Networking

Computer networking is a cornerstone of modern technology, enabling the interconnected systems that power the Internet, business communications, and everyday digital interactions. Understanding the fundamentals of computer networking is essential for anyone involved in technology, from enthusiasts to professionals. This article will explore the basics of computer networking, including network types, components, protocols, and essential services like the Domain Name System (DNS).

What is a Computer Network?

A computer network is a collection of interconnected devices that share resources and information. These devices can include computers, servers, printers, and other hardware. Networks allow for the efficient exchange of data, enabling various applications such as email, file sharing, and internet browsing.

How Does a Computer Network Work?

Basics building blocks of a Computer network are Nodes and Links. A Network Node can be illustrated as Equipment for Data Communication like a Modem, Router, etc., or Equipment of a Data Terminal like connecting two computers or more. Link in Computer Networks can be defined as wires or cables or free space of wireless networks.

The working of Computer Networks can be simply defined as rules or protocols which help in sending and receiving data via the links which allow Computer networks to communicate. Each device has an IP Address, that helps in identifying a device.

Basic Terminologies of Computer Networks

Network: A network is a collection of computers and devices that are connected together to enable communication and data exchange.

Nodes: Nodes are devices that are connected to a network. These can include computers, Servers, Printers, Routers, Switches, and other devices.

Protocol: A protocol is a set of rules and standards that govern how data is transmitted over a network. Examples of protocols include TCP/IP, HTTP, and FTP.

Topology: Network topology refers to the physical and logical arrangement of nodes on a network. The common network topologies include bus, star, ring, mesh, and tree. Service Provider Networks: These types of Networks give permission to take Network Capacity and Functionality on lease from the Provider. Service Provider Networks include Wireless Communications, Data Carriers, etc.

IP Address: An IP address is a unique numerical identifier that is assigned to every device on a network. IP addresses are used to identify devices and enable communication between them.

DNS: The Domain Name System (DNS) is a protocol that is used to translate human-readable domain names (such as www.google.com) into IP addresses that computers can understand.

Firewall: A firewall is a security device that is used to monitor and control incoming and outgoing network traffic. Firewalls are used to protect networks from unauthorized access and other security threats.

Types of Enterprise Computer Networks

LAN: A Local Area Network (LAN) is a network that covers a small area, such as an office or a home. LANs are typically used to connect computers and other devices within a building or a campus.

WAN: A Wide Area Network (WAN) is a network that covers a large geographic area, such as a city, country, or even the entire world. WANs are used to connect LANs together and are typically used for long-distance communication.

Cloud Networks: Cloud Networks can be visualized with a Wide Area Network (WAN) as they can be hosted on public or private cloud service providers and cloud networks are available if there is a demand. Cloud Networks consist of Virtual Routers, Firewalls, etc.

These are just a few basic concepts of computer networking. Networking is a vast and complex field, and there are many more concepts and technologies involved in building and maintaining networks. Now we are going to discuss some more concepts on Computer Networking.

Open system: A system that is connected to the network and is ready for communication.

Closed system: A system that is not connected to the network and can't be communicated with.

Types of Computer Network Architecture

Computer Network falls under these broad Categories:

Client-Server Architecture: Client-Server Architecture is a type of Computer Network Architecture in which Nodes can be Servers or Clients. Here, the server node can manage the Client Node Behaviour.

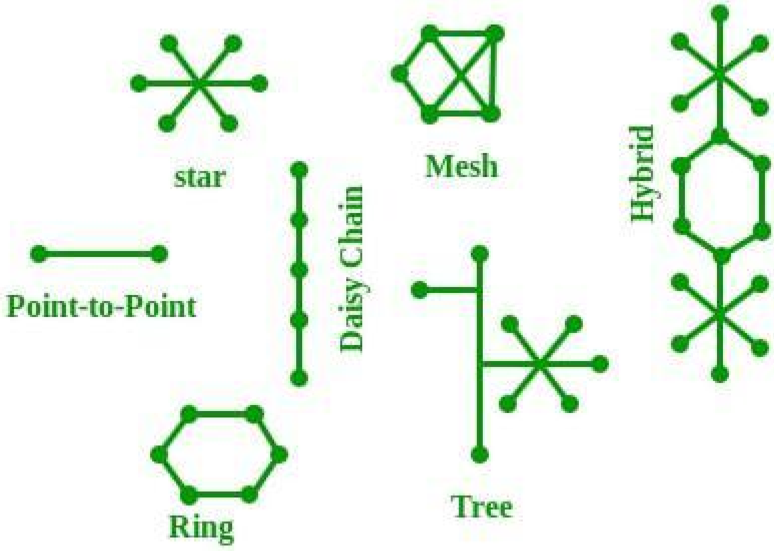
Peer-to-Peer Architecture: In P2P (Peer-to-Peer) Architecture, there is not any concept of a Central Server. Each device is free for working as either client or server.

Network Devices

An interconnection of multiple devices, also known as hosts, that are connected using multiple paths for the purpose of sending/receiving data or media. Computer networks can also include multiple devices/mediums which help in the communication between two different devices; these are known as Network devices and include things such as routers, switches, hubs, and bridges.

Network Topology

Network topology refers to the arrangement of different elements like nodes, links, or devices in a computer network. It defines how these components are connected and interact with each other. Understanding various types of network topologies helps in designing efficient and robust networks. Common types include bus, star, ring, mesh, and tree topologies, each with its own advantages and disadvantages.



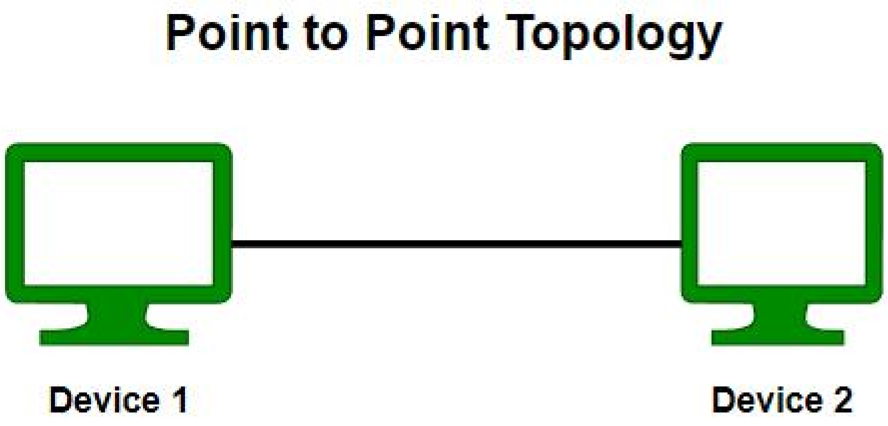
Types of Network Topology

The arrangement of a network that comprises nodes and connecting lines via sender and receiver is referred to as Network Topology . The various network topologies are:

1. Point to Point Topology
2. Mesh Topology
3. Star Topology
4. Bus Topology
5. Ring Topology
6. Tree Topology
7. Hybrid Topology

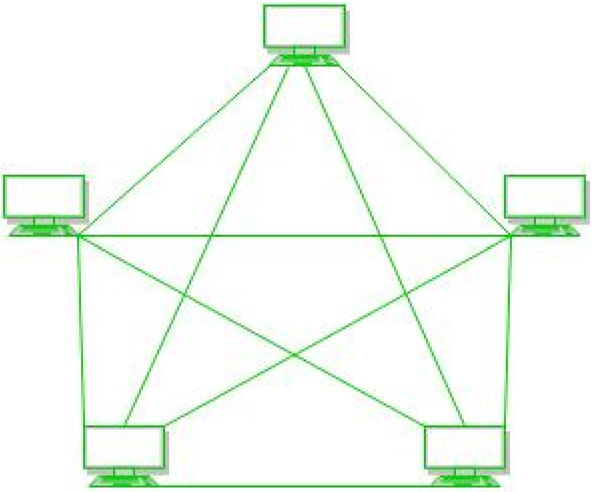
Point to Point Topology

Point-to-point topology is a type of topology that works on the functionality of the sender and receiver. It is the simplest communication between two nodes, in which one is the sender and the other one is the receiver. Point-to-Point provides high bandwidth.



Mesh Topology

In a mesh topology, every device is connected to another device via a particular channel. In Mesh Topology, the protocols used are AHCP (Ad Hoc Configuration Protocols), DHCP (Dynamic Host Configuration Protocol), etc.



- Communication is very fast between the nodes.
- Mesh Topology is robust.
- The fault is diagnosed easily. Data is reliable because data is transferred among the devices through dedicated channels or links.
- Provides security and privacy.

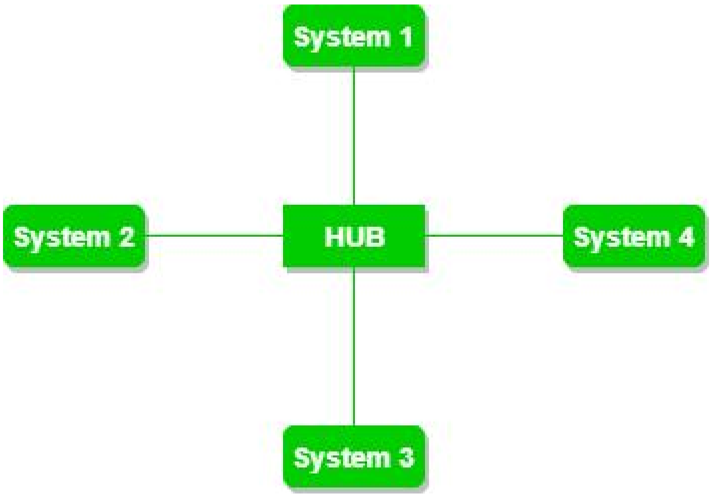
Disadvantages of Mesh Topology

- Installation and configuration are difficult.
- The cost of cables is high as bulk wiring is required, hence suitable for less number of devices.
- The cost of maintenance is high.

- A common example of mesh topology is the internet backbone, where various internet service providers are connected to each other via dedicated channels. This topology is also used in military communication systems and aircraft navigation systems.

Star Topology

In Star Topology, all the devices are connected to a single hub through a cable. This hub is the central node and all other nodes are connected to the central node. The hub can be passive in nature i.e., not an intelligent hub such as broadcasting devices, at the same time the hub can be intelligent known as an active hub. Active hubs have repeaters in them. Coaxial cables or RJ-45 cables are used to connect the computers. In Star Topology, many popular Ethernet LAN protocols are used as CD(Collision Detection), CSMA (Carrier Sense Multiple Access), etc.



Advantages of Star Topology

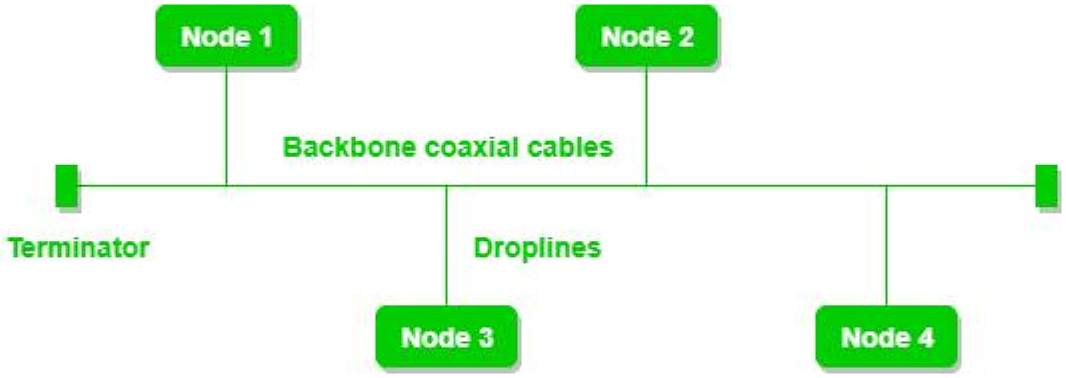
- If N devices are connected to each other in a star topology, then the number of cables required to connect them is N. So, it is easy to set up.
- Each device requires only 1 port i.e. to connect to the hub, therefore the total number of ports required is N.
- It is Robust. If one link fails only that link will affect and not other than that.
- Easy to fault identification and fault isolation.
- Star topology is cost-effective as it uses inexpensive coaxial cable.

Disadvantages of Star Topology

- If the concentrator (hub) on which the whole topology relies fails, the whole system will crash down.
- The cost of installation is high.
- Performance is based on the single concentrator i.e. hub.
- A common example of star topology is a local area network (LAN) in an office where all computers are connected to a central hub. This topology is also used in wireless networks where all devices are connected to a wireless access point.

Bus Topology

Bus Topology is a network type in which every computer and network device is connected to a single cable. It is bi-directional. It is a multi-point connection and a non-robust topology because if the backbone fails the topology crashes. In Bus Topology, various MAC (Media Access Control) protocols are followed by LAN ethernet connections like TDMA , Pure Aloha , CDMA, Slotted Aloha , etc.



Advantages of Bus Topology

- If N devices are connected to each other in a bus topology, then the number of cables required to connect them is 1, known as backbone cable, and N drop lines are required.
- Coaxial or twisted pair cables are mainly used in bus-based networks that support up to 10 Mbps.
- The cost of the cable is less compared to other topologies, but it is used to build small networks.
- Bus topology is familiar technology as installation and troubleshooting techniques are well known.
- CSMA is the most common method for this type of topology.

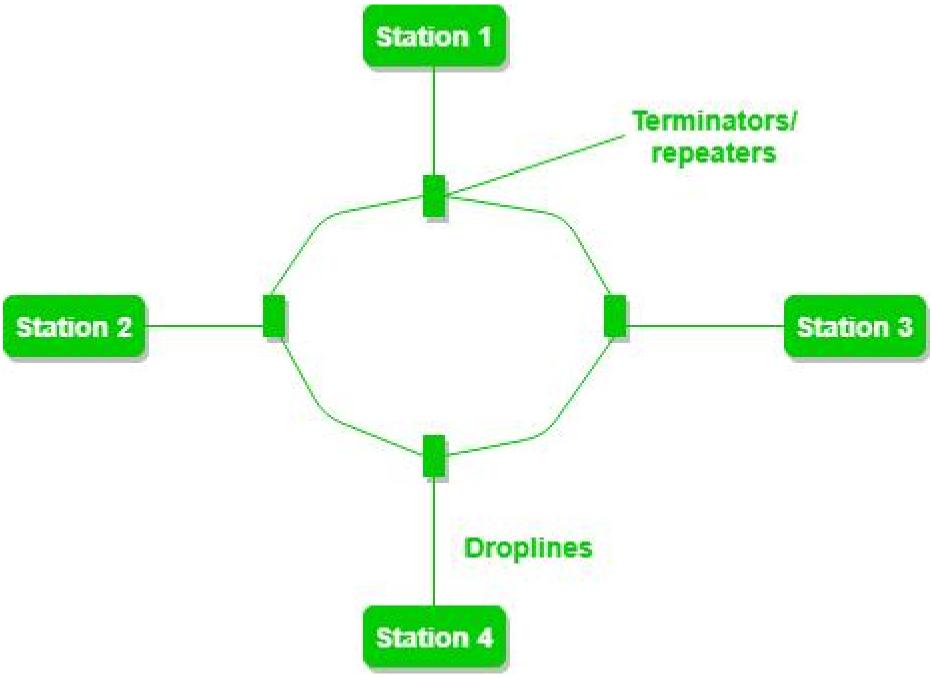
Disadvantages of Bus Topology

- A bus topology is quite simpler, but still, it requires a lot of cabling.
- If the common cable fails, then the whole system will crash down.
- If the network traffic is heavy, it increases collisions in the network. To avoid this, various protocols are used in the MAC layer known as Pure Aloha, Slotted Aloha, CSMA/CD, etc.
- Adding new devices to the network would slow down networks.
- Security is very low.
- A common example of bus topology is the Ethernet LAN, where all devices are connected to a single coaxial cable or twisted pair cable. This topology is also used in cable television networks.

Ring Topology

In a Ring Topology, it forms a ring connecting devices with exactly two neighboring devices. A number of repeaters are used for Ring topology with a large number of nodes, because if someone wants to send some data to the last node in the ring topology with 100 nodes, then the data will have to pass through 99 nodes to reach the 100th node. Hence to prevent data loss repeaters are used in the network.

The data flows in one direction, i.e. it is unidirectional, but it can be made bidirectional by having 2 connections between each Network Node, it is called Dual Ring Topology. In-Ring Topology, the Token Ring Passing protocol is used by the workstations to transmit the data.



The most common access method of ring topology is token passing.

Token passing: It is a network access method in which a token is passed from one node to another node.
Token: It is a frame that circulates around the network.
Operations of Ring Topology

- One station is known as a monitor station which takes all the responsibility for performing the operations.
- To transmit the data, the station has to hold the token. After the transmission is done, the token is to be released for other stations to use.
- When no station is transmitting the data, then the token will circulate in the ring.
- There are two types of token release techniques: Early token release releases the token just after transmitting the data and Delayed token release releases the token after the acknowledgment is received from the receiver.

Advantages of Ring Topology

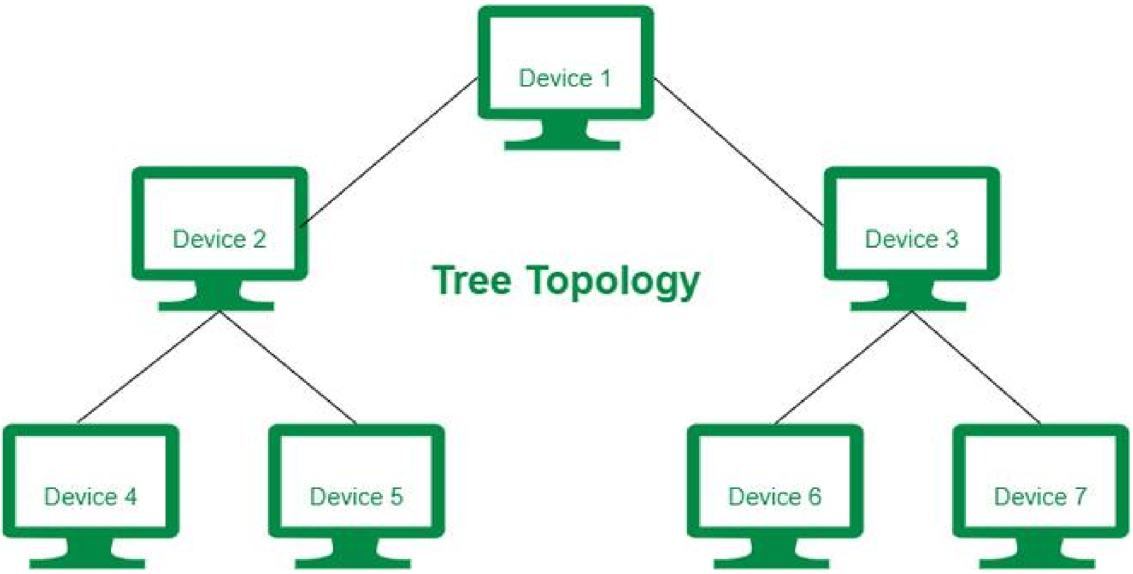
- The data transmission is high-speed.
- The possibility of collision is minimum in this type of topology.
- Cheap to install and expand.
- It is less costly than a star topology.

Disadvantages of Ring Topology

- The failure of a single node in the network can cause the entire network to fail.
- Troubleshooting is difficult in this topology.
- The addition of stations in between or the removal of stations can disturb the whole topology.
- Less secure.

Tree Topology

This topology is the variation of the Star topology. This topology has a hierarchical flow of data. In Tree Topology, protocols like DHCP and SAC (Standard Automatic Configuration) are used.



In this, the various secondary hubs are connected to the central hub which contains the repeater. This data flow from top to bottom i.e. from the central hub to the secondary and then to the devices or from bottom to top i.e. devices to the secondary hub and then to the central hub. It is a multi-point connection and a non-robust topology because if the backbone fails the topology crashes.

Advantages of Tree Topology

- It allows more devices to be attached to a single central hub thus it decreases the distance that is traveled by the signal to come to the devices.
- It allows the network to get isolated and also prioritize from different computers.
- We can add new devices to the existing network.
- Error detection and error correction are very easy in a tree topology.

Disadvantages of Tree Topology

- If the central hub gets fails the entire system fails.
- The cost is high because of the cabling.
- If new devices are added, it becomes difficult to reconfigure.

- A common example of a tree topology is the hierarchy in a large organization. At the top of the tree is the CEO, who is connected to the different departments or divisions (child nodes) of the company. Each department has its own hierarchy, with managers overseeing different teams (grandchild nodes). The team members (leaf nodes) are at the bottom of the hierarchy, connected to their respective managers and departments.

OSI Model

OSI stands for Open Systems Interconnection. It is a reference model that specifies standards for communications protocols and also the functionalities of each layer. The OSI has been developed by the International Organization For Standardization and it is 7 layer architecture. Each layer of OSI has different functions and each layer has to follow different protocols. The 7 layers are as follows:

1. Physical Layer
2. Data link Layer
3. Network Layer
4. Transport Layer
5. Session Layer
6. Presentation Layer
7. Application Layer

Network Protocols

A protocol is a set of rules or algorithms which define the way how two entities can communicate across the network and there exists a different protocol defined at each layer of the OSI model. A few such protocols are TCP, IP, UDP, ARP, DHCP, FTP, and so on.

Transmission Control Protocol/Internet Protocol (TCP/IP)

Function: The foundational protocol suite of the internet, enabling reliable communication.

Components:

TCP: Ensures data is delivered reliably and in order.

IP: Routes data packets to their destination based on IP addresses.

Hypertext Transfer Protocol (HTTP) and HTTPS

Function: The protocols used for transmitting web pages.

HTTP: Unsecured communication.

HTTPS: Secured communication using SSL/TLS encryption.

Simple Mail Transfer Protocol (SMTP)

Function: Protocol for sending email.

Components: Works with other protocols like POP3 and IMAP for email retrieval.

File Transfer Protocol (FTP)

Function: Protocol for transferring files between computers.

Components: Includes commands for uploading, downloading, and managing files on a remote server.

Dynamic Host Configuration Protocol (DHCP)

Function: Automatically assigns IP addresses to devices on a network.

Components: Reduces manual configuration and IP address conflicts.

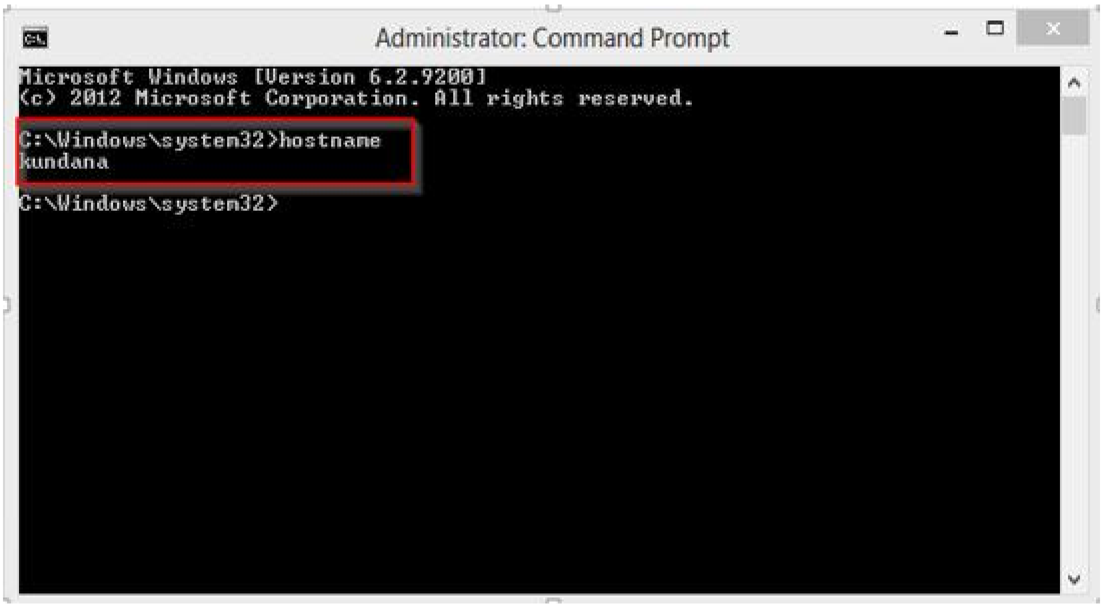
Domain Name System (DNS)

Function: Translates human-friendly domain names into IP addresses.

Components: Ensures seamless navigation on the internet.

Unique Identifiers of Network

Hostname: Each device in the network is associated with a unique device name known as Hostname. Type “hostname” in the command prompt(Administrator Mode) and press ‘Enter’, this displays the hostname of your machine.



```
Microsoft Windows [Version 6.2.9200]
(c) 2012 Microsoft Corporation. All rights reserved.

C:\Windows\system32>hostname
kundana

C:\Windows\system32>
```

IP Address (Internet Protocol address): Also known as the Logical Address, the IP Address is the network address of the system across the network. To identify each device in the world-wide-web, the Internet Assigned Numbers Authority (IANA) assigns an IPV4 (Version 4) address as a unique identifier to each device on the Internet. The length of an IPv4 address is 32 bits, hence, we have 232 IP addresses available. The length of an IPv6 address is 128 bits.

In Windows Type “ipconfig” in the command prompt and press ‘Enter’, this gives us the IP address of the device. For Linux, Type “ifconfig” in the terminal and press ‘Enter’ this gives us the IP address of the device.

MAC Address (Media Access Control address): Also known as physical address, the MAC Address is the unique identifier of each host and is associated with its NIC (Network Interface Card). A MAC address is assigned to the NIC at the time of manufacturing. The length of the MAC address is: 12-nibble/ 6 bytes/ 48 bits Type “ipconfig/all” in the command prompt and press ‘Enter’, this gives us the MAC address.

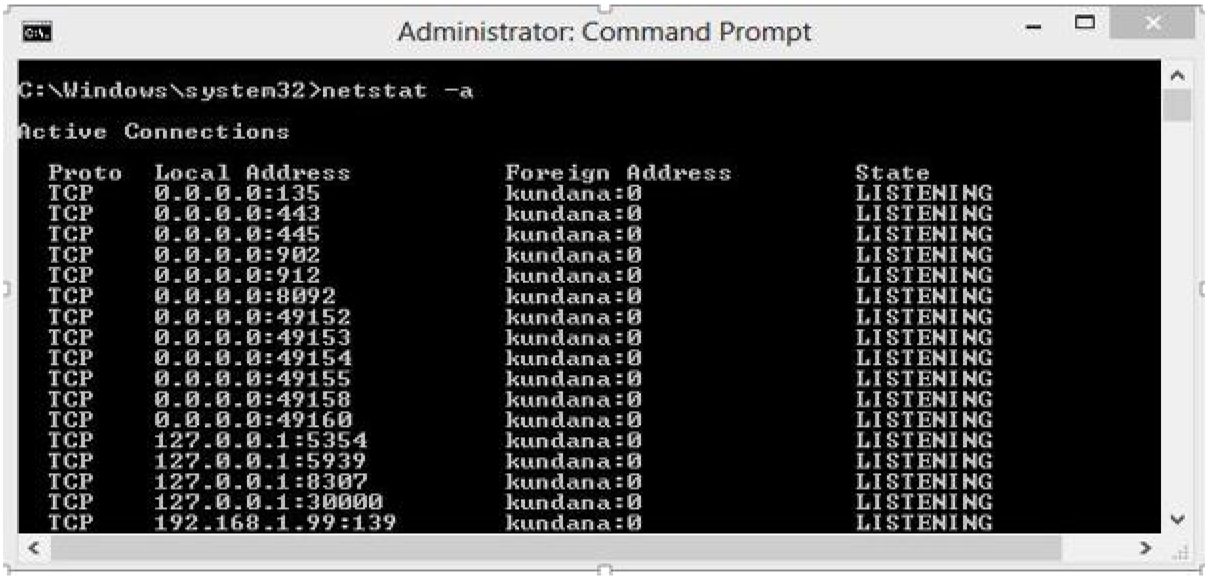
Port: A port can be referred to as a logical channel through which data can be sent/received to an application. Any host may have multiple applications running, and each of these applications is identified using the port number on which they are running.

A port number is a 16-bit integer, hence, we have 216 ports available which are categorized as shown below:

Port Types	**Range**
Well known Ports	0 – 1023
Registered Ports	1024 – 49151
Ephemeral Ports	49152 – 65535

Number of ports: 65,536
Range: 0 – 65535

Type “netstat -a” in the command prompt and press ‘Enter’, this lists all the ports being used.



```
C:\Windows\system32>netstat -a

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    0.0.0.0:135            kundana:0              LISTENING
  TCP    0.0.0.0:443            kundana:0              LISTENING
  TCP    0.0.0.0:445            kundana:0              LISTENING
  TCP    0.0.0.0:902            kundana:0              LISTENING
  TCP    0.0.0.0:912            kundana:0              LISTENING
  TCP    0.0.0.0:8092           kundana:0              LISTENING
  TCP    0.0.0.0:49152          kundana:0              LISTENING
  TCP    0.0.0.0:49153          kundana:0              LISTENING
  TCP    0.0.0.0:49154          kundana:0              LISTENING
  TCP    0.0.0.0:49155          kundana:0              LISTENING
  TCP    0.0.0.0:49158          kundana:0              LISTENING
  TCP    0.0.0.0:49160          kundana:0              LISTENING
  TCP    127.0.0.1:5354         kundana:0              LISTENING
  TCP    127.0.0.1:5939         kundana:0              LISTENING
  TCP    127.0.0.1:8307         kundana:0              LISTENING
  TCP    127.0.0.1:30000        kundana:0              LISTENING
  TCP    192.168.1.99:139       kundana:0              LISTENING
```

Socket: The unique combination of IP address and Port number together is termed a Socket.

Other Related Concepts

DNS Server: DNS stands for Domain Name System. DNS is basically a server that translates web addresses or URLs (ex: www.google.com) into their corresponding IP addresses. We don’t have to remember all the IP addresses of each and every website. The command ‘nslookup’ gives you the IP address of the domain you are looking for. This also provides information on our DNS Server.

ARP: ARP stands for Address Resolution Protocol. It is used to convert an IP address to its corresponding physical address(i.e., MAC Address). ARP is used by the Data Link Layer to identify the MAC address of the Receiver’s machine.

RARP: RARP stands for Reverse Address Resolution Protocol. As the name suggests, it provides the IP address of the device given a physical address as input. But RARP has become obsolete since the time DHCP has come into the picture.

The Domain Name System (DNS) is a critical component of computer networking. It converts easily recognizable domain names, such as www.example.com, into numerical IP addresses that computers use to identify each other on the network.

How DNS Works?

User Input: When a user enters a domain name in a browser, the system needs to find its IP address.

DNS Query: The user’s device sends a DNS query to the DNS resolver.

Resolver Request: The DNS resolver checks its cache for the IP address. If not found, it forwards the request to the root DNS server.

Root DNS Server: The root DNS server provides the address of the TLD (Top-Level Domain) server for the specific domain extension (e.g., .com).

TLD DNS Server: The TLD server directs the resolver to the authoritative DNS server for the actual domain.

Authoritative DNS Server: The authoritative DNS server knows the IP address for the domain and provides it to the resolver.

Response to User: The resolver stores the IP address in its cache and sends it to the user’s device.

Access Website: With the IP address, the user’s device can access the desired website.

DNS works efficiently, translating user-friendly domain names into IP addresses, allowing seamless navigation on the internet.

Network Security

Ensuring the security of a network is crucial to protect data and resources from unauthorized access and attacks. Key aspects of network security include:

Firewalls: Devices or software that monitor and control incoming and outgoing network traffic based on security rules.

Encryption: The process of encoding data to prevent unauthorized access. Commonly used in VPNs, HTTPS, and secure email.

Intrusion Detection Systems (IDS): Tools that monitor network traffic for suspicious activity and potential threats.

Access Control: Mechanisms that restrict access to network resources based on user identity and role.

Regular Updates and Patching: Keeping software and hardware up to date to protect against vulnerabilities.