized users can access and modify specific files.

Streamlined Workflows: Shared files can be integrated into collaborative workflows, allowing teams to automate processes, track changes, and receive notifications. Automation streamlines repetitive tasks, reducing manual effort and improving overall workflow efficiency.

Facilitates Learning and Knowledge Sharing: In educational institutions and professional training environments, shared files enable educators to distribute learning materials,

assignments, and resources to students. Similarly, professionals can share industry-related resources, fostering continuous learning and knowledge sharing.

Challenges of using shared files

File sharing also presents some challenges, including:

a. Security: Ensuring data security and preventing unauthorized access is crucial to protect sensitive information.

b. Copyright infringement: Sharing copyrighted material without proper authorization is illegal and can lead to legal consequences.

c. Version control: Managing multiple versions of shared files can be complex, requiring careful tracking and change management strategies.

d. Network bandwidth: Sharing large files can consume significant network bandwidth, potentially affecting overall network performance.

Applications of file sharing

File sharing is widely used in various settings, including:

a. Personal use: Individuals share photos, videos, documents, and other personal files with friends, family, and colleagues.

b. Professional use: Businesses share documents, presentations, project files, and other work-related materials with employees and clients.

c. Educational use: Educators share learning materials, assignments, and resources with students to enhance teaching and learning.

Practical Activity 4.1.2: Sharing file and folder

Task:

1: Read carefully and perform the following task

As network assistant you are requested to share file and folder named “your full name” and set permission based on trainer’s demonstration.

2: Follow the trainer's demonstration on sharing a file or folder, setting access permissions for a file or folder, and accessing shared files and folders.

3: Perform the given task based on trainer’s demonstration

4: Ask for assistance whenever necessary

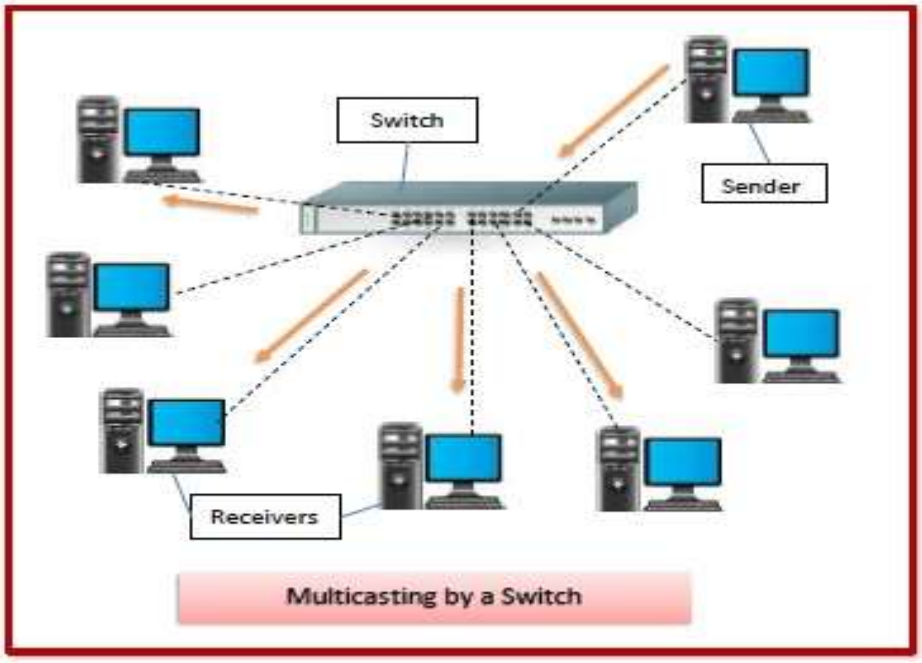
5: Present your task to trainer

6: Read key reading 4.1.2. in trainee’s manual

7: Perform the task provided in application of learning 4.1.2

Key readings 4.1.2

Share Files and Folder

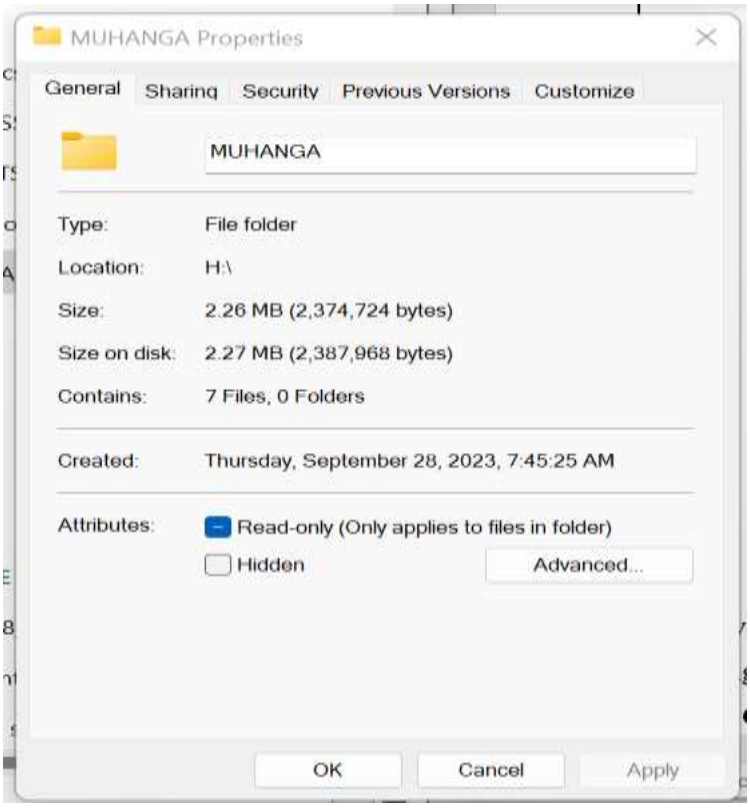


Sharing files and folders over a network can be a simple way to enable access to those resources for multiple users or devices. Here's a simple guide on how to do this on both Windows operating systems.

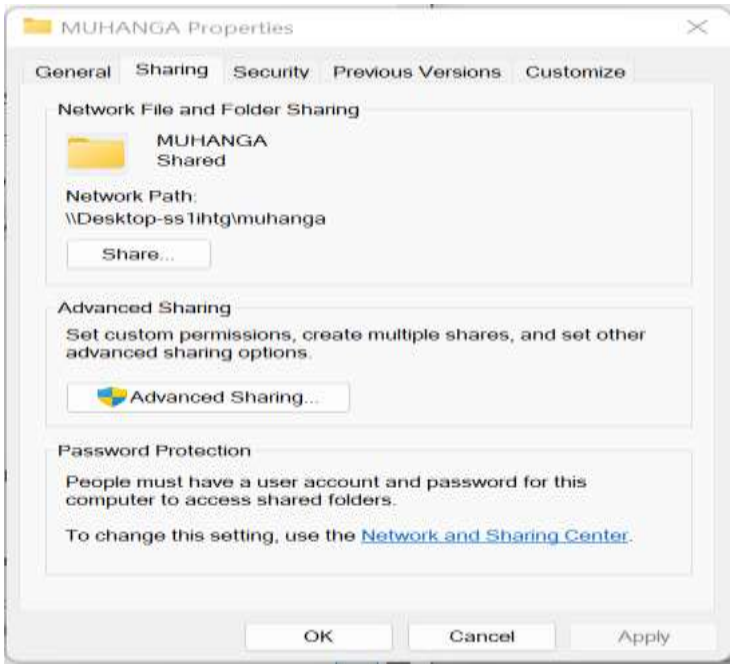
Steps to Share files and folder in Windows operating system:

1. **Right-Click on the Folder You Want to Share:** You can find the folder by opening the File Explorer (the yellow folder icon typically found on the taskbar). Once you find the folder you want to share, right-click on it.

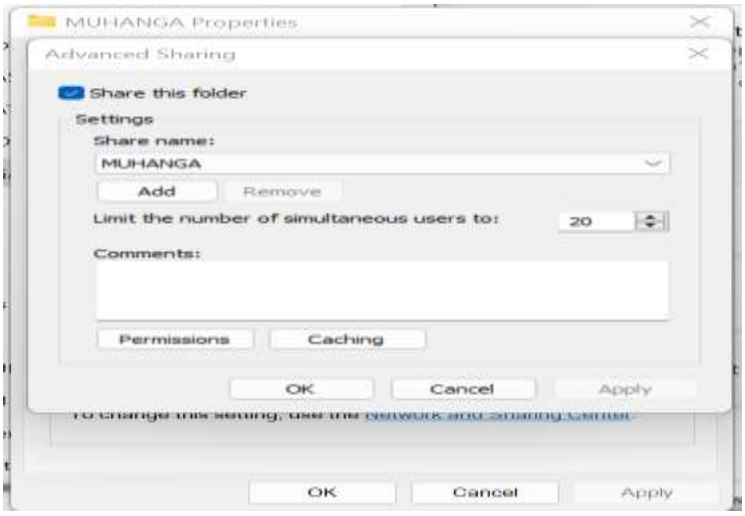
2. Select 'Properties': This will open a new window with a number of tabs.



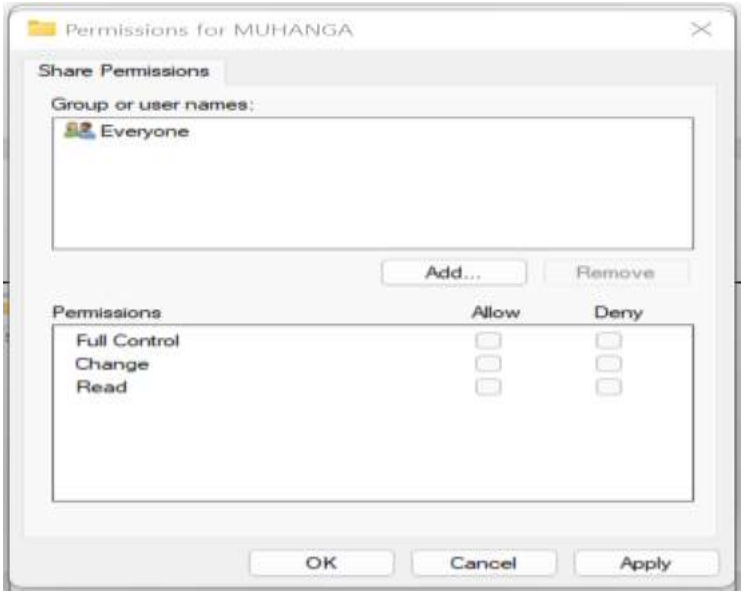
3. Navigate to the 'Sharing' Tab: Here you will find options related to network sharing.



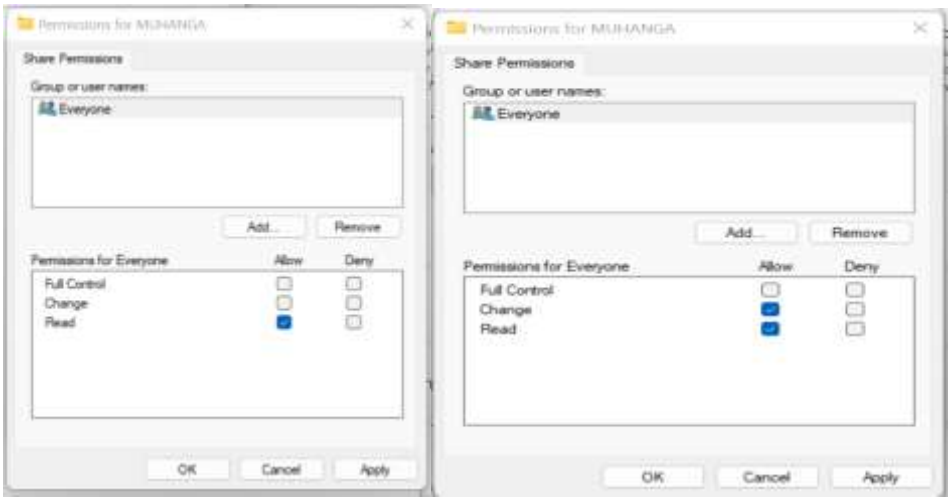
4. Click on 'Advanced Sharing...': This will open another window.



5. Check 'Share this folder': In the window that opens, you'll see a checkbox labelled "Share this folder." Check this box to enable sharing. You can also enter a share name, comments, and limit the number of simultaneous users.



6. **Set Permissions:** If you click on 'Permissions', you can set who can access the folder and what they can do (read, change, or full control).



7. **Apply and Close:** Click 'Apply' and then 'OK' to close the dialog boxes.

Now, your folder should be accessible on the local network. Other users can access it by entering your PC's IP address followed by the folder's share name, like this: **\\192.168.1.2\sharename.**

Assign Access Permission on Shared Files and Folder

The steps to assign access permissions on shared files and folders vary depending on the system and platform you are using. Here are general steps for Windows.

Windows

1. Right-click on the file or folder you want to set permissions for, then click **Properties**.

2. Click on the **Security** tab.

3. Click **Edit** to change permissions.

4. Click **Add** to add a new user or group.

5. Enter the name of the user or group you want to add and click **Check Names** (the system should recognize the name), then click **OK**.

6. Now select the user or group and check the permission boxes you want to grant them (Full control, Modify, Read & execute, List folder contents, Read, Write).

7. Click **Apply** and **OK** to save changes.

Access shared files and folders

Accessing shared files and folders over a network involves several steps and can differ depending on the operating system you're using.

On Windows:

1. Open the File Explorer. This can be done by clicking the folder icon in the taskbar, or by pressing the Windows key + E.

2. In the left-hand pane, click on "Network". This should display a list of all computers currently connected to your network.

3. Double-click on the computer that's sharing the files or folders you want to access.

4. If prompted, enter the username and password associated with that computer.

5. Once connected, you should be able to see and access the shared files or folders.

Steps to share file and folder in window computer

Sharing files and folders in Windows computers can be done easily using the built-in file sharing features. Here are the steps to share a file or folder on a Windows computer:

Sharing a Folder:

- ✓ **Select the Folder:** Locate the folder you want to share. Right-click on the folder and select "Properties" from the context menu.
- ✓ **Open the Sharing Tab:** In the Properties window, go to the "Sharing" tab.

- ✓ **Share the Folder:** Click on the "Share" button. If you don't see the "Share" button, click on the "Advanced Sharing" button and check the box that says "Share this folder."
- ✓ **Set Permissions:** You can set permissions for the shared folder by clicking on the "Permissions" button. Here, you can add specific users or groups and assign them permissions like Read or Read/Write.
- ✓ **Click OK:** After setting up sharing and permissions, click "OK" to apply the changes.

Sharing a File:

- ✓ **Select the File:** Locate the file you want to share. Right-click on the file.
- ✓ **Choose Share:** From the context menu, hover over "Give access to," and then select "Specific people."
- ✓ **Select Users or Groups:** In the File Sharing window, you can add specific users or groups. You can also choose whether they can only read the file or have read/write access.
- ✓ **Click Share:** After selecting the users or groups and setting the appropriate permissions, click the "Share" button.

Accessing Shared Files/Folders:

Once a folder or file is shared, other users on the same network can access it using File Explorer:

- ✓ **Open File Explorer:** Open File Explorer on another computer within the same network.
- ✓ **Find the Shared Computer:** In the left sidebar, look for the computer under the "Network" section. Click on the computer to see the shared folders and files.
- ✓ **Access Shared Files/Folders:** Double-click on the shared folder to access its contents. If prompted, enter the username and password of the account with access permissions.

Remember that both computers need to be on the same network, and the user account on the shared computer must have the necessary permissions to access the shared files or

folders. Additionally, you might need to adjust network and sharing settings in the Windows Control Panel if you encounter issues accessing shared content.

What Do File Permissions Look Like ?

Generally speaking, there are two categories that need to be considered when viewing file permissions: Actions and user groups.

Actions your site's plugins and files can make are:

- **Read** – allows access to a file to view its contents only
- **Write** – allows the file to be changed
- **Execute** – gives access to a file in order to run the programs or scripts that are contained in it

The user groups of the actions can be:

- **User** – you as the owner of your site
- **Group** – other users that can also have access to the files you choose such as the members of your site
- **World** – anyone with an internet connection who tries to view your files

File permissions are primarily viewed as three consecutive numbers:

- **First number** – the access to file actions granted to the **user**
- **Second number** – the file access given to the **group**
- **Third number** – the amount of file access given to the **world**

To come up with these numbers, a value is given to each possible action combination:

- **0** – no access
- **1** – execute
- **2** – write
- **3** – write and execute
- **4** – read
- **5** – read and execute
- **6** – read and write
- **7** – read, write and execute

How to use Share permissions to Share a folder

The best way to understand how share permissions work is to perform an all-too-common task for organizations that share network resources — that is, to share a network folder using Advanced Settings.

1. Use File Explorer to locate the folder you want to share, right-click on it and select Properties
2. Click the Sharing tab
3. Click on Advanced Sharing
4. Check the Share this folder checkbox
5. At this point, your folder is shared and users in the Everyone group will have read-only access. To assign any further permissions, click Permissions
6. You are now looking at the Share Permissions window. Here, you can change the share permissions assigned to users and groups by first clicking on the item you want to modify and then using checkboxes to check which share permissions you want to assign. The first group you will see is Everyone, which is assigned the lowest-level share permissions
7. Click Apply
8. Click OK

How to use share permissions to share a file

A related change new in Windows 10 is how to share with specific people. This change applies to both files and folders. To share a file with a specific person:

1. Use File Explorer to locate the file you want to share
2. Hover over “Give access to”
3. Select “Specific people”
4. You will me prompted with the Network Access Wizard
5. Select which user you want to share the file with
6. Or click “Add” to add other users
7. Click share

Permission levels can be set with a drop-down menu in the network access window. Specific users will then be prompted with their Windows credentials to access the shared file.

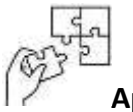
Points to Remember

- File sharing is the practice of distributing or providing access to digital media
- Benefits of file sharing, including: Collaboration, Communication, Efficiency, Cost-effectiveness, Accessibility
- Type of permission set on file and folder shared on network:
  - ✓ Read permission
  - ✓ Write permission

- ✓ Full(read and write) permission

There are two categories that need to be considered when viewing file permissions: Actions and user groups.

- Actions your site's plugins and files can make are: Read, Write and Execute.
- The user groups of the actions can be: User, Group and World
- File permissions are primarily viewed as three consecutive numbers: **First number** – the access to file actions granted to the user, **second number** – the file access given to the group and **Third number** – the amount of file access given to the world



Application of learning 4.1.

XYZ Marketing is a small marketing agency located in Kigali, Rwanda. The Agency has a small office with five employees who need to share files and collaborate on projects. The office has a local area network set up with a central file server.

They want to hire a network technician to set up the file server, Creating Shared Folders, and Setting Permissions.

Participants:

Office Manager (Eve), Employee 1 (Frank), Employee 2 (Grace), Employee 3 (Henry), Employee 4 (Ivy)

Task:

- The office manager, Eve, sets up a dedicated file server that all employees can access. This server is connected to the office LAN.
- Eve creates shared folders on the file server for different departments and projects.
- Eve configures permissions for each folder. For instance, the "Sales" folder is accessible only to Frank and Grace, while the "HR" folder is accessible to Henry and Ivy.
- She sets the "Marketing" folder to allow read and write access for all employees, as it will be used for collaborative projects.

Indicative content 4.2: Management of Network Printer

Duration: 1 hour

Theoretical Activity 4.2.1: Description of Management of Network Printer

Tasks:

1: Answer the following questions:

1. What is the main benefit of sharing a printer?
2. What is the process of sharing a printer called?
3. What is a print server?
4. What is a printer driver?

2: Create small groups and engage in discussions on the questions provided.

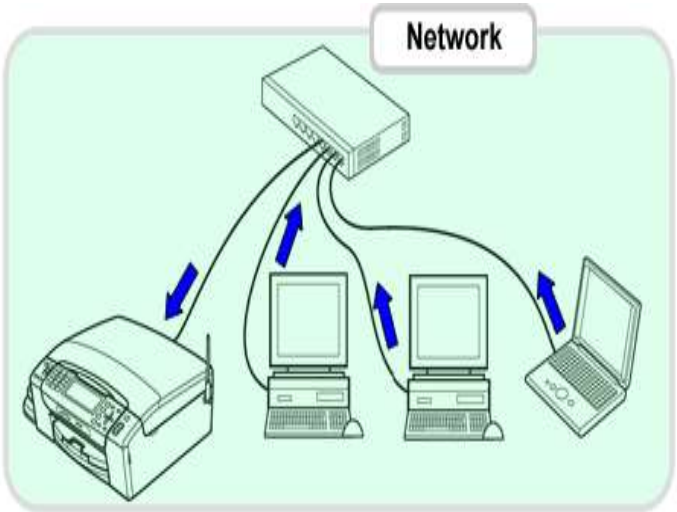
3: Present your findings to trainer and your colleagues

4: Take notes of key points and ask clarifying questions if needed.

5: Read key readings 4.2.1. in trainee's manual

Key readings 4.2.1.:

Discuss the Network Printer sharing



Configure Network Printer

Before network users can print on the network, the network's printers must be properly configured. For the most part, this is a simple task. All you have to do is configure each client that needs access to the printer.

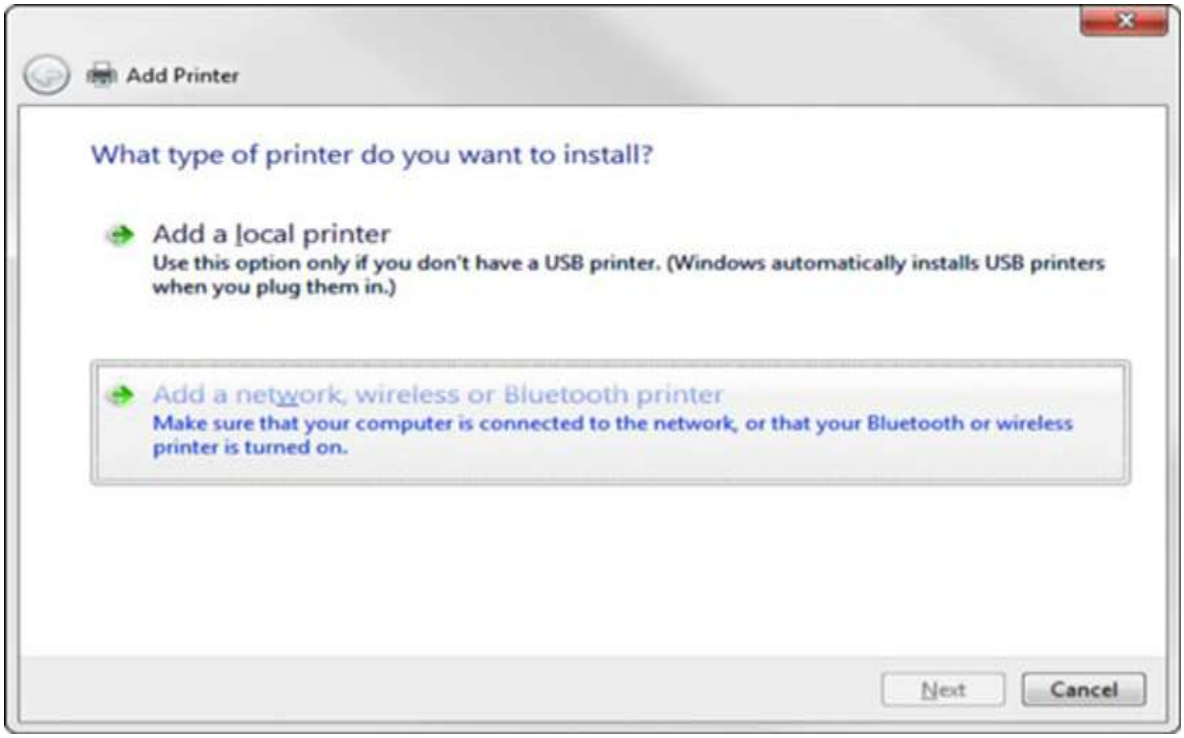
Before you configure a network printer to work with network clients, read the client configuration section of the manual that came with the printer. Many printers come with special software that provides more advanced printing and networking features than the standard features provided by Windows. If so, you may want to install the printer manufacturer's software on your client computers rather than use the standard Windows network printer support.

Adding a network printer

The exact procedure for adding a network printer varies a bit, depending on the Windows version that the client runs. The following steps describe the procedure for Windows 7 (the procedure for Windows Vista is similar):

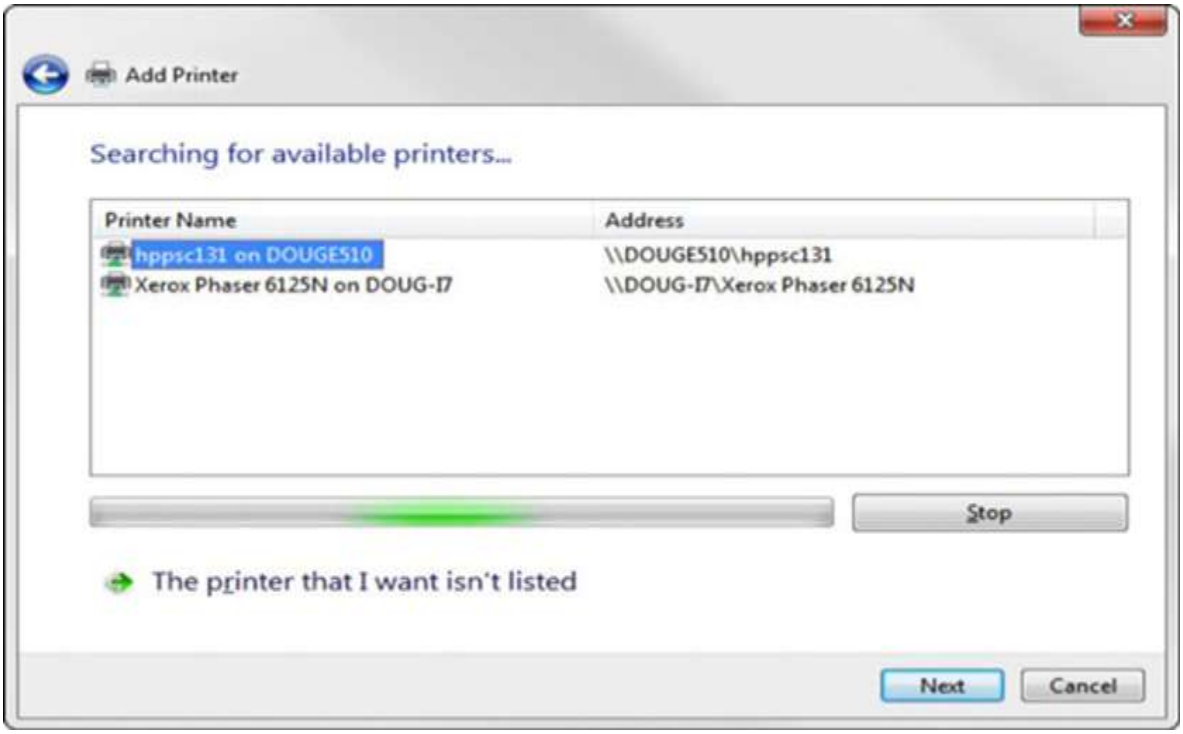
1. Choose Start→ Devices and Printers.
2. Click the Add a printer button on the toolbar.

This step starts the Add Printer Wizard.



3. Select the Add a Network, Wireless or Bluetooth Printer option.

The wizard searches the network for available printers and displays a list of the printers it finds.



4. Click the printer you want to use.

If you can’t find the printer you want to use, click The Printer That I Want Isn’t Listed and enter the UNC or IP address for the printer when prompted.

5. Click Next to add the printer.

The wizard copies to your computer the correct printer driver for the network printer. (You may be prompted to confirm that you want to add the driver. If so, click Install Driver to proceed.)

The Add Printer Wizard displays a screen that shows the printer’s name and asks whether you want to designate the printer as your default printer.

6. If you want, designate the printer as your default printer.

7. Click Next to continue.

A final confirmation dialog box is displayed.

8. Click Finish.

You’re done!

Share Network Printer

If you'd like to share a network printer across multiple computers, the steps vary based on the operating system you're using.

Windows

1. Connect the printer to your computer and ensure that it's powered on.
2. Open the "Control Panel" and select "Devices and Printers".
3. Right-click the printer you want to share, and select "Printer properties".
4. Click the "Sharing" tab.
5. Check the box that says "Share this printer".
6. In the "Share name" field, enter a name for the shared printer (this is the name that other computers on your network will use to connect to this printer).
7. Click "OK".

8. Now, on the other computers on your network, you can add the shared printer by going to "Devices and Printers" -> "Add a printer" -> "Select a shared printer by name" and then typing in the name of the shared printer.

Assign Access Permission on Shared Network Printer

The same way as files have security information, so do printers, and you need to set which users can perform actions on each network printer

1. Logon as an Administrator

2. Double click "My Computer" and then select printers

3. Right click on the printer whose permissions you wish to change and select properties

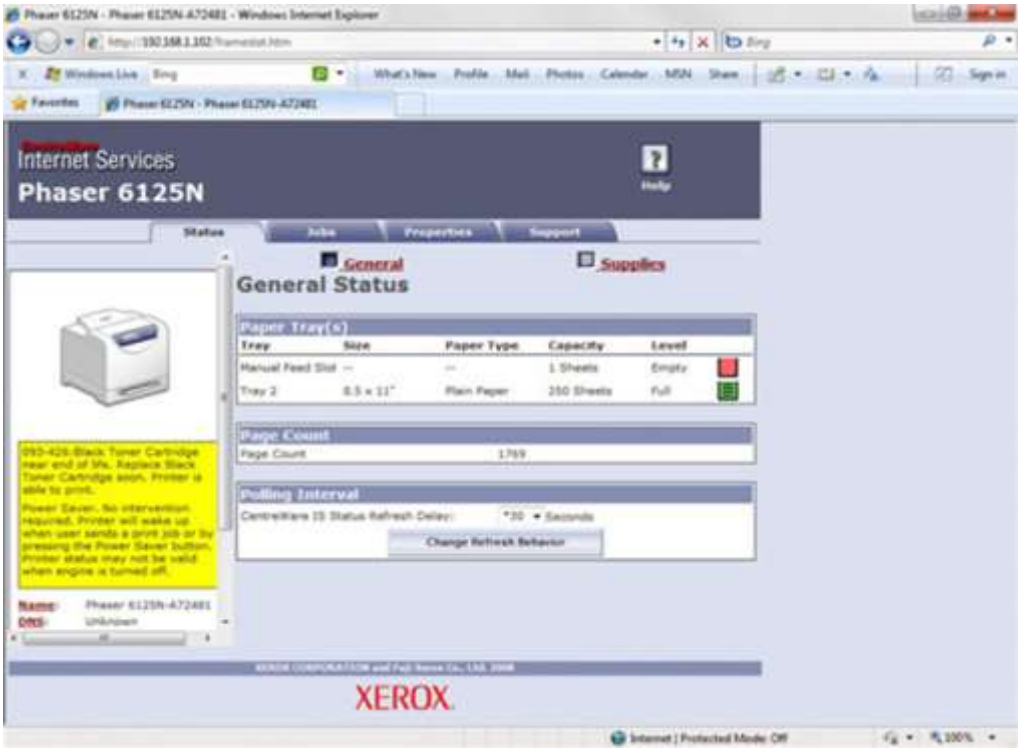
4. Click the security tag and select permissions

5. You can now add users/groups and grant them the appropriate privilege

6. Click OK when finished

Access shared printers

Printers that have a direct network connection often include a built-in web server that lets you manage the printer from any browser on the network. For example, the following illustration shows the home page for a Xerox Phaser 6125 printer. This web interface lets you view status information about the printer and check the printer's configuration. You can even view error logs to find out how often the printer jams.



To call up a printer's web interface, enter its IP address or host name in the address bar of any web browser.

In addition to simply displaying information about the printer, you can also adjust the printer's configuration from a web browser. For example, the following illustration shows the Network Settings page for the Xerox printer. Here, you can change the network configuration details, such as the TCP/IP host name, IP address, subnet mask, domain name, and so on.

Other configuration pages allow you to tell the printer to send an e-mail notification to an address that you specify whenever you encounter a problem with the printer.

As the network administrator, you may need to visit the printer's web page frequently, in fact you should add it to your browser's Favorites menu so that you can get to it easily. If you have several printers, add them under a folder named Network Printers.

Practical Activity 4.2.2: Configuring a Network Printer

Task:

1: Perform the task outlined below:
Refiring on the Theoretical Activity 4.2.1, do the following task:

i. Start by ensuring the printer is properly connected to the network.
ii. Install the printer driver on the computer you want to use for printing
iii. Once the driver is installed, configure it to recognize the printer on the network
iv. Once the printer is configured, perform a test print to ensure it's working correctly

2: Follow the trainer's demonstration of how to share and set permission on network printer

3: Repeat the task individually until perfect result

4: Read key readings 4.2.2 in trainee's manual

Key readings 4.2.2

Share Network Printer

If you'd like to share a network printer across multiple computers, the steps vary based on the operating system you're using.

Windows

1. Connect the printer to your computer and ensure that it's powered on.
2. Open the "Control Panel" and select "Devices and Printers".
3. Right-click the printer you want to share, and select "Printer properties".
4. Click the "Sharing" tab.
5. Check the box that says "Share this printer".
6. In the "Share name" field, enter a name for the shared printer (this is the name that other computers on your network will use to connect to this printer).
7. Click "OK".
8. Now, on the other computers on your network, you can add the shared printer by going to "Devices and Printers" -> "Add a printer" -> "Select a shared printer by name" and then typing in the name of the shared printer.

Connecting a printer to a Local Area Network (LAN) involves several steps, including physical connection, software installation, and network configuration. Here are key steps to connect a printer and manage it on a LAN:

SELECT THE RIGHT PRINTER:

Choose a printer that is compatible with your network and meets the requirements of your users. Ensure it has both wired and wireless connectivity options if needed.

Physical Connection:

Connect the printer to the LAN using either an Ethernet cable or a wireless connection, depending on the printer's capabilities and your network infrastructure.

Install Printer Drivers:

Install the printer drivers on the computer or server that will be used to manage the printer. You can usually find the drivers on the manufacturer's website or on the installation CD that

came with the printer.

Add Printer to the Network:

If the printer has a built-in network interface, access its settings through the control panel or a web browser. Configure the network settings, including IP address, subnet mask, and gateway, based on your LAN configuration.

Dynamic Host Configuration Protocol (DHCP):

If your LAN uses DHCP, ensure that the printer is set to obtain an IP address automatically. This is a common setting for home networks and small businesses.

Static IP Address (Optional):

For larger networks or when you want a fixed IP address for the printer, assign a static IP address to the printer to ensure consistency and ease of management.

Test the Connection:

Print a test page or use the printer's diagnostic tools to ensure that it's properly connected to the network.

Share the Printer (Optional):

If the printer is connected to a computer, share the printer on that computer to allow other devices on the network to use it. This is especially relevant in a home or small office environment.

Install Drivers on Client Devices:

Install the printer drivers on all devices that need to access the printer. This includes laptops, desktops, and any other devices on the LAN.

Configure Print Server (Optional):

If you have a dedicated print server, configure it to manage the printer centrally. This is common in larger networks and can simplify management and monitoring.

Monitor Printer Usage:

Use the printer management software or the printer's web interface to monitor usage, check ink or toner levels, and troubleshoot any issues.

Implement Print Policies (Optional):

Depending on your network requirements, you may want to implement print policies to control access, set printing quotas, or manage print job priorities.

Regular Maintenance:

Periodically check for firmware updates for the printer and apply them as needed. Regularly inspect the printer for any physical issues and perform routine maintenance tasks.

Points to Remember

- Connecting and using a printer on a LAN (local area network) involves a few key steps:
  - ✓ Hardware Setup
  - ✓ Software Installation
  - ✓ Driver Configuration
  - ✓ Test Printing
  - ✓ Network Sharing
  - ✓ Troubleshooting
- Remember, the specific steps may vary depending on the printer model and network configuration, but these general guidelines should help you connect and use a printer on a LAN effectively.

Application of learning 4.2.

A medium-sized office in Kigali, Rwanda, has several network printers shared among employees. The office manager is responsible for ensuring that printers are properly managed to meet the printing needs of the staff.

Participants:

-Office Manager (Alice)

-IT Support Technician (Brian)

-Employees (various roles)

Tasks:

- ✓ Connect the printers to the office LAN and configure their IP addresses.
- ✓ Installs the necessary printer drivers on all employee computers, ensuring that everyone can access the printers seamlessly.
- ✓ Sets up user access groups based on departments. For instance, the marketing team has access to color printers, while the finance team uses black-and-white printers.

- ✓ Brian may use printer management software to monitor the status of all network printers. He receives alerts for low ink levels or paper jams, allowing for timely maintenance.

Indicative content 4.3: Management of Network Visual Equipment

Duration: 1 hrs

Theoretical Activity 4.3.1: Description of Management of Network Visual

Tasks:

1: Read key reading 4.3.1 and answer the following questions:

i. What is the definition of network visual equipment?

ii. What is the importance of sharing a network visual equipment?

iii. What are the different types of network visual equipment?

2: Form small groups after introduction of the activity and discuss on provided questions

3: Present your findings to trainer and your colleagues

4: Take notes of key points and ask clarifying questions if needed

Key readings 4.3.1.:

1. **Network visual equipment**

Network visual equipment refers to devices that are used to display, project, or capture visual information within a network environment. These devices are essential for effective communication, collaboration, and information sharing.

2. **Importance of sharing a network visual equipment**

Sharing network visual equipment can:

- Make meetings more engaging and productive by allowing participants to share and interact with content in real-time.
- Enable effective communication with remote teams or clients regardless of geographical barriers.
- Reduce the need for multiple devices, leading to cost savings on hardware
- Video conferencing can minimize the need for travel, saving on transportation and accommodation expenses.
- Reduce the time spent setting up individual devices.

- Networked equipment can be centrally managed, ensuring that updates, troubleshooting.
- Visual equipment allows for real-time sharing of data, charts, and presentations, facilitating informed decision-making during meetings and discussions.
- Visual displays can make complex information easier to understand, aiding in quicker and more accurate decision-making.

Types of Network Visual Equipment

Here are some common types:

1. Displays and Monitors

- **Large-screen displays:** These are ideal for presenting presentations, displaying data, or conducting video conferences.
- **Interactive whiteboards:** Combining the functionality of a whiteboard with a touchscreen, these devices allow for collaborative brainstorming, note-taking, and presentations.
- **Computer monitors:** Used for displaying information from connected computers.

2. Projectors

- **Overhead projectors:** Used to project transparencies onto a screen.
- **Video projectors:** Project images and videos from various sources onto a screen.
- **Laser projectors:** Offer high-quality images and longer lifespans compared to traditional projectors.

3. Cameras

- **Webcams:** Used for video conferencing and live streaming.
- **Document cameras:** Capture images and videos of documents or objects.
- **Security cameras:** Used for surveillance and monitoring.

4. Video Conferencing Systems

- **Standalone units:** These systems include cameras, microphones, and speakers in a single package.
- **Software-based solutions:** Utilize internet-connected devices and software to enable video conferencing.

5. Interactive Displays

- **Touchscreen displays:** Allow users to interact with content by touching the screen.
- **Digital signage displays:** Used to display dynamic content, such as advertisements, announcements, or menus.

6. Input Devices

- **Keyboards:** Used for entering text and data.
- **Mice:** Used for navigating computer interfaces.
- **Touchpads:** Provide a touch-sensitive surface for navigation.

7. Audio Equipment

- **Microphones:** Capture sound for video conferencing, recording, or presentations.
- **Speakers:** Reproduce sound for audio output.
- **Headsets:** Combine microphones and headphones for hands-free communication.

Practical Activity 4.3.2: Managing Network Visual Equipment

Task:

1: Read the task carefully and perform the task described below:

By Considering projector installed in your computer LAB, set the projector to LAN so that may be used by any user on a network

2: Observe the trainer as demonstrate how to Setup and Configure Network Visual equipment on the LAN, taking notes and asking questions as needed.

3: Perform the given task and apply what you have learnt from step 2.

4: Read key readings 4.2.2 in trainee's manual

Key readings 4.3.2

Assign Access Permission on Shared Network Visual Equipment

Providing and managing access permissions for shared network visual equipment typically involves a combination of hardware configuration and software management. Here is a summary of steps you could follow:

1. **Know Your Equipment:** Understand what kind of visual equipment you

have, and how it's designed to share access. Examples include networked projectors, shared displays, or video conferencing systems. Check the user manual or online documentation for details on how to manage access.

2. **Define User Groups:** Determine which users need access to the equipment. This might be everyone in your organization, specific departments, or only certain individuals.

3. Set Up Hardware: Configure the physical setup of your equipment to connect to the network. This could involve configuring an IP address, setting up wireless access, or connecting ethernet cables.

4. **Configure Network Access:** This often involves logging into the equipment's built-in interface (usually via a web browser) and specifying which devices or IP addresses are allowed to connect. Depending on the device, you may also have to configure firewall settings to allow traffic to and from the device.

5. **Assign User Permissions:** Use the equipment's built-in interface to assign permissions to the user groups you've defined. These permissions might include the ability to turn the equipment on and off, change settings, or initiate broadcasts.

6. **Set Up Software Access:** If the equipment uses special software for access, install this software on the devices of the users who need access. In the software settings, specify the IP address or device name of the equipment.

7. Test Access: Have your users test their access to ensure it works properly. They should be able to connect to the device, use it as expected, and not have access to functions they shouldn't.

3. Document Everything: Keep track of your configuration settings, user groups, and access procedures in case you need to troubleshoot or reconfigure things in the future. Also, ensure that your users have access to

guides or documentation that explain how to use the equipment.

4. Monitor and Update: Regularly check in on your equipment to ensure it's working properly and meeting your users' needs. Be prepared to update the equipment's software, adjust permissions, or reconfigure settings as needed.

Notes: Remember that the specifics of these steps can vary significantly depending on the particular equipment you're using and the network it's connected to. Always refer to your equipment's documentation and your IT department's policies when setting up networked equipment.

Points to Remember

- Network visual equipment plays a crucial role in modern organizations, impacting various aspects of operations, communication, and productivity.
- Network visual equipment plays a crucial role in modern organizations, impacting various aspects of operations, communication, and productivity.

Application of learning 4.3.

The Kigali Employment Service Centre (KESC) is a government-funded organization that provides a range of services to job seekers and unemployed youth in Kigali, Rwanda. The centre was established in 2013 with the goal of reducing unemployment in the city.

Its target is to reduce unemployment rate and enhance skills by training and providing job application assistance to unemployed youth by free of charge.

Services offered by Kigali Employment Service Centre/City of Kigali includes:

1.Internet access to get information about jobs

2.Assistance in CV writing and interviews preparations

3.Trainings like Entrepreneurship, IT, English, Job search strategy and many other

4.Print and scanning service

As network technician connect projector on a network and permit 3 facilitators to use the projector and limit other trainers and trainees.

Learning outcome 4 end assessment

Theoretical assessment

Read each question carefully and select the best answer from the choices provided.

Management of Files

1. **Which command is used to copy a file in Windows?**

   A) move
   B) copy
   C) del
   D) touch

2. **In Windows, what is the command to display the contents of a directory?**

   A) list
   B) dir
   C) ls
   D) show

3. **What is the purpose of a file permissions system in Windows?**

   A) To compress files
   B) To protect files from unauthorized access
   C) To rename files
   D) To delete files

4. **Which command is used to change file attributes in Windows?**

   A) chown
   B) attrib
   C) chgrp
   D) chperms

5. **What is the default file system used by Windows?**

   A) NTFS
   B) ext4
   C) HFS+
   D) FAT32

Management of Network Printer

6. **What is a network printer?**

A) A printer connected directly to a computer
B) A printer that can be accessed over a network
C) A wireless printer
D) A portable printer

7. **Which protocol is commonly used for network printing?**

A) FTP
B) HTTP
C) IPP
D) SMTP

8. **How can you add a network printer in Windows?**

A) Control Panel > Devices and Printers > Add a printer
B) Control Panel > Network and Sharing Center > Add a printer
C) Control Panel > System > Add a printer
D) Control Panel > Security > Add a printer

9. **What is the purpose of a print server?**

A) To store print jobs in a queue
B) To manage print jobs and printers on a network
C) To scan documents
D) To convert files to PDF

10. **Which command can be used to list all printers on a Windows system?**

A) wmic printer list
B) print -l
C) printers -list
D) lp -list

Management of Network Visual Equipment

11. **What is an example of network visual equipment?**

A) Printer
B) Router
C) Projector
D) Scanner

12. **How can a network projector be accessed by multiple users?**

A) By connecting it to a single computer
B) By connecting it to a network
C) By using a USB hub
D) By using an HDMI splitter

13. What is the purpose of a digital signage system?

A) To display static images only
B) To provide dynamic visual content to multiple displays
C) To connect multiple monitors to one computer
D) To act as a backup display

14. Which protocol is often used to control networked AV equipment?

A) SNMP
B) HTTP
C) SSH
D) RS232

15. What is a key advantage of managing visual equipment over a network?

A) Reduced cost of equipment
B) Ability to control and update equipment remotely
C) Improved print quality
D) Faster data transfer speeds

Practical assessment

The Rwanda TVET Board (RTB) is a government institution that was established in 2020. The headquarters of RTB is equipped with a file server, a network printer, and a projector connected to the network. However, employees have been experiencing issues such as slow file transfers, frequent print job failures, and difficulties displaying presentations on the projector.

In response to these challenges, the IT team aims to implement a structured plan that focuses on improving file management on network servers, optimizing the setup and management of the network printer, and effectively controlling the network visual equipment, all while providing solutions to the identified issues.

END

References

Brown, P. D., & Clark, R. W. (2017). Effective Network Resource Management Strategies. International Journal of Networking, 12(1), 34-48.

Bozeman.D. (2024). DATASHEET AND OPERATING GUIDE . *teamwavelength*, Page 1.

CMW, G. V. (15 March 2023). A Step-by-Step Guide To Installing Slotted Trunking. *Cable Management Warehouse*, Page 1.

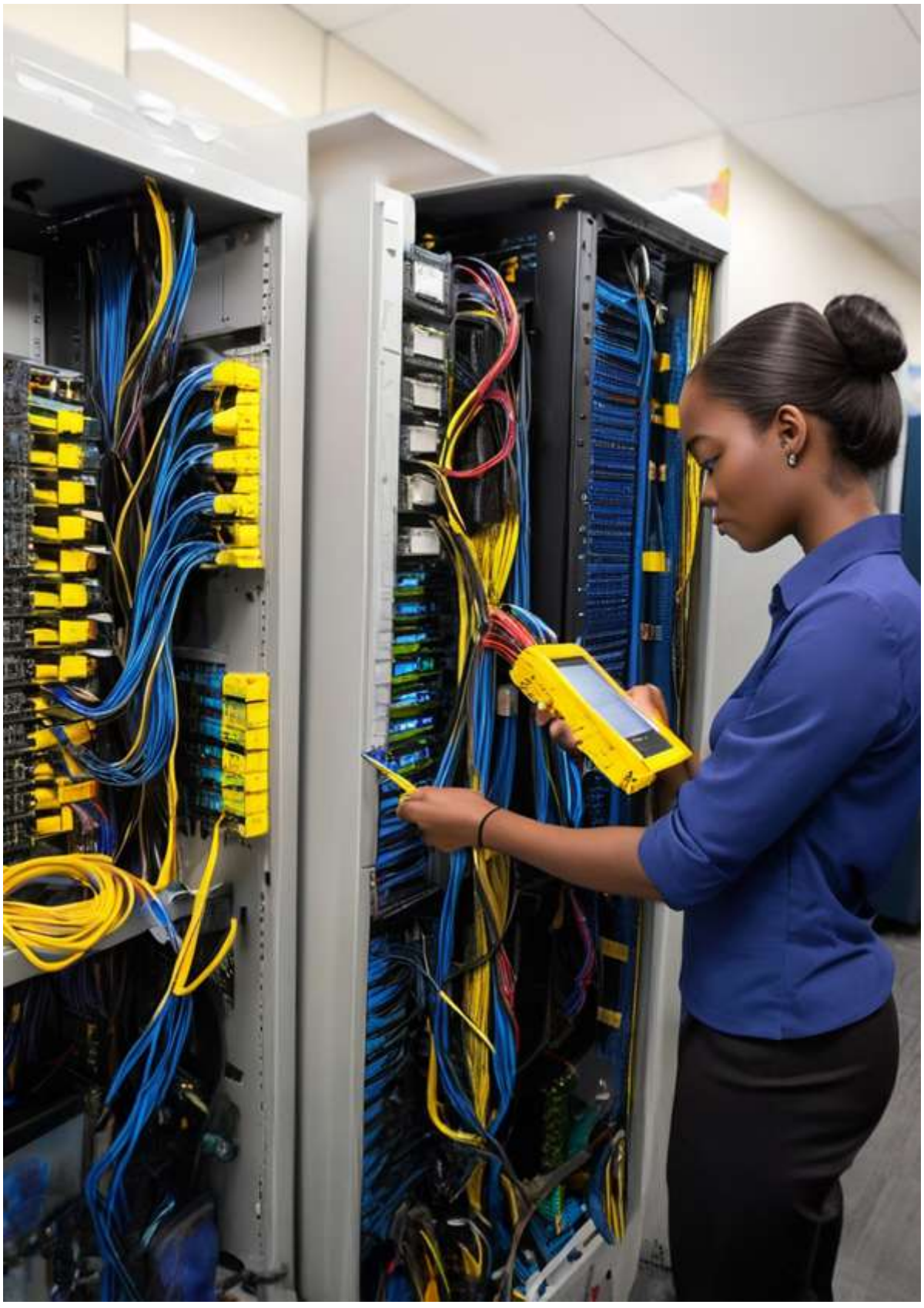
How to create a network diagram/. (2024). *miro*, Page 1.

https://www.teamwavelength.com/download/Datasheets/rackmt.pdf. (2024). DATASHEET AND OPERATING GUIDE. *teamwavelength*, Page 1.

Organizer, C. (2024). Cable Labels & Printers. *Cable Organizer*, Page 1.

types-of-network-topology. (06 Sep, 2024). *geeksforgeeks*, Page 1.

What-is-network-topology/. (2006-2023). *spiceworks*, Page 2.



Indicative contents
5.1. Identification of Testing Types
5.2· Selection of Testing Tools
5.3 · Connectivity Testing
5.4. Functionality Testing
5.5. Performance Testing
5.6. Documentation of Network installation

Key Competencies for Learning Outcome 5: Test LAN

Knowledge	Skills	Attitudes
• Description of testing type • Description of network testing tool	• Selecting testing tools • Testing the LAN • Documenting the installed LAN	• Having Critical thinking • Being Self-motivated • Having spirit of Accountability

Duration: 5 hrs

Learning outcome 5 objectives:

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

1. Identify properly Types of testing according to the LAN requirements
2. Select correctly Testing tools based on type of testing
3. Perform correctly Connectivity testing according to the configured network
4. Perform correctly Functional testing according to configured network
5. Perform correctly Performance testing according to the configured network
6. Document properly Network installation based on work done.

Resources

Equipment	Tools	Materials
• Computer • Router • Switch	• Network toolkit • Network Cable Testers • Network Analyzers • Spectrum Analyzers • Wireshark • SolarWinds Network Performance Monitor (NPM) • SolarWinds NetFlow Traffic Analyzer	• Network cables • Internet bundles

Indicative content 5.1: Identification of Types of Testing

Duration: 1 hour

Theoretical Activity 5.1.1: Identifying types of testing

Tasks:

1: Listen attentively as the trainer explains what network testing is and discuss on the following questions in your small groups:

a. Explain the following testing types:
b. Transmission testing
c. Connectivity testing
d. Functional testing
e. Performance testing

2: Present your findings to the trainer and whole class

3: Take notes of key points and ask clarifying questions if needed.

4: Read the key readings 5.1.1 in their manual for more clarifications

Key readings 5.1.1.:

Identification of Testing Types

- **Transmission testing**

Transmission testing in a Local Area Network (LAN) setup refers to the process of assessing the quality, speed, and reliability of data transmission within the network.

This involves a variety of tests to ensure that network devices (like switches, routers, and cables) are functioning as intended, and that the data can travel from its source to its destination without unacceptable levels of packet loss, latency, or jitter.

- **Connectivity testing**

Connectivity testing is the process by which we check if all the devices (like computers, printers, switches, routers, etc.) within a Local Area Network (LAN) are correctly connected and communicating with each other. This process is crucial in maintaining a functional network and ensuring that data can be transferred across the network as intended.

- **Functional testing**

Functional testing in a Local Area Network (LAN) context involves verifying that network devices, services, and software are operating as expected.

The focus is on testing the behaviour of these components under various conditions and ensuring that they meet specified functional requirements. In functional testing, the internal structure of the system is usually not considered, but rather the focus is on the outputs generated in response to selected inputs and execution conditions.

- **Performance testing**

Performance testing in a Local Area Network (LAN) involves assessing the speed, responsiveness, and stability of applications, systems, or network components within a confined geographical area.

The goal is to ensure that the network infrastructure can handle the expected load and deliver satisfactory performance to users.

Ping Test:

- Use the ping utility to test the connectivity between devices in the LAN.
- Ping different devices and record the response time and any packet loss.
- Analyze the results to identify any connectivity issues or delays.

Throughput Test:

- Transfer large files between devices in the LAN using tools like FTP or SCP.
- Measure the time taken to transfer the files and calculate the average data throughput.

- Compare the achieved throughput with the network's expected capacity.

Bandwidth Test:

- Utilize specialized tools or online services to conduct bandwidth tests within the LAN.
- Measure the network's upload and download speeds.
- Compare the measured speeds with the subscribed bandwidth to ensure it meets

Summary of Testing Types

- **Transmission testing:** Transmission testing in a LAN refers to the process of assessing the quality and reliability of data transmission within the network. It involves verifying that data packets are being successfully transmitted and received without errors or significant delays.
- **Connectivity testing** in a LAN is a crucial aspect of network maintenance to ensure that devices can communicate with each other effectively.
- **Functional testing** in a LAN refers to the process of verifying the functionality and performance of various network components, services, and applications within the network.

Performance testing in a LAN involves evaluating the network's performance, capacity, and responsiveness under various conditions and loads. It helps identify potential bottlenecks, measure network throughput, and ensure the network can handle the expected workload efficiently.

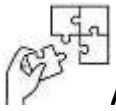
Points to Remember

- **The most common types of network testing tools**
  - ✓ Network protocol analyzers: Network protocol analyzers, such as Wireshark and tcpdump, are used to capture and analyze network traffic.
  - ✓ Network scanners: Network scanners, such as Nmap and Zenmap, are used to scan networks for active devices and open ports.

- ✓ Bandwidth testers: Bandwidth testers, such as iperf3 and hping3, are used to measure the maximum achievable bandwidth on a network.
- ✓ Latency testers: Latency testers, such as ping and traceroute, are used to measure the time it takes for data packets to travel across a network.
- ✓ Packet loss testers: Packet loss testers, such as mtr and nettest, are used to measure **the percentage of data packets that are lost during transmission.**

- **LAN connectivity testing can be done using a variety of tools, including:**

  Ping: Ping is a basic network connectivity test that sends a data packet to a specific device on the network and measures the time it takes for the packet to return.
- **There are a number of different types of LAN connectivity tests, but they all involve checking the following:**
  - ✓ Cable connections
  - ✓ Network devices
  - ✓ Network configuration
  - ✓ IP addresses
  - ✓ DHCP server
  - ✓ DNS server
  - ✓ Firewalls
  - ✓ Network traffic



Application of learning 5.1.

A company is setting up a new local area network (LAN) for its office. The IT team needs to identify the appropriate testing types to ensure that the LAN is functioning properly and can support the needs of the company's employees.

Indicative content 5.2: Selection of Testing Tools

Duration:1 hour

Theoretical Activity 5.2.1: Description of testing Tools

Tasks:

1: Encourage trainees to actively engage by asking questions and sharing their thoughts on the tools being presented.

2: Take notes of key points and ask clarifying questions if needed.

3: Proceed to the workshop, create small groups, and engage in discussions to describe the provided testing tools and their applications.

4: Present your findings to the whole class

5: Take notes of key points and ask clarifying questions if needed.

6: Read the key readings 5.2.1 in your manual for more clarifications

Key readings 5.1.1.:

A network testing tool is a software or hardware device that is used to assess the performance, health, and security of a computer network. These tools can be used to identify and troubleshoot problems with network devices, cabling, and software.

Selection of Testing Tools

- **Software tool**

  - ✓ **Wireshark**

Wireshark is a popular open-source packet analyser, often used in network troubleshooting and analysis tasks. It is widely used by network professionals around the world to troubleshoot network issues, analyse network protocols, and for educational purposes.

  - ✓ **cain & abel**

It's a password recovery tool for Microsoft Windows. It can recover many kinds of passwords using methods such as network packet sniffing, cracking encrypted passwords

using dictionary, brute-force and cryptanalysis attacks, recording VoIP conversations, decoding scrambled passwords, revealing password boxes, uncovering cached passwords and analysing routing protocols.

However, it's important to note that Cain & Abel is often regarded as a potentially dangerous tool, as it's frequently used by hackers for nefarious purposes due to its powerful capabilities.

It's not advisable to use this tool without fully understanding the consequences and potential risks involved. It's also critical to ensure you have proper permissions before using Cain & Abel to recover or crack passwords, as unauthorised use is illegal and unethical.

If you are interested in software testing tools, there are many other tools designed specifically for that purpose, such as Selenium, JUnit, TestNG, Apache JMeter, and many others depending on your specific needs (e.g., unit testing, integration testing, performance testing, etc.).

- ✓ **Advanced IP scanner**

It's a network scanning tool primarily used for IT and network administration purposes.

Advanced IP Scanner is a free, fast, and robust network tool for Windows that lets you scan your local network or IP addresses within any range to find any devices connected to your network. It offers a variety of features including:

- **IP Scanning:** The software scans your network to identify all computers and devices including their IP addresses, MAC addresses, and device names.
- **Remote Control:** It can remotely control systems (when integrated with RDP or Radmin). This allows an administrator to connect, shut down, and even wake up these machines remotely.
- **Easy Access:** Advanced IP Scanner provides easy access to network shares and FTP servers, enabling you to troubleshoot and manage network resources.

- **Multi-thread Scanning:** The software scans hundreds of IP addresses simultaneously and doesn't slow down your computer

- **Hardware tool**

  - ✓ **Cable tester**

A cable tester is a device that is used to test the strength and connectivity of a specific type of cable or network. It is a common tool in the fields of telecommunications and networking, and is used to detect if there are any breaks or faults in the cable being tested.

  - ✓ **Optical Time Domain Reflectometer (OTDR)**

An Optical Time Domain Reflectometer (OTDR) is a sophisticated piece of equipment used in the field of fibre optics to measure the characteristics of an optical fibre. Essentially, it works by injecting a series of light pulses into the fibre and then measuring the amount of light that is reflected back to the device. It's an essential tool used by professionals for the installation, maintenance, and troubleshooting of optical networks**.**

  - ✓ **Multi-meter**

A multimeter, also known as a volt-ohm metre, is a versatile tool that's used to measure several key aspects of electricity: voltage (volts), current (amperes), and resistance (ohms). In addition to these primary measurements, modern multimeters can often measure other quantities, such as capacitance, frequency, temperature, and more.

- ✓ **Splicing machine**

A splicing machine is a device used to join two or more pieces of material together. Splicing machines are used in a variety of industries, including manufacturing, construction, and electronics.

A splicing machine is a device used to join two or more pieces of material together. Splicing machines are used in a variety of industries, including manufacturing, construction, and electronics.

Two main types of splicing machines

1. **Fusion splicing** machines join two pieces of material together by melting them together.
2. **Butt splicing machines** join two pieces of material together by pressing them together with force. This type of splicing machine is often used for joining electrical wires and cables.

Practical Activity 5.2.2: Selecting the Testing Tools

Task:

1: Perform the task described below:

As network technician, go in workshop store and select the right testing tools to be used when testing the Connectivity and Performance with reference to the theoretical activity 5.2.1.

2: Listen attentively as the trainer providing instructions and ask questions for clarification

3: Ask for assistance while Selecting the Testing Tools where is necessary

4: Present your work to trainer and feel free to ask questions whenever necessary.

5: Read the key readings 5.2.2 for more explanations

Key readings 5.2.2

Benefits of network testing tools

Improved network performance: By identifying and correcting problems with the network, network testing tools can help to improve overall network performance.

Reduced downtime: By preventing network outages, network testing tools can help to reduce downtime and improve productivity.

Increased cost savings: By avoiding costly network repairs, network testing tools can help to save money.

Improved security: By ensuring that the network is secure from unauthorized access, network testing tools can help to protect sensitive data.

How to choose a network testing tool

When choosing a network testing tool, it is important to consider the following factors:

The size and complexity of the network: A larger and more complex network will require a more powerful and sophisticated network testing tool.

The specific needs of the network: Some network testing tools are better suited for specific tasks, such as troubleshooting performance problems or identifying security vulnerabilities.

The budget: Network testing tools can range in price from free and open-source to expensive commercial products.

Conclusion

Network testing tools are an essential part of network management. By regularly testing the network, network administrators can identify and correct problems before they cause major disruptions. This can help to improve network performance, reduce downtime, and increase user satisfaction.

Points to Remember

- **Software testing tools** are applications or programs used to test and validate the functionality, performance, security, and other aspects of software applications. These tools help in automating the testing process, identifying bugs, and ensuring the software meets specified requirements.
- **Hardware testing tools** are instruments or devices used to test and validate the performance, functionality, and reliability of hardware components and systems. These tools ensure that hardware meets the required specifications and operates correctly under various conditions.

- One of the main reasons why we test LANs is to identify and troubleshoot problems. This includes issues with cabling, hardware, software, and configuration. By testing the LAN, we can pinpoint the source of problems and take steps to fix them

Application of learning 5.2.

An IT administrator named Alice is responsible for managing the LAN at a medium-sized company. The LAN consists of approximately 100 devices, including computers, printers, and servers. Alice is currently in the process of selecting a new LAN testing tool to help her identify and troubleshoot network problems.

Indicative content 5.3: Connectivity Testing

Duration: 1 hour

Theoretical Activity 5.3.1: Description of connectivity testing

Tasks:

1: Respond to the following questions:

a. Define the Network Physical Testing used in LAN.
b. Explain 5 Logical Testing used in LAN.

2: Engage in group forming and discuss about provided questions

3: Present the findings in front of the class

4: Ask questions for further clarification.

5: Read the key reading 5.3.1 for more and doing the further research on Internet.

Key readings 5.3.1.:

Connectivity Testing

Network physical testing is an important part of the network engineering process, as it helps to ensure that the network infrastructure is in good working order.

- **Physical Testing**

Physical testing in a Local Area Network (LAN) involves a series of procedures designed to evaluate and validate the performance and reliability of the network's physical components.

This type of testing is critical to ensure that the network is properly functioning, to troubleshoot issues, and to optimise network performance.

Overall, physical testing in a LAN is about making sure that the hardware and infrastructure that make up the network are capable of supporting the data transmission needs of the organisation, and that they are reliable and secure.

- **Logical Testing**

Ping command

Ping is a command-line utility, available on virtually any operating system with network connectivity, that acts as a test to see if a networked device is reachable.
The ping command sends a request over the network to a specific device. A successful ping results in a response from the computer that was pinged back to the originating computer.

Traceroute Command

Traceroute is a network diagnostic tool used to track the pathway taken by a packet on an IP network from its source to its destination. It also records the transit delays of packets across an Internet Protocol (IP) network.

IPConfig/ifconfig

ipconfig (on Windows) and ifconfig (on Unix-based systems) are command-line tools that network administrators use to configure, control, and troubleshoot network interfaces on a system.

1.ipconfig (Internet Protocol Configuration):

It is used in Microsoft Windows. Executing 'ipconfig' in the command prompt will give you the details of all your network interfaces. You can see your IP address, subnet mask, default gateway, etc.

The following are some common uses of ipconfig:

1.ipconfig : Shows the IP configuration for all network interfaces on your machine.

2.ipconfig /all: Displays the full configuration information for all interfaces.

2.ifconfig (Interface Configuration)

It is used in Unix-like operating systems such as Linux, macOS, and BSD. The ifconfig utility is used to configure, or view the configuration of, a network interface.

1.**ifconfig**: Shows the status of all active interfaces.

2.**ifconfig** -a: Displays the status of all interfaces, even those that are down.

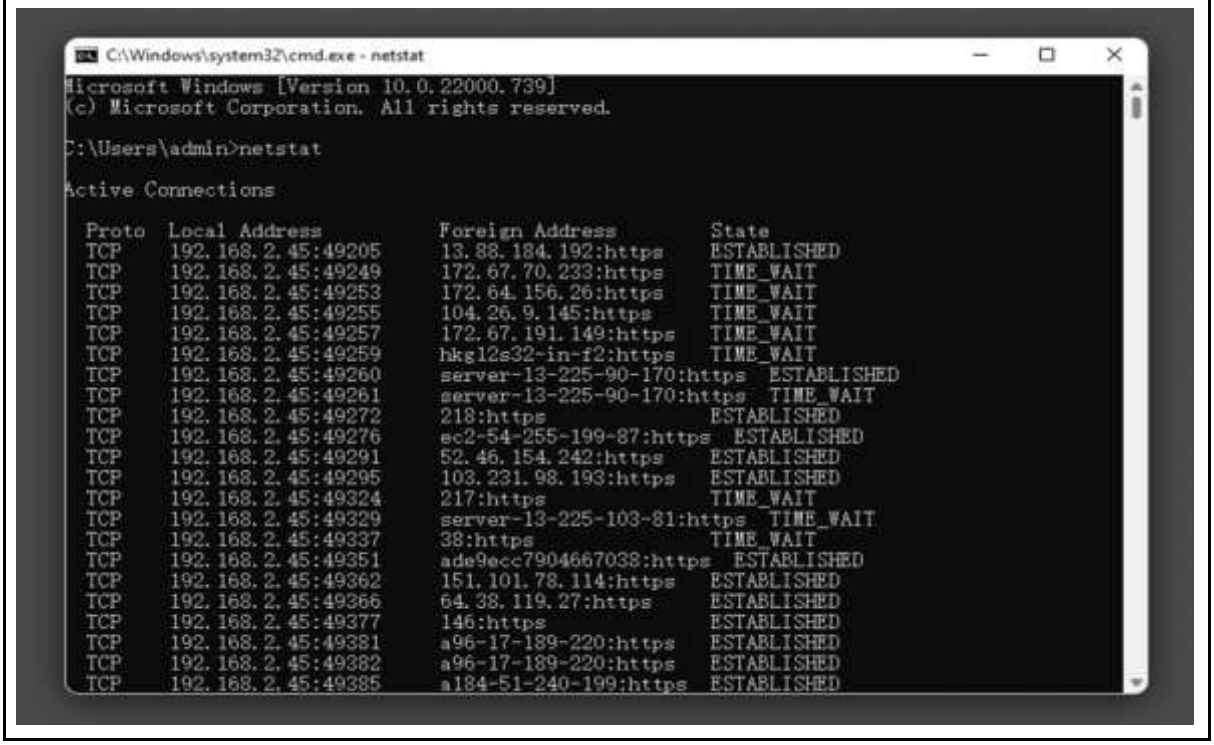
3.**ifconfig** [interface]: Shows information about a specific interface.

NSlookup

nslookup is a network administration command-line tool used for querying the Domain Name System (DNS) to obtain domain name or IP address mapping or for any other specific DNS records. The name "nslookup" stands for "name server lookup".

Netstat

netstat (network statistics) is a command-line tool used for network troubleshooting and performance measurement. It's available in Unix, Unix-like operating systems such as Linux, and also Windows.



Practical Activity 5.3.2.1: Testing the Network Connectivity

Task:

1: Read and perform the tasks described below:

X-company is experiencing intermittent network connectivity issues, with users reporting slow loading times, dropped connections, and frequent disconnects.

The IT team suspects that there may be physical issues with the network infrastructure. As network Technician do the possible testing process to solve this problem.

2: Identify the scope of testing by focusing on the network cabling and connectors in the affected areas.

3: Creates a test plan that outlines the specific tests to be performed, the tools and equipment needed.

4: Begin testing the network cables using a cable tester and identify several cables that are damaged or have excessive attenuation.

5: Analyse the results by determining the damaged cables that are causing the intermittent connectivity issues.

6: Replaces the damaged cables and tightens or replaces the loose connectors.

7: Present document of test results to trainer

8: Repeat the activity until perfect result

Key readings 5.3.2.1

Physical Testing:

1. **Cable Continuity Testing:**

   Use a cable tester to check the integrity and continuity of network cables.

   Verify that all cable connections are secure and free from any physical damage.

   Identify and address any faulty or damaged cables.

2. **Link Testing:**

   Check the physical link status of network devices, such as switches and routers.

   Ensure that all network interfaces are operational and properly connected.

   Verify that link lights are active and indicate the expected link speed and duplex mode.

3. **Power Testing:**

   Verify that network devices, such as switches and access points, are receiving power.

Logical Testing:

1. **Network Configuration Verification:**

   Validate the configuration of network devices, including IP addresses, subnet masks, and default gateways.

   Ensure that VLANs, if used, are properly configured and functioning as intended.

   Verify that routing tables and access control lists (ACLs) are correctly configured.

2. **Protocol Testing:**

   Test network protocols such as TCP/IP, DHCP, DNS, and SNMP to ensure proper functionality.

   Verify that protocols are correctly implemented and communication is established as expected.

   Monitor protocol traffic and analyze protocol-specific parameters for any abnormalities.

Points to Remember

- **Logical Testing**

✓ Ping command
✓ Traceroute Command
✓ IPConfig/ifconfig
✓ NSlookup
✓ Netstat

Application of learning 5.3.

X-company is experiencing an increase in network connectivity issues. Users are reporting that they are unable to access certain websites or applications, and they are also experiencing slow loading times and frequent disconnects.

The IT team suspects that there may be a problem with the network infrastructure. As a network Technician use appropriate Network tests to solve the problem stated above.

Indicative content 5.4: Functionality Testing

Duration:40 min

Theoretical Activity 5.4.1: Description of LAN Functionality Testing

Tasks:

1: Answer the following questions regards to the topic.

a. What does LAN functionality testing mean?
b. Explain what unit testing is in the context of networking.
c. Discus Network Integration Testing.

2: Present the answers to trainer and to whole class.

3: Take notes of key points and ask clarifying questions if needed.

4: Read the key readings 5.4.1 in trainee's manual

Key readings 5.4.1.:

Functionality Testing

Network functionality testing is the process of verifying that a network is operating correctly and meeting its intended purpose.

- **Unit Testing**

Unit testing in the context of a Local Area Network (LAN) might imply testing individual components of software or hardware which operate within that LAN.

- **Integration Testing**

Integration Testing in a Local Area Network (LAN) involves testing the combined parts of a network system and ensuring that they function correctly when they interact with each other.

The goal is to detect any interface defects between the modules in a LAN setting.

Network functionality testing is important for a number of reasons, including:

- Preventing downtime: Identifying and resolving problems before they cause network outages can save businesses time and money.
- Improving security: Identifying and remediating vulnerabilities can help to protect businesses from cyberattacks.
- Optimizing performance: Measuring and optimizing network performance can help to ensure that applications are running smoothly and that users are experiencing good performance.
- Ensuring compliance: Verifying compliance with regulations can help businesses to avoid fines and penalties.

Practical Activity 5.4.2: Testing the LAN functionality

Task:

1: Read carefully and perform the task described below:

As network Technician, install a small local area network or use the one installed during previous activities and apply unity testing and integration testing.

2: Individually complete activity 5.4.2 by applying the knowledge you gained from activity 5.4.1.

3: Present your test findings for each tool to trainer.

4: Continue repeating the activity until perfect results are achieved.

5: Read key readings 5.4.2 in their manual

Key readings 5.4.2

Network functionality testing tools:

A **ping test** is a basic network test that can be used to verify that two devices can communicate with each other. To perform a ping test, open a command prompt or terminal window and type the following command:

ping [destination_IP_address]

For example, to ping the Google DNS server, you would type:

ping 8.8.8.8

If the ping test is successful, you will see a series of replies from the destination host. If the ping test is unsuccessful, you will see an error message.

Traceroute Test

A traceroute test is a more advanced network test that can be used to identify the path that traffic takes between two devices. To perform a traceroute test, open a command prompt or terminal window and type the following command:

traceroute [destination_IP_address]

For example, to traceroute to the Google DNS server, you would type:

traceroute 8.8.8.8

The traceroute test will show you a list of hops that the traffic takes between your device and the destination host. Each hop will have an IP address and a response time. If there are any problems with the network, you will see an asterisk (*) instead of a response time.

DNS Lookup Test

A DNS lookup test is a network test that can be used to verify that a domain name can be resolved into an IP address. To perform a DNS lookup test, open a command prompt or terminal window and type the following command:

nslookup [domain_name]

For example, to lookup the IP address for the Google website, you would type:

nslookup google.com

The DNS lookup test will show you a list of IP addresses that are associated with the domain name. If the DNS lookup test is unsuccessful, you will see an error message.

Bandwidth Test

A bandwidth test is a network test that can be used to measure the amount of data that can be transferred over a network connection in a given amount of time. There are a number of different tools that can be used to perform bandwidth tests, such as iPerf3 and Ookla Speedtest.

To perform a bandwidth test using iPerf3, open a command prompt or terminal window and type the following command:

iperf3 -c [destination_IP_address]

For example, to test the bandwidth to the Google DNS server, you would type:

iperf3 -c 8.8.8.8

The iPerf3 test will show you the upload and download bandwidth between your device and the destination host.

Latency Test

A latency test is a network test that can be used to measure the time it takes for data packets to travel from one host to another. There are a number of different tools that can be used to perform latency tests, such as Ping and MTR.

To perform a latency test using Ping, open a command prompt or terminal window and type the following command:

ping -t [destination_IP_address]

For example, to test the latency to the Google DNS server, you would type:

ping -t 8.8.8.8

The Ping test will show you the average round-trip time (RTT) for the ping packets. The RTT is the time it takes for a ping packet to travel from your device to the destination host and back.

Security Test

A security test is a network test that can be used to identify and assess vulnerabilities in a network. There are a number of different tools that can be used to perform security tests, such as Nessus and OpenVAS.

Nessus and OpenVAS are both vulnerability scanners that can be used to identify vulnerabilities in network devices and applications. To perform a security test using Nessus or OpenVAS, you will need to install the tool on a computer and then scan the network.

Performance Test

A performance test is a network test that can be used to measure the performance of a network under load. There are a number of different tools that can be used to perform performance tests, such as JMeter and LoadRunner.

JMeter and LoadRunner are both load testing tools that can be used to simulate a large number of users accessing a network application.

Points to Remember

- **Unit testing** is a type of software testing where individual components or modules of a software application are tested in isolation. The goal is to validate that each unit of the software performs as expected
- **Integration testing** is a type of software testing where individual units or components are combined and tested as a group. The goal is to identify issues that occur when units interact with each other.

Application of learning 5.4.

X-company is implementing a new network infrastructure to support its expanding business operations. The new network consists of multiple LANs, routing protocols, and firewalls, and it must integrate seamlessly with the existing network.

Indicative content 5.5: Performance Testing

Duration: 40 min

Theoretical Activity 5.5.1: Description of Performance testing

Tasks:

1: Form small groups, read key reading 5.5.1 from the trainees' manual, and discuss the following questions:

1. What is jitter?
2. Explain signal latency.
3. Discuss QoS in the context of networking.

2: Instruct trainees to present their findings to the entire class.

3: Take notes of key points and ask clarifying questions if needed.

4: Read the key readings 5.4.1 and do further research on Internet.

Key readings 5.5.1.:

Network performance testing: is the process of measuring and evaluating the performance of a network to ensure that it is meeting the needs of its users and applications.

Jitter is the variation in the packet arrival time in a digital signal. It is often measured in milliseconds (ms) and is caused by a variety of factors, including network congestion, routing changes, and equipment malfunctions.

Jitter can be a major problem for real-time applications, such as voice over IP (VoIP) and video conferencing. It can cause choppy audio, distorted video, and even dropped calls. In extreme cases, it can make applications unusable.

Network latency, also known as lag, is the delay in network communication. It is the time it takes for a data packet to travel from one device to another. Network latency is typically measured in milliseconds (ms).

Causes of Network Latency

Distance: The greater the distance between two devices, the longer it will take for data packets to travel between them.

Network congestion: When a network is congested, there are more data packets competing for the same resources, which can increase latency.

Equipment limitations: Older or outdated network equipment may not be able to handle the demands of modern networks, which can lead to increased latency.

Routing issues: If data packets are routed incorrectly, it can add to the amount of time it takes for them to reach their destination.

Application issues: Some applications, such as video conferencing and online gaming, are more sensitive to latency than others.

High network latency can have a number of negative effects, including:

Slow loading times: Websites, applications, and files will take longer to load.

Choppy streaming: Video and audio streaming will be choppy and may experience buffering.

Increased lag: Real-time applications, such as online gaming and VoIP, will experience increased lag.

Dropped connections: In extreme cases, high network latency can cause connections to drop.

packet loss

This occurs when data packets, the small units of information that make up digital communication, fail to reach their intended destination.

This can happen due to a variety of reasons, such as network congestion, physical damage to cables or network devices, or software errors.

Consequences of Network Packet Loss

Slow loading times: When packets are lost, the receiving device has to request the missing data again, which can significantly increase the time it takes to load a website, download a file, or stream a video.

Choppy audio and video: In real-time applications like video conferencing and online gaming, packet loss can lead to choppy audio and video, making it difficult to communicate or enjoy the experience.

Application malfunctions: In some cases, packet loss can cause applications to malfunction or crash altogether. This is particularly true for applications that rely on real-time data exchange, such as online gaming and VoIP.

Network instability: Frequent packet loss can indicate a more serious underlying issue with the network, such as overloaded routers or faulty cables. If left unaddressed, this can lead to network instability and even complete downtime.

Quality of Service (QoS) in networking refers to the ability to prioritize and manage network traffic to ensure that critical applications and traffic receive the resources they need to perform optimally. It is crucial for ensuring reliable and consistent performance for real-time applications like video conferencing, VoIP, and online gaming.

The primary objectives of QoS in networking include:

Prioritizing traffic: QoS mechanisms allow network administrators to prioritize specific types of traffic, such as real-time or mission-critical applications, over other types of traffic, such as file transfers or web browsing.

Minimizing latency: QoS can help minimize latency, the time it takes for data packets to travel from one device to another. This is crucial for real-time applications, where even small delays can cause noticeable impairments.

Reducing jitter: Jitter refers to the variation in the time it takes for data packets to arrive at their destination. QoS techniques can help smooth out jitter, ensuring a consistent and predictable network experience.

Preventing packet loss: Packet loss occurs when data packets are lost during transmission. QoS can help prevent packet loss, ensuring that critical data reaches its destination reliably.

Enhancing network performance: By effectively managing network resources and prioritizing critical traffic,

1. What is Jitter?

Jitter refers to the variation in the time delay of received packets over a network. It is a measure of the inconsistency in packet arrival times, which can affect the quality of real-time communications, such as voice over IP (VoIP) and video conferencing. High jitter can lead to disruptions and poor user experience, as packets may arrive out of order or with significant delays.

2. Explain Signal Latency.

Signal latency is the time it takes for a data packet to travel from its source to its destination across a network. It is typically measured in milliseconds (ms) and can be affected by various

factors, including the physical distance between devices, the processing time at routers and switches, and the overall network congestion. Lower latency is crucial for applications that require real-time communication, as higher latency can result in noticeable delays.

3. Discuss QoS in the Context of Networking.

Quality of Service (QoS) refers to a set of technologies and techniques used to manage network resources and ensure the performance of specific applications or services. In networking, QoS aims to prioritize certain types of traffic, such as voice or video, over less critical data to maintain optimal performance and user experience. QoS can involve traffic shaping, bandwidth allocation, and prioritization of data packets to minimize latency, jitter, and packet loss, ensuring that critical applications receive the necessary resources to function effectively.

Practical Activity 5.5.2: Testing the LAN Performance

Task:

1: Read carefully the task described below:

As network Technician, install a small local area network or use the one installed during previous Practical Activities and perform the following Network Tests:

a. Jitter
b. Latency
c. Packet Loss
d. Quality of Service (QoS)

2: Listen attentively as the trainer provides clear work instructions and ask clarifying questions if needed.

3: Follow trainer as demonstrating network performance testing and ask questions for clarification if any.

4: Carry out the activity outlined in step one

5: Continually repeat the task individually until perfect result achieved

Key readings 5.5.2

- **Jitter** refers to the variability in packet arrival times during data transmission over a network. It measures the deviation from the average delay (latency) between successive packets.
- **Latency** is the time it takes for a data packet to travel from the source to the destination across a network. It is usually measured in milliseconds (ms).
- **Packet loss** occurs when one or more data packets fail to reach their destination during transmission across a network. It can be caused by network congestion, faulty hardware, or poor signal quality.
- **Quality of Service (QoS)** is a set of techniques and mechanisms used to manage and prioritize network traffic, ensuring the efficient use of network resources and maintaining the performance of various applications and services.

Points to Remember

- **Quality of Service (QoS)** is a set of techniques and mechanisms used in networking to manage and prioritize network traffic, ensuring the efficient use of network resources and maintaining the performance of various applications and services.
- **QoS** aims to provide a certain level of performance to different types of network traffic, which is crucial for applications that require real-time data transmission, such as VoIP (Voice over IP), video conferencing, and online gaming.
- **Benefits of QoS**
  - ✓ QoS can help to ensure that critical applications, such as VoIP and video conferencing, are able to run smoothly without experiencing jitter or lag.
  - ✓ By prioritizing traffic, QoS can help to reduce network congestion and improve overall network performance.
  - ✓ Users are more likely to be satisfied with their network experience if they are able to use their applications without experiencing any problems.

Application of learning 5.5.

A company is experiencing slow loading times and timeouts when accessing a web application. The IT team suspects that the network may be congested, but they need to confirm this and identify the root cause of the problem.

Indicative content 5.6: Document the network Installations

Duration: 40 min

Theoretical Activity 5.6.1: Description of network Installation's documentation

Tasks:

1: Listen attentively as the trainer explains what is network documentation and why is needed to document the network after the installations. Take notes and ask clarifying questions if needed.

2: Discus with trainees the elements of documentation and network documentation process

3: Read the key readings 5.6.1 in trainees manual and do further research on Internet.

Key readings 5.6.1.:

Network Installation Documentation

This document provides a comprehensive guide to the installation of a network, including hardware setup, software configuration, and testing procedures.

It is intended for network administrators, technicians, and anyone involved in the implementation of a network infrastructure.

Scope

This documentation covers the installation of a basic network, including the following components:

- **Network devices:** Routers, switches, access points, and other networking equipment
- **Networking cables**: Ethernet cables, fiber optic cables, and other cabling infrastructure
- **Networking software:** Operating systems, network management tools, and other software required for network operation

Assumptions

It is assumed that the reader has a basic understanding of networking concepts and terminology. Additionally, it is assumed that the reader has access to the necessary hardware and software for network installation.

Hardware Setup

1. Unpack and inspect all network devices to ensure they are in good condition and free from damage.
2. Position the network devices in a central location with adequate ventilation and power access.
3. Connect the network devices using appropriate cables.

- **Routers:** Connect the router's WAN port to the external network (e.g., ISP modem) and connect the router's LAN ports to the switches.
- **Switches**: Connect the switches' ports to the network devices (e.g., computers, printers, servers).
- **Access Points (APs):** Connect the APs to the switches and position them strategically to provide wireless coverage.

4. Power on the network devices in the following order:

- Router
- Switches
- Access Points
- Computers and other network devices

Practical Activity 5.6.2: Documenting an Installed LAN

Task:

1: Referring to the knowledge gained from Theoretical Activity 5.6.1, Perform the task described below:

As Network technician, document the local area network of your school if any. If not, install a small network and document it.

2: Present your work to trainer and ask clarifying questions if needed.

3: Continually repeat the activity until they achieve a perfect result

4: Read key readings 5.6.2 in trainees manual

Key readings 5.6.2

Network documentation is a crucial aspect of managing and maintaining a complex network infrastructure. It serves several essential purposes:

Knowledge Transfer: Network documentation provides a comprehensive record of the network's design, configuration, and components. This documentation facilitates knowledge transfer between network administrators, technicians, and new team members, ensuring that everyone has a clear understanding of the network's operation.

Troubleshooting and Problem-solving: Network documentation serves as a valuable resource for troubleshooting and resolving network issues. When problems arise, network administrators can refer to the documentation to identify potential causes, pinpoint specific components, and streamline the troubleshooting process.

Change Management: Network documentation is essential for managing changes to the network infrastructure. As the network evolves and new components are added or configurations are modified, documentation plays a critical role in tracking these changes and ensuring that the network remains stable and functional.

Compliance and Security: Network documentation can aid in compliance with regulatory requirements and security standards. Detailed documentation can demonstrate adherence to industry best practices and provide evidence of proper security measures in place.

Network Optimization and Capacity Planning: Network documentation provides insights into network performance and resource utilization. By analyzing traffic patterns, bandwidth usage, and device configurations, network administrators can identify areas for

optimization and plan for future capacity needs.

Onboarding and Training: Network documentation can serve as a training tool for new network administrators and technicians. By providing a comprehensive overview of the network's components, configurations, and procedures, new team members can quickly gain a working understanding of the network.

Risk Management and Disaster Recovery: Network documentation plays a crucial role in risk management and disaster recovery planning. In the event of a network outage or security breach, detailed documentation can expedite the recovery process and minimize downtime.

Asset Management and Cost Control: Network documentation can aid in asset management and cost control. By tracking the inventory of network devices, licenses, and configurations, organizations can optimize resource allocation, identify potential cost savings, and make informed decisions regarding upgrades and replacements.

Communication and Collaboration: Network documentation facilitates effective communication and collaboration among network administrators and other stakeholders. By providing a shared reference point, documentation ensures that everyone is on the same page regarding the network's design, operation, and maintenance.

Future Growth and Expansion: Network documentation serves as a foundation for future network growth and expansion. As the network expands to accommodate new devices, applications, and users, well-maintained documentation provides a clear roadmap for future planning and implementation.

Points to Remember

- **Knowledge Transfer:** Network documentation provides a comprehensive record of the network's design, configuration, and components.
- **Troubleshooting and Problem-solving:** Network documentation serves as a valuable resource for troubleshooting and resolving network issues.
  When problems arise, network administrators can refer to the documentation to identify potential causes, pinpoint specific components, and streamline the troubleshooting process.
- **Change Management:** Network documentation is essential for managing changes to the network infrastructure. As the network evolves and new components are added or configurations are modified, documentation plays a critical role in tracking these changes and ensuring that the network remains stable and functional.

Application of learning 5.6.

A small business, "Tech Solutions Inc.," has a local area network (LAN) that supports its daily operations, including internet access, file sharing, printing, and email services. The company employs 25 people and operates out of a single office location. As part of IT best practices, the network administrator is tasked with creating comprehensive LAN documentation to ensure efficient network management, troubleshooting, and future upgrades.

Learning outcome 5 end assessment

Theoretical assessment

Section A: Answer the following questions true if the statement is correct and False if the statement incorrect

1. Wireshark is primarily used for network performance measurement.
2. Nmap is a tool for discovering hosts on a network.
3. Ping is used to capture and analyze network traffic.
4. Connectivity testing verifies the ability of network devices to communicate.
5. Performance testing evaluates a network's ability to handle increased traffic.
6. Functionality testing ensures network services and applications work correctly.
7. Traceroute is used to check network reachability between two devices.
8. Ping provides detailed information about the path packets take to a destination.
9. Testing email and file sharing is part of functionality testing.
10. Verifying correct implementation of network protocols is a connectivity test.
11. Measuring network latency is part of performance testing.
12. Identifying network bottlenecks is a goal of performance testing.
13. Creating network diagrams is part of documentation.
14. Documentation is unnecessary for troubleshooting.

Section B: Match the testing tool with its primary function.

Item No.	Tool	Function
1……..	Wireshark	Network traffic capture and analysis
2……..	Nmap	Host discovery
3……..	Ping	Network performance measurement
4……..	iperf	Basic network reachability check

Section C: Match the testing type with its description.

Item No	Testing type	Description
1…..	Connectivity testing	Verifies network devices can communicate
2…..	Performance testing	Evaluates network capacity under load
3…..	Functionality testing	Ensures network services and applications work correctly

Practical assessment

Bella Company is a medium sized business that work as Forex bureau, the services it provides includes exchange various currencies, allowing customers to buy foreign currency or sell their local currency. These bureaus located next to Kanombe airports, Kicukiro District.

The Company is a newly established forex bureau that has recently installed a Local Area Network (LAN) at its headquarters. This office features both wired and wireless LAN along with a small server room housing a file server, print server, and router.

As a network technician, you are tasked to conduct thorough testing of the newly installed LAN to ensure it operates effectively and meets the required performance standards. After successfully completing the testing phase, you will end up by proper documentation for future maintenance and troubleshooting.

END

References

Garcia, L. M., & Turner, K. R. (2021). LAN Testing and Troubleshooting Techniques. Network Testing Journal, 56(2), 89-105.

ARWD. (2023). Different Types of LAN. *thewifispecialist*, Page 1.

Ashikuzzaman.Md. (December 28, 2023). Components of Local Area Network (LAN). *LIS EDUCATION NETWORK*, 3.

Indicative contents
6.1 Performing hardware and software Preventive maintenance
6.2 Performing Corrective maintenance
6.3 Checking hardware and software functionalities.
6.4: Elaboration of maintenance report

Key Competencies for Learning Outcome 6: Maintain LAN

Knowledge	Skills	Attitudes
• Description of LAN preventive and corrective measures • Identification of common problems and their causes • Identification of LAN problem	• Implementing preventive measures • Repairing damaged devices • Troubleshoot network configurations • Elaboration maintenance report	• Having Critical thinking • Being Self-motivated • Having spirit of Accountability

Duration: 5 hrs

Learning outcome 6 objectives:

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

1. Check properly Hardware and software functionalities as per manufacturer's guidelines
2. Install properly Features updates based on manufacturer's guidelines
3. Check properly LAN protection measures in accordance with the installation design
4. Apply correctly Corrective maintenance measures based on LAN problem identified.
5. Elaborate properly Maintenance report based on the work done

Resources

Equipment	Tools	Materials
● Computer ● Air Brower ● Router ● Switch	● Networking Toolkit	● Cables

Indicative content 6.1: Performing Hardware and Software Preventive Maintenance

Duration: 1 hour 30 min

Theoretical Activity 6.1.1: Description LAN maintenance

Tasks:

1: Answer the following questions in your small groups

i. Define LAN maintenance

ii. Describe types of LAN maintenance

iii. Discuss Hardware and Software Preventive Maintenance

2: Present your findings to the class

3: Listen attentively as the trainer providing feedback to presentations and ask clarifying questions if needed.

4: Read key readings 6.1.1 in your manuals

Key readings 6.1.1.:

1. LAN Maintenance

LAN Maintenance refers to the process of regularly monitoring, updating, troubleshooting, and optimizing a Local Area Network (LAN) to ensure its continuous performance, reliability, and security.

LAN maintenance includes both hardware (cables, routers, switches, etc.) and software components (firmware updates, security patches, monitoring tools, etc.).

2. Types of Maintenance

There are two main types of maintenance:

- ✓ **Preventive Maintenance:** This involves performing regular checks and maintenance on equipment to prevent failures and breakdowns.

It's designed to keep equipment in good working condition and avoid unexpected downtime. It prevents issues before they occur, such as updating software, inspecting hardware, and optimizing network performance.

- ✓ **Corrective Maintenance:** This is reactive maintenance that occurs when equipment fails or malfunctions.

  It involves repairing or replacing faulty components or troubleshooting connectivity to restore the equipment to working order. It fixes network problems as they arise.

3. Hardware and Software Preventive Maintenance

Preventive maintenance ensures whether both hardware and software components of a LAN function smoothly, efficiently, and securely.

- **Hardware Preventive Maintenance:** This involves regular inspections, cleaning, and testing of physical components to ensure they remain in good working condition and to prevent unexpected failures. Common activities include:
  - ✓ **Cleaning:** Dust and debris can accumulate in computer components, such as fans, power supplies, and keyboards. Regular cleaning reduces overheating and hardware malfunctions.
  - ✓ **Checking Cables and Connections:** Ensuring that all cables are securely connected and not damaged.
  - ✓ **Updating Firmware:** Keeping the hardware's firmware up to date to improve performance and security.
  - ✓ **Component Testing:** Running diagnostics on components like the hard drive, memory, and power supply to detect any early signs of failure.
  - ✓ **Temperature Monitoring:** Ensuring that cooling systems (fans, heat sinks) are functioning correctly to prevent overheating.
  - ✓ **Battery Maintenance:** For devices like laptops, checking the health of batteries and replacing them when necessary.

4. Software Preventive Maintenance

This focuses on keeping software systems optimized, secure, and free of unnecessary errors through regular updates and checks. Key activities include:

- ✓ **Software Updates:** Applying the latest updates for operating systems, applications, and security software to fix bugs, improve performance, and address vulnerabilities.
- ✓ **Backup Management:** Ensuring regular backups of important data and system files to prevent data loss in case of hardware failure or software corruption.
- ✓ **Disk Cleanup:** Removing temporary files, cache, and unnecessary applications to free up space and maintain system performance.
- ✓ **Defragmentation:** For traditional hard drives (HDD), defragmentation organizes data for faster access, improving system performance.

- ✓ **Malware Scanning:** Regularly scanning for viruses, spyware, and other malicious software to ensure the system's security.
- ✓ **Performance Monitoring:** Running system diagnostics to detect any abnormalities or performance drops that could indicate software issues.

Practical Activity 6.1.2: Setting and Implementing LAN threats preventive

Task:

1: Read and carefully perform the following task:

As Network technician, you are requested to Performing hardware and software Preventive maintenance of your Local Area Network.

1. List common LAN threats.
2. Identify all possible threats to your LAN
2. Create a table with two columns: Threat, Preventive Measures.
3. List possible LAN threats in the first column.
4. For each threat, identify at least two preventive measures and list them in the second column.
5. Implement identified preventive measures to the LAN

2: Proceed to the workshop and follow the trainer as demonstrating how to select preventive measures and selection criteria.

3: Perform the task provided on step2

4: Present your work to trainer

5: Read key reading 6.1.2 from trainee's manual

Key readings 6.1.2

Setting Preventive Measures in LAN Maintenance

The **setting of preventive measures** is a critical part of LAN maintenance that involves proactively establishing strategies, tools, and procedures to avoid potential network issues before they occur.

These measures are aimed at ensuring that the LAN infrastructure remains operational, efficient, and secure.

By implementing these preventive measures, network administrators can reduce downtime, optimize performance, and extend the life of network components.

Steps in Setting Preventive Measures:

Step 1. Identify Critical Hardware and Software Components

This step determine which parts of the LAN are most critical to its operation and need regular monitoring and maintenance.

- **Actions**:
  - ✓ **Inventory Network Devices**: Compile a list of all hardware devices, such as routers, switches, access points, servers, and client devices.
  - ✓ **Identify Key Software**: List all essential software, including operating systems, network management tools, firewalls, and applications critical to network performance.

Step 2. Establish Routine Inspection Schedules

This step ensures that hardware and software components are regularly checked for performance, health, and security.

- **Actions**:
  - ✓ **Set Timelines**: Define how often each device and system should be inspected (e.g., daily, weekly, monthly, quarterly).
  - ✓ **Automate Tasks**: Where possible, automate routine checks using network monitoring tools to reduce manual work.

Step 3. Implement Monitoring Tools

This steps continuously track network performance, detect issues early, and ensure all systems are functioning within normal parameters.

- **Actions**:
  - ✓ **Select Monitoring Software**: Choose tools that provide real-time data on hardware and software health, bandwidth usage, traffic patterns, and security events.
  - ✓ **Set Alerts**: Configure the system to send automated alerts when performance thresholds are breached (e.g., CPU usage too high, memory running low).
  - ✓ **Log Data**: Ensure all monitoring data is logged for future analysis and reporting.

Step 4. Regular Software Updates and Patching

This step keeps all software up-to-date and free from vulnerabilities or bugs.

- **Actions**:
  - ✓ **Create an Update Schedule**: Plan regular intervals for checking for software updates, patches, and firmware upgrades.
  - ✓ **Test Updates**: Before applying updates, test them in a controlled environment to ensure they don't introduce new issues.
  - ✓ **Apply Patches**: Ensure that critical patches, especially security patches, are applied as soon as possible to avoid potential exploits.

Step 5. Hardware Maintenance and Replacement

This step prevents hardware failure by performing regular maintenance and replacing components before they fail.

- **Actions**:
  - ✓ **Perform Physical Inspections**: Regularly inspect physical devices for signs of wear, overheating, or damage.
  - ✓ **Replace End-of-Life Hardware**: Proactively replace outdated or failing devices that no longer meet performance or security standards.
  - ✓ **Clean and Maintain Equipment**: Clean hardware, such as switches and routers, to remove dust and ensure proper ventilation.

Step 6. Backup and Recovery Planning

This step ensures data and configurations are backed up and can be restored quickly in case of a failure.

- **Actions**:
  - ✓ **Regular Backups**: Schedule regular data backups (daily, weekly, or as needed) for all critical systems and configurations.

- ✓ **Test Backups**: Periodically test backup files to ensure they are complete and can be restored without issues.
- ✓ **Off-Site Storage**: Store backups in a secure off-site location or cloud service to protect against physical damage or loss.

Step 7. Network Security Protocols

This step protects the network from potential threats, such as unauthorized access, malware, and data breaches.

- **Actions**:
  - ✓ **Deploy Firewalls and Intrusion Detection Systems (IDS)**: Install and configure security tools to monitor traffic and detect suspicious activity.
  - ✓ **Regular Security Audits**: Perform security audits to identify vulnerabilities and implement necessary countermeasures.
  - ✓ **User Authentication and Access Control**: Ensure that only authorized users have access to sensitive network areas, and use strong authentication protocols.

Step 8. Documentation of Procedures and Configurations

Its purpose is to maintain clear and detailed records of all preventive measures, configurations, and maintenance activities.

- **Actions**:
  - ✓ **Document Network Layouts**: Keep updated diagrams of the network infrastructure, showing device locations, IP addresses, and cable routes.
  - ✓ **Record Maintenance Activities**: Log all maintenance activities, including hardware inspections, software updates, and performance checks.
  - ✓ **Create Troubleshooting Guides**: Develop guides to help technicians quickly diagnose and resolve common issues.

Points to Remember

- LAN (Local Area Network) Maintenance refers to the routine tasks and procedures performed to ensure the optimal functioning, reliability, and security of a local area network.
- Types of LAN maintenance Preventive Maintenance and Corrective Maintenance, where preventive Maintenance refers to routine tasks designed to prevent issues before they occur, such as updating software, inspecting hardware, and optimizing network performance. Whereas Corrective Maintenance refers to fixing network

problems as they arise, including troubleshooting connectivity issues and repairing or replacing faulty devices.

- LAN maintenance includes both hardware (cables, routers, switches, etc.) and software components (firmware updates, security patches, monitoring tools, etc.).

Application of learning 6.1.

XYZ Corp is a medium-sized company that relies heavily on its Local Area Network (LAN) for daily operations, including file sharing, communication, and access to internal applications. Recently, the IT department has noticed an increase in unauthorized access attempts and some employees have reported phishing emails. To enhance network security, the company decides to hire a Network Technician to set and implement preventive measures against potential threats from their Local Area Network.

Indicative content 6.2: Performing Corrective maintenance

Duration: 1 hour 30 min

Theoretical Activity 6.2.1: Description of Corrective maintenance

Tasks:

1: Listen attentively as the trainer differentiating preventive maintenance from corrective maintenance, take notes and ask clarifying questions if needed.

2: Identify different common network problems and their causes in your group discussion

3: After discussion present your findings to trainer

4: Take notes of key points and ask clarifying questions if needed.

5: Read key readings in trainees manual about identification of common problems and their causes

6: Listen attentively as the trainer explaining the following:

- ✓ Tools Used for Corrective Maintenance in LAN (Either hardware or software)
- ✓ Steps to implement LAN corrective maintenance

7: Read key readings 6.2.1 in their manuals and ask clarifying questions if needed.

Key readings 6.2.1.:

Performing corrective maintenance involves identifying, isolating, and repairing faults or issues in a system or equipment to restore its functionality and operational efficiency. It is an essential part of overall maintenance strategies, complementing preventive maintenance, which focuses on preventing problems before they occur.

Steps in Corrective Maintenance:

1. **Problem Identification:** The first step is to identify and report the problem or issue. This may involve user reports, system alerts, or observations during routine operations.

2. **Problem Isolation:** Once the problem is identified, it is crucial to isolate it to a specific component or equipment within the system. This involves narrowing down the possible causes and systematically testing or examining individual components.

3. **Problem Diagnosis:** After isolating the problem, the next step is to diagnose the root cause. This may involve using diagnostic tools, analyzing error logs, or consulting technical documentation.

4. **Problem Correction:** Once the problem is diagnosed, the appropriate corrective action is taken. This may involve repairing, replacing, or adjusting the faulty component.

5. **Testing and Validation:** After completing the corrective action, the system or equipment is thoroughly tested to verify that the problem has been resolved and that the system is functioning properly.

Importance of Corrective Maintenance:

1. **Restores Functionality:** Corrective maintenance restores the functionality of the system or equipment, preventing downtime and ensuring its continued operation.

2. **Reduces Costs:** By addressing problems promptly, corrective maintenance can prevent further damage, extended downtime, and costly repairs or replacements.

3. **Improves System Performance:** Corrective maintenance helps maintain the overall performance and efficiency of the system, minimizing disruptions and ensuring optimal productivity.

4. **Enhances Safety:** Corrective maintenance can identify and address potential safety hazards, preventing accidents and ensuring a safe working environment.

Preventive vs. Corrective Maintenance:

Preventive maintenance focuses on preventing problems before they occur by performing regular inspections, servicing, and updates. Corrective maintenance, on the other hand, addresses problems that have already arisen. Both types of maintenance are essential for maintaining system reliability and minimizing downtime.

Notes: Combining corrective maintenance with preventive maintenance strategies provides a comprehensive approach to ensuring optimal system health and longevity.

Practical Activity 6.2.2: Troubleshooting and resolving a network problem

Task:

1: Read carefully and perform the task outlined below:

Create a simple LAN with a router, switch, and several client computers. Configure the network devices with appropriate IP addresses, subnet masks, and default gateways. Verify that all client computers can successfully ping the router and access the internet.

- ✓ Randomly:(1) disable a network connection, such as a cable or a network interface card, on one of the client computers. (2) Set Incorrect router settings. (3) Aged network router or switch
- ✓ Observe the network behaviours and identify the symptoms of the malfunction.
- ✓ Document the observed symptoms and the affected client computer.

2: Follow the trainer's demonstration, take notes, and ask any questions for clarification as needed.

3: Identify, diagnose, and resolve the network issues from the LAN you have installed.

4: Present your work to trainer and ask assistance if necessary

5: Read key readings 6.2.2 in trainee's manuals

Key readings 6.2.2

Evaluation:

Your performance will be evaluated based on the following criteria:

- Accurate identification of the malfunction: You should have correctly identified the symptoms and affected area of the network malfunction.
- Effective troubleshooting and problem isolation: You should have employed a structured approach to isolate the root cause of the problem.
- Successful implementation of corrective measures: You should have taken the appropriate steps to resolve the network issue and restore normal operation.
- Documentation and communication: You should have documented the troubleshooting process and communicated effectively with relevant stakeholders.

Additional Tips:

- Familiarize yourself with the features and functionalities of the network simulation software.
- Utilize network diagnostic tools and techniques to gather relevant information about the network status.
- Maintain a detailed log of your troubleshooting steps and observations.
- Seek assistance from experienced network engineers if you encounter difficulties during the troubleshooting process.

Benefits of LAN Corrective Maintenance

Regular LAN corrective maintenance provides several benefits, including:

1. Reduced Downtime: Prompt identification and resolution of network issues minimize downtime and disruptions to business operations.

2. Improved Network Performance: Corrective maintenance optimizes network performance by addressing bottlenecks, resolving hardware failures, and optimizing software configurations.

3. Enhanced Security: By addressing security vulnerabilities and implementing appropriate security measures, corrective maintenance safeguards the network against cyberattacks and data breaches.

4. Increased User Satisfaction: A well-maintained LAN ensures consistent and reliable network access for users, improving their productivity and overall satisfaction.

A practical activity on LAN corrective maintenance:

Objective: To troubleshoot and resolve a network connectivity issue in a simulated LAN environment.

Step1: Prepare the following materials

Materials:

- A computer with internet access
- Network simulation software (e.g., GNS3, Cisco Packet Tracer)
- A basic understanding of network concepts and troubleshooting techniques

Step2: listen and reread careful the following instructions

Instructions:

1. Set up a simulated LAN:

a. Use network simulation software to create a simple LAN topology with a router, switch, and several client computers. b. Configure the network devices with appropriate IP addresses, subnet masks, and default gateways. c. Verify that all client computers can successfully ping the router and access the internet.

2. Introduce a network malfunction:

   a. Randomly disable a network connection, such as a cable or a network interface card, on one of the client computers. b. Observe the network behaviour and identify the symptoms of the malfunction. c. Document the observed symptoms and the affected client computer.

3. Troubleshooting and problem isolation:

   a. Use network diagnostic tools, such as ping and traceroute, to identify the point of failure. b. Check the network status indicators on the affected client computer and network devices. c. Analyse network traffic patterns to identify any anomalies or bottlenecks.

4. Problem correction:

   a. Based on the troubleshooting results, identify the root cause of the malfunction. b. Enable the disabled network connection or replace the faulty component. c. Verify that the network connectivity has been restored and the affected client computer can access the network resources.

5. Testing and validation:

   a. Conduct thorough testing across the LAN to ensure all devices and services are functioning properly. b. Monitor network performance and user feedback to ensure the problem does not recur.

Points to Remember

Key Aspects of Corrective Maintenance for LAN

- Identification of Issues
- Diagnosis
- Planning and Scheduling
- Repair or Replacement
- Testing and Verification
- Documentation
- Follow-Up

Application of learning 6.2.

You are the network administrator responsible for maintaining the LAN at a medium-sized company. One morning, you receive reports from several employees experiencing network connectivity issues. They describe slow loading times, intermittent internet access, and inability to access shared resources. As network technician troubleshoot and resolve a network problem.

Indicative content 6.3: Checking hardware and software functionalities.

Duration: 1hour

Theoretical Activity 6.3.1: Description of hardware and software functionality checking

Tasks:

1: Listen attentively as the trainer explaining network functionality checking

2: In your small group, discuss the importance of checking the performance of network software and hardware in the context of network maintenance.

3: Brainstorm with your trainer about physical part and software aspects that have to be checked in Network maintenance

4: Explain to the trainees the process of checking network functionality.

5: Read key readings 6.3.1 in trainees manual

Key readings 6.3.1.:

Checking Hardware and Software Functionalities

Regularly checking LAN hardware and software functionalities is essential for maintaining the performance and reliability of your network.
By following checkpoints and practical steps outlined below, you can ensure that your systems are running optimally and are prepared to handle any challenges that arise.

Hardware

When checking network hardware functionality, two key factors are taken into account: connectivity and device status.

1. **Connectivity:** Ensures that all hardware components are properly connected and communicating with each other.

Checkpoints:

- **Cabling:**

  - ✓ Inspect Ethernet cables for any visible damage, such as fraying or cuts.
  - ✓ Ensure that cables are properly plugged into devices (computers, switches, routers) and are securely connected.
- **Network Devices**

  - ✓ Confirm that all network devices (routers, switches, access points) are powered on and functioning.
  - ✓ Check for proper LED indicators on devices to ensure they are connected and operational.
- **Network Configuration**

  - ✓ Use network diagnostic tools (e.g., ping, traceroute) to test connectivity between devices.
  - ✓ Verify that devices are on the same subnet and can communicate with each other.

2. Status: Identifies the current operational state of hardware components.

Checkpoints:

- ✓ Check power status indicators (LEDs) on hardware devices
- ✓ Access the router's web interface to view connected devices and their status.
- ✓ Look for any devices that are not connected or showing error messages.

Software

When checking network hardware functionality, the following key factors are taken into account: Software performance, Status, Updates and Services of features.

1. Performance: Evaluates the efficiency and speed of software applications and systems.

Checkpoints:

- ✓ Measure response times and performance of software applications.
- ✓ Monitor CPU, memory, and disk usage on network devices to ensure they are not overloaded.
- ✓ Conduct speed tests to measure the upload and download speeds of the LAN.
- ✓ Compare results with expected performance levels to identify any differences
- ✓ Check for any applications consuming excessive bandwidth.

2. Status: Determines the operational state and readiness of software applications.

Checkpoints:

- ✓ Check for error messages or system alerts indicating software issues.
- ✓ Ensure all software services are running as expected.
- ✓ Verify log files for any anomalies or warnings.

3. **Updates:** Ensures that software is up-to-date with the latest versions and patches.

Checkpoints:

- ✓ Update applications regularly to benefit from new features and bug fixes.
- ✓ Check for compatibility with the current operating system version.
- ✓ Enable automatic updates where possible.

4. **Services or Features:** Verifies that all required software services and features are enabled and functioning.

Checkpoints:

- ✓ List all necessary services and features for the software.
- ✓ Confirm that each service is running and properly configured.
- ✓ Test specific features to ensure they perform as expected.

Practical Steps for Checking Functionalities

1. **Prepare Tools and Documentation:**
   - ✓ Gather necessary tools such as network testers, performance monitoring software, and update management systems.
   - ✓ Keep documentation of hardware and software configurations for reference.
2. **Conduct Initial Assessment:**
   - ✓ Perform a visual inspection of hardware connections.
   - ✓ Log into systems to check the status of hardware and software components.
3. **Execute Functional Tests:**
   - ✓ Run connectivity tests using ping, traceroute, or network management tools.
   - ✓ Use performance testing tools to simulate user load and measure software responsiveness.
   - ✓ Check for software updates and apply patches as needed.
4. **Review and Document Findings:**
   - ✓ Record the results of connectivity and status checks.
   - ✓ Document any performance issues and steps taken to resolve them.
   - ✓ Keep a log of software updates applied and their impact on system performance.
5. **Implement Continuous Monitoring:**
   - ✓ Set up continuous monitoring tools to track hardware and software status in real-time.

- ✓ Schedule regular maintenance and review sessions to keep systems running smoothly.

Practical Activity 6.3.2: Checking LAN functionalities.

Task:

1: Read carefully and perform the task described below:

Create a simple Local Area Network with a router, switch, and several client computers. Configure the network devices with appropriate IP addresses, subnet masks, and default gateways. Verify that all client computers can successfully ping the router and access the internet.

1. Identify physical issues with network cables and devices.
2. Verify the functionality of network components and update firmware.
3. Ensure all software components are up-to-date and secure.

2: Carry out the activity mentioned above and ask for assistance as needed.

3: Present your work to trainer

4: Based on the feedback, repeat the task until a perfect result is achieved.

5: Read key readings 6.3.2 in trainees manual

Key readings 6.3.2

STEP-BY-STEP GUIDE TO CHECKING LAN FUNCTIONALITIES

Follow the following steps for effective check and maintain the functionalities of your LAN:

Step 1: Prepare for the Check

Gather Necessary Tools:

- A laptop or desktop computer connected to the LAN.

- Network diagnostic tools (e.g., ping, traceroute).
- Access to the router's web interface.

Step 2: Check Hardware Connectivity

1. Inspect Cabling:
    - Examine Ethernet cables for any visible damage (fraying, cuts).
    - Ensure that all cables are securely connected to devices (computers, switches, routers).
2. Verify Network Devices:
    - Check that all network devices (routers, switches, access points) are powered on.
    - Look for LED indicators to confirm that devices are functioning properly.
3. Test Physical Connections:
    - Use a network cable tester to ensure cables are transmitting signals correctly.
    - If using wireless, ensure the Wi-Fi is enabled on devices and check signal strength.

Step 3: Assess Network Connectivity

1. Ping Test:
    - Open the command prompt or terminal on your computer.
    - Use the command `ping [IP address] ` to test connectivity to other devices on the network (e.g., the router or another computer).
    - Analyze the response times and packet loss.
2. Traceroute Test:
    - Use the command `tracert [IP address] ` (Windows) or `traceroute [IP address] ` (Mac/Linux) to track the path packets take to a destination.
    - Identify any delays or failures in the path.

Step 4: Check Device Status

1. Access Router Interface:

- Open a web browser and enter the router's IP address to access its web interface.

- Log in with the administrator credentials.

2. View Connected Devices:

- Navigate to the section that shows connected devices.

- Check the status of each device to ensure they are connected and functioning.

3. Review Error Logs:

- Look for any error messages or warnings in the router's logs that may indicate issues.

Step 5: Monitor Network Performance

1. Conduct Speed Tests:

- Use an online speed test tool to measure the upload and download speeds of the LAN.

- Compare results with expected performance levels.

2. Check Resource Utilization:

- Monitor CPU and memory usage on the router and switches via the web interface.

- Identify any devices or applications consuming excessive bandwidth.

Step 6: Review Software Status

1. Check Network Configuration:

- Review the settings on routers and switches to ensure they are configured correctly.

- Verify DHCP and DNS settings to ensure proper network functionality.

2. Update Firmware and Software:

- Check for firmware updates for routers and switches and install them if available.

- Ensure that network management software is up to date.

Step 7: Test Services and Features

1. Verify Essential Services:

- Test network services such as DHCP and DNS to ensure they are functioning correctly.

- Use commands like `ipconfig /all` (Windows) or `ifconfig` (Mac/Linux) to check IP addresses and DNS settings.

2. Monitor User Access:

- Review user permissions and access controls to ensure only authorized users can access the network.

- Check for any unauthorized connections or access attempts.

Step 8: Document Findings

1. Record Results:

- Document any issues discovered during the checks, including connectivity problems, performance issues, or configuration errors.

2. Plan for Resolution:

- Create a plan to address any identified issues and improve overall LAN functionality.

TESTING LAN HARDWARE FUNCTIONALITIES

Testing LAN hardware functionalities, focusing on **Connectivity** and **Status**, involves verifying that all physical components of the network are functioning correctly and that devices are properly connected. Here's a step-by-step guide:

1. Visual Inspection

- **Purpose:** To identify any obvious issues with the physical connections and hardware.
- **Steps:**
  - ✓ **Check Cables:** Inspect Ethernet cables for damage, ensuring they are securely connected to the correct ports on devices like routers, switches, and

computers.

- ✓ **Verify LEDs:** Look at the status LEDs on network devices (routers, switches, network interface cards). Green lights typically indicate a good connection, while amber or red lights might signal issues.
- ✓ **Power Supply:** Ensure that all network devices are powered on and that power adapters and cords are functioning.

2. Connectivity Testing

- **Purpose:** To confirm that all devices on the LAN are properly connected and can communicate with each other.
- **Steps:**
  - ✓ **Ping Test:**
    - Use the ping command from one device to ping the IP addresses of other devices on the network, including the default gateway (router).
    - A successful ping indicates that the devices are connected and can communicate.
    - Example: ping 192.168.1.1 (replace with the appropriate IP address).
  - ✓ **Traceroute Test:**
    - Use the tracert (Windows) or traceroute (Linux/Mac) command to trace the path packets take to reach another device, helping to identify where connectivity issues might occur.
  - ✓ **Switch and Router Testing:**
    - Access the management interface of switches and routers to check their connectivity status with connected devices.
    - Ensure all devices are recognized by the network infrastructure.

3. Status Verification

- **Purpose:** To check the operational status of network hardware and ensure all devices are functioning as expected.
- **Steps:**
  - ✓ **Network Interface Status:**
    - On each computer or device, check the status of the network interface card (NIC) to ensure it is enabled and operational.
    - In Windows, use ipconfig /all to check the NIC status. On Linux, use ifconfig or ip a.
    - Look for a "Connected" or "Up" status for the network interface.
  - ✓ **Port Status on Switches and Routers:**
    - Access the switch or router's management interface to check the status of each port.
    - Ensure that all active ports are showing as "Up" or "Connected." Ports should indicate active data transmission if devices are connected and communicating.
  - ✓ **Error Logs:**
    - Review logs on network devices like switches, routers, and firewalls

for any error messages or warnings that might indicate connectivity issues.
    - Common issues include port errors, collision detection, or interface drops.

TESTING LAN SOFTWARE FUNCTIONALITIES

Testing LAN software functionalities involves assessing the performance, status, updates, and services of the network's software components. This ensures that the network operates smoothly, securely, and efficiently. Below is a step-by-step guide for each aspect:

1. Performance Testing

- **Purpose:** To evaluate the efficiency and speed of the network's software-related functions.
- **Steps:**
    - ✓ **Bandwidth Utilization:**
        - Use tools like NetFlow, Wireshark, or SolarWinds to monitor and analyze network traffic. Check if the bandwidth is being utilized efficiently and identify any unnecessary or excessive data flow.
    - ✓ **Latency and Jitter Measurement:**
        - Measure latency (delay) and jitter (variation in packet arrival time) using tools like PingPlotter or iPerf. High latency and jitter can affect the performance of real-time applications like VoIP or video conferencing.
    - ✓ **Throughput Testing:**
        - Conduct throughput tests to measure the rate of successful data transfer. Tools like iperf or LAN Speed Test can be used to assess how much data the network can handle at once.
    - ✓ **Application Performance Monitoring:**
        - Use APM tools like Nagios, Zabbix, or PRTG to monitor the performance of specific applications running on the network, checking for bottlenecks or performance degradation.

2. Status Verification

- **Purpose:** To ensure that all network software components are functioning correctly and that there are no active issues.
- **Steps:**
    - ✓ **Service Status:**
        - Check the status of essential network services like DNS, DHCP, and firewall services using commands such as systemctl status on Linux or the Services panel on Windows. Ensure all necessary services are running without errors.
    - ✓ **Log Review:**
        - Review system and application logs for errors or warnings that could

indicate software malfunctions. Logs can be checked using tools like Syslog or the built-in event viewer in Windows.

- ✓ **SNMP Monitoring:**
  - Use Simple Network Management Protocol (SNMP) tools to monitor the health of network devices and services. Tools like Cacti or ManageEngine can provide real-time status updates and alerts.
- ✓ **Network Map:**
  - Use network mapping tools like Nmap or Microsoft Network Monitor to visualize the network's structure and verify that all devices and services are correctly connected and operational.

3. Software Updates

- **Purpose:** To ensure that all network software, including operating systems, firmware, and applications, are up-to-date and secure.
- **Steps:**
  - ✓ **Check for Updates:**
    - Regularly check for software and firmware updates for routers, switches, firewalls, and connected devices. This can often be done through the device's management interface or software management tools.
  - ✓ **Patch Management:**
    - Use patch management tools like WSUS (Windows Server Update Services) or SolarWinds Patch Manager to automate and manage updates across the network. Ensure all critical patches are applied promptly to prevent security vulnerabilities.
  - ✓ **Version Control:**
    - Maintain a log of the current software versions running on all network devices. Compare them against the latest available versions to ensure that everything is up-to-date.
  - ✓ **Backup Before Updates:**
    - Before applying updates, ensure that you have a complete backup of configurations and critical data. This helps in restoring the system if the update causes any issues.

4. Service Testing

- **Purpose:** To verify that all network services are available and functioning as expected.
- **Steps:**
  - ✓ **DHCP Service Test:**
    - Check that the DHCP service is correctly assigning IP addresses to devices on the network. This can be tested by releasing and renewing the IP address on a client device using ipconfig /release and ipconfig /renew (Windows).
  - ✓ **DNS Service Test:**

- Verify DNS functionality by using commands like nslookup or dig to ensure domain names are resolving correctly to IP addresses.

✓ **File and Printer Sharing:**
- Test file sharing services by accessing shared folders across the network. Ensure that shared printers are accessible and functioning from all devices.

✓ **Firewall Service:**
- Ensure that the firewall is correctly filtering traffic based on established rules. Use tools like Firewall Analyzer or built-in tools like ufw (Linux) or Windows Defender Firewall to test rules and logs.

✓ **Authentication Services (e.g., LDAP, Active Directory):**
- Test authentication services to ensure users can log in and access resources based on their permissions. Check for any issues in the authentication process and review access logs.

5. Documentation

- **Purpose:** To maintain accurate records of all tests conducted, updates applied, and current software statuses.
- **Steps:**
  - ✓ **Test Results:** Document the results of all performance, status, update, and service tests, noting any issues encountered and the actions taken to resolve them.
  - ✓ **Update Logs:** Keep a detailed log of all updates applied to network software, including the date, version numbers, and any issues that arose during the update process.
  - ✓ **Service Configuration:** Document the configuration settings of all critical services to provide a reference for troubleshooting and future maintenance.

Points to Remember

- Checking hardware and software functionalities is a crucial aspect of Local Area Network (LAN) maintenance.
- Regular checks help ensure that the network operates smoothly, minimizes downtime, and enhances overall performance.
- Maintaining a Local Area Network (LAN) requires regular checks of both hardware and software components to ensure smooth operation and quick resolution of issues.

Application of learning 6.3.

You are part of the IT support team for a mid-sized company that relies heavily on its Local Area Network (LAN) for daily operations. Recently, users have reported intermittent connectivity issues, slow network performance, and problems accessing shared resources. Your team has been tasked with diagnosing and resolving these issues by checking both the hardware and software functionalities of the network.

- Identify and troubleshoot hardware-related issues affecting the network.
- Diagnose and resolve software-related problems impacting network performance.
- Document findings and corrective actions taken for future reference.

Indicative content 6.4: Elaboration of maintenance report

Duration: 1 hour

Theoretical Activity 6.4.1: Description of maintenance report

Tasks:

1: Listen attentively as the trainer explains maintenance report

2: In your small group, discuss the importance of creating a network maintenance report.

3: Present your findings to the class

4: Take notes of key points and ask clarifying questions if needed.

5: Read key readings 6.4.1 in the trainee manual importance of creating a network maintenance report.

Key readings 6.4.1.:

Description of maintenance report

Introduction to Maintenance Report

A maintenance report is a comprehensive document that records the activities performed during maintenance tasks, the condition of the equipment or system before and after maintenance, and any recommendations for future actions.

A well-prepared maintenance report is essential for documenting the maintenance process, ensuring that all necessary actions have been taken, and providing valuable insights for future maintenance planning.

This report is essential for ensuring transparency, accountability, and continuous improvement in maintenance practices.

Major Types of Maintenance Reports

Here are the major types of maintenance reports that are commonly used:

1. Preventive Maintenance Report

- **Purpose:** To document scheduled maintenance activities aimed at preventing equipment failures.
- **Contents:**
  - ✓ List of preventive tasks performed.
  - ✓ Equipment condition before and after maintenance.
  - ✓ Compliance with the maintenance schedule.
  - ✓ Recommendations for future preventive actions.

2. Corrective Maintenance Report

- **Purpose:** To record maintenance activities carried out to correct equipment failures or issues.
- **Contents:**
  - ✓ Detailed description of the problem.
  - ✓ Diagnostic methods used.
  - ✓ Corrective actions taken.
  - ✓ Tools and materials used.
  - ✓ Equipment status after maintenance.

3. Predictive Maintenance Report

- **Purpose:** To detail maintenance activities based on predictive data analysis and condition monitoring.
- **Contents:**
  - ✓ Data from sensors and monitoring tools.
  - ✓ Analysis and interpretation of data.
  - ✓ Predictions about potential equipment failures.
  - ✓ Maintenance actions taken based on predictions.
  - ✓ Future maintenance recommendations.

4. Routine Maintenance Report

- **Purpose:** To summarize regular, routine maintenance tasks performed on equipment.
- **Contents:**
  - ✓ List of routine tasks performed.
  - ✓ Frequency of tasks.
  - ✓ Equipment condition during routine checks.
  - ✓ Any issues identified and addressed.
  - ✓ Recommendations for adjustments to routine schedules.

5. Emergency Maintenance Report

- **Purpose:** To document unscheduled maintenance activities carried out in response to urgent equipment failures.
- **Contents:**

- ✓ Description of the emergency situation.
- ✓ Immediate actions taken.
- ✓ Root cause analysis.
- ✓ Detailed description of repairs.
- ✓ Preventive measures to avoid future emergencies.

Benefits of maintenance reports

Maintenance reports provide numerous advantages to organizations, equipment managers, and maintenance teams. Including:

1. **Improved Asset Management**

Maintenance reports give a clear picture of how assets are performing and their condition. This information can be used to schedule maintenance activities more efficiently and optimize asset utilization.

2. **Reduced Downtime and Costs**

By providing a record of all maintenance activities and their outcomes, maintenance reports can help businesses identify and address repeated issues leading to unexpected costs.

3. **Improved Communication and Collaboration**

Maintenance reports can be shared with all stakeholders, including maintenance teams, operations teams, and management. This promotes transparency and improves communication and collaboration between all parties.

4. **Data-Driven Decision Making/informed decision making**

Maintenance reports provide valuable data that can be used to make informed decisions regarding asset management, maintenance scheduling, and equipment replacement.

5. **Enhance communication and Customer Satisfaction**

Maintenance reports facilitate clear communication between maintenance teams, management, and clients, ensuring everyone is informed about equipment status and maintenance activities.

Well-documented maintenance reports can improve customer satisfaction by demonstrating professionalism, accountability, and effective service delivery.

Elements of Maintenance Report

1. Client Information:

- **Client Name:** The name of the individual or organization requesting the maintenance service.

- **Contact Information:** Phone number, email address, and physical address of the client.
- **Service Location:** The specific location where the maintenance was performed.

2. Status Before Maintenance

- **Condition Assessment:** A detailed description of the equipment or system's condition prior to maintenance, including any observed issues or malfunctions.
- **Operational Status:** Note whether the equipment was operational, partially operational, or non-operational.
- **Previous Maintenance Records:** Reference any prior maintenance activities and their outcomes.

3. Implementation of Solution

- **Description of Work Performed:** Outline the specific maintenance tasks carried out, including repairs, replacements, and adjustments.
- **Timeline:** Indicate the date and duration of the maintenance work.
- **Challenges Encountered:** Mention any difficulties faced during the maintenance process and how they were resolved.

4. Used Tools, Materials, and Equipment

- **Tools Used:** List all tools utilized during the maintenance process (e.g., wrenches, screwdrivers, diagnostic tools).
- **Materials and Parts:** Specify any materials or replacement parts used (e.g., filters, lubricants, components).
- **Equipment:** Mention any specialized equipment employed for the maintenance tasks.

5. Status After Maintenance

- **Condition Assessment:** Describe the condition of the equipment or system after maintenance, highlighting improvements made.
- **Operational Status:** Indicate whether the equipment is fully operational, partially operational, or still experiencing issues.
- **Testing Results:** Include any tests conducted post-maintenance to verify functionality and performance.

6. Recommendations

- **Future Maintenance:** Suggest a schedule for routine maintenance to prevent future issues.
- **Upgrades or Replacements:** Recommend any upgrades or replacements that could enhance performance or reliability.
- **Training Needs:** Identify any training requirements for the client’s staff to ensure proper operation and maintenance of the equipment.

Practical Activity 6.4.2: Elaborating Maintenance report

Task:

1: Use sample of maintenance report provided by trainer, analyse how to elaborate maintenance report

2: Ask for assistance and clarification where needed

3: After reading and analysing the provided sample of maintenance report, perform the task described below:

> As network technician, referring to the Practical Activity 6.2.2: Troubleshooting and resolving a network problem. Elaborate maintenance report.

4: Present their work to trainer

5: Based on the feedback, repeat the task until a perfect result is achieved.

6: Read key readings 6.4.2 in their Manual

Key readings 6.4.2

Elaborating Maintenance report

The report serves as a valuable tool for tracking maintenance history, identifying potential issues, and planning future maintenance schedules.

Elements of a Maintenance Report

- **Client Information:** Clearly identify the client or asset owner, including name, contact information, and asset details.
- **Status Before Maintenance:** Describe the condition of the equipment or system before the maintenance work began. Include any existing problems or malfunctions.
- **Implementation of Solution:** Outline the steps taken to address the identified issues. Provide a detailed explanation of the maintenance tasks performed.
- **Used Tools, Materials, and Equipment:** List all the tools, materials, and equipment utilized during the maintenance process.
- **Status After Maintenance:** Describe the condition of the equipment or system after the maintenance work is completed. Include any performance improvements or remaining issues.
- **Recommendations:** Provide suggestions for future maintenance or improvements based on the findings of the report.

SAMPLE OF LAN MAINTENANCE REPORT

Date:

[Insert Date]

Client Information

- **Client Name:** ABC Enterprises
- **Client Contact:** MUGABO Jacques
- **Address:** 789 Dawn Town, City, Kigali
- **Client ID:** 1234

Status Before Maintenance

- **Initial Condition:**
  - ✓ **Network Devices:** Routers, switches, and access points showing intermittent connectivity issues.
  - ✓ **Observed Issues:** Frequent network drops, slow internet speed, and unresponsive network devices.
  - ✓ **Operational Impact:** Reduced productivity due to network interruptions affecting communication and access to critical applications.

Implementation of Solution

- **Actions Taken:**
  - ✓ Inspected and rebooted all network devices.
  - ✓ Updated firmware on routers and switches.
  - ✓ Replaced faulty Ethernet cables.
  - ✓ Reconfigured network settings for optimal performance.
  - ✓ Conducted a comprehensive network diagnostics test.
- **Step-by-Step Process:**

1. **Inspection and Reboot:**
   - Inspected all routers, switches, and access points for visible damage or loose connections.
   - Rebooted all devices to clear temporary issues.
2. **Firmware Update:**
   - Checked current firmware versions.
   - Downloaded and installed the latest firmware updates for routers and switches.
3. **Cable Replacement:**

- Identified and replaced damaged or worn-out Ethernet cables.

4. **Reconfiguration:**

   - Accessed network device settings and optimized configurations for better performance.
   - Adjusted settings for QoS (Quality of Service) to prioritize critical traffic.

5. **Diagnostics Test:**

   - Ran network diagnostics to check for latency, packet loss, and overall performance.
   - Identified and resolved minor configuration issues.

- **Technicians Involved:**
  - ✓ Technician 1: Michael MUNYURWA
  - ✓ Technician 2: Lisa MURAVA

Used Tools, Materials, and Equipment

- **Tools:**
  - ✓ Network diagnostic tools (e.g., Wireshark)
  - ✓ Firmware update utilities
  - ✓ Cable testers
  - ✓ Screwdrivers and pliers
- **Materials:**
  - ✓ Replacement Ethernet cables (Cat6)
  - ✓ Firmware files
- **Equipment:**
  - ✓ Laptops for configuration and diagnostics
  - ✓ Safety gear

Status After Maintenance

- **Final Condition:**
  - ✓ Network devices are fully operational with stable connectivity.
  - ✓ Improved internet speed and overall network performance.
  - ✓ No unresponsive devices detected.
- **Issues Resolved:**
  - ✓ Network drops and slow internet speed.
  - ✓ Faulty cables replaced, eliminating physical connection issues.
- **Operational Status:**
  - ✓ The LAN is functioning optimally, supporting all network-dependent operations without interruption.

Recommendations

- **Future Maintenance:**
  - ✓ Schedule bi-monthly network maintenance checks.
  - ✓ Regularly update firmware to keep network devices secure and efficient.
- **Upgrades:**
  - ✓ Consider upgrading to gigabit switches for faster internal data transfer.
  - ✓ Explore the implementation of a network monitoring solution for real-time performance tracking.
- **Operational Guidelines:**
  - ✓ Educate employees on basic troubleshooting steps to minimize downtime.
  - ✓ Ensure network devices are properly ventilated and protected from physical damage.

Prepared by:

- **Technician 1:** Michael MUNYURWA
- **Technician 2:** Lisa MURAVA

Approved by:

- **Supervisor:** HANYURWIMFURA Omar

Date: [Insert Date]

Client Acknowledgment:

I acknowledge that the maintenance activities described above were performed to my satisfaction.

Client Signature:

Date:

Points to Remember

- Detailed maintenance report would serve as a valuable tool for the IT department to improve network reliability and performance, as well as to communicate effectively with management and staff about the state of the LAN.
- **Elements of a Maintenance Report**

  - ✓ **Client Information:** Clearly identify the client or asset owner, including name, contact information, and asset details.
  - ✓ **Status Before Maintenance:** Describe the condition of the equipment or system before the maintenance work began. Include any existing problems or malfunctions.
  - ✓ **Implementation of Solution:** Outline the steps taken to address the identified issues. Provide a detailed explanation of the maintenance tasks performed.
  - ✓ **Used Tools, Materials, and Equipment:** List all the tools, materials, and equipment utilized during the maintenance process.
  - ✓ **Status After Maintenance:** Describe the condition of the equipment or system after the maintenance work is completed. Include any performance improvements or remaining issues.
  - ✓ **Recommendations:** Provide suggestions for future maintenance or improvements based on the findings of the report.

Application of learning 6.4.

XYZ Corp, has experienced several network disruptions over the past month, impacting their daily operations. The IT department conducted a comprehensive LAN maintenance session to identify and resolve the issues. An elaborated maintenance report is required to document the activities, findings, actions taken, and provide recommendations for future improvements.

Learning outcome 6 end assessment

Theoretical assessment

SECTION ONE

Choose the best answer for each question.

I. When performing routine LAN maintenance, what should be checked FIRST?
   a) Cabling for damage and loose connections
   b) Network switch configuration and firmware updates
   c) Firewall logs for suspicious activity
   d) Antivirus software on all connected devices

II. Overheating can significantly shorten the lifespan of network devices. Which component requires the most attention for temperature control?
   a) Patch panel
   b) Router
   c) Wireless access point
   d) Network cable

III. Dust buildup can disrupt airflow and cause equipment failure. What is the MOST appropriate tool for cleaning dust from sensitive network hardware?
   a) Regular vacuum cleaner
   b) Wet cloth
   c) Canned air (compressed air)
   d) Paper towels

IV. A sudden drop in network performance might be caused by:
   a) A software update requiring a reboot
   b) Worn-out patch panel connections
   c) Excessive file sharing activity
   d) Expired security certificates on the network switch

V. Which of the following is NOT a recommended practice for maintaining LAN cable integrity?
   a) Labeling cables for easy identification
   b) Avoiding sharp bends and kinks
   c) Exposing cables to direct sunlight
   d) Regularly testing cables for continuity

VI. Firmware updates for network devices often include:
   a) New features and bug fixes
   b) Increased power consumption
   c) Compatibility changes with outdated hardware
   d) Automatic virus removal

VII. Which common hardware failure can cause intermittent network connectivity issues?
   a) Failing hard drive in a network storage device
   b) Overloaded power supply unit

c) Defective network adapter on a client device
d) Malfunctioning router fan

VIII. Unsecured access points introduce significant security risks to a LAN. What is the recommended minimum-security protocol for wireless connections?
a) WEP
b) WPA
c) WPA2
d) WPA3

IX. To ensure optimal network performance, it's essential to monitor key metrics. Which of the following is NOT typically monitored on a LAN?
a) Network traffic volume
b) Available bandwidth
c) CPU utilization of network devices
d) Printer toner levels

X. Regular backups are crucial for data recovery in case of hardware failure. What is the MOST secure backup storage location for important LAN data?
a) Local hard drive on a network server
b) USB flash drive connected to a workstation
c) Cloud storage service with strong encryption
d) External hard drive kept on the same site as the LAN

Practical Assessment

Bella Company is a small-medium sized business that work as Forex bureau. Forex bureau provide services to exchange various currencies, allowing customers to buy foreign currency or sell their local currency.

The Bella company headquarter offices have Wired and wireless LAN, with a small server room housing a file server, print server, and router. Users are experiencing intermittent internet connectivity issues and slow file transfer speeds.

You are hired as a network technician to troubleshoot and resolve the network issues.

END

References

ARWD. (2023). Different Types of LAN. *thewifispecialist*, Page 1.

Ashikuzzaman.Md. (December 28, 2023). Components of Local Area Network (LAN). *LIS EDUCATION NETWORK*, 3.

Bozeman.D. (2024). DATASHEET AND OPERATING GUIDE . *teamwavelength*, Page 1.

CMW, G. V. (15 March 2023). A Step-by-Step Guide To Installing Slotted Trunking. *Cable Management Warehouse*, Page 1.

How to create a network diagram/. (2024). *miro*, Page 1.

https://www.teamwavelength.com/download/Datasheets/rackmt.pdf. (2024). DATASHEET AND OPERATING GUIDE. *teamwavelength*, Page 1.

Inc, T.-S. T. (April 2024). A Guide to the Different Types of Cable Labeling. *Tri Star Technologies*, Page 1.

Inc., L. S. (2024). How to Draw a Network Diagram. *lucidchart*, Page 1-3.

M, L. (2024). Cable Labelling . *Caledonian*, Page 1.

Organizer, C. (2024). Cable Labels & Printers. *Cable Organizer*, Page 1.

Oulu, K. (2024). Cable Trunking System Installation and Operation Manual. *Meka*, Page 1-14.

Oulu, K. (2024, 01 01). *Cable Trunking System Installation and Operation Manual.* Retrieved from meka.eu: https://meka.eu/wp-content/uploads/2023/01/Instal-Installation-and-Operation-Manual-Meka-1.pdf

Paradigm, V. (2024). How to Create Network Diagram?https://www.visual-paradigm.com/tutorials/how-to-create-network-diagram/. *visual-paradigm-tutorials*, Page 1-2.

types-of-network-topology. (06 Sep, 2024). *geeksforgeeks*, Page 1.

What-is-network-topology/. (2006-2023). *spiceworks*, Page 2.

White, S. G., & Davis, A. R. (2019). LAN Maintenance and Upkeep: Key Practices for Network

Stability. Network Administration Quarterly, 40(3), 72

https://networklessons.com/cisco/ccie-routing-switching-written/network-maintenance

RTB | RWANDA TVET BOARD

October 2024