Basics OF Networks

Network

A network is a collection of devices that are interconnected and can communicate with each other. These devices can include computers, servers, routers, switches, and other network equipment.

Networks can be local, connecting devices within a small area like a home or office, or they can be wide, connecting devices across multiple locations or even across the globe.

or

It is a connection of devices connected together with peripheral devices to share information is known as a network

Packet

Packets are envelopes of information used to transmit data over a network. They break data into smaller pieces to transmit efficiently.

Network Interface

A network interface is a point of connection, like a Wi-Fi card or an Ethernet cable, that allows devices to connect to a network.

Types of Networks

LAN (Local Area Network): Covers a small area like a home, office, or campus.

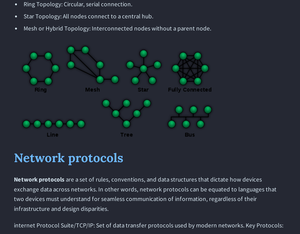
WAN (Wide Area Network): Spans larger geographical areas, often connecting LANs. MAN (Metropolitan Area Network): Covers a city or a metropolitan area.

PAN (Personal Area Network): A small network typically for personal devices. SAN (Storage Area Network): Used for high-speed data storage.

Network Topologies

Topologies define how devices or nodes are connected in a network.

- Bus Topology: Nodes are serially connected.
- Ring Topology: Circular, serial connection.
- Star Topology: All nodes connect to a central hub.
- Mesh or Hybrid Topology: Interconnected nodes without a parent node.



Network protocols

Network protocols are a set of rules, conventions, and data structures that dictate how devices exchange data across networks. In other words, network protocols can be equated to languages that two devices must understand for seamless communication of information, regardless of their infrastructure and design disparities.

Internet Protocol Suite/TCP/IP: Set of data transfer protocols used by modern networks. Key Protocols:

TCP——transmission control protocol——connection to connect internet[ ]

UDP——user datagram protocol——————graphical format——video streaming[ ] VOIP---voice over internet protocol———audio streaming[ ]

HTTP---hyper text transfer protocol————send data over browser[ ]

HTTPS--hyper text transfer protocol secure———HTTP+SSL(Secure Socket Layer)[ ]

FTP——file transfer protocol——file sharing over intranet connection(local connection)[ ] SSH——secure shell protocol———terminal security(Linux)[ ]

SMTP---simple mail transfer protocol——Sending mail over communication channel(/ /) TELNET---telicom services[ ]

POP ——post office protocol ——Receiving + Storing mail into the server.[ ]

DHCP—— dynamically host configuration protocol——Get the ip address from the router.[ ]

PORTS

Ports are the doors from where data comes and goes out of any device connected to a network can be LAN WAN or WAN.

Types of Ports

Physical Ports : They are tangible in nature. i.e we can seen touch and feel the ports, and as its nature data comes and goes out from these ports.

For Example: USB Ports, LAN, HDMI, VGA etc etc.

Virtual Ports : There are total 65535 ports available as it clear from the virtual they non tangible ports which you can see and feel but cant touch. For Example: Ports 80,8080 for HTTP : data comes and goes from client to server. Some well known ports:

File Transfer Protocol (FTP)

Secured shell (Ssh)

Telnet

SMTP

HyperText Transfer Protocol (http)

Registered Ports: The registered port numbers are the port numbers that companies and other users register with the Internet Corporation for Assigned Names and Numbers (ICANN) for use by the applications that communicate using the Internet's Transmission Control Protocol (TCP) or the User Datagram Protocol (UDP).

The registered port numbers are in the range from 1024 through 49151.

Dynamic Ports: Besides the well-known port numbers and the registered port numbers, the remaining ports in the port number spectrum are referred to as dynamic ports or private ports and are numbered from 49152 through 65535.

Proxy or Proxy Servers:

A proxy server is basically another computer which serves as a hub through which internet requests are processed. By connecting through one of these servers, your computer sends your requests to the server which then processes your request and returns what you were wanting.

A proxy server is a computer that acts as a gateway between a local network and a larger-scale network such as the Internet

Proxy servers provide increased performance and security. Example: **www.hidemyass.com**
https://www.proxysite.com

VPN(Virtual Private Network)

A virtual private network, or VPN, extends across a public or shared network, and acts like a tunnel so you can exchange data securely and anonymously across the internet as if you were connected directly to a private network.

Once you connect through a VPN, all your traffic becomes encrypted and your IP (Internet Protocol) address gets replaced with the address of the VPN server.

Services:

Online Services : hidemyass

extension based : hoxx vpn, Anonymox Stand Alone Services : Psiphon

DNS (Domain Name System)

The Domain Name System (DNS) is the phonebook of the Internet. google.com--> 121.123.23.212

Web browsers interact through Internet Protocol (IP) addresses. DNS translates domain names to IP addresses so browsers can load Internet resources.

WHAT IS AN IP ADDRESS ?

An IP address is a 32-bit unique address assigned to a computer on the internet for communication.

IPv4: 32-bit (4.29 billion unique addresses).

IPv6: 128-bit (340 undecillion unique addresses

example 192.168.1.1 -> an ip address 8bit.8bit.8bit.8bit

Now the question is -> How 4 billion ip address are enough or were enough for today's world and how did we even we make it so far with only 4 billion ip address and That is with help of NAT or NETWORK ADDRESS TRANSLATION

NAT (Network Address Translation)

Network Address Translation (NAT) is designed for IP address conservation. It enables private IP networks that use unregistered IP addresses(common personal computers) to connect to the Internet. NAT operates on a router, usually connecting two networks together, and translates the private (not globally unique) addresses in the internal network into legal addresses, before packets are forwarded to another network.

Basically, NAT allows a single device, such as a router, to act as an agent between the Internet (or public network) and a local network (or private network), which means that only a single unique IP address is required to represent an entire group of computers to anything outside their network.

Private vs. Public IP Addresses

An ip address is of two types 1 Private 2 Public

Private ip address -> Internal IP address valid on LAN but not on the internet For example All the devices connected to your wifi network have recieved a private ip address

Public ip address ->

Public ip address on the other-hand are globally unique and valid on the internet Example the ip address assigned to my WAN interface wireless router by ISP eg 42.111.108.97

www.whatismyip.com ---will show global ip

IP Subnets

A subnetwork or subnet is a logical subdivision of an IP network. The practice of dividing a network into two or more networks is called sub-netting

One network into many networks so that it can be easily managed and be secured

DHCP Server

Dynamic Host Configuration Protocol Server assigns IP addresses to devices on a network.

DHCP server assigns IP addresses with lease durations.

IP address assignment is done when devices connect to the network.

every time some device is connected to wifi router an ip address is assigned to the device and that assigning of the task is done by dhcp server in wifi router

The ip address is assigned with a lease (Time limit) to which the ip address will remain functional for a device

Example Router ip address =192.168.15.1

so The router can assign ip address to the devices from 192.168.15.2 to 192.168.15.255 And This Assigning is done with the help of dhcp server

OSI MODEL AND TCP IP MODEL

The OSI (Open Systems Interconnection) model and the TCP/IP (Transmission Control Protocol/Internet Protocol) model are both conceptual frameworks that describe the functions of a telecommunication or networking system. They are used to understand and standardize the communication processes in computer networks. Let's take a closer look at each model:

OSI Model:

The OSI model is a conceptual framework developed by the International Organization for Standardization (ISO) to facilitate communication between different systems. It consists of seven layers, each representing a specific functionality:

1. **Physical Layer:** Deals with the physical connection between devices. It defines hardware elements such as cables, connectors, and network interface cards.
2. **Data Link Layer:** Responsible for creating a reliable link between two directly connected nodes. It includes protocols for addressing, error detection, and flow control.
3. **Network Layer:** Manages the addressing, routing, and forwarding of data packets between devices across different networks. IP (Internet Protocol) operates at this layer.
4. **Transport Layer:** Provides end-to-end communication, ensuring that data is delivered error-free and in the correct order. TCP (Transmission Control Protocol) and UDP (User Datagram Protocol) operate at this layer.
5. **Session Layer:** Manages sessions or connections between applications on different devices, ensuring communication is established, maintained, and terminated.
6. **Presentation Layer:** Translates data between the application layer and the lower layers. It deals with data format translation, encryption, and compression.
7. **Application Layer:** Provides network services directly to end-users or applications. It includes application-specific protocols like HTTP, FTP, and SMTP.

TCP/IP Model:

The TCP/IP model is a more practical and widely used networking architecture. It has four layers, which correspond to some extent with the OSI model:

1. **Link Layer (equivalent to OSI Data Link and Physical Layers):** Combines the OSI model's first two layers, dealing with hardware addressing and physical transmission.
2. **Internet Layer (equivalent to OSI Network Layer):** Handles packet routing and addressing. IP operates at this layer.
3. **Transport Layer (equivalent to OSI Transport Layer):** Manages end-to-end communication, similar to the OSI Transport Layer. TCP and UDP operate here.
4. **Application Layer (equivalent to OSI Application, Presentation, and Session Layers):** Combines functionalities from the OSI model's top three layers, providing network services directly to applications.

The TCP/IP model is the basis for the Internet, and its protocols (such as TCP, IP, UDP, and others) are fundamental to modern networking. While the OSI model is a theoretical framework, the TCP/IP model is more widely adopted in practice.