NETWORK FUNDAMENTAL

Course Description: This introductory level course will cover the fundamentals required to begin a career as a network engineer. Recognising network devices such as hubs, routers, switches, bridges, servers, transmission media, and related hardware falls under this category. This course will cover the fundamentals of installing and configuring various network devices. This course will teach students how to recognise and understand network topologies, as well as how to provide feedback on network requirements.

Goals:

- Demonstrate knowledge of network equipment such as hubs, routers, switches, bridges, servers, transmission media, and related devices.
- Set up and optimise network hubs, routers, and switches (for example, higher-level protocols and tunnelling).
- Knowledge of network equipment capabilities and applications, such as hubs, routers, switches, bridges, servers, transmission media, and related gear. Install and update network infrastructure device operating system software (for example, IOS and firmware).
- Ability to develop, implement, and test network infrastructure contingency and recovery plans.
- Provide input on network requirements, such as network architecture and infrastructure.

Contents:

Introduction :

Network fundamentals are the building blocks of modern communication infrastructures that enable the exchange of data, information, and resources among devices, computers, and servers. Networks are essential for connecting people, businesses, and organizations across the globe. Understanding network fundamentals is crucial for anyone interested in the world of information technology, as networks are at the core of modern computing.

What is a Network? A network is a collection of interconnected devices, such as computers, servers, routers, switches, and other hardware, designed to communicate with each other and share information. Networks can be local, connecting devices within a confined area like a home or office (Local Area Network - LAN), or they can be vast, spanning across cities, countries, or even the entire globe (Wide Area Network - WAN).

Types of Networks - There are several types of networks, including:

LAN (Local Area Network): A LAN connects devices within a limited geographical area, like a home, office, or campus. It allows for high-speed data transfer and resource sharing.

WAN (Wide Area Network): A WAN spans a larger geographical area and connects multiple LANs. The Internet itself is the most extensive example of a WAN, connecting networks worldwide.

MAN (Metropolitan Area Network): A MAN covers a larger area than a LAN but smaller than a WAN, typically serving a city or a metropolitan region.

WLAN (Wireless Local Area Network): A WLAN allows devices to connect to a LAN wirelessly using Wi-Fi technology.

VPN (Virtual Private Network): A VPN is a secure and encrypted private network that utilizes a public network (usually the Internet) to connect remote users or offices securely.

Network Topologies: Network topology refers to the arrangement of devices and connections in a network. Common topologies include:

Star Topology: All devices connect to a central hub or switch.

Bus Topology: Devices are connected in a linear fashion along a single cable.

Ring Topology: Devices are connected in a circular manner, forming a closed loop.

Mesh Topology: Devices are interconnected with multiple redundant paths, enhancing reliability.

Network Protocols: Network protocols are a set of rules and conventions that govern how data is transmitted and received across a network. They ensure compatibility and proper communication between devices. Examples of network protocols include TCP/IP (Transmission Control Protocol/Internet Protocol), HTTP (Hypertext Transfer Protocol), and DNS (Domain Name System).

OSI Model: The OSI (Open Systems Interconnection) model is a conceptual framework that standardizes the functions of a telecommunication or computing system into seven distinct layers. Each layer serves a specific purpose and collaborates with adjacent layers to facilitate communication between devices on a network.

Understanding these fundamental concepts is essential for troubleshooting network issues, designing efficient networks, and ensuring secure data transmission. As technology continues to advance, networks will play an increasingly vital role in our interconnected world, making network fundamentals a fundamental aspect of modern-say technology literacy.

- **Wireless Protocol :**

A network protocol is a set of rules that govern how data is delivered between different devices in the same network.

- It enables linked devices to communicate with one another independent of any obstacles.
- Differences in their internal procedures, structure, or design Network Protocols are the reason you can effortlessly communicate with individuals all across the world
- There are numerous wireless network technologies with variable network speeds:
  802.11b, 802.11g, 802.11a, 802.11n, 802.11ac
- IoT refers to the linking of computing devices embedded in objects over the internet.
- There are numerous types of IoT devices:
  Home automation, Smart lighting, Intelligent locks
- They have their own IoT protocols, such as: Bluetooth, ZigBee, and Z-Wave.
- These protocols normally transmit at significantly lower rates and ranges, but they accommodate a wide range of devices.
- As cellular protocols, cellular devices have their own protocols: 2G, 3G, 4G, and 5G

- **Network Devices:**

  - The Open System Interconnection Model (OSI Model)
    - It's a conceptual framework that helps describe the functions of a network.
    - It has seven layers that characterise and standardise communication across these distinct services.
  - Host layers are Application, Presentation, Session and Transport layer
  - Media layers are Network, Data link and Physical layers
  - Physical layer is where our cables and connection are situated
  - Data link layer provides the node-to-node data transfer (They are also in charge of error correction from the physical layer)
  - Routing occurs in the Network layer, where IP addresses are maintained.
    - There are various network devices such as Hubs, Switches, Router, Bridges, Servers,
  - Transmission Media and other related hardware
    - Network maps give us the visual layout of the network
  - Network Architecture is the design of a computer network
    - It is a framework for the specialization of a network's physical components and their functional organization and configuration
  - In Network protocols there are:
    - Internet Protocol such as Ipv4 and Ipv6
    - Wireless Protocols
    - Routing Protocols
  - Network topologies are the layouts of the connections between computer
    - Some examples are Star, Bus, Ring and Mesh
  - In Ring networks, computer is connected to a closed loop cable
    - No terminating ends'
    - Computer/devices function as repeaters
    - Tokens are required to send data
  - Devices on a bus network are commonly referred to as nodes
    - Nodes are connected to a single network cable
    - Each end of cable must be terminated
  - In Mesh networks, all devices are connected to each other, they are expensive networks with high redundancy
  - Star networks are most common type of Ethernet networks
    - All devices are to a central hub or switch

- **Hubs:**

  - ● Hub is connection point for devices in a network
    - Typically used to connect segments of a LAN
    - Usually contain at least four ports
  - Hub is represented as a single small 3D box with just one arrow
  - Setting up a Network Hub:
    - Plug in your network cables
    - Plug in the power ports
    - Turn on the power button

- **Switches:**

  - Switches are also known as bridges or network bridges
    - Operate at layer 2 of the OSI model

- Can be of two types: Managed vs. Unmanaged
- Its uses frames instead of packets
- Has an ability to connect many devices to a single LAN
- It contains MAC addresses table

➢ Switch is represented as a single small 3D box with four arrows
- Two pointing left and two pointing right

➢ Most hubs are unmanaged although Switches are typically managed
➢ Setting up an unmanaged switch is just like setting up a hub
➢ For a managed switch, we need to configure it.

▪ **Routers:**

➢ Router operates at level three of the OSI Model
- It can forward and drop packets
- It can also provide some wireless capabilities as well

➢ Routers can learn routes in two different ways statically and dynamically
➢ In static router, network engineer has input directly into the router
➢ Dynamic Router uses some sort of routing protocols
➢ Router has 4 arrows, two pointing in and other two pointing out
➢ Cisco Router has different rack like structure
➢ Design of different routers have different structures based on their purpose of installing
➢ Routers handle packets in between networks while switches handle inter networking that
➢ is basically on the same network
➢ Setting up a Router:
- Plug in deice and power on
- Enter enable mode as en
- Set up configuration: Open ports, set hostname, set DHCP services, etc
- Plug in Ethernet connections

▪ **Servers:**

➢ Server is a program or device that provides a service
➢ There are many types of servers:
- File servers
- Print servers
- Web servers
- Email servers

➢ Server is represented as a tower-like computer having its label underneath.
➢ Servers can be of different shapes and sizes.
- We can have a server on a small Raspberry Pi.

➢ Server setup are of two types tower servers and rack mounted servers
➢ For tower servers:
- Plug in power, networking cable, monitor, mouse, and keyboard
- Power up
- Configure based on needs

➢ For rack mounted servers:
- Rack server in rack
- Plug in networking cable, power and if the Datacenter/ rack uses it, crash cart or built-in cables
- Configure based on needs

▪ **Transmission Media**

➢ It is the channel that carries the information from receiver to the sender
➢ There are different types of transmission media:

- Ethernet (twisted pair)
- Coaxial
- Optical (Fiber)

- The main form of transmission media that is widely used is twisted pair Ethernet:
  - There are further two types of Ethernet cables: Shielded twisted pair (STP) and Unshielded twisted pair (UTP)
  - Straight through cables are used of connect computing devices to hub, switches or routers.
  - Crossover cables are used to connect computing devices directly to each other
- STP vs UTP
  - STP has an outside layer or shield of conductive material around the internal conductors, which needs to be grounded to cancel the effect of electromagnetic interference.
  - That results in faster transfer speeds and fewer data errors.
  - Whereas unshielded means no additional shield is used like meshes or aluminium foil is used.
  - UTP is cheaper and lighter than STP
  - UTP provided much less protection than STP
- There are many types of servers:
  - File servers
- Two main types of connectors are: RJ45 and RJ11
- Coaxial Cables:
  - Single copper conductor
  - Highly resistant to single interference
  - Thick and thin
  - Bayonet-Neill-Concelman Connectors
- Optical (Fiber):
  - Uses light to transmit data
  - Little to no interference
  - Extremely fast
  - Expensive and fragile
  - Single and multi-mode
- There are many categories in twisted pair connectors and fiber connectors as well

Maintaining Network Devices: Software and Firmware

- Inventory
  - Know what you have
  - Network maps
  - Keep it up to date
- Change control plan
  - Set up patching schedules
- Steps for change control are:
  Request for change
  Impact analysis
  Approve/Deny
  Implement change
  Review/Reporting
- Patching is the set of changes to a computer program or network device designed to update, fix or improve it.
  - This can include fixing vulnerabilities or other bugs or improving the functionality, usability or performance of the device
  - Patches are extremely important to keep all the devices running smooth and securely
- Compliance
  - Ensure all compliance requirements/standards for your organization

- Monitoring the health/status
  - Live monitoring of all network devices
  - Check dependencies
  - Set up alerts
- One of the best ways to manage your network is SNMP
  - Simple Network Management Protocol
  - Used to manage and monitor network devices
  - Part of TCP/IP suite of protocols
- Components of SNMP:
  - SNMP manager
  - Managed devices
  - SNMP agents
  - MIB
- Watching Traffic
  - Trust but verify
  - Keep an eye on the traffic of different areas of the network
  - Know normal things about the network, it is what you see in your baseline and in the terminal what is going on

- **Network Contingency and Recover**

- Contingency is something that could happen depending on other occurrences
- It is be easy to follow, it should not be too complex or complicated
- Every contingency plan should answer three questions:
  - What could happen?
  - What to do in case it happens?
  - What can you do to prevent it from happening?
- Configuration Backups and Restorations:
  - Enter enable mode
  - Copy the configuration from your network device to your servers
  - Restore the configuration from server to network device

Glossary in Network Fundamentals	
Bridges	A network bridge is a computer networking device that creates a single aggregate network from multiple communication networks or network segments.
Bus Network	A bus network is an arrangement in a local area network (LAN) in which each node (workstation or other device) is connected to a main cable or link called the bus.
Cellular network	A cellular network or mobile network is a communication network where the last link is wireless.
CLI	A command-line interface (CLI) processes commands to a computer program in the form of lines of text.

Coaxial Cable	Coaxial cable, or coax is a type of electrical cable consisting of an inner conductor surrounded by a concentric conducting shield, with the two separated by a dielectric; many coaxial cables also have a protective outer sheath or jacket.
Datacenter	A data center, or data centre, is a building, dedicated space within a building, or a group of buildings used to house computer systems and associated components, such as telecommunications and storage systems.
DHCP	The Dynamic Host Configuration Protocol is a network management protocol used on Internet Protocol networks whereby a DHCP server dynamically assigns an IP address and other network configuration parameters to each device on a network so they can communicate with other IP networks.
Ethernet	Ethernet is a family of computer networking technologies commonly used in local area networks, metropolitan area networks and wide area networks.
Fiber Optic	Fiber-optic communication is a method of transmitting information from one place to another by sending pulses of infrared light through an optical fiber.
GTM	Guided transmission media are cables like twisted pair cables, coaxial cables, and fiber optic cables.
Hubs	A hub, also called a network hub, is a common connection point for devices in a network.
Infrastructure	Network infrastructure is the hardware and software resources of an entire network that enable network connectivity, communication, operations and management of an enterprise network.
IoT	The Internet of things (IoT) is a system of interrelated computing devices, mechanical and digital machines provided with unique identifiers (UIDs) and the ability to transfer data over a network without requiring human-to-human or human-to-computer interaction.
IP	An Internet Protocol address is a numerical label assigned to each device connected to a computer network that uses the Internet Protocol for communication.
IPv4	Internet Protocol version 4 (IPv4) is the fourth version of the Internet Protocol (IP). It is one of the core protocols of standards-based internetworking methods in the Internet and other packet-switched networks.
IPv6	Internet Protocol version 6 (IPv6) is the most recent version of the Internet Protocol (IP), the communications protocol that provides an identification and location system for computers on networks and routes traffic across the Internet.
LAN	A local area network (LAN) is a computer network that interconnects computers within a limited area.
MAC address	A Media Access Control address (MAC) is a unique identifier assigned to a network interface controller for use as a network address in communications within a network segment.
MAN	A metropolitan area network (MAN) is a computer network that interconnects users with computer resources in a geographic region of the size of a metropolitan area.
Mesh Network	A mesh network (or simply meshnet) is a local network topology in which the infrastructure nodes connect directly, dynamically and non-hierarchically to as many other nodes as possible and cooperate with one another to efficiently route data from/to clients.
Network	A network is defined as a group of two or more computer systems linked together.
Network Architecture	Network architecture is the design of a computer network.
Network Contingency	Something that could happen depending on other occurrences;
Network Devices	Networking devices may include gateways, routers, network bridges, modems, wireless access points, networking cables, line drivers, switches, hubs, and repeaters.
Networking	Networking is the process of interacting with others to exchange information.
Network mapping	Network mapping is the study of the physical connectivity of networks.
Network Packet	A network packet is a formatted unit of data carried by a packet-switched network.
Network Protocols	A network protocol is an established set of rules that determine how data is transmitted between different devices in the same network.
Network Recovery	Network recovery is the process of recovering and restoring normal working operations on a computer network.

Network Topology	Network topology is the arrangement of the elements of a communication network.
OSI Model	The Open Systems Interconnection model.
Patching	Patching is usually developed or distributed for replacement or insertion in a compiled code i-e,. a binary or an object file.
Ports	A port is a communication endpoint.
Ring Network	A ring network is a network topology in which each node connects to exactly two other nodes, forming a single continuous pathway for signals through each node - a ring.
Routers	
Routing protocols	A routing protocol specifies how routers communicate with each other to distribute information that enables them to select routes between any two nodes on a computer network.
Servers	A server is a computer program or a device that provides functionality for other programs or devices, called "clients".
SNMP	Simple Network Management Protocol.
Star Network	A star network is a local area network (LAN) in which all nodes
STP	STP Cabling is twisted-pair cabling with additional shielding to reduce crosstalk and other forms of electromagnetic interference (EMI).
Switches	A network switch is networking hardware that connects devices on a computer network by using packet switching to receive and forward data to the destination device.
UTM	Unguided transmission media are wireless, such as infrared, radio waves, and microwaves.
WAN	A Wide area network (WAN) is a telecommunications network that extends over a large geographical area for the primary purpose of computer networking.

Published: Chadly MN