RQF LEVEL 3

GENNF301

NETWORKING AND INTERNET

Network Fundamentals

TRAINEE'S MANUAL

October, 2024

NETWORK FUNDAMENTALS

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 October, 2024

ACKNOWLEDGEMENTS

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

Rwanda TVET Board (RTB) extends its appreciation to all parties who contributed to the development of the trainer's and trainee's manuals for the TVET Certificate III in Networking and Internet Technologies, specifically for the module **"GENNF301: Network Fundamentals."**

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

NIYITURAGIYE Vedaste

TUYISENGE Speratha

Validation

UWURUKUNDO Marie Grace

NSABIMANA Samuel

Conception, Adaptation and Editorial works

HATEGEKIMANA Olivier

GANZA Jean Francois Regis

HARELIMANA Wilson

NZABIRINDA Aimable

DUKUZIMANA Therese

NIYONKURU Sylvestre

NYINAWUMUNTU Gaudence

Formatting, Graphics, Illustrations, and infographics

YEONWOO Choe
SUA Lim
SAEM Lee
SOYEON Kim
WONYEONG Jeong
Joseph BYIMANA

Financial and Technical support

KOICA through TQUM Project

TABLE OF CONTENT

ACRONYMS

ADSL: Asymmetric Digital Subscriber Line

API: Application Programming Interface

APIPA: Automatic Private IP Addressing

ARP: Address Resolution Protocol

BGP: Border Gateway Protocol

BSC: Broadband System Corporation

CIDR: Classless Inter-Domain Routing

DDoS: Distributed Denial of Service

DHCP: Dynamic Host Configuration Protocol

DHCPv6: Dynamic Host Configuration Protocol for IPv6

DNS: Domain Name System

DSL: Digital Subscriber Line

EGP: Exterior Gateway Protocol

FTP: File Transfer Protocol

FTPES: FTP Explicit SSL

FTPS: File Transfer Protocol Secure

HTTP: Hypertext Transfer Protocol

HTTPS: Hypertext Transfer Protocol Secure

ICMP: Internet Control Message Protocol

ICT: Information Communication Technology

IEEE: Institute of Electrical and Electronics Engineers

IGP: Interior Gateway Protocol

IMAP: Internet Message Access Protocol

IoT: Internet of Things

IP: Internet Protocol

IPv4: Internet Protocol version 4

IPv6: Internet Protocol version 6

ISP: Internet Service Provider

IT: Information Technology

LACP: Link Aggregation Control Protocol

LAN: Local Area Network

LDAP: Lightweight Directory Access Protocol

MAC Address: Media Access Control Address

MAC: Media Access Control

MAN: Metropolitan Area Network

MODEM: Modulator Demodulator

MPLS: Multiprotocol Label Switching

MTU: Maximum Transmission Unit

NAS: Network-Attached Storage

NAT: Network Address Translation

NIC: Network Interface Card

OSI: Open Systems Interconnection

PAN: Personal Area Network

POP3: Post Office Protocol, version 3

QoS: Quality of Service

RAID: Redundant Array of Independent Disks

RARP: Reverse ARP

RIP: Routing Information Protocol

RTB: Rwanda TVET Board

SDN: Software-Defined Networking

SFC: System File Checker

SMTP: Simple Mail Transfer Protocol

SMTPS: SMTP Secure

SPD: Surge Protection Device

SSH: Secure Shell

SSID: Service Set Identifier

SSL/TLS: Secure Sockets Layer/Transport Layer Security

SSO: Single Sign-On

TCP/IP: Transmission Control Protocol/Internet Protocol

TCP: Transmission Control Protocol

TLS/SSL: Transport Layer Security/Secure Sockets Layer

TQUM Project: TVET Quality Management Project

TTL: Time to Live

UDP: User Datagram Protocol

URL: Uniform Resource Locator

VLAN: Virtual Local Area Network

VoIP: Voice over Internet Protocol

VPN: Virtual Private Network

WAN: Wide Area Network

WEP: Wired Equivalent Privacy

WIFI: Wireless Fidelity

WLAN: Wireless Local Area Network

WPA: Wi-Fi Protected Access

INTRODUCTION

This trainee's manual includes all the knowledge and skills required in Networking and Internet Technology specifically for the module of **"Network Fundamentals".** 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: GENNF301 NETWORK FUNDAMENTALS

Learning Outcome 1: Identify network concepts
Learning Outcome 2: Apply network protocols and communications
Learning Outcome 3: Apply IP addressing (IPv4&IPv6)

Indicative contents
1.1 Description of network concepts and technologies **1.2 Description of Network topology** **1.3 Description of Network components** **1.4 Classification of network devices** **1.5 Description of network models**

Key Competencies for Learning Outcome 1: Identify network concepts

Knowledge	Skills	Attitudes
• Description of network components/Devices/Equipment • Description of PPEs • Description of communication medium • Description of network topology diagram • Description of computer networks protocols • Description of network model	• Drawing network topology diagram • Classifying network devices	• Being Honest • Having Creativity • Having Accountability • Having a Teamwork spirit • Being a Problem Solver • Having Patience • Having Punctuality • Having Curiosity • Being a Critical thinker

Duration: 20 hrs

Learning outcome 1 objectives:

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

1. Define clearly a network based on their classification
2. Differentiate correctly types of network based on their functionalities
3. Describe correctly network topology based on their types
4. Describe correctly network devices, components based on their functions
5. Classify clearly network devices based on their use
6. Draw correctly network topology diagram based on identified network topology type

Resources

Equipment	Tools	Materials
• Router • Hubs • Switch • NIC • Computer • Access points • Antenna • Gateways	• Networking toolkit • Simulation tools	• Network Cables • Internet

Indicative content 1.1: Description of network concepts and technologies

Duration: 4 hrs

Theoretical Activity 1.1.1: Introduction to network concepts and technologies

Tasks:

1: Answer the following questions

i. What is a computer network, and why are they important in today's digital world?

ii. What are the types of network based on geographical area and based on components roles?

iii. In the context of network architecture, what is the difference between a client-server and a peer-to-peer network?

iv. How are wireless networks like Wi-Fi structured, and what factors affect signal strength and quality?

2: Present your findings to trainer, workshop assistant, the whole class or one of your colleagues.

3: Read the Key readings 1.1.1 in this manual.

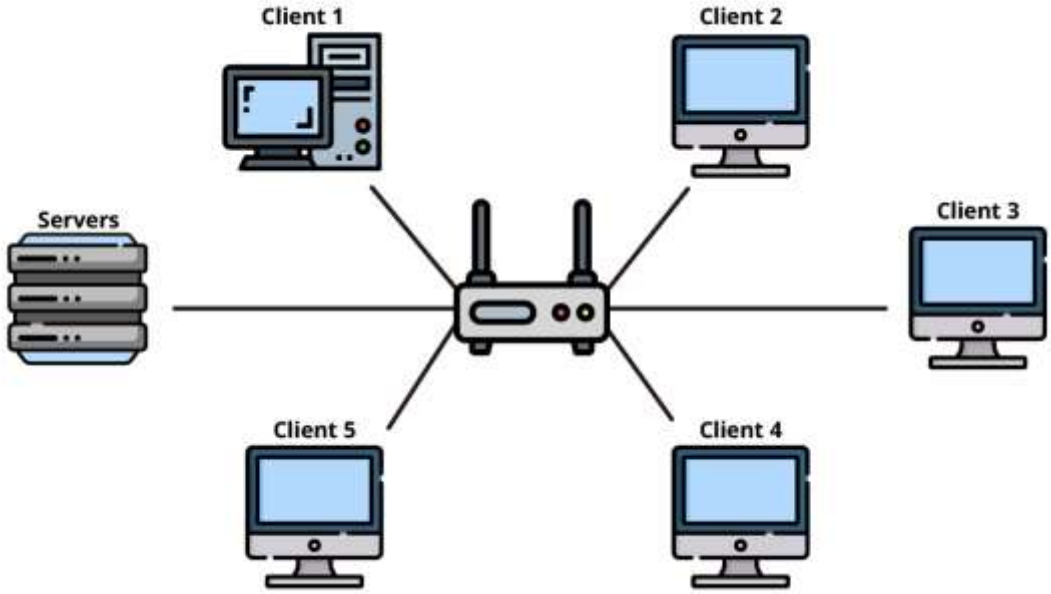
4: Ask to the trainer for clarifications if necessary.

Key readings 1.1.1.: Introduction to network concepts and technologies

- **A computer network**: A computer network consists of two or more computers and other hardware devices that are linked together through communication channels to share electronic communications and resources, such as printers with various users. In computer networks, computing devices are called **nodes** and share data with each other through **data links**. These links are sent over cable media such as wires, optic cables, or wireless media such as Wi-Fi. The connected computers also share resources, such as access to printers, with the most common resource being the internet.
- **Types of network:** There are different types of computer networks based on various criteria such as transmission medium, architecture, size or geographical area and topology.
  - **Types of network based on geographical area**
    - ✓ **LAN (local area network)**: A LAN connects computers over a relatively short distance, allowing them to share data, files, and resources. For example, a

LAN may connect all the computers in an office building, school, or hospital. Typically, LANs are privately owned and managed.

A LAN, or local area network, is a group of connected computing devices within a localized area that usually share a centralized Internet connection.



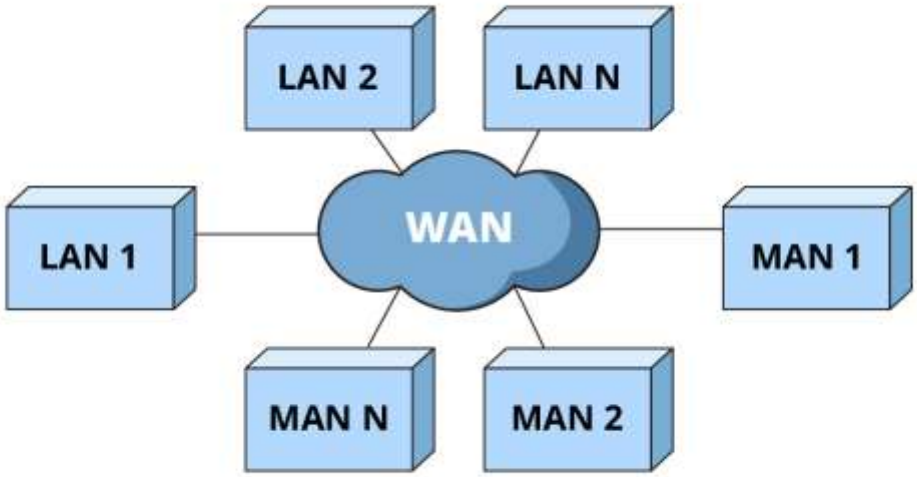
Most LANs connect to the **Internet** at a central point: a **router**. Home LANs often use a single router, while LANs in larger spaces may additionally use **network switches** for more efficient packet delivery.

LANs almost always use Ethernet, Wi-Fi, or both in order to connect devices within the network. Ethernet is a protocol for physical network connections that requires the use of Ethernet cables. Wi-Fi is a protocol for connecting to a network via radio waves.

A variety of devices can connect to LANs, including servers, desktop computers, laptops, printers, IoT devices, and even game consoles. In offices, LANs are often used to provide shared access to internal employees to connected printers or servers.

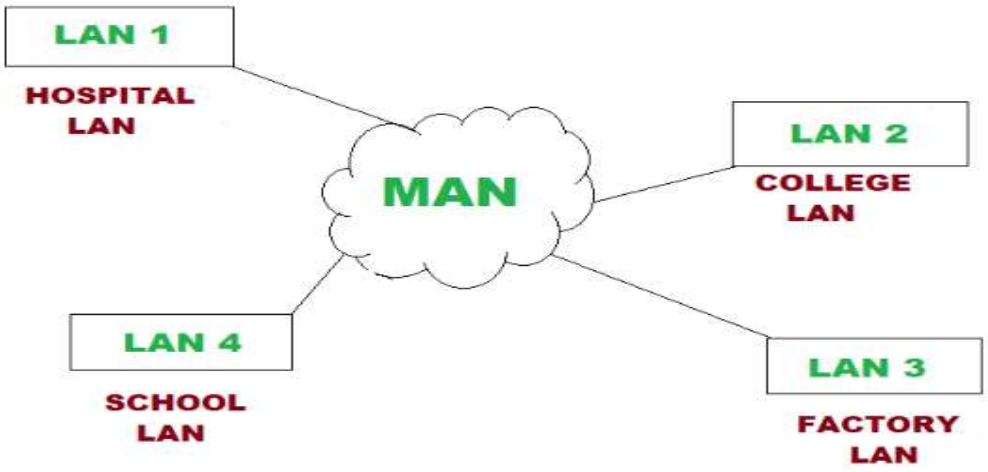
✓ **WLAN (wireless local area network)**

A WLAN is just like a LAN but connections between devices on the network are made wirelessly.

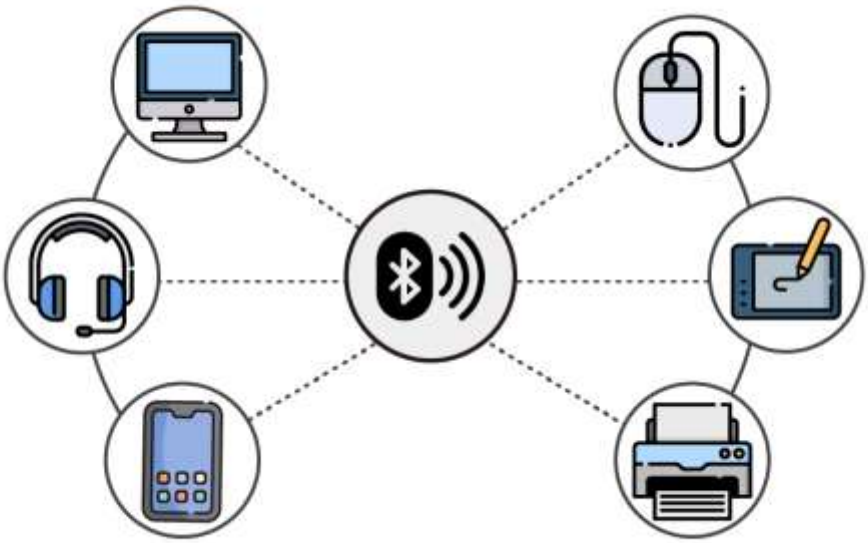


As the name implies, a WAN connects computers over a wide area, such as from region to region or even continent to continent. The internet is the largest WAN, connecting billions of computers worldwide. You will typically see collective or distributed ownership models for WAN management.

✓ **MAN (metropolitan area network)**: MANs are typically larger than LANs but smaller than WANs. Cities and government entities typically own and manage MANs.

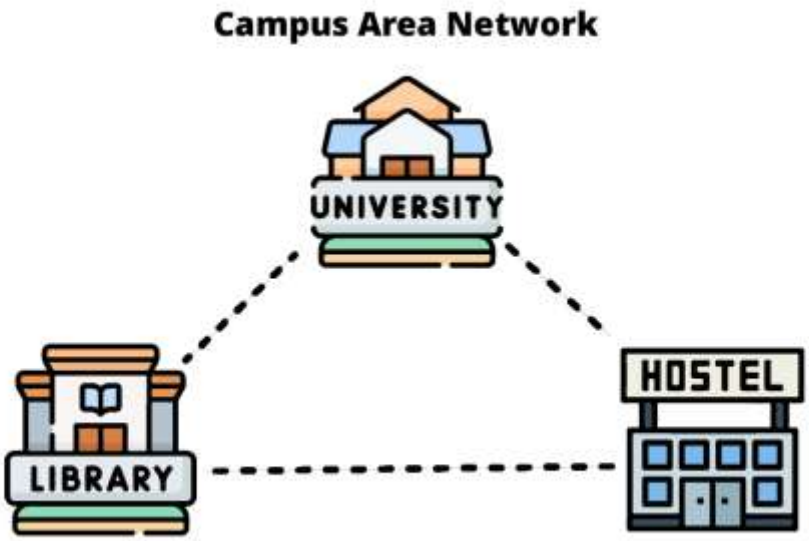


- ✓ **PAN (personal area network)**: A PAN serves one person. For example, if you have an iPhone and a Mac, it's very likely you've set up a PAN that shares and syncs content text messages, emails, photos, and more across both devices.



- ✓ **SAN (storage area network)** : A SAN is a specialized network that provides access to block-level storage, shared network or cloud storage that, to the user, looks and works like a storage drive that's physically attached to a computer.
- **CAN (campus area network)**

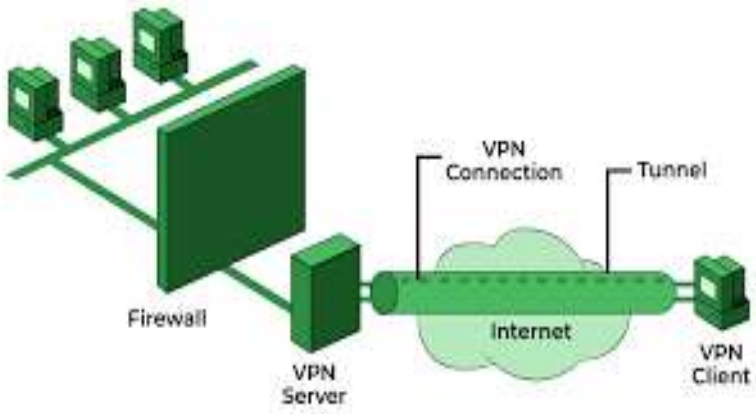
A CAN is also known as a corporate area network. A CAN is larger than a LAN but smaller than a WAN. CANs serve sites such as colleges, universities, and business campuses.



- **VPN (virtual private network)**

A VPN is a secure, point-to-point connection between two network end points.

A VPN establishes an encrypted channel that keeps a user's identity and access credentials, as well as any data transferred, inaccessible to hackers.



- **Uses of networks**

So far, you have learned that networks can be used in a variety of environments; from schools to businesses to homes.

There are many different uses and applications for computer networks, including:

- ✓ **Resource sharing:** One of the primary uses of computer networks is to share resources, such as printers, scanners, and data storage devices.
- ✓ **Communication:** Computer networks also facilitate communication between individuals and groups, whether through email, instant messaging, or video conferencing.
- ✓ **Internet access:** Computer networks provide access to the internet, which is essential for many businesses and individuals. This allows users to browse

websites, access online resources, and communicate with others around the world.

- ✓ **Data sharing:** Networks allow for the sharing of data and information, whether between users in the same organization or between different organizations.
- ✓ **Security:** Computer networks can be used to implement security measures, such as firewalls and encryption, which can help to protect sensitive information and prevent unauthorized access.

- **Network technologies**

Network Technology involves the use of data systems to manage and deliver digital resources over a computer network. A variety of industries use computer hardware and system software that maintains a network, creating a need for specialists to manage them. Some of them are the following: IEEE802.3 Ethernet, IEEE802.5 token ring, IEEE802.8 fibre optics and IEEE 802.11 Wireless.

- ✓ **IEEE802.3 Ethernet**

Ethernet is a set of technologies and protocols that are used primarily in LANs. It was first standardized in the 1980s by IEEE 802.3 standard. IEEE 802.3 defines the physical layer and the medium access control (MAC) sub-layer of the data link layer for wired Ethernet networks. Ethernet is classified into two categories: classic Ethernet and switched Ethernet.

Classic Ethernet is the original form of Ethernet that provides data rates between 3 to 10 Mbps. The varieties are commonly referred to as 10BASE-X. Here, 10 is the maximum throughput, i.e. 10 Mbps, BASE denoted use of baseband transmission, and X is the type of medium used. Most varieties of classic Ethernet have become obsolete in the present communication scenario.

A switched Ethernet uses switches to connect to the stations in the LAN. It replaces the repeaters used in classic Ethernet and allows full bandwidth utilization.

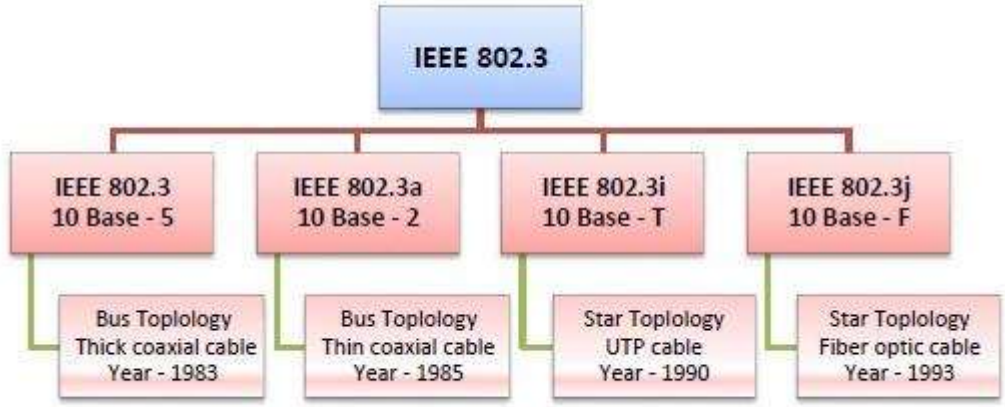
- ✓ **IEEE 802.3 Popular Versions**

There are a number of versions of IEEE 802.3 protocol. The most popular ones are:

- **IEEE 802.3:** This was the original standard given for 10BASE-5. It used a thick single coaxial cable into which a connection can be tapped by drilling into the cable to the core. Here, 10 is the maximum throughput, i.e. 10 Mbps, BASE denoted use of baseband transmission, and 5 refers to the maximum segment length of 500m.
- **IEEE 802.3a:** This gave the standard for thin coax (10BASE-2), which is a thinner variety where the segments of coaxial cables are connected by BNC connectors. The 2 refers to the maximum segment length of about 200m (185m to be precise).
- **IEEE 802.3i:** This gave the standard for twisted pair (10BASE-T) that uses unshielded twisted pair (UTP) copper wires as physical layer medium. The further

variations were given by IEEE 802.3u for 100BASE-TX, 100BASE-T4 and 100BASE-FX.

- **IEEE 802.3i:** This gave the standard for Ethernet over Fiber (10BASE-F) that uses fiber optic cables as medium of transmission.



✓ **Frame Format of Classic Ethernet and IEEE 802.3**

The main fields of a frame of classic Ethernet are:

- **Preamble:** It is the starting field that provides alert and timing pulse for transmission. In case of classic Ethernet, it is an 8-byte field and in case of IEEE 802.3 it is 7 bytes.
- **Start of Frame Delimiter:** It is a 1-byte field in a IEEE 802.3 frame that contains an alternating pattern of ones and zeros ending with two ones.
- **Destination Address:** It is a 6-byte field containing the physical address of destination stations.
- **Source Address:** It is a 6-byte field containing the physical address of the sending station.
- **Length:** It is a 7 bytes' field that stores the number of bytes in the data field.
- **Data:** This is a variable sized field that carries the data from the upper layers. The maximum size of the data field is 1500 bytes.
- **Padding:** This is added to the data to bring its length to the minimum requirement of 46 bytes.
- **CRC:** CRC stands for cyclic redundancy check. It contains the error detection information.

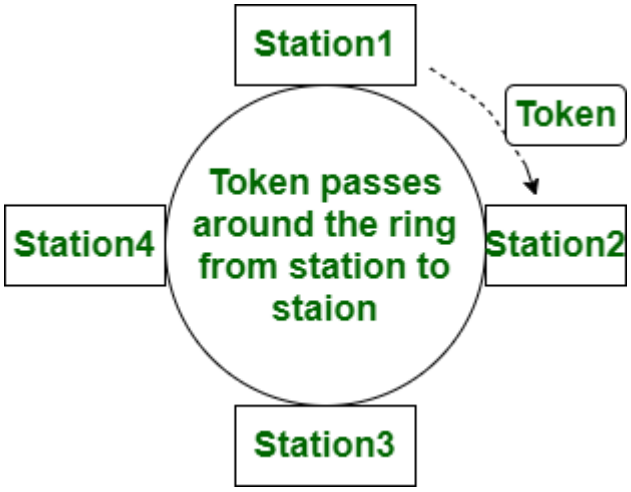
✓ **IEEE802.5 token ring**

Token ring (IEEE 802.5) is a communication protocol in a local area network (LAN) where all stations are connected in a ring topology and pass one or more tokens for channel acquisition. A token is a special frame of 3 bytes that circulates along the ring of stations. A station can send data frames only if it holds a token. The tokens are released on successful receipt of the data frame.

- **Token Passing Mechanism in Token Ring**

If a station has a frame to transmit when it receives a token, it sends the frame and then passes the token to the next station; otherwise it simply passes the token to the next station. Passing the token means receiving the token from the preceding station and transmitting to the successor station. The data flow is unidirectional in the direction of the token passing.

In order that tokens are not circulated infinitely, they are removed from the network once their purpose is completed.



- **IEEE802.8 fiber optics**

The Fiber optic technical advisory group was to create a LAN standard for fibre optic media used in token passing computer networks like FDDI. This is part of the IEEE 802 group of standards.

- **IEEE 802.11 Wireless**

IEEE 802.11 is part of the IEEE 802 set of local area network (LAN) technical standards, and specifies the set of media access control (MAC) and physical layer (PHY) protocols for implementing wireless local area network (WLAN) computer communication.

The standard and amendments provide the basis for wireless network products using the Wi-Fi brand and are the world's most widely used wireless computer networking standards. IEEE 802.11 is used in most home and office networks to allow laptops, printers, smartphones, and other devices to communicate with each other and access the Internet without connecting wires. IEEE 802.11 is also a basis for vehicle-based communication networks with IEEE 802.11p.

The standards are created and maintained by the Institute of Electrical and Electronics Engineers (IEEE) LAN/MAN Standards Committee (IEEE 802). The base version of the standard was released in 1997 and has had subsequent amendments. While each amendment is officially revoked when it is incorporated in the latest version of the standard, the corporate world tends to market to the revisions because they concisely denote the capabilities of their products. As a result, in the marketplace, each revision tends to become its own standard.

IEEE 802.11 uses various frequencies including, but not limited to, 2.4 GHz, 5 GHz, 6 GHz, and 60 GHz frequency bands. Although IEEE 802.11 specifications list channels that might be used, the radio frequency spectrum availability allowed varies significantly by regulatory domain.

The protocols are typically used in conjunction with IEEE 802.2, and are designed to interwork seamlessly with Ethernet, and are very often used to carry Internet Protocol traffic.

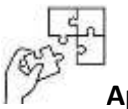
- **Protocol**

A network protocol is a set of established rules that specify how to format, send and receive data so that computer network endpoints, including computers, servers, routers and virtual machines, can communicate despite differences in their underlying infrastructures, designs or standards.

To successfully send and receive information, devices on both sides of a communication exchange must accept and follow protocol conventions. In networking, support for protocols can be built into the software, hardware or both.

Points to Remember

- Understanding types of computer network based on different factors such size or distance coverage, transmission medium, management, and topology.
- Understanding roles of network protocols to operate and manage networks. They ensure reliable data transmission, security, and network management, facilitating communication between different devices and applications. Understanding these protocols is crucial for network design, troubleshooting, and security
- Understanding IP addressing is crucial for network configuration, management, and troubleshooting. Whether dealing with IPv4 or IPv6, subnetting, DHCP, or address allocation, these concepts form the backbone of network communication and organization.
- Understanding the functions and characteristics of these network devices is crucial for designing, implementing, and managing efficient and secure networks. Each device plays a specific role in ensuring data is transmitted correctly, securely, and efficiently across the network.
- Understanding of network technologies to cover a comprehensive variety of tools and techniques that facilitate connectivity, communication, management, and security of networks. Understanding these technologies is essential for designing, implementing, and maintaining efficient, secure, and scalable networks.



Application of learning 1.1.

You have completed the module on “Network Fundamentals”. The XYZ construction company does not have any IT technicians available to advise on purchase network devices and to draft a network topology diagram used to build a network. Now you are recruited by that company to draft a network topology diagram and to advise to purchase network devices.

Indicative content 1.2: Description of Network topology

Duration: 4 hrs

Theoretical Activity 1.2.1: Identification of network topologies

Tasks:

1: Answer the following questions:

i. What is a network topology, and why is it important in network design?
ii. Can you name and describe the main types of network topologies?
iii. What are the advantages of a star topology in terms of reliability and ease of troubleshooting?
iv. In a bus topology, how are devices connected to the main communication channel, and what challenges may arise in such a setup?
v. Explain the ring topology, including the path data travels and the role of token passing in ring networks.
vi. How does a mesh topology differ from other topologies?
vii. Which topology is commonly used in modern Ethernet networks, and why?
viii. In a large network, what challenges might you encounter when using a ring topology?
ix. What are the potential disadvantages of a star topology, and how can they be mitigated?
x. In a wireless network, what type of physical topology is often used, and how does it differ from traditional wired topologies?
xi. How does a network's physical topology differ from its logical topology?
xii. What role does cabling and hardware play in determining the physical topology of a network?

2: Present your findings to the whole class or one of your colleagues.

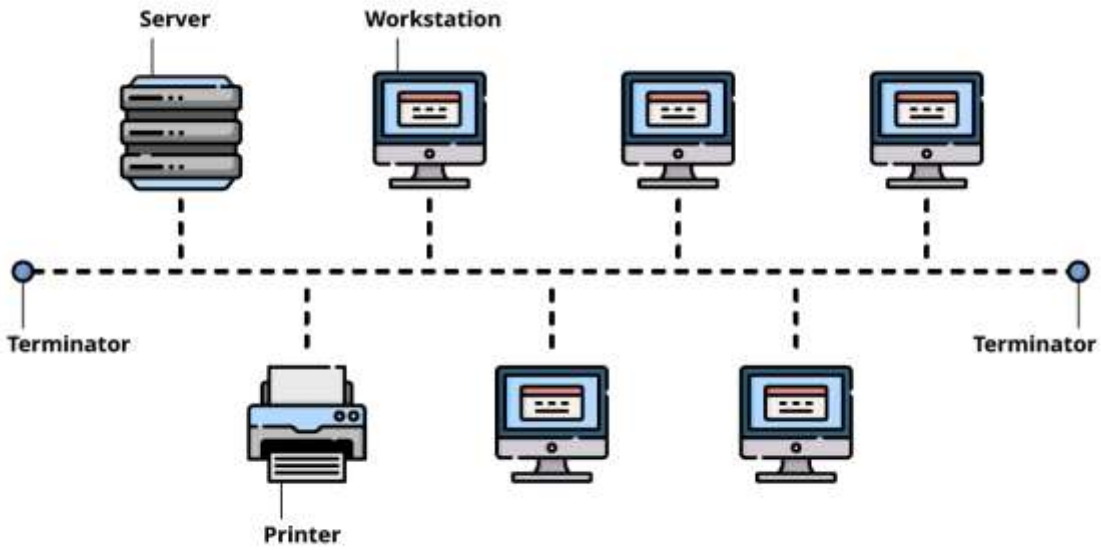
3: Read the Key readings 1.2.1 in this manual.

4: Ask to the trainer for clarifications if necessary.

Key readings 1.2.1.: Identification of network topologies

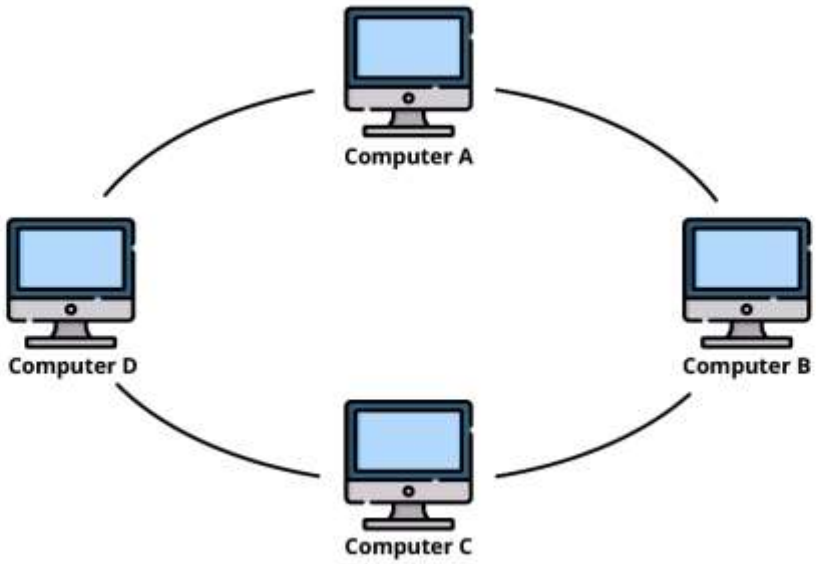
- **Network topology:** A network topology is the physical and logical arrangement of nodes and connections in a network. Nodes usually include devices such as switches, routers and software with switch and router features. Network topology describes the methods in which all the elements of a network are mapped. The topology term refers to both the physical and logical layout of a network.
- **Logical topology:** A logical topology is a concept in networking that defines the architecture of the communication mechanism for all nodes in a network. or A logical topology is a concept in networking that defines the architecture of the communication mechanism for all nodes in a network. Using network equipment such as routers and switches, the logical topology of a network can be dynamically maintained and reconfigured.
- **Physical topology**: Physical network topology is the placement of the various components of a network and the different connectors usually represent the physical network cables, and the nodes usually the physical network devices. The most popular physical topologies are:
    - ✓ Bus Topology
    - ✓ Ring Topology
    - ✓ Star Topology
    - ✓ Tree Topology
    - ✓ Mesh Topology
    - ✓ Hybrid Topology

✓ **Bus Topology :** a Bus topology is also known as line topology, is a type of network topology in which all devices in the network are connected by one central RJ-45 network cable or coaxial cable. The single cable, where all data is transmitted between devices, is referred to as the bus, backbone, or trunk



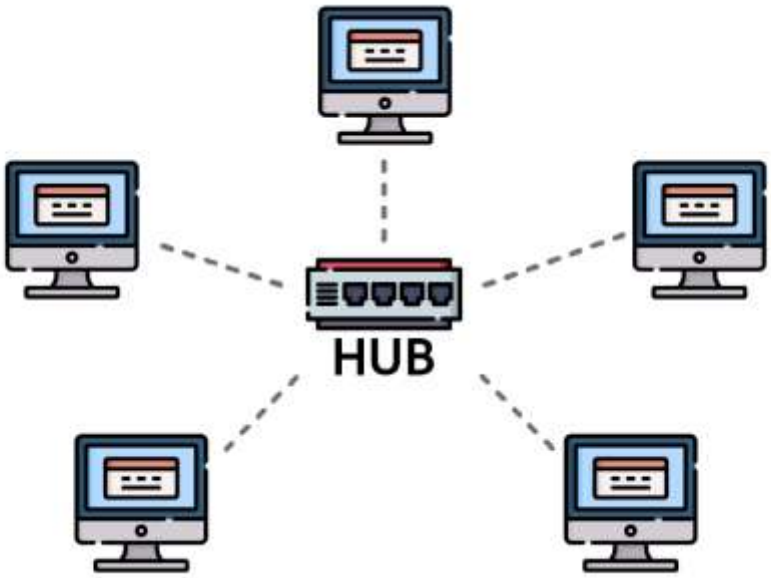
- **Advantages:** Here are pros/benefits of using a bus topology:
  - Cost of the cable is very less as compared to other topologies, so it is widely used to build small networks.
  - Famous for LAN networks because they are inexpensive and easy to install.
  - It is widely used when a network installation is small, simple, or temporary.
  - It is one of the passive topologies. So computers on the bus only listen for data being sent, and are not responsible for moving the data from one computer to others.
- **Disadvantages:** Here are the cons/drawbacks of bus topology:
  - In case if the common cable fails, then the entire system will crash down.
  - When network traffic is heavy, it develops collisions in the network.
  - Whenever network traffic is heavy, or nodes are too many, the performance time of the network significantly decreases.
  - Cables are always of a limited length

✓ **Ring Topology :** a ring topology is a type of network topology in which each device is connected to two other devices on either side via an RJ-45 cable or coaxial cable. This forms a circular ring of connected devices which gives it its name. Data is commonly transferred in one direction along the ring, known as a unidirectional ring.



- **Advantages:**
  - Easy to install and reconfigure.
  - Adding or deleting a device need you to move only two connections.
  - The troubleshooting process is difficult in a ring topology.
  - Failure of one computer can disturb the whole network.
  - Offers equal access to all the computers of the networks
  - Faster error checking and acknowledgment.
- **Disadvantages:**
  - Unidirectional traffic.
  - Break in a single ring can risk the breaking of the entire network
  - Modern day high-speed LANs made this topology less popular.
  - It is very difficult to troubleshoot the ring network.
  - Adding or removing the computers can disturb the network activity.

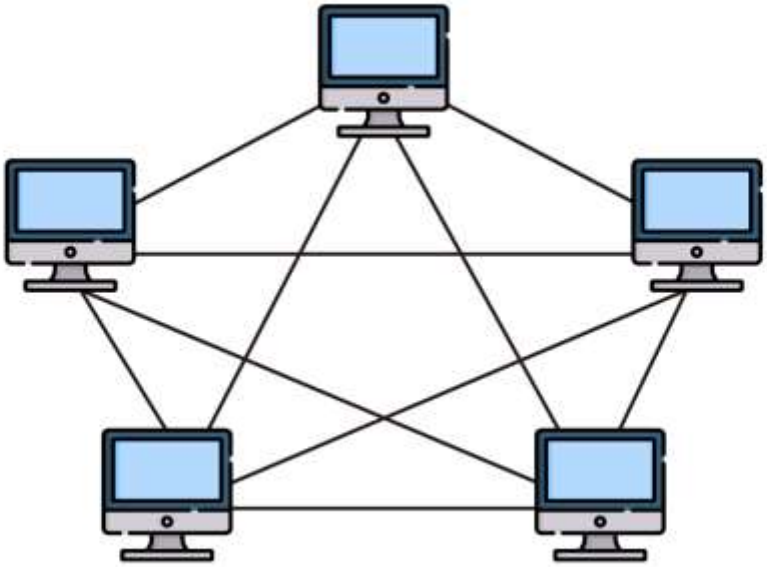
✓ **Star Topology:** In the star topology, all the computers are connected with the help of a hub. This cable is called a central node, and all other nodes are connected using this central node.



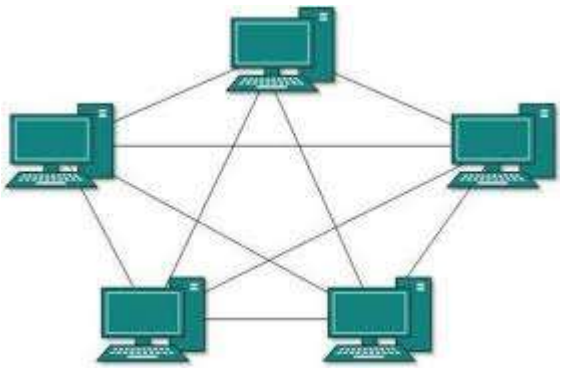
- **Advantages:**
  - Easy to troubleshoot, set up, and modify.
  - Only those nodes are affected, that has failed. Other nodes still work.
  - Fast performance with few nodes and very low network traffic.
  - In Star topology, addition, deletion, and moving of the devices are easy.
- **Disadvantages:**
  - If the hub or concentrator fails, attached nodes are disabled.
  - Cost of installation of star topology is costly.
  - Heavy network traffic can sometimes slow the bus considerably.
  - Performance depends on the hub's capacity
  - A damaged cable or lack of proper termination may bring the network down

✓ **Mesh Topology:** The mesh topology has a unique network design in which each computer on the network connects to every other.

- **Partial Mesh Topology**: In this type of topology, most of the devices are connected almost similarly as full topology. The only difference is that few devices are connected with just two or three devices



- **Full Mesh Topology**: In this topology, every nodes or device are directly connected with each other

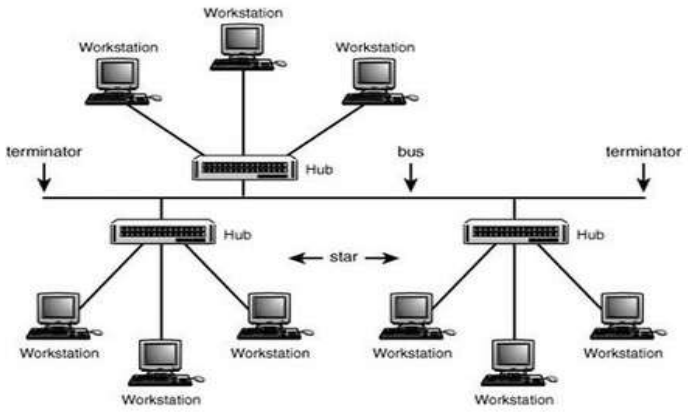


Reference: https://www.quora.com/what-is-a-mesh-topology

- **Advantages:** Here, are pros/benefits of Mesh topology
  - The network can be expanded without disrupting current users.
  - Need extra capability compared with other LAN topologies.
  - No traffic problem as nodes have dedicated links.
  - Dedicated links help you to eliminate the traffic problem.
  - A mesh topology is robust.
  - P2P links make the fault identification isolation process easy.
  - It helps you to avoid the chances of network failure by connecting all the systems to a central node.
  - Every system has its privacy and security.
- **Disadvantages:**
  - Installation is complex because every node is connected to every node.

- It is expensive due to the use of more cables.
- Complicated implementation.
- It requires more space for dedicated links.
- Because of the number of input-outputs, it is expensive to implement.
- It requires a large space to run the cables.

✓ **Tree Topology:** A tree topology has a root node, and all other nodes are connected which form a hierarchy. So It is also known as hierarchical topology



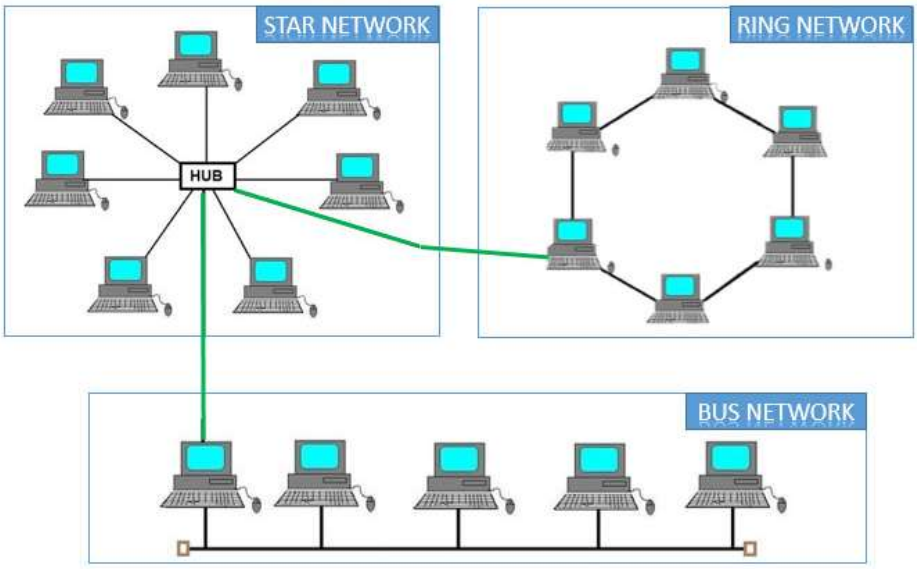
Advantages: Here are pros/benefits of tree topology:

- Failure of one node never affects the rest of the network.
- Node expansion is fast and easy.
- Detection of error is an easy process
- It is easy to manage and maintain

Disadvantages: Here are cons/drawback of tree topology:

- It is heavily cabled topology
- If more nodes are added, then its maintenance is difficult
- If the hub or concentrator fails, attached nodes are also disabled.

✓ **Hybrid topology:** As the term suggests, hybrid topology is a type of network topology in which two or more different topologies are integrated or combined to lay out a network. In Lay man's terms, hybrid topology is the combination of two or more networks. The network type could be Star, Ring, Bus, or Mesh.



- **Advantages:** Here, are advantages/pros using Hybrid topology:
  - Offers the easiest method for error detecting and troubleshooting
  - Highly effective and flexible networking topology
  - It is scalable so you can increase your network size
- **Disadvantages:**
  - The design of hybrid topology is complex
  - It is one of the costliest processes

Practical Activity 1.2.2: Design/draw a network topology diagram

Task:

1: Individually, perform the following activities:
You are hired by XYZ Networks as a medium-sized company located in Ruhango district to design a network topology diagram which will be used to implement that network in order to deliver its services and communicate between its employees.
3: Referring to the list provided on step 2, select the right tools, materials, and equipment required to draw a network topology diagram.
4: Present your work to the trainer, workshop assistant or your classmate

5: Read the key reading 1.2.2.
6: Perform the task provided in application of learning 1.2

Key readings 1.2.2: Design/draw a network topology diagram

- **Network topology:** refers to the physical or logical arrangement of network devices and connections within a network. Understanding network topology is crucial for designing, implementing, and troubleshooting networks. Determine Network Topology such as star, bus, ring, mesh, hybrid, etc.

Network simulation Software: Network simulation software is used to model and simulate network behavior and performance, helping in network design, and troubleshooting. Here are some popular network simulation tools, along with their key features:

Cisco Packet Tracer: Designed by Cisco, it is used for creating and simulating network topologies and provides a visual interface to design networks and a simulation mode to test network behavior.

GNS3 (Graphical Network Simulator-3): Allows the simulation of real network devices by integrating with virtual machines and emulators and useful for advanced network design and troubleshooting.

NS3 (Network Simulator 3): An open-source discrete-event network simulator designed for research and education, provides a comprehensive simulation environment with support for various network protocols and technologies and allows for the simulation of complex network scenarios and performance analysis.

Central Device: Place the core device (e.g., router or switch) at the center if using a star topology or at strategic points for other topologies.

- **Peripheral Devices:** Arrange devices around the central device based on their connections.
- **Connections:** Draw lines to represent wired connections and indicate wireless connections as needed.
- **Router:** Central device connecting to external networks and managing internal traffic.
- **Switches:** Distribute network traffic among connected devices.
- **End Devices:**
  - ✓ **Computers:** Desktops, laptops.
  - ✓ **Printers:** Networked printers.
  - ✓ **Servers:** File servers, application servers.
  - ✓ **Access Points:** For wireless connectivity.
- **Connections:**
  - ✓ **Wired Connections:** Use solid lines for Ethernet connections.
  - ✓ **Wireless Connections:** Use dashed lines or Wi-Fi symbols.
- **Network Services:**

- ✓ **DHCP Server:** Assigns IP addresses dynamically.
- ✓ **DNS Server:** Resolves domain names to IP addresses.
- ✓ **Firewall/VPN:** For security.

Points to Remember

- Clearly define the purpose of the network and the requirements of the users, and the size and scale of the network, including the number of devices and the physical layout.
- Decide on the most suitable network topology (e.g., star, bus, ring, mesh) based on the network's needs, performance requirements, and budget.
- Represent all network devices, such as routers, switches, hubs, access points, and servers.
- Clearly show how devices are connected, including wired and wireless connections.
- Include end-user devices like computers, printers, and mobile devices.
- Include details such as IP addresses, device names, and port numbers if relevant.
- Utilize diagramming software like Packet tracer, EdrawMax, GNS3 and other like Microsoft Visio, draw.io to create professional and accurate diagrams.
- Document the network design with notes explaining the choices and configurations.

Application of learning 1.2.

The school wants to implement a network project for its staffs and students and also it has chosen you to design a network topology diagram which will incorporate both wired and wireless networks. This project will enhance the school's technological capabilities and provide a reliable and flexible network for students and staff. Your task is to select and to design/draw the appropriate network diagram.

Indicative content 1.3: Description of Network components

Duration: 4 hrs

Theoretical Activity 1.3.1: Identification of network components

Tasks:

1: Respond to the following questions

i. What is the primary function of a router in a network, and how does it differ from a switch?
ii. Can you name some common physical network components found in a typical network infrastructure?
iii. Describe the role of access points (APs) in a wireless network and how they relate to routers.
iv. What is the purpose of a network switch, and how does it facilitate data transmission within a local network?
v. Explain the distinction between network hubs and switches. What are the advantages of using switches over hubs?
vi. What is the significance of network cabling in a wired network, and can you name different types of network cables?
vii. What is the purpose of a modem in a network, and in what scenarios might it be used?
viii. What role do network interfaces (e.g., network cards) play in connecting devices to a network?

2: Present your findings to the whole class or one of your colleagues.

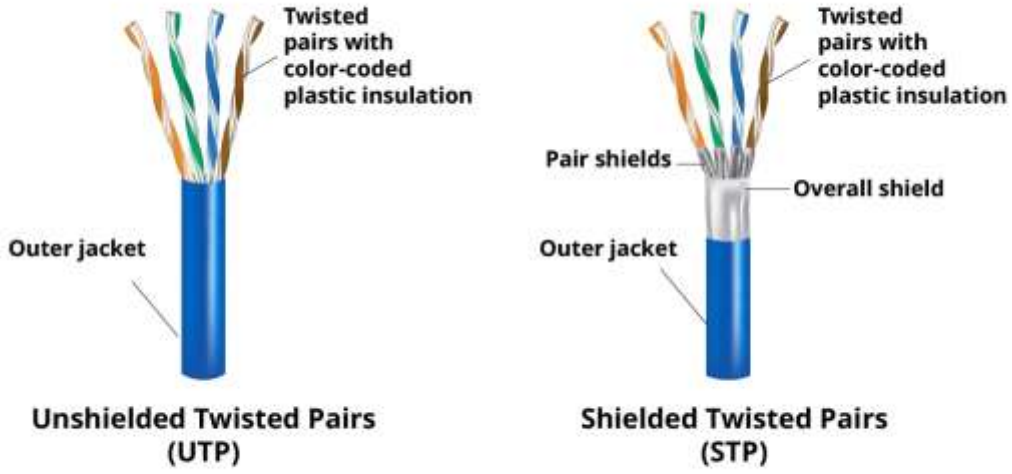
3: Read the Key readings 1.3.1 in this manual.

4: Ask to the trainer for clarifications if necessary.

Key readings 1.3.1.: Identification of network components

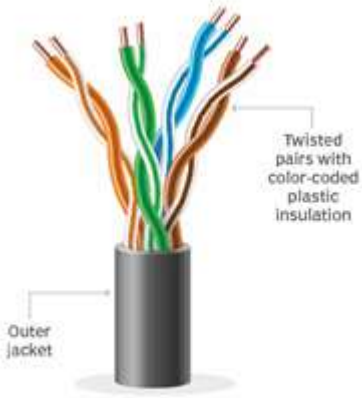
- **Network media:** Network media refers to the communication channels used to interconnect nodes on a computer network.
- **Types of network media:** Devices can exchange information along various media, physically (wired) and logically(wireless).
- **Physical media:** Physical media describes the common types of network media, including twisted-pair cable, coaxial cable, fiber-optic cable.
  - ✓ **Twisted Pair Cable:** The most popular form of traditional copper-wired cables is the **twisted pair cable**, which can also be called a CAT# cable. Standard CAT5

cable contains 4 pairs of wires, and older phone cable is CAT3, with 2 pairs of wires. There is also CAT5E, an upgraded version of CAT5, and CAT6 which is recommended for gigabit Ethernet.



These copper wires are crimped into a plastic **RJ-45** connector, which is similar to a telephone cable connector. Twisted pair is susceptible to interference, therefore CAT5 can only run a maximum of 100m or 320 ft. before signal loss occurs. CAT5E can run to 350m and CAT6 to 550m. Twisted-pair cables are of two types as Unshielded twisted pair (UTP) and Shielded twisted pair (STP).

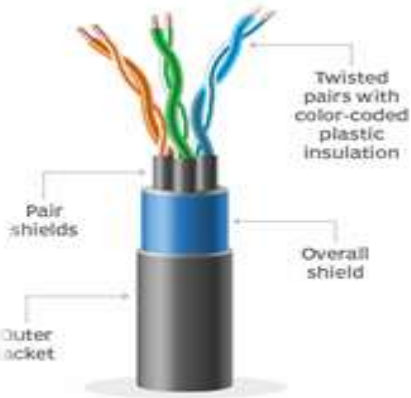
- **Unshielded twisted pair (UTP):** These cables generally comprise wires and insulators. A UTP cable has no internal shielding. The UTP cable is the most common twisted-pair cable used in Ethernet networks. It also is used for traditional telephone (UTP-Cat1) systems. UTP cables are popular all over the world due to their low cost, ease of installation and flexibility. They also support high data transfer speeds of up to 1 gigabit per second (Gbps) for transmission distances of up to 100 meters (m). These cables are also easy to expand and troubleshoot. One crucial drawback of UTP is that it is vulnerable to signal interference, which can affect output quality. Moreover, it is not suitable for long-distance transmissions. To support distances longer than 100 m, repeaters are required.



Unshielded twisted pair

- ✓ **Shielded twisted pair (STP):** These cables come with a braided, wired mesh that encases each pair of insulated copper wires. STP cables include a shielding, usually made of aluminum foil, around the conductors to isolate the conductors and improve the cables' resistance to noise and signal interference. One drawback is that STP cables are more difficult to connect at termination points. Also, STP cables are more expensive than UTP cables. Nonetheless, they prevent signal interference better than UTP cables, so their additional cost can be worth it, depending on the application.

Shielded cables support data transfer rates of 10 to 100 megabits per second (Mbps). They are best suited for transmission distances of up to 100 m.



Shielded twisted pair

Categories of twisted-pair cabling systems based on rated speeds

a. **Cat1:** This UTP cable supports a maximum data rate of 1 Mbps. It was primarily designed for analog voice communications and is not suitable for networking applications.
b. **Cat2:** This category was used in IBM token ring networks in the 1980s. It is capable of voice and data communications, although it is not commonly used now on high-speed networks.
c. **Cat3:** This category was introduced in the early 1990s and is currently used in telephone wiring. It consists of four twisted pairs and was the first to support

10Base-T Ethernet networks and digital communications. The cable is not considered suitable for modern networking since it only supports data transmission rates of up to 10 Mbps.

d. **Cat4:** Like Cat3, Cat4 cables are also typically found in older buildings. Originally, it was used in IBM token ring networks.
e. **Cat5:** Introduced in 1995, Cat5 twisted-pair cables support a data transmission rate of up to 100 Mbps. They are suitable for 100Base-T Ethernet networks. They are capable of transmitting video, data, and telephone signals and are used in backbone cabling and telephone lines.
f. **Cat5e:** Considered an enhanced version of Cat5, Cat5e supports speeds of up to 1 Gbps. Cat5e achieves this by increasing the number of twists, which makes it more resistant to crosstalk and signal attenuation. This cable is used in Ethernet, Fast Ethernet and Gigabit Ethernet networks.
g. **Cat6:** Cat6 was considered a significant upgrade to Cat5e, as it supports greater data transfer rates of up to 10 Gbps for distances up to 37 m. It includes a physical separator called a **spline** to reduce crosstalk. It also includes shielding to reduce electromagnetic interference (EMI). Cat6 cables are backward-compatible with Cat5 and Cat5e cables.
h. **Cat6a:** Introduced in 2009, Cat6a supports a greater bandwidth of 500 megahertz (MHz) and speeds of 10 Gbps. It is usually called an augmented Cat6 cable.
i. **Cat7:** Cat7 is a newer copper cable specification. It supports speeds of up to 10 Gbps at distances of up to 100 m. This cable features four individually shielded copper wires to prevent crosstalk and EMI. The individual shielding also enables the cable to operate at much higher frequencies.
j. **Cat7a:** Cat7a is an upgrade to Cat7. It offers maximum data transfer of 10 Gbps at 100 m and 40 Gbps at 50 m. It also supports a maximum bandwidth of 1 gigahertz (GHz). This type of cable is well suited for 10 Gigabit Ethernet.
k. **Cat8:** Suitable for switch-to-switch communications in 25 Gbps and 40 Gbps networks, Cat8 offers a maximum bandwidth of 2 GHz. Wrapped in foil for shielding, this cable virtually eliminates crosstalk. But, because of this shielding, the cable can be quite rigid and, therefore, difficult to install in tight or small spaces. Cat8 can replace fiber in data centers for short connections.

✓ **Coaxial Cable:** Coaxial cable is the second form of commonly used wired media. Coaxial cabling has a single copper conductor at its center, and a plastic layer that provides insulation between the center conductor and a braided metal shield. The metal shield helps block any outside interference from fluorescent lights, motors, or other computers.

Coaxial cable provides good insulation and durability. This wire is best suited for long, one way connections between devices. Coaxial cable is less susceptible to interference than twisted pair cable. High quality coax cable supports a maximum length of 500m before signal loss is experienced.

Fiber Optic: Fiber optic cables are the fastest option for wired and wireless connections. These cables use pulses of light traveling at or near the speed of light for long distances inside small strands of translucent fibers. The translucent plastic or glass fibers form the core of the cable, and are encased in a plastic coating for cushioning. Around the cushion are Kevlar fibers that protect the cable from breaking. Beyond the Kevlar is an outer Teflon or PVC coating that contains the wire system.

Fiber optic cabling is not susceptible to electronic interference like traditional copper wired connections because data travels as light pulses. Fiber optic cables can run 145 km (90mi) without signal loss.

- **Logical media**

Logical media refers to the use of radio waves or other wireless technologies to connect devices in a network. It includes technologies such as Wi-Fi, Bluetooth, and cellular data networks.

- **802.11 Wireless Standards:**

The development of wireless computer communication is controlled and documented by the Institute of Electrical and Electronics Engineers (IEEE) 802.11 wireless standards. The 802.11 standard specifies an over-the-air interface between a wireless client and a base station, or between two wireless clients. This method of communication is known as Wireless Fidelity (Wi-Fi).

Multiple-Input and Multiple-Output (MIMO): Multiple-Input and Multiple-Output (MIMO) is a type of "smart antenna" technology implemented in the 802.11n wireless standard. MIMO uses multiple antennas on both the receiving end and the transmitting end of a connection to boost communication performance.

Bluetooth: Bluetooth allows for short ranged wireless networks to be established, and is used most often to establish networks between devices and a computer, or a similarly controlled device. Keyboards, mice, and joysticks can all have Bluetooth capability. Additionally, nearly all cell phones are Bluetooth capable for hands-free use of the device, or to sync the device to a computer. Most Bluetooth devices have a range of 10m, but the technology does allow for ranges up to 100m. Bluetooth operates in the 2.45 GHz band. Bluetooth 2.0 allows transmission speeds up to 2.1 Mbit/s. Bluetooth 3.0 supports speeds up to 24 Mbit/s

- **Cell Phone Internet/WiMax:** Cell Phones use the same protocols as computers when accessing a network, but the physical network they connect to is different. The main standard for cell phone network connections is the G standard, such as 3G or 4G. This refers to a standard set by the International Telecommunication Union, and is based on a minimum speed to transfer data between the phone and a cell phone tower. 3G has a base of 200kb/s, and 4G has a minimum speed of 100 Mb/s. Speeds up to approximately 1 Gb/s are possible.
- **Worldwide Interoperability for Microwave Access (WiMAX)** is a form of broadband internet, which operates over the same signals cell phones use. It's defined under IEEE protocol 802.16 and offers 40MB/s of data transfer. A pending version will offer up to 1GB/s of bandwidth. Using existing cell phone towers and additional hardware, WiMAX is being used in many metropolitan areas, with the intent of making it the first national broadband system in the US.

- **communications satellite**

A communications satellite is an artificial satellite that relays and amplifies radio telecommunication signals via a transponder; it creates a communication channel between a source transmitter and a receiver at different locations on Earth.

- **Data:** In computing, data is information that has been translated into a form that is efficient for movement or processing. Relative to today's computers and transmission media, data is information converted into binary digital form.
- **Protocols:** A network protocol is an established set of rules that determine how data is transmitted between different devices in the same network. Essentially, it allows connected devices to communicate with each other, regardless of any differences in their internal processes, structure or design. for example **TCP/IP** (Transmission Control Protocol/Internet Protocol), **HTTPS** (Secure Hypertext Transmission Protocol), SMTP (Simple Mail Transfer Protocol), and **DNS** (Domain Name System).
- **Devices:** Network devices, also known as networking hardware, are physical devices that allow hardware on a computer network to communicate and interact with one another. For example, Repeater, Hub, Bridge, Switch, Routers, Gateway, Brouter, and NIC, etc.

Practical Activity 1.3.2: Connecting network devices for a small network

Task:

1: Individually, perform the following tasks:
As an IT Technician, you are hired by KIKI company Ltd to draw/design, select, connect, and testing the network devices which will be used to create network.
2: Wear the PPE
3: List out the tools/Instrument, Material and equipment required in devices connection.
4: Referring to the list provided on step 2, select the right tools, materials, and equipment required in connecting devices.
5: Present your work to the trainer, workshop assistant or your classmate
6: Read the key reading 1.3.2.
7: Perform the task provided in application of learning 1.3

Key readings 1.3.2: Connecting network devices for a small network

- **Planning the Network**
  - ✓ **Number of Devices:** Determine how many computers, printers, servers, and other devices will be connected.
  - ✓ **Network Services:** Identify the need for services like file sharing, printing, email, and internet access.
  - ✓ **Budget:** Establish a budget for networking hardware and software.
- **Choose Network Topology**
  - ✓ **Star Topology:** Common for small offices; all devices connect to a central switch or hub.
  - ✓ **Hybrid Topology:** Combines star and other topologies if needed for scalability.
- **Select Network Equipment**
  - ✓ **Router:** Provides internet access and manages traffic between internal and external networks. Choose a router with adequate speed and features (e.g., firewall, DHCP).
  - ✓ **Switch:** Connects multiple devices within the office network. Choose a switch with enough ports for all devices and potential future expansion.
  - ✓ **Access Points:** Provide wireless connectivity. Choose based on coverage area and the number of wireless devices.
  - ✓ **Modem:** Provided by the ISP for internet connection, may be combined with the router in some devices.
  - ✓ **Cabling:** Ethernet cables (Cat5e or Cat6) for wired connections. Consider cable length and management.
  - ✓ **Network Interface Cards (NICs):** Ensure all devices have compatible NICs for network connectivity.

Setup Network Hardware

- ✓ **Physical Setup:** Plug the modem into the router's WAN port using an Ethernet cable.
- ✓ **Connect the Router to the Switch:** Use an Ethernet cable to connect the router's LAN port to the switch's uplink port.
- ✓ **Connect Devices to the Switch:** Plug Ethernet cables from the switch to each wired device (e.g., computers, printers).
- ✓ **Setup Access Points:** Connect the access points to the switch or router using Ethernet cables. Place them strategically for optimal coverage.

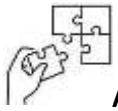
- **Power Up and Initial Configuration**
  - ✓ **Power On Devices:** Turn on the modem, router, switch, and all connected devices.

- ✓ **Configure the Router:** Access the router's admin interface via a web browser (usually http://192.168.1.1 or http://192.168.0.1).
  Set up WAN settings, configure DHCP, set up Wi-Fi SSID and password, and update firmware if necessary.
- ✓ **Configure the Switch:** Typically plug-and-play; configure only if it's a managed switch with advanced features.
- ✓ **Configure Access Points:**
  - Access the access points' admin interface (usually through their IP address).
  - Set up SSID, security settings (WPA2/WPA3), and connect them to the network.

- **Network Configuration**
  - ✓ **Assign IP Addresses**
    - **Dynamic IP Assignment:** Ensure the router's DHCP server is enabled to automatically assign IP addresses to devices.
    - **Static IP Addresses:** Assign static IP addresses to critical devices (e.g., servers, printers) for consistency.
- **Set Up Network Services**
  - ✓ **File Sharing and Printers:**
    - Configure file sharing on computers and set up network printers.
    - Ensure printers have static IP addresses if needed.
  - ✓ **Security Configuration:**
    - Enable firewall settings on the router.
    - Set up network security protocols for Wi-Fi (WPA2 or WPA3).
    - Consider network segmentation if needed (e.g., separate guest and internal networks).
- **Testing and Troubleshooting**
  - ✓ **Check Wired Connections:** Verify that all wired devices are connected and have network access.
  - ✓ **Check Wireless Connections**: Ensure all wireless devices can connect to the Wi-Fi network and access the internet.

Points to Remember

- Understanding the various network components such as router, switch, bridge, Repeater, Gateway, firewall, hub, WAP, modem, NICs is crucial for designing, implementing, and managing efficient and secure networks.
- Identifying network components involves to recognize their physical characteristics, port configurations, and LED indicators. And also to understand these components and their roles is crucial for setting up, managing, and troubleshooting network environments.
- Understanding the types, categories, and proper installation techniques of network cables ensures efficient data transmission and network reliability.
- Choosing the right cable type and managing it effectively can significantly impact network performance and scalability.



Application of learning 1.3.

BALOS Co. Ltd, situated in NYARUGENGE District, has established a network spanning three buildings. Unfortunately, technical issues and cable failures have emerged after 6 months of operation. As a network technical assistant, your responsibility is to address these challenges promptly and efficiently by:

1. Diagnosing the network media issues
2. Testing the network media to guarantee functionality
3. Replacing any damaged cables with new ones.

Indicative content 1.4: Classification of network devices

Duration: 4 hrs

Theoretical Activity 1.4.1: Describing network devices classification

Tasks:

1: Answer the following questions:

i. What are the primary categories used for classifying network devices, and how do they differ in terms of their functions and roles in a network?
ii. Define the concept of a modem, and explain its classification as a network device. In what situations would you use a modem in a network setup?
iii. Differentiate between an unmanaged and a managed network switch, highlighting the benefits of using managed switches in specific network environments.
iv. How do network bridges classify and connect separate network segments, and what are their applications in network design?
v. Explain the classification of network devices in the context of home networks, including the roles of routers, switches, and access points.
vi. Provide examples of hybrid devices that combine the functions of multiple network devices, and discuss the advantages and challenges of using such devices.
vii. How do network devices like network-attached storage (NAS) devices and print servers classify data and resources for efficient sharing in a network?

2: Present your findings to the whole class or one of your colleagues.

3: Read the Key readings 1.4.1 in this manual.

4: Ask to the trainer for clarifications if necessary.

Key readings 1.4.1.: Classification of network devices

- **Interconnection Devices**

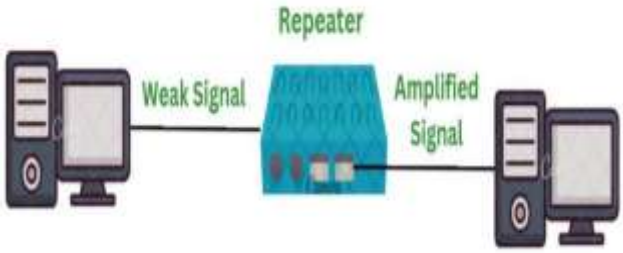
Interconnection devices are responsible for connecting different networks or network segments together. They facilitate the transmission of data between networks and ensure proper routing.

✓ **Repeater**

Repeaters are non-intelligent network devices that receive a signal through one port. They regenerate that signal and then transmit the signal again on all remaining ports. To extend the length of a network, repeaters can be used to connect network segments (a

portion of a computer network) but they can't be used to connect different networks using different access methods.

Repeaters reduce the loss of signal along a cable (known as attenuation) which in turn provides a more stable connection to the devices connected the repeater.



✓ **Bridge**

Unlike repeaters, a bridge can extend the capacity as well as the length of a network because each port on a bridge has a MAC address. They are used to connect two or more LANs of the same type, e.g. Ethernet to Ethernet. When activating a bridge on an Ethernet network, they automatically start to capture and Analyse addresses of incoming frames, building up a routing table and learning the topology of the network. Because bridges learn about the network, they are considered intelligent devices and can manage traffic, resulting in reduced bandwidth and a more efficient flow of data on a network.

✓ **Switch**

The switch has replaced a lot of hubs and bridges in Local Area Networks as it's considered a more intelligent device, improving network performance and reducing the chances of errors occurring on a network. A switch keeps a record of all MAC address connected to it so it can then identify which device is connected to which port. When a frame is received, it then looks at the destination MAC address and knows exactly which port to send the data on to. It doesn't just send the data out on all ports like a hub does. Switches also allocate full bandwidth to all ports so if a switch is 10/100Mbps, all ports are allocated 10/100Mbps speed. This is not the case with the hub where that bandwidth is shared across all ports. They can be used to link a number of end-user devices (e.g. workstations) or they can also interconnect multiple network segments.

Router If a network has a number of sub-networks (segments) that use different networking protocols and architectures, it requires a sophisticated device to manage the

data flow. This device is known as a router which determines how incoming packets get to destination networks in the most efficient way possible. Routers can communicate information about their network with routers on different networks and they store information in a routing table.

✓ **Routers**

Routers are located at the edge of networks (known as gateways) which is the point at which two or more networks connect. For example, your home router connects to your ISP. Your home router manages traffic and devices in your home while simultaneously talking to your ISP and ensuring data is sent and received efficiently.

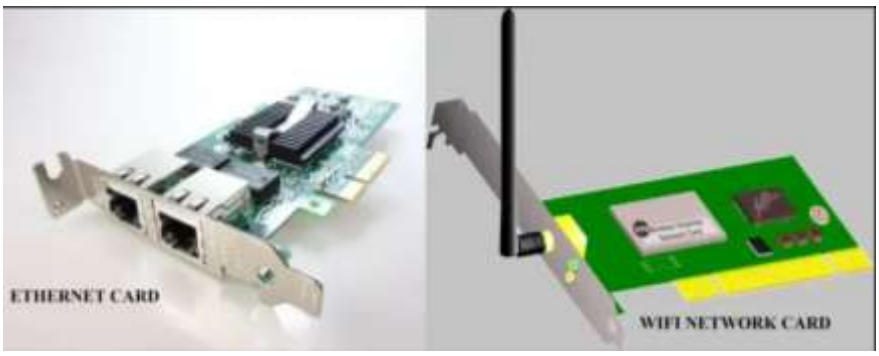
- **Access Devices**

Access Devices provide connectivity for end devices to access a network or network services. They serve as the entry point for users or devices to connect to a network. Examples of access devices include:

✓ **Network Interface Card (NIC)**

A NIC is also known as a network adapter. Any device that wants to communicate and send / receive data must have a NIC installed. They are usually located in a computer's

expansion slot, similar to how you'd see a graphics card or sound card installed. The NIC contains a transceiver which is a combination of a transmitter and receiver. This facilitates data transmission, enabling the device to send and receive data.



The NIC also contains a MAC address (also known as a hardware address) which is a unique, 48-bit identifier used by many networking protocols including Ethernet and 802.11 wireless. A MAC address looks something like this: 65:85:45: F2:C3:8E

- ✓ **Hub**

Hubs are used in Ethernet networks to connect multiple Ethernet devices together, forming a network segment (group of computers that is a portion of a network).

A hub, like a repeater has no intelligence so simply broadcasts all network data across all ports. However, most hubs can detect basic errors such as collision and because every computer connected to the hub has its own dedicated connection to the hub, this means that if there is a connection failure, it only affects a single device and not the entire hub and all of its associated connections / devices.

Hub

- ✓ **Access point**

An access point is a device that creates a wireless local area network, or WLAN, usually in an office or large building. An access point connects to a wired router, switch, or hub via an Ethernet cable, and projects a Wi-Fi signal to a designated area. For example, if you want to enable Wi-Fi access in your company's reception area but don't have a router within range, you can install an access point near the front desk and run an Ethernet cable through the ceiling back to the server room.

- **End Devices**

End devices are the devices at the edge of a network that generate, consume, or process network data. They are typically the final destination or source of data within a network. Some examples of end devices include:

- ✓ **Computers (Desktops, Laptops)**

Computers are the most common type of end devices. They generate and consume data within the network and can run various applications and services.

- ✓ **Mobile Devices (Smartphones, Tablets):**

Mobile devices connect to networks wirelessly and allow users to access network resources and applications on the go.

✓ **Printers**

Printers are end devices that provide printing services over the network. They can be connected directly to the network or through a print server.

Practical Activity 1.4.2: Perform connection of networking devices

Task:

1: Individually, referring to the previous activity 1.4.1, you are requested to go in the computer lab or workshop and select the right tools, materials, and equipment required in order to create a basic home network using a modem, router, computers, and configuring it for internet access and wireless connectivity.

2: Wear the PPE

3: List out the tools/Instrument, Material and equipment required to create a home network.

4: Referring to the list provided on step 2, select the right tools, materials, and equipment required to create a network.

5: Present your work to the trainer, workshop assistant or your classmate

6: Read the key reading 1.4.2.

7: Perform the task provided in application of learning 1.4

Key readings 1.4.2: Perform connection of networking devices

- **Router**
  - ✓ **Bandwidth usage:** Measures the amount of data transmitted and received by the router.
  - ✓ **Routing table:** Displays the entries that define the routes the router uses to forward packets.
  - ✓ **CPU and memory utilization:** Monitors the usage of the router's processing power and memory resources.
  - ✓ **Interface statistics:** Provides information about the traffic flowing through each router interface.
- **Switch**
  - ✓ **Port statistics:** Tracks the traffic and utilization of individual switch ports.
  - ✓ **VLAN information:** Shows the configured VLANs and associated ports.
  - ✓ **MAC address table:** Lists the MAC addresses learned by the switch and the corresponding switch port.
    - **Firewall**
  - ✓ **Traffic logs:** Records information about network traffic, including source and destination IP addresses, ports, and protocols.
  - ✓ **Rule statistics:** Shows the number of packets or connections matching specific firewall rules.
  - ✓ **Threat detection:** Alerts or reports on potential security threats, such as intrusion attempts or malware activity.
- **Access Point**
  - ✓ **Signal strength:** Measures the strength of the wireless signal in different areas.
  - ✓ **Client connections:** Provides details about the connected wireless clients, including signal quality and data rates.
  - ✓ **Channel utilization:** Monitors the occupancy and interference on different wireless channels.
- **Network Interface Card (NIC)**
  - ✓ **Link status:** Indicates whether the NIC is connected to the network or not.
  - ✓ **Link speed:** Displays the negotiated data transfer rate between the NIC and the network.
  - ✓ **Error statistics:** Tracks transmission errors, collisions, and other network-related issues.

- **Network Cable:** Although network cables themselves don't have key readings, certain cable testers can check for cable continuity, wiring faults, and signal quality.
- **Network Protocol:**
  - ✓ **Packet analysis:** In-depth inspection and analysis of network packets to understand protocol behavior and diagnose issues.
  - ✓ **Protocol-specific metrics:** Each protocol may have its own set of performance metrics and statistics, such as latency, retransmission rates, or error rates.
- **Network Hub:** Similar to network cables, hubs themselves don't have specific key readings, as they are passive devices that simply replicate incoming signals to all connected devices.

Points to Remember

- Understanding the classification of network devices helps in designing, implementing, and managing networks effectively. Each device plays a specific role, from facilitating communication and connectivity to ensuring security and optimizing performance. Familiarity with these components and their functions is essential for network professionals and anyone involved in network administration.
- Connecting networking devices involves setting up physical connections with appropriate cables and configuring each device according to network requirements. By following these steps, you can establish a functional and efficient network that meets your connectivity and performance needs.

Application of learning 1.4.

As a Network Technician, you are requested to set up a small network by connecting one router to one switch and three computers and make required configurations so that all computer users will have the ability to share information over a secured network.

Indicative content 1.5: Description of network models

Duration: 4 hrs

Theoretical Activity 1.5.1: Identify network models

Tasks:

1: Answer the following questions:

i. What is a network model, and why are they important in the field of networking?
ii. Explain the OSI (Open Systems Interconnection) model. What are the seven layers in the OSI model, and what is the primary function of each layer?
iii. Compare and contrast the OSI model and the TCP/IP model. What are the key differences and similarities between these two models?
iv. Why is it essential to have a layered approach in network models like OSI and TCP/IP? What are the advantages of this approach?
v. What is the purpose of the Physical layer in the OSI model? Provide examples of the types of devices and media associated with this layer.
vi. Describe the functions of the Transport layer in network models. What are the key protocols associated with this layer, and how do they ensure reliable data transfer?
vii. How does the Network layer handle routing and addressing in the OSI model? What is the role of IP (Internet Protocol) in this layer?
viii. What is the role of the Data Link layer in network models, and how does it manage data at the link level? Mention some common Data Link layer protocols.
ix. What are the four layers in the TCP/IP model, and how do they compare to the OSI model layers? Explain the main functions of each layer in the TCP/IP model.
x. Describe the role of the Application layer in network models. How does it handle user interactions and support various application-level protocols?

2: Present your findings to the whole class or one of your colleagues.

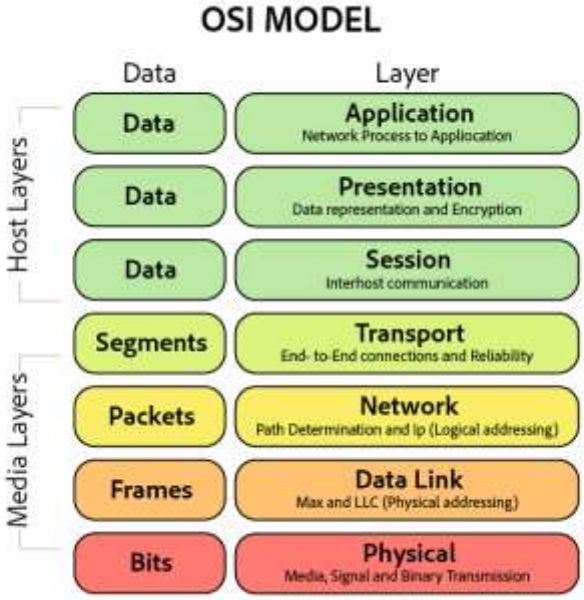
3: Read the Key readings 1.5.1 in this manual.

4: Ask to the trainer for clarifications if necessary.

Key readings 1.5.1. Description of network models :

- **Networking models:** describes the architecture, components, and design used to establish communication between the source and destination systems. Aliases for network models include protocol stacks, protocol suites, network stacks, and network protocols.

- **Types of network models** such as Open Systems Interconnection (OSI) Model and Transmission Control Protocol/Internet Protocol (TCP/IP) Model
  - ✓ **Open Systems Interconnection (OSI) Model:** The open systems interconnection (OSI) model is a conceptual model created by the International Organization for Standardization, which enables diverse communication systems to communicate using standard protocols. The Open Systems Interconnect (OSI) model is a conceptual framework that describes networking or telecommunications systems as seven layers, each with its own function. The seven abstraction layers of the OSI model can be defined as follows, from top to bottom:



The application layer

This is the only layer that directly interacts with data from the user. Software applications like web browsers and email clients rely on the application layer to initiate communications. But it should be made clear that client software applications are not part of the application layer; rather the application layer is responsible for the protocols and data manipulation that the software relies on to present meaningful data to the user. Application layer protocols include HTTP as well as SMTP (Simple Mail Transfer Protocol is one of the protocols that enables email communications).

The presentation layer

This layer is primarily responsible for preparing data so that it can be used by the application layer; in other words, layer 6 makes the data presentable for applications to consume. The presentation layer is responsible for translation, encryption, and compression of data.

Two communicating devices communicating may be using different encoding methods, so layer 6 is responsible for translating incoming data into a syntax that the application layer of the receiving device can understand

- **The session layer**

This is the layer responsible for opening and closing communication between the two devices. The time between when the communication is opened and closed is known as the session. The session layer ensures that the session stays open long enough to transfer all the data being exchanged, and then promptly closes the session in order to avoid wasting resources.

- **The transport layer**

Layer 4 is responsible for end-to-end communication between the two devices. This includes taking data from the session layer and breaking it up into chunks called segments before sending it to layer 3. The transport layer on the receiving device is responsible for reassembling the segments into data the session layer can consume.

- **The network layer**

The network layer is responsible for facilitating data transfer between two different networks. If the two devices communicating are on the same network, then the network layer is unnecessary. The network layer breaks up segments from the transport layer into smaller units, called packets, on the sender's device, and reassembles these packets on the receiving device. The network layer also finds the best physical path for the data to reach its destination; this is known as routing

- **The data link layer**

The data link layer is very similar to the network layer, except the data link layer facilitates data transfer between two devices on the *same* network. The data link layer takes packets from the network layer and breaks them into smaller pieces called frames. Like the network layer, the data link layer is also responsible for flow control and error control in intra-network communication (The transport layer only does flow control and error control for inter-network communications).

When obtaining data from the Physical layer, the Data Link layer checks for physical transmission errors and packages bits into data frames. The Data Link layer also manages physical addressing schemes such as MAC addresses for Ethernet networks, controlling access of network devices to the physical medium.

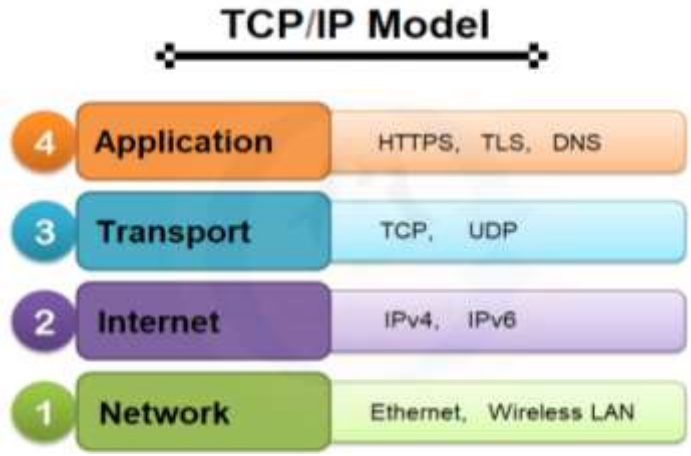
- **The physical layer**

This layer includes the physical equipment involved in the data transfer, such as the cables and switches. This is also the layer where the data gets converted into a bit stream, which is a string of 1s and 0s. The physical layer of both devices must also agree on a signal convention so that the 1s can be distinguished from the 0s on both devices.

At Layer 1, the Physical layer of the OSI model is responsible for the ultimate transmission of digital data bits from the Physical layer of the sending (source) device

over network communications media to the Physical layer of the receiving (destination) device.

- ✓ **Transmission Control Protocol/Internet Protocol (TCP/IP) Model**: The Transmission Control Protocol/Internet Protocol (TCP/IP) model is a conceptual framework that standardizes the functions of computer networking. It is a set of protocols that enable computers and devices to communicate and share data over networks, including the global internet. The TCP/IP model is the foundation for the internet and forms the basis for modern networking.



The TCP/IP model consists of four primary layers, which differ from the seven layers in the OSI model. These layers are as follows:

- **Network Interface Layer (Link Layer)**

This layer corresponds to the OSI model's Data Link and Physical layers. It deals with the physical connection to the network and includes network hardware such as network cards and switches. It also manages the addressing of devices on the local network.

- **Internet Layer**

Equivalent to the OSI model's Network layer, this layer is responsible for routing data between networks. It uses IP addresses to route packets to their destination across multiple networks.

- **Transport Layer**

Similar to the OSI model's Transport layer, this layer ensures end-to-end communication between devices. It includes protocols like TCP (Transmission Control Protocol) for reliable, connection-oriented communication, and UDP (User Datagram Protocol) for connectionless communication.

- **Application Layer**

Corresponding to the OSI model's Session, Presentation, and Application layers, the Application layer is the top layer of the TCP/IP model. It handles application-specific protocols and data exchange between software applications on different devices. Examples of application layer protocols include HTTP (Hypertext Transfer Protocol), SMTP (Simple Mail Transfer Protocol), and FTP (File Transfer Protocol).

Practical Activity 1.5.2: Implement network models

Task:

1: Individually, referring to the previous activity 1.5.1, you are requested to go in the computer lab or workshop and select the right tools, materials, and equipment required in order to design a Small Network Using OSI or TCP/IP Model and Connect a mobile device to the newly created network.
2: Wear the PPE
3: List out the tools/Instrument, Material and equipment required to create a home network.
4: Referring to the list provided on step 2, select the right tools, materials, and equipment required to create a network.
5: Present your work to the trainer, workshop assistant or your classmate
6: Read the key reading 1.5.2.
7: Perform the task provided in application of learning 1.5

Key readings 1.5.2

- **Layered Structure:** Network models are organized into layers, and each layer has a specific set of functions. Understanding the purpose of each layer and how they interact is crucial for effective network design and troubleshooting.
- **Protocols:** Be aware of the protocols associated with each layer of the model. Different protocols serve different purposes and are used for communication between devices.
- **Interoperability:** Devices on the network must support and be configured to work with the same network model. Ensuring interoperability is essential for consistent and reliable communication.
- **Data Encapsulation:** Data moves through the layers of the model with encapsulation and de-encapsulation. Understanding this process is vital for comprehending how data is prepared for transmission.
- **Network Troubleshooting:** When diagnosing network issues, the layered structure of network models can help pinpoint the location of the problem. Start troubleshooting at the relevant layer to narrow down the issue.
- **Scalability:** Consider the scalability of the network when designing it. The network model should be able to accommodate future growth and changes in requirements.
- **Security:** Implement security measures at various layers to protect the network. Consider firewalls, access controls, encryption, and other security mechanisms.

- **Standardization:** Network models help establish standardized practices and terminology, ensuring that network professionals worldwide can communicate effectively and work with common principles.
- **Adherence to Standards:** Ensure that network devices and configurations adhere to the standards associated with the network model you are using. This promotes consistency and compatibility.
- **Documentation:** Maintain detailed documentation of the network design, configurations, and changes made over time. This documentation is invaluable for troubleshooting and network management.
- **Performance Monitoring:** Implement network monitoring tools to assess the performance of your network. This helps identify issues, optimize performance, and plan for upgrades or expansions.
- **Troubleshooting Tools:** Familiarize yourself with network troubleshooting tools, such as ping, traceroute, and Wireshark, which can help diagnose network problems at various layers.

Points to Remember

- Understanding the OSI and TCP/IP models is essential for networking professionals as these models provide a structured approach to network design and troubleshooting. The OSI model is more comprehensive and theoretical, providing a detailed framework of functions. The TCP/IP model, while more streamlined and practical, is the backbone of the internet and most modern networks, emphasizing its protocols and their real-world implementation.
- Implementing network models involves understanding and configuring each layer's devices and protocols to ensure seamless communication and optimal performance. The OSI model provides a detailed framework, while the TCP/IP model offers a practical approach for real-world networking. Following the step-by-step guide helps in setting up and managing networks effectively.

Application of learning 1.5

You are a network technician tasked with designing and implementing a network for a tech start up. The company currently has 20 employees and anticipates growing to 100 employees over the next year. They need a network that can handle VoIP, video conferencing, cloud services, and secure data transfer.

Learning outcome 1 end assessment

Written assessment

Multiple Choice Questions

1. **What is the primary function of a router in a network?**
   - A) To connect multiple devices within a local network
   - B) To manage network traffic between different networks
   - C) To amplify the network signal
   - D) To provide wireless connectivity
2. **Which protocol is used to securely send emails over the internet?**
   - A) SMTP
   - B) IMAP
   - C) POP3
   - D) TLS
3. **What does the acronym LAN stand for?**
   - A) Local Area Network
   - B) Large Area Network
   - C) Limited Access Network
   - D) Long-range Area Network
4. **Which layer of the OSI model is responsible for routing and forwarding packets?**
   - A) Physical
   - B) Data Link
   - C) Network
   - D) Transport
5. **What type of cable is commonly used for Ethernet connections?**
   - A) Coaxial
   - B) Fiber Optic
   - C) Cat5e
   - D) HDMI
6. **Which device operates at the data link layer of the OSI model?**
   - A) Router
   - B) Switch
   - C) Hub
   - D) Modem
7. **In IP addressing, what does the subnet mask 255.255.255.0 indicate?**
   - A) All devices are on the same network
   - B) The network is divided into subnets
   - C) Only one device is on the network
   - D) The IP address range is for private networks

8. **Which wireless standard operates at 5 GHz frequency?**
    A) 802.11b
    B) 802.11g
    C) 802.11n
    D) 802.11ac
9. **What is the purpose of a firewall in a network?**
    A) To monitor network traffic
    B) To filter and control incoming and outgoing traffic
    C) To boost signal strength
    D) To store network data
10. **Which of the following is NOT a network topology?**
    A) Star
    B) Ring
    C) Mesh
    D) Grid
11. **Select the protocols that operate at the application layer of the OSI model:**
    A) HTTP
    B) FTP
    C) IP
    D) TCP
12. **Select the types of network devices that can act as a gateway:**
    A) Router
    B) Switch
    C) Firewall
    D) Hub
13. **Select the layers of the OSI model that handle data encryption:**
    A) Application
    B) Presentation
    C) Session
    D) Transport
14. **Select the types of cables that can be used for network connections:**
    A) Fiber Optic
    B) Coaxial
    C) HDMI
    D) Cat6

Matching Questions

16. **Match the following network devices with their primary functions:**
    A) Router
    B) Switch
    C) Modem
    D) Access Point

- Provides wireless connectivity
- Connects multiple networks and manages traffic between them
- Converts signals between digital and analog
- Connects devices within the same network

17. **Match the following OSI model layers with their functions:**

A) Physical
B) Data Link
C) Network
D) Transport

1. Provides error detection and correction
2. Handles end-to-end communication and error recovery
3. Defines the electrical and physical specifications of the network
4. Routes packets between different networks

18. **Match the following types of network cables with their characteristics:**

A) Cat5e
B) Cat6
C) Fiber Optic
D) Coaxial

1. Supports high-speed data transmission over long distances
2. Used for traditional cable TV and internet connections
3. Provides higher performance and bandwidth compared to Cat5e
4. Standard for Ethernet networks with speeds up to 1 Gbps

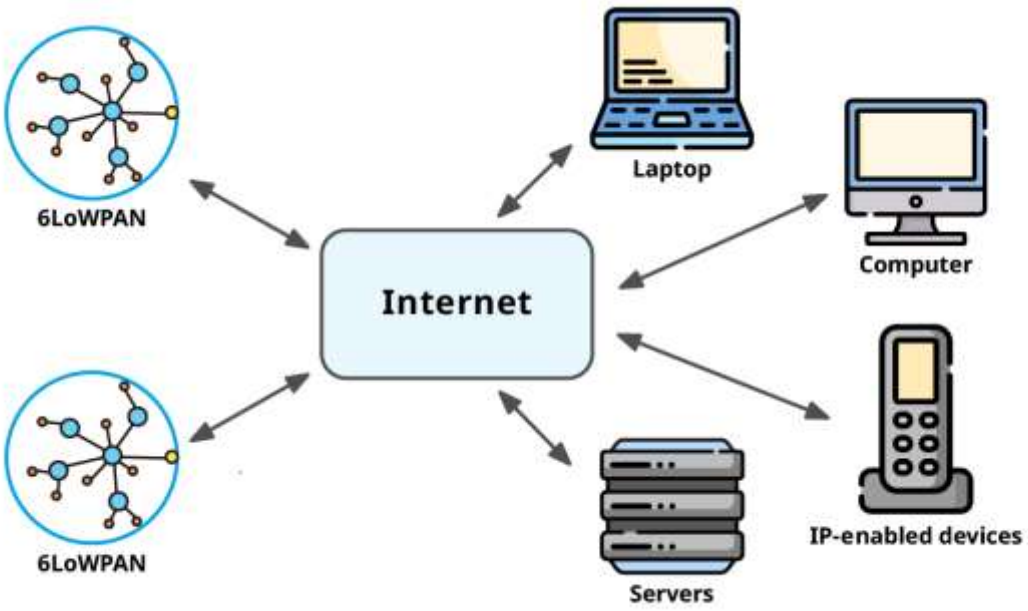
Practical assessment

As a Network Technical Assistance professional, you have been tasked with addressing the network connectivity problems at ABcd Co. Ltd, situated in NYABUGOGO, spanning across three buildings. Your responsibilities include:

1. Troubleshooting network issues
2. Replacing damaged network cables
3. Testing the integrity of network media"

References

A Top-Down Approach" by James F. Kurose and Keith W. Ross
CompTIA offers study guides for its Network+ certification
The Protocols" by W. Richard Stevens


6LoWPAN
6LoWPAN
Internet
Laptop
Computer
IP-enabled devices
Servers

Indicative contents

2.1. Description of Network Protocols

2.2. Identification of Network standards

2.3. Description of Network Media and Transmission

Key Competencies for Learning Outcome 2: Apply network protocols and communications

Knowledge	Skills	Attitudes
• Description of network protocols • Description of network standards • Description of computer networks protocols • Description of network media and transmission	• Analysing network topology diagram • Creating and maintaining network diagrams • Connecting network devices • Applying networking Standards • Configuring network and communication protocols • Implementing and managing network Services • Monitoring and Troubleshooting network tools	• Being Innovative • Having Creativity • Working in Teamwork • Being a Problem Solver • Having Patience • Having Critical thinking • Being Honesty • Being Passionate

Duration: 25 hrs

Learning outcome 2 objectives:

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

1. Describe correctly Protocols in line with network protocol models
2. Identify correctly Network models based on their standards
3. Describe network media types based on transmission technologies

Resources

Equipment	Tools	Materials
• Router • Hubs • Switch • Computer • Access points • Antenna • Gateways	• Simulation tools (Edraw max, cisco packet tracer, GNS 3)	• Internet bundles

Indicative content 2.1: Description of Network Protocols

Duration: 15 hrs

Theoretical Activity 2.1.1: Identification of network protocols

Tasks:

1: Read carefully and respond to the following questions

i. What is a network protocol?
ii. What are the most common network protocols models?
iii. Write in full words:
   a) TCP/IP
   b) OSI
   c) IPX
iv. What does NetBEUI stand for, and what is its primary use in networking?
v. Describe the OSI model and its seven layers. What is the purpose of each layer in the model?

2: Present your findings to the whole class or one of your colleagues

3: Read the Key readings 2.1.1 in this manual

4: Ask to the trainer for clarifications if necessary

Key readings 2.1.1.: Description of Network Protocols

- **A network protocol** is an established set of rules that determine how data is transmitted between different devices in the same network. Essentially, it allows connected devices to communicate with each other, regardless of any differences in their internal processes, structure or design.
- **NetBEUI** stands for NetBIOS Extended User Interface, is a networking protocol developed by IBM and Microsoft in 1985 that is used for workgroup-size local area networks (LANs) with up to 200 stations. NetBEUI is an extension of the NetBIOS protocol.
- **TCP/IP** stands for Transmission Control Protocol/Internet Protocol and is a suite of communication protocols used to interconnect network devices on the internet. TCP/IP is also used as a communications protocol in a private computer network (an intranet or extranet).
- **AppleTalk** is a communications network system interconnecting personal computer workstations, computers acting as file servers and print servers,

printers, and shared modems allowing them to exchange information through a variety of types of communications hardware and software.

- **Novell netware IPX/SPX** stands for **Internetwork Packet Exchange/Sequenced Packet Exchange**. IPX and SPX are networking protocols used initially on networks using the (since discontinued) Novell NetWare operating systems. They also became widely used on networks deploying Microsoft Windows LANS, as they replaced NetWare LANS, but are no longer widely used. IPX/SPX was also widely used prior to and up to Windows XP, which supported the protocols, while later Windows versions do not, and TCP/IP took over for networking.
- **The Open Systems Interconnection protocols** are a family of information exchange standards developed jointly by the ISO and the ITU-T. The standardization process began in 1977.
  While the seven-layer OSI model is often used as a reference for teaching and documentation, the protocols originally conceived for the model did not gain popularity, and only X.400, X.500, and IS-IS have achieved lasting impact. The goal of an open-standard protocol suite instead has been met by the Internet protocol suite, maintained by the Internet Engineering Task Force (IETF).
- **Cisco Discovery Protocol (CDP)** is a proprietary data link layer protocol developed by Cisco Systems in 1994 by Keith McCloghrie and Dino Farinacci. It is used to share information about other directly connected Cisco equipment, such as the operating system version and IP address.

Practical Activity 2.1.2: Apply network protocols

Task:

1: Individually, referring to the previous activity 2.1.2, you are requested to go in the computer lab or workshop and select the right tools, materials, and equipment required in order to do the following task:

The school has a computer lab with 10 computers connected to the Local Area Network and Internet. A trainer uses his/her computer to share a document and copy it in all computers but he/she does not have any storage devices to facilitate the task. What are the protocols required to be used in order to obtain the document in all computers to achieve the target and justify your answer?

2: Wear the PPE

3: List out the tools/Instrument, Material and equipment required

4: Referring to the list provided on step 2, select the right tools, materials, and equipment required

5: Present your work to the trainer, workshop assistant or your classmate

6: Read the key reading 2.1.2

7: Perform the task provided in application of learning 2.1

Key readings 2.1.2

- **IP Addressing protocols and Subnetting**: Plan your IP addressing scheme carefully to avoid IP conflicts and overlapping subnets. Ensure that each device has a unique IP address within the same subnet. Proper subnetting helps in organizing and efficiently using IP addresses.
  - ✓ **IPv4 Configuration:**
    - **Assign IP Addresses:** Configure static IP addresses or set up DHCP for automatic IP allocation.
    - **Default Gateway:** Configure the default gateway for routing traffic between subnets or to the internet.
    - **DNS Servers:** Set DNS servers to resolve domain names.
  - ✓ **IPv6 Configuration:**
    - **Assign IPv6 Addresses:** Use SLAAC or DHCPv6 for automatic address assignment.
    - **Subnetting:** Implement IPv6 prefixes and subnetting (e.g., /64).
    - **Default Gateway:** Configure IPv6 gateways for routing.
    - **DNS Servers:** Set IPv6 DNS servers.
- **Routing Protocols**
  - ✓ **Static Routing:** Manually configure routing tables on routers.
  - ✓ **Dynamic Routing Protocols:**
    - **RIP (Routing Information Protocol):** Configure RIP to dynamically share routing information between routers.
    - **OSPF (Open Shortest Path First):** Configure OSPF to dynamically route and manage large networks.
    - **EIGRP (Enhanced Interior Gateway Routing Protocol):** Configure EIGRP for efficient routing within an autonomous system.
- **Ethernet Protocols**
  - ✓ **Switching:** Configure Ethernet switches for VLANs, port security, and spanning tree protocol (STP).
  - ✓ **Speed and Duplex Settings:** Configure speed and duplex settings on Ethernet interfaces.
- **Application Layer Protocols**
  - ✓ **HTTP/HTTPS (Hypertext Transfer Protocol/Secure)**

- **Web Servers:** Configure web servers to serve content over HTTP or HTTPS.
- **SSL/TLS:** Set up SSL/TLS for secure HTTPS connections.

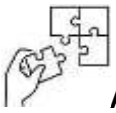
✓ **FTP/SFTP (File Transfer Protocol/Secure File Transfer Protocol)**

- **FTP Servers:** Set up FTP servers for file transfer.
- **SFTP:** Configure SFTP for secure file transfers.

- **Network Management Protocols**
  - ✓ **SNMP (Simple Network Management Protocol):** Enable SNMP on routers, switches, and other devices for monitoring and management.
  - ✓ **DHCP (Dynamic Host Configuration Protocol)**
    - **DHCP Server:** Set up DHCP servers to assign IP addresses and network configuration automatically.
    - **DHCP Relay:** Configure DHCP relay agents to forward DHCP requests between clients and servers.
- **Security Protocols**
  - ✓ **VPN (Virtual Private Network)**
  - ✓ **Access Control Lists (ACLs):** Define rules for allowing or denying traffic based on IP addresses, ports, and protocols.

Points to Remember

- Understanding their functions, classifications by OSI and TCP/IP models, key protocols, and considerations for their use is crucial for network design, implementation, and management.
- Applying network protocols involves configuring and using them to establish, manage, and secure network communications. Each protocol has specific functions and configurations, and their proper implementation is crucial for effective network operation.



Application of learning 2.1.

XCSX Company is a small business with 10 employees, and they recently set up a LAN to facilitate communication and collaboration among their staff. However, they are facing a network connectivity issue where two computers, belonging to employees in different departments, are unable to connect and have no reachability. This issue is hindering their ability to share files and collaborate effectively. You have been appointed as the IT Technician to diagnose and resolve this problem.

You need to apply the TCP/IP model and systematically diagnose and resolve the network connectivity issue between Computer A and Computer B, ensuring that they can communicate effectively. Your goal is to identify the root cause of the problem and take appropriate steps to enable reachability between the two computers.

Indicative content 2.2: Identification of Network standards

Duration: 10 hrs

Theoretical Activity 2.2.1: Identify network standards

Tasks:

1: Ask trainees to do the following:

i. Define network standard
ii. What are the importance of standards?
iii. Give and explain types of standards
iv. Explain the term “Internet standards”.
v. Write in full words:
   a) ISO
   b) IEEE
   c) ANSI
   d) ITU-Formally CCITT
   e) EIA
   f) Telcodia

2: Present your findings to the trainer, workshop assistant, your classmate or to the whole class.

3: Read the Key readings 2.2.1 in this manual

4: Ask to the trainer for clarifications if necessary

Key readings 2.2.1.: Identification of Network standards

- **Network standards** refer to the set of guidelines, protocols, and specifications that govern the design, implementation, and operation of computer networks. These standards define how data is transmitted, how devices communicate, and how networks are structured. Network standards ensure compatibility, interoperability, and reliability across different network devices and technologies.
- **Internet Standards:** Internet standards are a subset of network standards specifically focused on the protocols and technologies used for communication over the Internet. The Internet is a global network of networks, and its standards enable the seamless exchange of data and information across interconnected systems. Internet standards cover a wide range of areas, including addressing (IP addressing), routing (BGP), data transmission (TCP/IP), email (SMTP), web protocols (HTTP), and security (SSL/TLS).

- **Importance of standards**

Overall, standards provide a common language, framework, and set of rules that enable harmonization, interoperability, and progress in various industries. They benefit consumers, businesses, and society as a whole by fostering innovation, reliability, safety, and market access.

- **Types of standards**
  - ✓ **De Facto standards:** De facto standards are standards that emerge and become widely adopted without being formally developed or endorsed by a recognized standardization organization. They are often established through market dominance, industry practices, or widespread acceptance by users and stakeholders. Examples of De Facto Standards:
    - **Microsoft Windows**: The Windows operating system has become a de facto standard for personal computers due to its widespread use, market dominance, and compatibility with various applications and hardware.
    - **USB (Universal Serial Bus)**: USB has become a de facto standard for connecting peripheral devices to computers and other electronic devices. It gained popularity due to its ease of use, versatility, and wide support across multiple platforms.
    - **MP3**: The MP3 audio format emerged as a de facto standard for digital music compression and distribution. It gained widespread adoption due to its efficient file size, compatibility with portable devices, and early dominance in the digital music industry.
    - **Google Search**: Google's search engine has become a de facto standard for internet search due to its superior technology, accuracy, and market share. It has influenced user expectations and shaped the way information is discovered online.
    - **Wi-Fi:** The Wi-Fi wireless networking standard, based on the IEEE 802.11 family of protocols, has become a de facto standard for wireless local area networks (LANs). It is widely used for wireless internet access in homes, offices, and public spaces.
  - ✓ **De Jure standards:** De Jure standards are formal standards that are established and endorsed by recognized standardization organizations or regulatory bodies. These standards are developed through a structured and consensus-based process that involves technical experts, industry stakeholders, and public input. Here are some examples of de jure standards:
    - **ISO 9001:** ISO 9001 is a widely adopted de jure standard for quality management systems. It provides a framework for organizations to establish and maintain effective quality management practices and achieve customer satisfaction.

- **IEC 60335:** IEC 60335 is a de jure standard developed by the International Electro Technical Commission for the safety of household electrical appliances. It outlines safety requirements that manufacturers must comply with to ensure the safety of their products.
- **ANSI/IEEE 802.11:** The IEEE 802.11 standard, commonly known as Wi-Fi, is a de jure standard for wireless local area networks (LANs). It defines protocols and specifications for wireless communication, enabling interoperability and compatibility between different Wi-Fi devices.
- **GDPR (General Data Protection Regulation):** While not a traditional technical standard, GDPR is a de jure standard in the form of legislation. It sets out regulations and guidelines for the protection of personal data and privacy within the European Union.

- **Standards organizations**

There are several prominent standards organizations that play a significant role in the development and maintenance of standards across various industries. Here are some notable ones:

- ✓ **International Organization for Standardization (ISO)**: ISO is an independent, non-governmental international organization that develops and publishes international standards. It covers a wide range of sectors, including technology, manufacturing, healthcare, agriculture, and more. ISO standards provide specifications for products, services, and systems to ensure quality, safety, and efficiency.
- ✓ **International Electro Technical Commission (IEC):** The IEC is an international standards organization focused on electrical and electronic technologies. It develops and publishes standards related to electrical equipment, components, and systems. The IEC works in collaboration with ISO on joint standards and addresses areas such as energy efficiency, renewable energy, and smart grids.
- ✓ **International Telecommunication Union (ITU):** The ITU is a specialized agency of the United Nations responsible for telecommunications and information and communication technologies (ICTs). It develops standards and recommendations for global telecommunication networks, wireless technologies, satellite communications, and more. The ITU collaborates with industry stakeholders and regulators to promote interoperability and global connectivity.
- ✓ **Institute of Electrical and Electronics Engineers (IEEE):** IEEE is a professional association dedicated to advancing technology in various fields, including electrical engineering, electronics, telecommunications, and computing. It develops standards, publishes technical papers, and organizes conferences. The IEEE is known for its extensive portfolio of technology standards, such as Ethernet (IEEE 802.3) and Wi-Fi (IEEE 802.11).

- ✓ **American National Standards Institute (ANSI):** ANSI is a private, non-profit organization that oversees the development and adoption of standards in the United States. It facilitates the creation of consensus-based standards and represents the interests of various stakeholders, including industry, government, and consumers. ANSI accredited standards development organizations and promotes the use of standards in various sectors.
- ✓ **World Wide Web Consortium (W3C):** W3C is an international consortium that focuses on developing standards and guidelines for the World Wide Web. It addresses web technologies, including HTML, CSS, JavaScript, and web accessibility. W3C's standards help ensure interoperability and compatibility across different web platforms and devices.

Points to Remember

- Understanding the network standards helps to ensure reliable, secure, and efficient network operations, and also ensure compatibility and interoperability between different network devices and technologies. They cover various aspects of network design, implementation, and management, from physical cabling and wireless communication to protocol specifications and security measures.

Indicative content 2.3: Description of network media and transmission

Duration: 10 hrs

Theoretical Activity 2.3.1: Introduce network media and transmission

Tasks:

1: Read carefully and respond to the following questions

i. What is network media?
ii. Differentiate between wireless and wired transmission media
iii. What is baseband and broadband transmission technologies?
iv. Which type of network cable is commonly used to connect office computers to the local network?
   a) Coaxial cable
   b) Twisted-pair cable
   c) Glass fiber-optic cable
   d) Plastic fiber-optic cable

2: Present your work to the trainer, workshop assistant or your classmate

3: Read the Key readings 2.3.1 in this manual

4: Ask to the trainer for clarifications if necessary

Key readings 2.3.1.: Description of network media and transmission

- **Network media** refers to the physical or wireless communication channels and technologies used to transmit data between networked devices. It plays a crucial role in establishing connections and enabling data communication within a network.
- **Network media types:** refer to the physical transmission media used for transmitting data in a network. Here are some major network media types commonly used in networking:
  - ✓ **Twisted Pair Cable**
    - **Unshielded Twisted Pair (UTP):** UTP cables are widely used for Ethernet networks. They consist of pairs of twisted copper wires and come in different categories, such as Cat5e, Cat6, and Cat7, offering varying data transmission speeds and capabilities.
    - **Shielded Twisted Pair (STP):** STP cables have an additional shielding layer to reduce electromagnetic interference (EMI) and crosstalk. They are commonly used in environments with high interference levels.
  - ✓ **Coaxial Cable:** Coaxial cables consist of a central conductor, insulating layer, shielding, and an outer jacket. They are commonly used in cable television (CATV)

and broadband Internet connections. Coaxial cables provide high bandwidth and can transmit data over longer distances compared to twisted pair cables.

- ✓ **Fiber Optic Cable:** Fiber optic cables use optical fibers made of glass or plastic to transmit data as pulses of light. They offer high-speed, long-distance data transmission and are immune to electromagnetic interference. Fiber optic cables are commonly used in telecommunications, backbone networks, and high-speed internet connections.

- **Wireless Media:** refers to the transmission of data and communication signals over the airwaves, using wireless technologies that do not require physical cables to connect networked devices. This type of network media relies on the propagation of radio waves, microwaves, or infrared signals to facilitate communication between devices. Wireless media offers the advantage of flexibility, mobility, and the elimination of physical cable constraints. Here are some key aspects of wireless media
  - ✓ **Wireless Network Types**: There are various types of wireless networks, including:
    - **Wi-Fi (Wireless LAN):** Commonly used for local area networks (LANs), allowing devices like smartphones, laptops, and tablets to connect to the internet or a local network without physical cables.
    - **Cellular Networks:** Used for mobile communications and data transfer, enabling mobile phones to connect to the internet and make calls.
    - **Satellite Communication:** Involves the use of satellites in space to relay data and communication signals, providing global coverage.
    - **Bluetooth:** A short-range wireless technology for connecting devices like headphones, keyboards, and speakers to computers and smartphones.
    - **Infrared (IR):** Uses infrared light for short-range communication, often found in remote controls and some older data transfer technologies.
  - ✓ **Key Advantages**
    - **Mobility:** Wireless networks allow devices to connect and communicate while on the move.
    - **Flexibility:** Devices can be connected without the limitations of physical cables.
    - **Scalability:** Wireless networks are easily expandable, making them suitable for various environments.
    - **Accessibility:** Wireless access points can be placed in locations that are difficult to wire with physical cables.
  - ✓ **Challenges and Considerations**
    - **Interference:** Wireless signals can be susceptible to interference from other electronic devices, physical obstacles, and even environmental factors like weather.
    - **Security:** Wireless networks need strong security measures to protect against unauthorized access or data breaches.

- **Range:** The range of wireless networks can vary, with some technologies offering short-range connections and others providing long-range coverage.
- **Bandwidth:** The available bandwidth and data transfer speeds may vary depending on the wireless technology and its specifications.

✓ **Applications:** Wireless media is widely used in applications such as home and business Wi-Fi networks, cellular communication, wireless IoT (Internet of Things) devices, satellite communication for global coverage, and more.

- **Baseband and broadband:** Baseband and broadband are two different transmission technologies used in networking.

✓ **Baseband Transmission:** uses the entire bandwidth of a communication medium to transmit digital signals without modulation. In baseband transmission, the digital signals are directly transmitted over the medium without any frequency division or modulation techniques. Baseband transmission is commonly used in local area networks (LANs), such as Ethernet, where the entire bandwidth of the medium is dedicated to transmitting data. It is typically used for short-range communication and is suitable for transmitting digital signals directly over twisted pair cables, coaxial cables, or fiber optic cables.

✓ **Broadband Transmission:** divides the available bandwidth of a communication medium into multiple channels, allowing simultaneous transmission of multiple signals. In broadband transmission, analog or digital signals are modulated onto carrier frequencies within specific frequency ranges. Broadband transmission is commonly used in wide area networks (WANs) and internet connections where multiple signals, such as voice, data, and video, need to be transmitted simultaneously. **Examples** of broadband transmission technologies include cable modems, DSL (Digital Subscriber Line), and fiber optic networks.

✓ **Key Differences:**

- Baseband transmission uses the entire bandwidth of the medium for transmitting a single signal, while broadband transmission divides the bandwidth into multiple channels for simultaneous transmission of multiple signals. Baseband transmission is typically used for short-range communication, while broadband transmission is used for long-range communication.
- Baseband transmission is primarily used in LANs, while broadband transmission is used in WANs and internet connections.
- Baseband transmission is typically used for transmitting digital signals, while broadband transmission can accommodate both analog and digital signals.

- It's important to note that the distinction between baseband and broadband transmission is not always strict, as certain technologies may utilize a combination of both techniques depending on the specific application and requirements.

- **Wireless Transmission Techniques:** Wireless transmission techniques refer to the methods and technologies used to transmit data wirelessly without the need for physical cables. Here are some commonly used wireless transmission techniques:
  - ✓ **Radio Frequency (RF) Transmission:** RF transmission uses radio waves to transmit data wirelessly. It is widely used in wireless communication systems such as Wi-Fi, Bluetooth, and cellular networks. RF transmission operates within specific frequency bands allocated for wireless communication. Different frequency bands are used for various applications and services.
  - ✓ **Infrared (IR) Transmission:** Infrared transmission utilizes infrared light waves to transmit data wirelessly. It is commonly used for short-range communication, such as TV remote controls and infrared data transfer between devices. Infrared transmission requires a direct line of sight between the transmitter and receiver, as infrared signals do not pass through obstacles.
  - ✓ **Microwave Transmission:** Microwave transmission uses high-frequency microwave signals to transmit data wirelessly over long distances. It is commonly used in point-to-point communication links and satellite communication systems. Microwave transmission requires specialized equipment, such as microwave antennas, to transmit and receive signals.
  - ✓ **Satellite Communication:** Satellite communication involves the use of communication satellites in space to transmit data over large distances. Data is sent to and received from satellites using RF signals. Satellite communication enables global coverage and is used for various applications, including television broadcasting, internet connectivity, and long-distance communication.
  - ✓ **Near Field Communication (NFC):** NFC is a short-range wireless communication technology that enables data exchange between devices in close proximity (within a few centimeters). It is commonly used for contactless payments, mobile device pairing, and data transfer between smartphones and NFC-enabled devices.
  - ✓ **Ultrasonic Transmission:** Ultrasonic transmission uses high-frequency sound waves above the human audible range to transmit data wirelessly. It is used in applications such as proximity sensing, object tracking, and underwater communication.

Practical Activity 2.3.2: Apply network media and transmission

Task:

1: Individually, referring to the previous activity 2.3.2, you are requested to go in the computer lab or workshop and select the right tools, materials, and equipment required.
As an IT Operator, your task is to identify and select the appropriate network media and transmission techniques to connect the school's 10 computers to a Local Area Network (LAN) and the internet. This network will facilitate communication and document sharing among administrative staff, teaching staff, and students. Justify your choice of network media and transmission techniques.
2: Wear the PPE
3: List out the tools/Instrument, Material and equipment required
4: Referring to the list provided on step 2, select the right tools, materials, and equipment required
5: Present your work to the trainer, workshop assistant or your classmate
6: Read the key reading 2.3.2
7: Perform the task provided in application of learning 2.3

Key readings 2.3.1: Apply network media and transmission

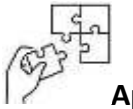
- **AM Demodulation:** Uses envelope detection to extract the original signal from the amplitude-modulated carrier.
- **Amplitude Modulation (AM):** Varies the amplitude of the carrier wave to encode information.
- **Analog Signals:** Continuous signals that vary smoothly over time. They can take any value within a range.
- **Balanced Transmission:** Twisted pairs maintain balanced transmission lines, which improves noise rejection and signal quality.
- **Bandwidth** defines the frequency range a cable can support, with higher categories offering higher bandwidth.
- **Cable Twisting:** Some cables have an overall twist to help with additional noise reduction.
- **Crimping Tool:** Used for attaching connectors to cables.

- **Crosstalk Reduction:** Helps prevent crosstalk between pairs of wires within the same cable, which can lead to signal degradation.
- **Demodulation**: The process of extracting the original information signal from the modulated carrier wave.
- **Digital Signals:** Discrete signals that take on specific values at distinct intervals. They represent data in binary form (0s and 1s).
- **Distance Limitations** refer to the maximum length over which a cable can transmit data effectively before signal degradation occurs. Fiber optics offer longer transmission distances compared to copper cables.
- **Distance:** Can transmit data over several kilometers with minimal signal loss. Ideal for long-distance connections.
- **FM Demodulation:** Uses frequency detection to extract the original signal from the frequency-modulated carrier.
- **Foiled Twisted Pair (FTP):** Includes a foil shield around each twisted pair but not around the entire cable. Offers moderate protection.
- **Frequency Modulation (FM):** Varies the frequency of the carrier wave to encode information.
- **Interference Protection:** Shielding protects against external electromagnetic interference (EMI) and radio frequency interference (RFI) that can degrade signal quality.
- **Light Transmission:** Uses a single light path (mode) for transmitting data, which minimizes modal dispersion.
- **Modulation:** Varies carrier signal properties to encode information; types include AM, FM, PM, and QAM.
- **Multi-Mode Fiber (MMF):** Ideal for shorter distances with moderate bandwidth requirements. It is commonly used in local area networks and data centers for intra-building connections.
- **Pair Twisting:** Each pair of wires is twisted together to reduce crosstalk within the pair.
- **Patch Panel:** Provides a central location for cable termination and management.
- **Performance:** Suitable for shorter-distance transmission with moderate bandwidth. **Single-Mode Fiber (SMF):** Best suited for long-distance communication with high bandwidth and minimal signal loss. It is typically used in telecommunications and long-haul data connections.
- **Phase Modulation (PM):** Varies the phase of the carrier wave to encode information.
- **PM Demodulation:** Uses phase detection to extract the original signal from the phase-modulated carrier.
- **Quadrature Amplitude Modulation (QAM):** Combines amplitude and phase modulation to increase data rate by varying both amplitude and phase.

- **Screened Twisted Pair (ScTP):** Combines shielding around each pair and an additional shield around all pairs, providing high protection.
- **Shielded Twisted Pair (STP):** Includes shielding around each pair of wires and/or the entire cable. Provides better protection against interference.
- **Shielding** protects against interference and crosstalk, with various types (UTP, STP, FTP, ScTP) offering different levels of protection.
- **Signal Degradation:** As distance increases, the signal strength degrades due to attenuation (loss of signal strength) and interference.
- **Signal Integrity:** Reduced signal degradation and attenuation compared to MMF.
- **Single-Mode Fiber (SMF):** Can transmit over several kilometers with minimal loss. Suitable for long-distance applications.
- **Speed:** The maximum data transfer rate a cable can handle, often measured in megabits per second (Mbps) or gigabits per second (Gbps).
- **Telecommunications:** Used for long-distance and high-speed data transmission in telecommunications networks.
- **Twisting** helps maintain signal integrity and reduce crosstalk by ensuring balanced transmission.
- **Unshielded Twisted Pair (UTP):** No additional shielding. Commonly used for general network applications.
- **Wavelengths:** Operates at wavelengths of 850 nm and sometimes 1300 nm.
- **Wireshark:** A popular network protocol analyzer that captures and analyzes packet data.

Points to Remember

- **Network media** encompasses the physical means of transmitting data, including twisted pair cables, coaxial cables, fiber optics, and wireless technologies. **Transmission technologies** define how data is transmitted over these media, including simplex, half-duplex, and full-duplex modes, as well as encoding, modulation, and error detection techniques. Understanding both network media and transmission technologies is crucial for designing, implementing, and managing effective and efficient network communication systems.
- Understanding the budget available for implementing the network. Choose cost-effective solutions that meet the network requirements without unnecessary expenditures.
- Ensure that the selected network media and transmission techniques are compatible with the existing hardware and software used in the network, including operating systems and network protocols.



Application of learning 2.3.

The school aims to create an efficient network to enable seamless communication and document sharing among various user groups, including administrative staff, teaching staff, and students. Your responsibilities are to:

a) Select the most appropriate network media and transmission techniques that align with the school's requirements.

b) Create a technical report that includes explanation of their benefits and limitations of chosen network media and transmission techniques.

Learning outcome 2 end assessment

Theoretical assessment

Choose the correct answer for the following questions stated:

1. Identify types of network media:

a) Fiber optic, Copper, Wireless
b) LAN, WAN, MAN
c) Router, Switch, Hub
d) TCP, UDP, IP

2. Differentiate Baseband and broadband transmission technologies:

a) Baseband uses multiple frequencies, while broadband uses a single frequency
b) Baseband transmits one signal at a time, broadband transmits multiple signals simultaneously
c) Baseband is used for long-distance transmission, broadband is for short-distance transmission
d) Baseband is wireless, while broadband is wired-only technology

3. Give the difference between physical transmission and logical transmission, and two examples of each:

a) Physical transmission deals with actual hardware components, while logical transmission deals with the software representation of data flow
b) Physical transmission refers to wireless media, while logical transmission refers to wired media
c) Physical transmission involves data compression, while logical transmission involves error correction
d) Physical transmission is secure, while logical transmission is insecure

4. Define network standard and internet standard:

a) Network standard is a model for user interfaces, while internet standard is a protocol for data storage
b) Network standard refers to rules that define network functions, while internet standard refers to protocols ensuring global interoperability on the internet
c) Network standard defines programming languages, while internet standard defines encryption methods
d) Network standard applies only to wireless devices, while internet standard applies only to wired devices

5. State the importance of standards:

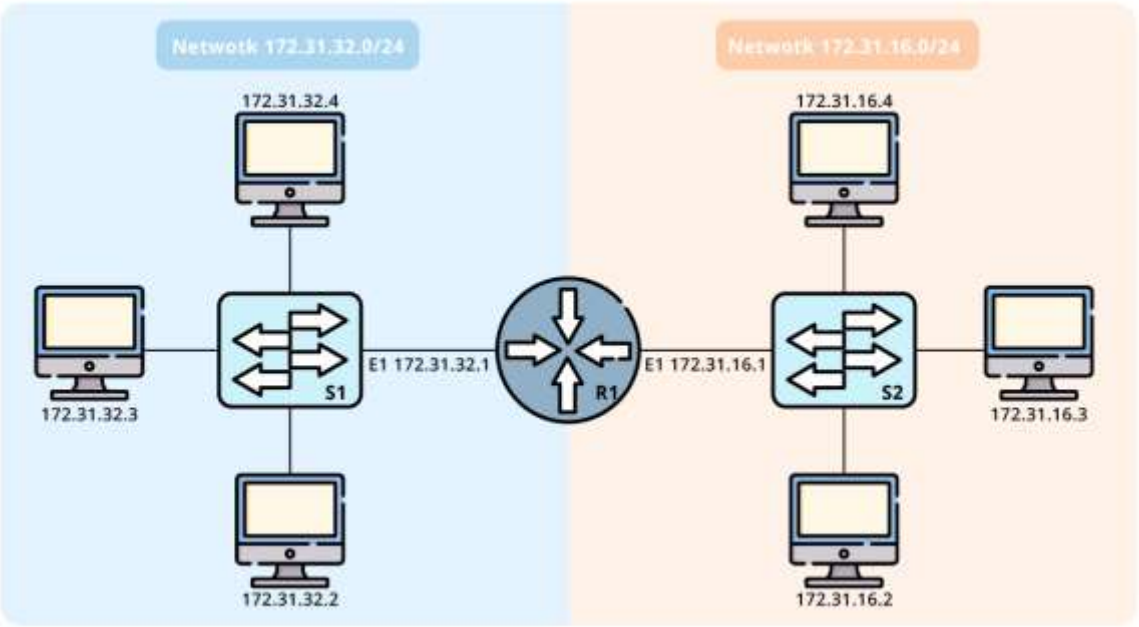
a) Standards help ensure that all devices on a network are from the same manufacturer
b) Standards allow for interoperability, compatibility, and better communication between different devices and networks
c) Standards ensure that only wireless networks can be used in an office environment
d) Standards allow for more efficient use of fiber optic cables over copper cables

Practical assessment

Joe, managing director of ABC hotel call a technician to repair a broken cable due to the sun light. While inspecting the site, he decides to make new cable. Explain all steps technician followed for making Ethernet cable

References

Computer Networks" by Andrew S. Tanenbaum and David J. Wetherall
TCP/IP Illustrated, Volume 1: The Protocols by W. Richard Stevens
Network Warrior by Gary A. Donahue
Wireshark Network Analysis: The Official Wireshark Certified Network Analyst Study Guide" by Laura Chappell and Gerald Combs
Network Programming with Go: Essential Skills for Using and Securing Networks by Jan Newmarch


Network 172.31.32.0/24
Network 172.31.16.0/24
172.31.32.4
172.31.16.4
172.31.32.3
S1
E1 172.31.32.1
R1
E1 172.31.16.1
S2
172.31.16.3
172.31.32.2
172.31.16.2

Indicative contents

3.1. Description of IP addressing concepts
3.2. Identification of IP Addresses types
3.3. Application of IPv4 concepts
3.4. Application of IPv6 concepts
3.5. Application of IP Configurations

Key Competencies for Learning Outcome 3: Apply IP addressing (IP v4&IPv6)

Knowledge	Skills	Attitudes
• Description IP Address • Identification of IP Address types • Description subnetting	• Calculating IP addresses • Summarizing IP Address • Assigning IP addresses • Subnetting network • Applying IP Configurations • Troubleshooting IP addresses • Diagnosing of network	• Being Innovative • Having Creativity • Working in Teamwork • Being Problem Solver • Being Patient • Being Critical thinker • Being Honesty • Having Passion

Duration: 35 hrs

Learning outcome 3 objectives:

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

1. Describe correctly IP address based on their classifications
2. Identify correctly IP address based on their types
3. Assign properly IP address based on their configuration types and versions
4. Configure efficiently IP address based on Application

Resources

Equipment	Tools	Materials
• Router • Hubs • Switch • Computer • Access points • Gateways	• Calculators • Simulation tools	• Internet cables

Indicative content 3.1: Description of IP addressing concepts

Duration: 10 hrs

Theoretical Activity 3.1.1: Introduction to IP addressing concepts

Tasks:

1: Read carefully and respond to the following questions

i. What is an IP address?
ii. What is the use of an IP address?
iii. Which version of IP is covered by this document?
iv. How does a host determine its IP address?
v. Is there any relation between the MAC address and IP address of a host?
vi. Can a single network interface have more than one IP address associated with it?
vii. What is the difference between a host name and an IP address?
viii. How a host name is resolved to the corresponding IP address?
ix. What is the size of an IP address?
x. How is an IP address represented?
xi. What are the components of an IP address?
xii. What is a network ID?
xiii. What is a host ID?

2: Present your findings to the whole class or one of your colleagues.

3: Read the Key readings 3.1.1 in this manuals.

4: Ask to the trainer for clarifications if necessary.

Key readings 3.1.1.: Description of IP addressing concepts

- **IP (Internet Protocol):** is the principal communications protocol in the Internet protocol suite for relaying datagrams across network boundaries. Its routing function enables internetworking, and essentially establishes the Internet. IP has the task of delivering packets from the source host to the destination host solely based on the IP addresses in the packet headers
- **IP addressing classification:** divided into further 5 Classes and each class has its use and property. These classes are Class **A** (0-127)**,** Class **B** (128-191), Class **C** (192-223)**,** Class **D** (224-239) and Class **E** (240-255)

✓ **CLASS A IP Address:** Class A is one of the five classes of IP addresses defined in the Internet Protocol version 4 (IPv4) addressing scheme. Class A IP addresses

are typically used to address large networks and offer a vast number of host addresses. Here are some key characteristics of Class A IP addresses:

- **Address Range:** Class A IP addresses have their first octet (the first 8 bits) reserved for the network identifier, and the remaining 24 bits for host addresses. The first octet of Class A addresses falls in the range 1.0.0.0 to 126.0.0.0.
- **Subnet Mask:** The default subnet mask for Class A addresses is 255.0.0.0, which means that the first octet is used to identify the network, and the remaining three octets can be used for host addresses.
- **Number of Networks:** Class A provides for a maximum of 128 networks, each with the potential to contain up to 16,777,214 host addresses. This makes Class A IP addresses suitable for very large organizations or internet service providers.
- **Usage:** Historically, Class A addresses were allocated to large corporations and institutions. However, due to their sheer size, they have become scarce, and Classless Inter-Domain Routing (CIDR) notation is often used to allocate smaller portions of Class A addresses to organizations.
- Examples:
  A typical Class A IP address might look like: 10.0.0.1
  Reserved Class A addresses include 10.0.0.0 (commonly used for private networks) and 127.0.0.0 (loopback address).

✓ **CLASS B IP Address:** is one of the five classes of IP addresses defined in the Internet Protocol version 4 (IPv4) addressing scheme. Class B IP addresses are typically used to address medium-sized networks and offer a substantial number of host addresses. Here are some key characteristics of Class B IP addresses:

- **Address Range:** Class B IP addresses have their first two octets (the first 16 bits) reserved for the network identifier, and the remaining 16 bits for host addresses. The first octet of Class B addresses falls in the range 128.0.0.0 to 191.255.0.0.
- **Subnet Mask:** The default subnet mask for Class B addresses is 255.255.0.0, which means that the first two octets are used to identify the network, and the remaining two octets can be used for host addresses.
- **Number of Networks:** Class B provides for a maximum of 16,384 networks, each with the potential to contain up to 65,534 host addresses. This makes Class B IP addresses suitable for medium-sized organizations and regional internet service providers.
- **Usage:** Class B addresses were historically allocated to organizations that required a moderate number of host addresses. They are more

common on the public internet than Class A addresses but are still relatively limited in number.

- **Examples:**
  - A typical Class B IP address might look like: 172.16.0.1
  - Reserved Class B addresses include 172.16.0.0 to 172.31.255.255, which are often used for private networks.

✓ **Class C IP Address**: Class C is one of the five classes of IP addresses defined in the Internet Protocol version 4 (IPv4) addressing scheme. Class C IP addresses are typically used for small to medium-sized networks and offer a moderate number of host addresses. Here are some key characteristics of Class C IP addresses:

- **Address Range:** Class C IP addresses have their first three octets (the first 24 bits) reserved for the network identifier, and the remaining 8 bits for host addresses. The first octet of Class C addresses falls in the range 192.0.0.0 to 223.255.255.0.
- **Subnet Mask:** The default subnet mask for Class C addresses is 255.255.255.0, which means that the first three octets are used to identify the network, and the last octet can be used for host addresses.
- **Number of Networks:** Class C provides for a maximum of 2,097,152 networks, each with the potential to contain up to 254 host addresses. This makes Class C IP addresses well-suited for small organizations and local networks.
- **Usage:** Class C addresses are widely used for local area networks (LANs), such as those in homes, small businesses, and educational institutions. They provide an adequate number of host addresses for most small-scale applications.
- **Examples:**
  - A typical Class C IP address might look like: 192.168.0.1
  - Reserved Class C addresses include 192.168.0.0 to 192.168.255.255, often used for private networks, and 224.0.0.0 to 223.255.255.255 for multicast and special purposes.

✓ **Class D IP Address:** Class D is one of the five classes of IP addresses defined in the Internet Protocol version 4 (IPv4) addressing scheme. Unlike Classes A, B, and C, Class D addresses are not used for traditional unicast communication (one-to-one); instead, they are specifically reserved for multicast purposes. Here are some key characteristics of Class D IP addresses:

- **Address Range:** Class D IP addresses are identified by an address range that falls within the first octet, specifically from 224.0.0.0 to 239.255.255.255.

- **Multicast Addresses:** Class D addresses are reserved for multicast groups. Multicast communication is a one-to-many or many-to-many communication method, where data is sent from one source to multiple recipients who have joined the same multicast group.
- **Usage:** Class D addresses are used for applications and services that involve broadcasting data to multiple recipients simultaneously, such as audio and video streaming, online gaming, and other real-time content delivery systems.
- **Examples:** Some well-known Class D multicast addresses include:
  - 224.0.0.1: All hosts on a local network.
  - 224.0.0.2: All multicast routers on a local network.
  - 239.255.255.255: Limited scope "all hosts" multicast group.

✓ **Reserved Addresses:** Some Class D addresses are reserved for specific purposes, and others may be used for various multicast applications. Network administrators are responsible for managing and configuring multicast groups.

✓ **TTL (Time to Live):** In multicast communication, each packet has a Time to Live (TTL) value, which specifies how many network hops it can traverse. This prevents packets from endlessly circulating in the network.

✓ **Class E IP Address**: Class E is one of the five classes of IP addresses defined in the Internet Protocol version 4 (IPv4) addressing scheme. Class E addresses are reserved for experimental and research purposes and are not intended for general use in standard networking. Here are some key characteristics of Class E IP addresses:

- **Address Range:** Class E IP addresses are identified by an address range that falls within the first octet, specifically from 240.0.0.0 to 255.255.255.255.
- **Reserved for Experimental Use:** Class E addresses are reserved by the Internet Assigned Numbers Authority (IANA) for experimental and research purposes. They are not allocated for routine network operations.
- **Usage:** Historically, Class E addresses were intended for experimental and future use cases that might require addressing beyond the existing classes (A, B, C, and D). However, they have seen limited practical application, and the majority of the address space is unused.
- **Examples:** Class E addresses, such as 255.255.255.255, are reserved and not typically used in contemporary networking. The class as a whole remains unallocated for general use.

- **Not Routable:** Class E addresses are not routable on the public internet, and they are not assigned to devices or hosts in typical network configurations.
- **Usage Evolution:** While Class E addresses were initially reserved for experimental purposes, their intended use has evolved over time. In practice, they are not widely used, and other IP address classes and schemes have proven sufficient for networking needs.

- **IP addresses grouping**: An IP address group is a collection of IP addresses that can use the same security group rules or network ACL rules. You can use an IP address group to manage IP addresses that have the same security requirements or whose security requirements change frequently. You can create an IP address group and add IP addresses that need to be managed in a unified manner to the group. Then, you can select this IP address group when configuring a security group rule. The rule will take effect for all IP addresses in the IP address group
- **IP addressing scheme**: IP address scheme is the requirement for communication in computer networks with an addressing scheme packets are forwarded from one location to another. They are types of Address scheme which are IP address and DNS.
  - ✓ **IP addressing subnet masks:** A subnet mask is a 32-bit number created by setting host bits to all 0s and setting network bits to all 1s. In this way, the subnet mask separates the IP address into the network and host addresses. The “255” address is always assigned to a broadcast address, and the “0” address is always assigned to a network address. Neither can be assigned to hosts, as they are reserved for these special purposes. You can determine the number and type of IP addresses any given local network requires based on its default subnet mask
    - Class A: 255.0.0.0
    - Class B: 255.255.0.0
    - Class C: 255.255.255.0
  - ✓ **The prefix length:** The prefix length is a fundamental concept in IP addressing, particularly in the context of Classless Inter-Domain Routing (CIDR) notation and subnetting. It is used to define the size of the network portion of an IP address and, indirectly, the number of available host addresses within that network. Here are some key points to remember about the prefix length:
    - **CIDR Notation:** The prefix length is commonly used in CIDR notation, which combines the IP address and the prefix length using a slash ("/") followed by the number. For example, "192.168.1.0/24" indicates an IP address with a network portion of 24 bits.
    - **Subnet Mask Equivalence:** The prefix length is equivalent to the subnet mask used to divide an IP address into its network and host portions. For

example, a prefix length of 24 is equivalent to a subnet mask of 255.255.255.0.

- ✓ **Range of Values:** The prefix length can vary, but it is typically represented in the range from 0 to 32 in IPv4 (since IPv4 addresses use 32 bits) and from 0 to 128 in IPv6 (as IPv6 addresses use 128 bits).
- **Number of Hosts:** The prefix length determines the number of available host addresses within a network. In IPv4, 2^(32 - prefix length) hosts are possible, and in IPv6, 2^(128 - prefix length) hosts can be accommodated.
- **Longer Prefixes and Subnetting:** Longer prefix lengths (smaller subnets) indicate more specific network segments, allowing for more subdivisions or subnetworks within an address space.
- **Shorter Prefixes and Larger Networks:** Shorter prefix lengths (larger subnets) encompass larger address spaces but offer fewer subdivisions for subnetworking.
- **Routing and Aggregation:** Prefix length plays a crucial role in routing. Shorter prefixes are preferred in routing tables as they allow for more efficient routing and aggregation of IP addresses.
- **Network Design:** Properly selecting the prefix length is essential for efficient network design. It should align with the specific requirements of a network, including the number of required hosts and the need for subnets.

Examples:

- Common prefix lengths include /24 (for a Class C-like subnet), /16 (for a Class B-like subnet), and /8 (for a Class A-like subnet) in IPv4.
- In IPv6, /64 is a frequently used prefix length for individual subnets

Points to Remember

- Understand the differences between public, private, and special IP addresses in both IPv4 and IPv6.
- Learn how to divide IP networks into subnets to optimize network performance and manageability.
- Utilize NAT to enable multiple devices to share a single public IP address and manage traffic between internal and external networks.
- Use IPAM tools to effectively manage and plan IP address spaces, ensuring smooth network operations and scalability.

Application of learning 3.1.

You are a network administrator tasked with setting up a new network for a medium-sized company that has recently moved into a new office space. The company needs a well-organized IP addressing scheme to ensure efficient network management, connectivity, and scalability. Your task is to design an IP Addressing Scheme.

Indicative content 3.2: Identification of IP Addresses types

Duration: 5 hrs

Theoretical Activity 3.2.1: Identification of IP addressing types

Tasks:

1: Answer the following questions:

i. What is IPv4, and what are the characteristics of IPv4 addressing?
ii. How does IPv6 differ from IPv4 in terms of addressing?
iii. What is a public IP address, and how is it different from a private IP address?
iv. What is a dynamic IP address?
v. What is a static IP address?
vi. What are reserved IP addresses, and why are they important in IP addressing?

2: Present your findings

3: Read the Key readings 3.2.1 in this manual.

4: Ask to the trainer for clarifications if necessary.

Key readings 3.2.1.: Identification of IP Addresses types

- **Private:** is a computer network that uses a private address space of IP addresses. These addresses are commonly used for local area networks in residential, office, and enterprise environments. Both the IPv4 and the IPv6 specifications define private IP address ranges**.** The organizations that distribute IP addresses to the world reserve a range of IP addresses for private networks as shown below:
  - ✓ 192.168.0.0 – 192.168.255.255 (65,536 IP addresses)
  - ✓ 172.16.0.0 – 172.31.255.255 (1,048,576 IP addresses)
  - ✓ 10.0.0.0 – 10.255.255.255 (16,777,216 IP addresses)
- **Public:** a public IP address is a unique IP address assigned to your network router by your internet service provider and can be accessed directly over the internet and Used for communicating outside your private network, over the internet, Assigned and controlled by your internet service provider. Example: 8.8.8.8**.** The public address range is any number not used in the private IP address, such as 8.8.8.8, whereas the private IP address range is
  - ✓ 10.0.0.0-10.255.255,
  - ✓ 172.16.0.0-172.31.255.255
  - ✓ 192.168.0.0-192.168.255.255

- **Shared IP addresses**
  - ✓ Shared IP addresses are those that are assigned to multiple devices or websites. This is common in shared hosting environments, where multiple websites share the same IP address.
  - ✓ Shared IP addresses are cost-effective but may have limitations when it comes to SSL/TLS certificates and some SEO considerations.
- **Dedicated IP Addresses**
  - ✓ Dedicated IP addresses are assigned exclusively to a single device or service. They are not shared with other devices or websites.
  - ✓ Dedicated IP addresses are often used for services that require secure connections, such as e-commerce websites that need their SSL/TLS certificates.
  - ✓ They provide more control and flexibility but may come at a higher cost.

Points to Remember

- Understanding IP address types and their characteristics helps in designing networks, configuring devices, and troubleshooting network issues.

Indicative content 3.3: Application of IPv4 concepts

Duration: 10 hrs

Theoretical Activity 3.3.1: Description of IPv4 concepts

Tasks:

1: Answer the following questions:

i. What is the purpose of an IP Address?
   a) A unique identifier for a computer
   b) A unique location identifier
   c) A network location identifier
   d) None of the above

ii. There are _____ bits in an octet?
   a) 8
   b) 5
   c) 4
   d) 9

iii. What does IPV4 stands for?

iv. Explain the format of an IPv4 address and the role of each part.

v. What is a subnet mask in IPv4, and how does it determine the network and host portions of an IP address?

vi. Explain the purpose of the loopback address (127.0.0.1) in IPv4.

2: Present your findings

3: Read the Key readings 3.3.1 in this manual.

4: Ask to the trainer for clarifications if necessary.

Key readings 3.3.1.: Application of IPv4 concepts

- **IPv4 (Internet Protocol version 4)** is a foundational protocol used for addressing and routing data packets across computer networks, including the internet. It uses 32-bit addresses to uniquely identify devices on a network.
- **Anatomy of IPv4 Address**
  - ✓ An IPv4 address consists of 32 bits divided into four 8-bit octets.
  - ✓ Each octet is represented in decimal notation (e.g., 192.168.0.1).
  - ✓ It is divided into two parts: the network portion and the host portion.
- **Methods of Assigning IP Addresses**
  - ✓ **Static:** IP addresses are manually configured, and they remain fixed.
  - ✓ **Dynamic:** IP addresses are assigned automatically by a DHCP server when a device joins the network.

- ✓ **Automatic:** A variation of dynamic addressing where devices self-assign an IP address within a specific range.

- **Calculation of IP Addresses**
  - ✓ **Binary to Decimal Conversion:** Converting binary IP addresses to decimal notation.
  - ✓ **Decimal to Binary Conversion:** Converting decimal IP addresses to binary notation.
  - ✓ **Summarization:** Aggregating IP address ranges into a single, more efficient address.
- **Subnetting**
  - ✓ **Fixed Length Subnet Masks (FLSM):** Subnetting with a consistent subnet mask across all subnets.
  - ✓ **Variable Length Subnet Masks (VLSM):** Subnetting with different subnet mask lengths for each subnet.
  - ✓ **Classless Inter-Domain Routing (CIDR) Notation:** A notation that represents IP address ranges with prefix lengths, allowing for flexible addressing.
- **IP Addresses Diagnostic Tools:** tools like Ping, Traceroute, and Ipconfig are used to diagnose network-related issues, check connectivity, and gather information about IP addresses.
- **IP Addressing Forms**
  - ✓ **Unicast:** One-to-one communication, where data is sent from one sender to one receiver.
  - ✓ **Broadcast:** One-to-all communication, where data is sent from one sender to all devices on the network.
  - ✓ **Multicast:** One-to-many communication, where data is sent from one sender to multiple specific recipients.
- **IP Address Translation:** IP address translation refers to techniques like Network Address Translation (NAT), which allow multiple devices within a private network to share a single public IP address when accessing the internet. NAT is used to conserve public IP addresses.

Practical Activity 3.3.2: Apply IPV4 concepts

Task:

1: Individually, you are requested to do the following activity:
The Speratha Co. Ltd wants to install a wired and wireless network in staff office. You have been tasked with configuring the IPv4 settings for the office network to ensure that all devices can communicate and access the internet. As a network administrator you are required to install and configure network devices so that all services will be delivered Quicky and easily. you also needed to set up a server and printer devices with static IP addresses for specific network services then Set the subnet mask, default gateway, and DNS server addresses.
2: Wear the PPE
3: List out the tools/Instrument, Material and equipment required to create a home network.
4: Referring to the list provided on step 2, select the right tools, materials, and equipment required to create a network.
5: Present your work to the trainer, workshop assistant or your classmate
6: Read the key reading 3.3.2.
7: Perform the task provided in application of learning 3.3.

Key readings 3.3.2

- **Format:** 32-bit address divided into four octets (8 bits each), represented in decimal format as four numbers separated by periods (e.g., 192.168.1.1).
- **Network Portion:** Identifies the specific network.
- **Host Portion:** Identifies the specific device within the network.
- **Address Classes**
  - ✓ **Class A:** 0.0.0.0 to 127.255.255.255 (Large networks, e.g., 10.0.0.0/8)
  - ✓ **Class B:** 128.0.0.0 to 191.255.255.255 (Medium-sized networks, e.g., 172.16.0.0/12)
  - ✓ **Class C:** 192.0.0.0 to 223.255.255.255 (Small networks, e.g., 192.168.0.0/16)
  - ✓ **Special Addresses:**
    - **Private Addresses:** Used within private networks (e.g., 10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16)
    - **Loopback Address**: 127.0.0.1 (used for testing)
    - **Broadcast Address:** Sends packets to all devices on the network (e.g., 255.255.255.255)
- **Subnetting:** Divides a large network into smaller subnetworks to improve organization and security.

- ✓ Subnet Mask: Defines the boundary between the network and host portions (e.g., 255.255.255.0).
- ✓ CIDR Notation: Compact notation for IP addresses and subnet masks (e.g., 192.168.1.0/24).

- **Configuring IPv4 Addresses**
  - ✓ **Static IP Addressing:** Manually assigning an IP address to a device.
  - ✓ **Dynamic IP Addressing**: Automatically assigning IP addresses using DHCP (Dynamic Host Configuration Protocol).

Points to Remember

- Manually configure the IP address or Static configuration on the device's network settings by ensuring that the IP address is within the correct subnet and does not conflict with other addresses.
- Use DHCP (Dynamic Host Configuration Protocol) to automatically assign IP addresses from a defined pool.
- Configure IP addresses on network interfaces to enable routing and network management.
- Determine the subnet mask based on the number of required subnets and hosts per subnet.
- Configure NAT rules on the router or firewall to translate private addresses to public addresses and vice versa.
- Employ IPAM software to monitor IP address allocation, detect conflicts, and plan subnetting strategies.
- Use tools like Ping, Traceroute, and Ipconfig to diagnose network-related issues, check connectivity, and gather information about IP addresses.

Application of learning 3.3.

XZ Company wants to hire someone involves on planning, selecting, installing, and configuring network devices to facilitate rapid and straightforward service delivery. Now you are hired to perform the following tasks:

a. Create a network plan that encompasses both wired and wireless connectivity.
b. Select suitable network devices, including routers, switches, access points, and network cables.
c. Physically install and set up network devices in strategically chosen locations throughout the office.

d. Establish the IPv4 configuration settings for both the wired and wireless network segments.
e. Assign a static IPv4 address to the server
f. Configure the appropriate subnet mask, default gateway, and DNS server addresses on the server.

Indicative content 3.4: Application of IPv6 concepts

Duration: 10 hrs

Theoretical Activity 3.4.1: Description of IPv6 concepts

Tasks:

1: Answer the following questions:

i. What is IPv6, and why was it developed as a successor to IPv4?
ii. Why is IPv6 designed with 128-bit addresses?
iii. What is the hexadecimal representation of an IPv6 address?
iv. Describe the main advantages of IPv6 over IPv4 in terms of address space, addressing efficiency, and security.
v. What is the structure of an IPv6 address, including the different components such as the network prefix and interface identifier?
vi. Describe the addressing types in IPv6, including unicast, multicast, and anycast.
vii. What are the IPv6 link-local and site-local addressing concepts, and when are they typically used?
viii. Discuss the challenges and considerations associated with the adoption of IPv6, both in terms of infrastructure and end-user devices.

2: Present your findings to the whole class or one of your colleagues.

3: Read the Key readings 3.4.1 in this manual.

Key readings 3.4.1.: Application of IPv6 concepts

- **Introduction to IPv6:** IPv6 (Internet Protocol version 6) is the successor to IPv4 and is designed to address the limitations of IPv4, such as the exhaustion of available IPv4 addresses.
- An IPv6 address is 128 bits long. It is most often presented as 32 hexadecimal characters. Each hexadecimal character is the equivalent of 4 bits (4 x 32 = 128). A non-abbreviated IPv6 host address is shown here: 2001:0DB8:0001:0000:0000:0000:0000:0001
- An IPv6 address is 8 hextets long, separated by colons. An IPv4 address is 4 octets and is commonly written or displayed in decimal notation. 255.255.255.255
- An IPv6 address is 8 hextets and is commonly written or displayed in hexadecimal notation. FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF
- In an IPv6 address, each individual hextet is 16 bits long. Eight hextets equals one 128-bit IPv6 address. 1111111111111111 = FFFF

1111111111111111.1111111111111111.1111111111111111.1111111111111111.
1111111111111111.1111111111111111.1111111111111111.1111111111111111 =FFFF:
FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF

If we read an IPv6 address starting from the left, the first (or far left) hextet identifies the IPv6 address type. For example, if the IPv6 address has all zeros in the far left hextet, then the address is possibly a loopback address.

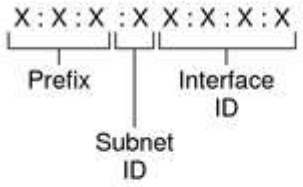
0000:0000:0000:0000:0000:0000:0000:0001 = loopback address

::1 = loopback address abbreviated

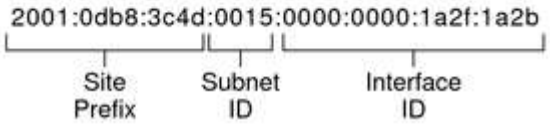
As another example, if the IPv6 address has FE80 in the first hextet, then the address is a link-local address. FE80:0000:0000:0000:C5B7:CB51:3C00:D6CE = link-local address

FE80::C5B7:CB51:3C00:D6CE = link-local address abbreviated

- **Migration from IPv4 to IPv6:** This involves transitioning from the use of IPv4 to IPv6 to ensure the continued growth of the internet. It includes dual-stack implementations, tunneling, and other techniques.
- **Anatomy of IPv6 Address:** an IPv6 address is 128 bits in length and consists of eight, 16-bit fields, with each field bounded by a colon. Each field must contain a hexadecimal number, in contrast to the dotted-decimal notation of IPv4 addresses.



Example:



The next field is the 16-bit subnet ID, which you (or another administrator) allocate for your site. The subnet ID describes the private topology, also known as the site topology, because it is internal to your site. The rightmost four fields (64 bits) contain the interface ID, also referred to as a token. The interface ID is either automatically configured from the interface's MAC address or manually configured in EUI-64 format.

- **Identification of Methods of Assigning IP Address:** IPv6 addresses can be assigned using different methods:
  - ✓ **Static:** Manually configuring IP addresses.
  - ✓ **Dynamic:** Using DHCPv6 to automatically assign addresses.
  - ✓ **Automatic:** Stateless address auto-configuration, where devices generate their addresses.

Calculation of IP Addresses

When we design a network, we always need to know how many addresses do we need in this network. Also, we would like to know the range of IP addresses in our network so that we can assign an address for each device in the network.

In this tutorial, we're going to show a simple method to find the range of IP addresses given a subnet mask.

- ✓ **Binary to decimal conversion:** Binary to decimal conversion is done to convert a number in a binary number system (base-2) to a number in a decimal number system (base-10). It is very necessary to understand the binary to decimal conversion for computer programming applications
- ✓ **Decimal to binary conversion:** A decimal number has base 10 and a binary number has base 2. In decimal to binary conversion, the base of the number also changes, i.e. from base 10 to base 2. All the decimal numbers have their equivalent binary numbers. These binary numbers are majorly used in computer applications, where it is used for programming or coding purposes.
- ✓ **Summarization:** means we advertise one summary route that represents multiple networks. Also known as route aggregation or supernetting. Saves CPU cycles, bandwidth and memory. Reduces the size of the routing table. Summarization has a number of advantages:
  - Summarization means we advertise one summary route that represents multiple networks.
  - Also known as route aggregation or supernetting.
  - Saves CPU cycles, bandwidth and memory.
  - Reduces the size of the routing table.
  - Prevents routing table instability
- **Subnetting:** IPv6 was designed to replace IPv4. The simple reason is that the IPv4 address space is running out. The world has reached the point where there are not enough 32-bit addresses to link every device which wants to connect to the Internet. IPv6 uses 128 bits. The subnet mask recommended for end host use in IPv6 is always a **/64**. This means that even if you have 200 devices on a single /64 network prefix, you still have 264-200 unused address spaces.

Practical Activity 3.4.2: Apply IPV6 concepts

Task:

1: Individually, perform the following activity

you work as a network operator for a medium-sized company that is transitioning from IPv4 to IPv6 due to the exhaustion of available IPv4 addresses. Your task is to configure IPv6 addresses on the company's local area network (LAN) to ensure that all devices can communicate using the new protocol.

2: Wear the PPE

2: List out the tools/Instrument, Material and equipment required to create a home network.

3: Referring to the list provided on step 2, select the right tools, materials, and equipment required to create a network.

4: Present your work to the trainer, workshop assistant or your classmate

5: Read the key reading 3.4.2.

6: Perform the task provided in application of learning 3.4

Key readings 3.4.2

- **Format:** 128-bit address represented in hexadecimal format, divided into eight 16-bit blocks, separated by colons (e.g., 2001:0db8:85a3:0000:0000:8a2e:0370:7334).
- **Simplification:** Leading zeros in each block can be omitted, and consecutive blocks of zeros can be replaced with:: (e.g., 2001:0db8::8a2e:0370:7334).
- **Static IPv6 Addressing**: Manually assigning an IPv6 address to a device.
  - ✓ **Configuration Steps:**
    - **Access Device Settings:** Navigate to the network settings of the device.
    - **Enter IPv6 Address:** Assign a unique IPv6 address within the network's range.
    - **Set Prefix Length:** Define the network prefix length (e.g., /64).
    - **Set Default Gateway:** Specify the gateway address to access other networks.
    - **Configure DNS Servers:** Enter the IPv6 addresses of DNS servers for name resolution.
- **Dynamic IPv6 Addressing:** Automatically assigning IPv6 addresses using Stateless Address auto configuration (SLAAC) or DHCPv6.
  - ✓ **SLAAC Configuration:**
    - **Enable SLAAC:** Devices automatically configure their IPv6 address based on router advertisements.

- **Router Advertisement:** Routers send advertisements containing network prefix information.

✓ **DHCPv6 Configuration:**

- **Enable DHCPv6:** Devices obtain IPv6 addresses and other configuration parameters from a DHCPv6 server.
- **Configure DHCPv6 Server:** Set up a DHCPv6 server to manage address allocation and provide additional settings.

- **Troubleshooting tools and commands**
  - ✓ **Ping:** Tests connectivity between devices using IPv6 (e.g., ping6 2001:db8::1 or ping -6 2001:db8::1).
  - ✓ **Traceroute/Tracert:** Maps the path packets take to a destination using IPv6 (e.g., traceroute6 google.com or tracert -6 google.com).
  - ✓ **IPConfig/IFConfig:** Displays IPv6 configuration information (e.g., ipconfig on Windows with IPv6, ifconfig on Unix/Linux with IPv6).
  - ✓ **Netstat:** Displays network connections and listening ports (e.g., netstat -an with IPv6 addresses).
- **Security Considerations**
  - ✓ **Implement IPv6 Security:** Apply security measures such as firewalls, access control lists (ACLs), and encryption.
  - ✓ **Monitor IPv6 Traffic:** Regularly monitor network traffic and address usage to detect and respond to security threats.
- **Transition from IPv4**
  - ✓ **Dual-Stack Deployment:** Run IPv4 and IPv6 simultaneously during the transition period to ensure compatibility and gradual migration.
  - ✓ **IPv6 Readiness:** Ensure applications, services, and network devices support IPv6 and are properly configured.

Points to Remember

- Familiarize yourself with the fundamentals of IPv6, including its address structure, notation, and key differences from IPv4.
- Assign fixed IP addresses to critical devices such as servers, network printers, and infrastructure devices.
- Manually configure IPv6 addresses on devices' network interfaces.
- Automatically assign IPv6 addresses to client devices like laptops and smartphones using DHCPv6 or Stateless Address Auto configuration (SLAAC) to assign IPv6 addresses.

- Configure NAT64 on a router to enable communication between an IPv6 network and an IPv4 server.
- Use IPAM tools to document and track IPv6 address allocations.
- Use network monitoring tools to identify and resolve connectivity issues

Application of learning 3.4.

The Head of the Department (HOD) at KTK University faced a recurring problem with the dynamic allocation of IP addresses for his computer. In his role, he required a stable and fixed IP address to ensure seamless access to network resources and services. To address this issue, he sought the assistance of IT technicians to configure his computer, leveraging the benefits of IPv6 for reliable and consistent IP address assignment.

Indicative content 3.5: Application of IP Configurations

Duration: 10 hrs

Theoretical Activity 3.5.1: Description of IP Configurations

Tasks:

1: Answer the following questions:

i. What is the purpose of IP configuration in a network?
ii. What are the two main versions of the Internet Protocol, and how do they differ in terms of IP configuration?
iii. Explain the difference between a static IP address and a dynamic IP address. When might you use one over the other?
iv. How do you configure a static IP address on a Windows computer?
v. What is DHCP, and how does it work in IP configuration? Explain the DHCP lease process.
vi. What is APIPA, and when does it come into play in IP configuration?
vii. Describe the role of a subnet mask in IP configuration. How does it affect IP address assignments?
viii. How can you troubleshoot network connectivity issues related to IP configuration?
ix. What is the purpose of the default gateway in IP configuration, and how do you set it up on a device?
x. How can you assign multiple IP addresses to a single network interface on a server? What is the use case for this configuration?
xi. What are DNS servers, and how do they relate to IP configuration? How can you configure DNS settings on a device?
xii. Explain the concept of IP address reservation in DHCP. Why might you reserve IP addresses on a network?
xiii. How can you configure a loopback IP address, and what is its purpose in IP configuration?
xiv. What is a public IP address, and how is it different from a private IP address? How are these used in network configuration?
xv. Describe the steps involved in setting up a virtual IP address or a VIP for load balancing and high availability in a network.
xvi. Explain the process of subnetting and provide an example of how it can be applied in IP configuration.
xvii. How does NAT (Network Address Translation) impact IP configuration in a network, especially in the context of IPv4 exhaustion?
xviii. Describe the difference between an IPv4 and an IPv6 address in terms of IP configuration. How do you configure IPv6 addresses on a device?

xix. What security measures should be taken into consideration when configuring IP addresses and network services on a device or a network?

2: Present your findings

3: Read the Key readings 3.5.1 in this manual.

Key readings 3.5.1.: Application of IP Configurations

- **Introduction to IPv6:** IPv6 (Internet Protocol version 6) is the successor to IPv4 and is designed to address the limitations of IPv4, such as the exhaustion of available IPv4 addresses.
  - ✓ An IPv6 address is 128 bits long. It is most often presented as 32 hexadecimal characters. Each hexadecimal character is the equivalent of 4 bits (4 x 32 = 128). A non-abbreviated IPv6 host address is shown here: 2001:0DB8:0001:0000:0000:0000:0000:0001
  - ✓ An IPv6 address is 8 hextets long, separated by colons. An IPv4 address is 4 octets and is commonly written or displayed in decimal notation. 255.255.255.255
  - ✓ An IPv6 address is 8 hextets and is commonly written or displayed in hexadecimal notation. FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF
  - ✓ In an IPv6 address, each individual hextet is 16 bits long. Eight hextets equals one 128-bit IPv6 address. 1111111111111111 = FFFF

1111111111111111.1111111111111111.1111111111111111.1111111111111111.
1111111111111111.1111111111111111.1111111111111111.1111111111111111
=FFFF: FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF

If we read an IPv6 address starting from the left, the first (or far left) hextet identifies the IPv6 address type. For example, if the IPv6 address has all zeros in the far left hextet, then the address is possibly a loopback address.

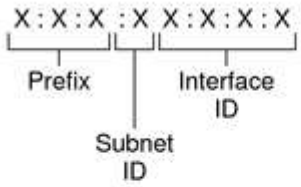
0000:0000:0000:0000:0000:0000:0000:0001 = loopback address

::1 = loopback address abbreviated

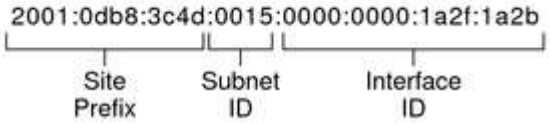
As another example, if the IPv6 address has FE80 in the first hextet, then the address is a link-local address. FE80:0000:0000:0000:C5B7:CB51:3C00:D6CE = link-local address

FE80::C5B7:CB51:3C00:D6CE = link-local address abbreviated

- **Migration from IPv4 to IPv6:** This involves transitioning from the use of IPv4 to IPv6 to ensure the continued growth of the internet. It includes dual-stack implementations, tunneling, and other techniques.
- **Anatomy of IPv6 Address:** an IPv6 address is 128 bits in length and consists of eight, 16-bit fields, with each field bounded by a colon. Each field must contain a hexadecimal number, in contrast to the dotted-decimal notation of IPv4 addresses.



Example:



The next field is the 16-bit subnet ID, which you (or another administrator) allocate for your site. The subnet ID describes the private topology, also known as the site topology, because it is internal to your site. The rightmost four fields (64 bits) contain the interface ID, also referred to as a token. The interface ID is either automatically configured from the interface's MAC address or manually configured in EUI-64 format.

- **Identification of Methods of Assigning IP Address:** IPv6 addresses can be assigned using different methods:
  - ✓ **Static:** Manually configuring IP addresses.
  - ✓ **Dynamic:** Using DHCPv6 to automatically assign addresses.
  - ✓ **Automatic:** Stateless address auto-configuration, where devices generate their addresses.
- **Calculation of IP Addresses**

When we design a network, we always need to know how many addresses do we need in this network. Also, we would like to know the range of IP addresses in our network so that we can assign an address for each device in the network.

In this tutorial, we're going to show a simple method to find the range of IP addresses given a subnet mask.

- ✓ **Binary to decimal conversion:** Binary to decimal conversion is done to convert a number in a binary number system (base-2) to a number in a decimal number system (base-10). It is very necessary to understand the binary to decimal conversion for computer programming applications
- ✓ **Decimal to binary conversion:** A decimal number has base 10 and a binary number has base 2. In decimal to binary conversion, the base of the number also changes, i.e. from base 10 to base 2. All the decimal numbers have their equivalent binary numbers. These binary numbers are majorly used in computer applications, where it is used for programming or coding purposes.
- ✓ **Summarization:** means we advertise one summary route that represents multiple networks. Also known as route aggregation or supernetting. Saves CPU cycles, bandwidth and memory. Reduces the size of the routing table. Summarization has a number of advantages:

- Summarization means we advertise one summary route that represents multiple networks.
- Also known as route aggregation or supernetting.
- Saves CPU cycles, bandwidth and memory.
- Reduces the size of the routing table.
- Prevents routing table instability

- **Subnetting:** IPv6 was designed to replace IPv4. The simple reason is that the IPv4 address space is running out. The world has reached the point where there are not enough 32-bit addresses to link every device which wants to connect to the Internet. IPv6 uses 128 bits. The subnet mask recommended for end host use in IPv6 is always a **/64**. This means that even if you have 200 devices on a single /64 network prefix, you still have 264-200 unused address spaces.

Practical Activity 3.42: Apply IPV6

Task:

1: Individually, perform the following activity
You work for a small technology start up called "TechWidgets Inc." The company has around 50 employees and a network infrastructure that currently relies on IPv4. Due to the increasing number of devices and a move towards more advanced applications and services, you've decided to transition to IPv6 to ensure long-term network scalability.
Your task is to plan and execute the migration from IPv4 to IPv6 for TechWidgets Inc.'s internal network. This involves configuring IPv6 for various network components, including routers, switches, and servers.
2: List out the tools/Instrument, Material and equipment required to create a home network.
3: Referring to the list provided on step 2, select the right tools, materials, and equipment required to create a network.
4: Present your work to the trainer, workshop assistant or your classmate
5: Read the key reading 3.5.2.
6: Perform the task provided in application of learning 3.5

Key readings 3.5.2: Apply IPV6

- **IPv6 Address Structure**
  - ✓ **128-bit Address:** Written in hexadecimal, separated by colons (e.g., 2001:0db8:85a3:0000:0000:8a2e:0370:7334).
  - ✓ **Address Simplification:** Leading zeros can be omitted, and consecutive blocks of zeros can be replaced with :: (e.g., 2001:0db8::8a2e:0370:7334).
- **IPv6 Address Types**
  - ✓ **Unicast:** Identifies a single network interface (e.g., Global Unicast, Link-Local).
  - ✓ **Multicast:** Sends packets to multiple interfaces in a group (e.g., Global Multicast).
  - ✓ **Anycast:** Delivered to the nearest interface among a group of potential receivers.
  - ✓ **Global Unicast Addresses:** Assigned by IANA and regional registries, routable on the global internet.
  - ✓ **Unique Local Addresses (ULAs):** Used within an organization, similar to private IPv4 addresses (e.g., fc00::/7)
- **Configuring IPv6 Addresses**
  - ✓ **Static IPv6 Addressing:** Manually assign IPv6 addresses and configure subnet prefix length, default gateway, and DNS servers.
  - ✓ **Dynamic IPv6 Addressing:**
    - **SLAAC:** Automatically configures addresses based on router advertisements.
    - **DHCPv6:** Obtains addresses and configuration parameters from a DHCPv6 server.
- **Troubleshooting IPv6 Issues:** Address conflicts, incorrect prefix length, misconfigured default gateway, DNS resolution problems.
- **Tools and Commands:**
  - ✓ **Ping6:** Test connectivity using IPv6 (e.g., ping6 2001:db8::1).
  - ✓ **Traceroute6:** Trace the path of packets using IPv6 (e.g., traceroute6 google.com).
  - ✓ **IPConfig/IFConfig:** Display IPv6 configuration information.
  - ✓ **Netstat:** Show network connections and listening ports with IPv6 addresses.
  - ✓ Best Practices
- **Address Planning:** Design and organize IPv6 addressing to avoid conflicts and ensure efficient use.
- **IPv6 Security:** Apply security measures such as firewalls, ACLs, and encryption.
- **Transition from IPv4:** Use dual-stack deployment during the transition and ensure IPv6 readiness for applications and services.

Points to Remember

- Choose an IP address that is within the appropriate subnet and not in conflict with other addresses.
- Create a detailed network diagram highlighting current IPv4 addressing and subnetting. And Identify key network segments and critical interconnections.
- Check if current network devices and server operating systems support IPv6. And Identify devices and software that require updates or replacements.
- Enable IPv6 routing and Configure interfaces to support both IPv4 and IPv6
- Enable IPv6 on switches (if applicable)
- Add IPv6 addresses to server network interfaces
- Ensure DNS servers are IPv6-compatible and running the latest software versions.
- Check IP addresses, subnet masks, gateways, and DNS settings.

Application of learning 3.5.

As a network administrator at TechWidgets Inc., you have been tasked with leading the transition to IPv6 and ensuring a seamless migration from IPv4 to IPv6. Here are the tasks you need to undertake to successfully carry out this critical project:

a) Conduct a comprehensive assessment of the current network infrastructure, including all network devices, services, and applications reliant on IPv4
b) Develop a detailed IPv6 address plan
c) Configure routers, switches, and servers to support both IPv4 and IPv6 simultaneously.
d) Configure network routers and switches to fully support IPv6, enabling IPv6 routing, and assign IPv6 addresses to their interfaces.
e) Update server operating systems to be IPv6-compatible
f) Set up and configure DNS servers to handle both IPv4 and IPv6 addresses

Learning outcome 3 end assessment

Theoretical assessment

Choose the correct answer from the following questions

1. What is the standard format of an IPv4 address, and what is its range of values?

   a. A 32-bit number, written as four decimal octets separated by dots; range: 0.0.0.0 to 255.255.255.255
   b. A 64-bit number, written as eight hexadecimal blocks separated by colons; range: 0::0 to ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff
   b) A 32-bit number, written as eight hexadecimal blocks separated by colons; range: 0.0.0.0 to 255.255.255.255
   c) A 128-bit number, written as four decimal octets separated by dots; range: 0.0.0.0 to 255.255.255.255

2. How do you configure a static IPv4 address on a Windows operating system?

   a) Open Network and Sharing Center, select the network, click Properties, select TCP/IPv4, and enter the IP address, subnet mask, and default gateway.
   b) Open Network and Internet settings, choose the network adapter, and use the IP Configuration tool to set the address.
   c) Open Command Prompt and use netsh commands to set the IP address.
   d) Open Device Manager, find the network adapter, and configure the IP address directly from the adapter properties.

3. What is DHCP, and how does it facilitate dynamic IPv4 address assignment?

   a) DHCP (Dynamic Host Configuration Protocol) assigns static IP addresses to devices manually.
   b) DHCP dynamically assigns IP addresses and other network configuration settings to devices from a pool of available addresses.
   c) DHCP is used to manually configure network addresses and does not support dynamic assignment.
   d) DHCP configures IP addresses through a command-line interface for each device individually.

4. Explain the purpose of subnet masks in IPv4 address configuration.

   a) Subnet masks determine the IP address range available for dynamic allocation.
   b) Subnet masks define the portion of the IP address used for the network and the portion used for hosts, facilitating the division of IP addresses into subnets.
   c) Subnet masks provide a means to encrypt IP addresses for security purposes.
   d) Subnet masks are used to configure the default gateway for devices on the network.

5. Describe the structure of an IPv6 address. How is it different from an IPv4 address?

a) IPv6 addresses are 128 bits long, written in hexadecimal and separated by colons; IPv4 addresses are 32 bits long, written in decimal and separated by dots.
b) IPv6 addresses are 32 bits long and use decimal notation; IPv4 addresses are 128 bits long and use hexadecimal notation.
c) IPv6 addresses are 64 bits long and use decimal notation; IPv4 addresses are 32 bits long and use hexadecimal notation.
d) IPv6 addresses are 128 bits long and use decimal notation; IPv4 addresses are 32 bits long and use hexadecimal notation.

6. What is the purpose of the Link-Local address in IPv6, and how is it automatically configured?

a) Link-Local addresses are used for communication between devices on the same local network segment and are automatically configured using SLAAC.
b) Link-Local addresses are used for communication over the internet and are manually assigned by network administrators.
c) Link-Local addresses are for global communication and are dynamically assigned by DHCP.
d) Link-Local addresses are used for secure communication across different networks and are assigned through IPsec.

7. What is Stateless Address Autoconfiguration (SLAAC), and how does it work in IPv6?

a) SLAAC allows devices to automatically generate their IPv6 addresses based on network prefixes and their own MAC addresses without needing a DHCP server.
b) SLAAC requires manual configuration of IP addresses on each device and does not use network prefixes.
c) SLAAC provides static IP addresses through DHCP for devices on the network.
d) SLAAC enables devices to configure their IPv6 addresses dynamically using a central configuration server.

8. Why might an organization choose to implement a dual-stack network configuration that supports both IPv4 and IPv6?

a) To ensure compatibility with legacy systems and applications while transitioning to IPv6.
b) To reduce the complexity of network management by using only IPv4.
c) To eliminate the need for network security measures.
d) To simplify addressing by using a single protocol.

9. Explain the process of configuring a network router for dual-stack operation, enabling IPv4 and IPv6 routing.

a) Enable IPv4 and IPv6 routing protocols, configure separate routing tables for IPv4 and IPv6, and ensure that both protocols are supported by the router.
b) Disable IPv4 routing, configure IPv6 addresses only, and use separate routers for IPv4 and IPv6.
c) Configure only IPv4 routing, use IPv6 addresses statically, and ignore routing protocols.

d) Enable NAT for IPv4 and disable it for IPv6 to support dual-stack operation.

10. In an IPv4 network, what is Network Address Translation (NAT), and how is it configured on a home router?

a) NAT allows multiple devices to share a single public IP address by mapping private IP addresses to a public address; it is configured through the router's web interface or management console.
b) NAT enables devices to have unique public IP addresses; it is configured through manual settings on each device.
c) NAT is used for encrypting data packets; it is configured through firewall settings.
d) NAT provides static IP addresses for devices on the network; it is configured via a central IP address management server.

11. Is NAT applicable in IPv6 networks? If not, what are the alternatives for providing network security and address conservation?

a) NAT is not applicable in IPv6 due to its large address space; alternatives include using IPsec for security and efficient address planning.
b) NAT is used in IPv6 to conserve address space; alternatives include manual address assignment and minimal use of security measures.
c) NAT is mandatory in IPv6 for address conservation; alternatives include disabling IPsec.
d) NAT is not required in IPv6; alternatives include using multiple NAT devices for security.

12. How do you secure an IPv4 network against unauthorized access and attacks, and what are common security measures?

a) Implement firewalls, use encryption (e.g., IPsec), configure access control lists (ACLs), and regularly update software and firmware.
b) Disable all security features, use only static IP addresses, and rely on physical security measures.
c) Use NAT for security, disable firewalls, and do not implement encryption.
d) Rely solely on user authentication and ignore network segmentation.

13. What are some unique security features or considerations specific to IPv6 networks?

a) IPv6 includes mandatory IPsec support for encryption and authentication, and the large address space reduces the need for NAT.
b) Pv6 relies solely on NAT for security and does not support encryption.
c) IPv6 addresses are less secure than IPv4 due to their length.
d) IPv6 requires manual configuration for security features, and IPsec is optional.

14. What are some of the transition mechanisms used to facilitate the coexistence of IPv4 and IPv6 during the migration phase?

a) Dual Stack, Tunneling (e.g., 6to4, Teredo), and Translation (e.g., NAT64, DNS64).
b) NAT for IPv4, Static Addressing for IPv6, and disabling IPv6 features.
c) Dual Stack and NAT only; no need for tunneling or translation.
d) Transition only through complete migration to IPv6 without IPv4 support.

Practical assessment

You are tasked with configuring IP addresses for IPv4 and IPv6 on a Windows computer and a network router. The goal is to demonstrate your ability to set up IP addresses for both versions correctly. You will configure a computer with a static IPv4 address and a Link-Local IPv6 address, and configure a router to route IPv4 and IPv6 traffic.

Requirements:

1. A Windows computer with IPv4 and IPv6 support.
2. A network router with IPv4 and IPv6 routing capabilities.
3. An Ethernet cable for connecting the computer to the router.

Tasks:

1. Configure the Windows computer with a static IPv4 address in the 192.168.1.0/24 subnet. Choose an appropriate IPv4 address, subnet mask, default gateway, and DNS server.
2. Configure the same Windows computer with a Link-Local IPv6 address. Use the "fe80::" prefix and the computer's MAC address to create the IPv6 address.
4. Set up DHCP for IPv4 on the router to provide dynamic addressing to other devices.
5. Configure the router with an IPv6 LAN interface.
6. Test connectivity from the computer to the router using both IPv4 and IPv6 addresses.
7. Verify that the computer can access the internet using both IPv4 and IPv6 connectivity.

References

7/e, P. P. (n.d.). *Signaling in ATM Networks.* Artech House.

Andrew S.Tanenbaum. (n.d.). *Computer Networks.*

Beyda, W. (2000). *Data Communications from Basics to Broadband* (3/e ed.). Prentice Hall.

Black, U. (1995). *ATM: Foundation for Broadband Networks.* Prentice Hall.

Comer, D. (2006). *Internetworking with TCP/IP* (5rd Edition ed., Vol. Volume I). Prentice Hall.

Comer, D. (2007). *Computer and Communication Networks.* Prentice Hall.

Comer, D. E. (n.d.). *Computer Networks and Internets.*

D. Bertsekas and R. Gallager. (1992). *Data Networks, 2nd Edition.* Prentice Hall.

RTB | RWANDA TVET BOARD

October, 2024