Computer Networking

**1. Basic of Computer Networking**

-------------------------------------------------------------------------------------------------------

Computer Networking is the practice of connecting computers together to enable communication and data exchange between them.

In general, Computer Network is a collection of two or more computers. It helps users to communicate more easily.

**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,](https://www.geeksforgeeks.org/introduction-of-a-router/) [Switches](https://www.geeksforgeeks.org/types-of-switches-in-computer-network/), 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](https://www.geeksforgeeks.org/tcp-ip-model/), [HTTP](https://www.geeksforgeeks.org/http-full-form/), and [FTP](https://www.geeksforgeeks.org/file-transfer-protocol-ftp-in-application-layer/).
* **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)](https://www.geeksforgeeks.org/domain-name-system-dns-in-application-layer/) 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](https://www.geeksforgeeks.org/introduction-of-firewall-in-computer-network/) 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)](https://www.geeksforgeeks.org/types-of-area-networks-lan-man-and-wan/)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)](https://www.geeksforgeeks.org/wan-full-form/) 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](https://www.geeksforgeeks.org/cloud-networking/) 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.
* **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.

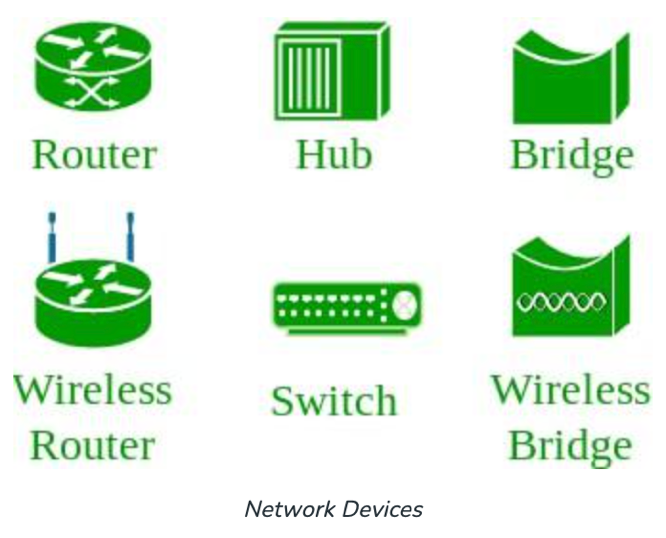
## Types of Computer Network Architecture

Computer Network falls under these broad Categories:

* **Client-Server Architecture:** [Client-Server Architecture](https://www.geeksforgeeks.org/client-server-model/) 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](https://www.geeksforgeeks.org/what-is-p2ppeer-to-peer-process/), there is not any concept of a Central Server. Each device is free for working as either client or server.

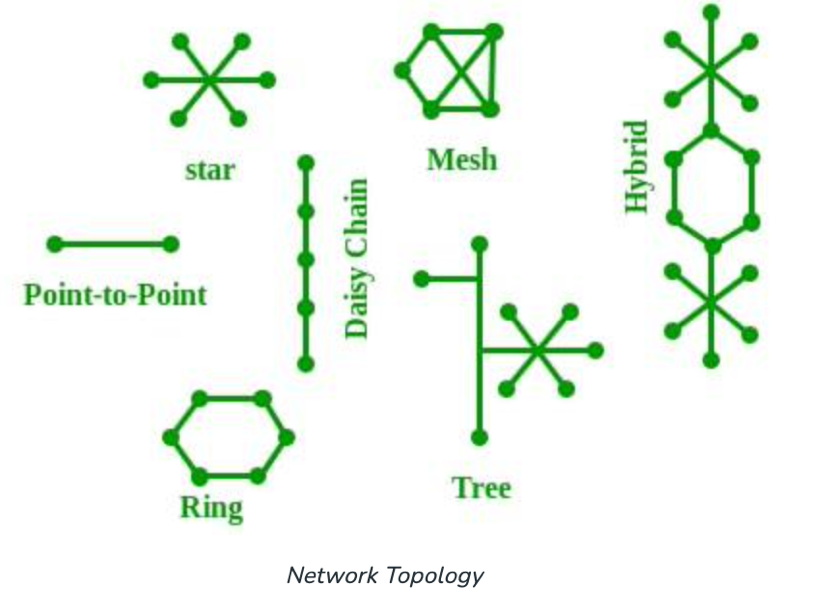
## Network Devices

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](https://www.geeksforgeeks.org/network-devices-hub-repeater-bridge-switch-router-gateways/) and include things such as routers, switches, hubs, and bridges.



## Network Topology

The [Network Topology](https://www.geeksforgeeks.org/types-of-network-topology/) is the layout arrangement of the different devices in a network. Common examples include Bus, Star, Mesh, Ring, and Daisy chain.



**OSI Model**

OSI stands for [Open Systems Interconnection](https://www.geeksforgeeks.org/layers-of-osi-model/). 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:

* [Physical Layer](https://www.geeksforgeeks.org/physical-layer-in-osi-model/)
* [Data link Layer](https://www.geeksforgeeks.org/data-link-layer/)
* [Network Layer](https://www.geeksforgeeks.org/network-layer-services-packetizing-routing-and-forwarding/)
* [Transport Layer](https://www.geeksforgeeks.org/transport-layer-responsibilities/)
* [Session Layer](https://www.geeksforgeeks.org/session-layer-in-osi-model/)
* [Presentation Layer](https://www.geeksforgeeks.org/presentation-layer-in-osi-model/)
* [Application Layer](https://www.geeksforgeeks.org/application-layer-in-osi-model/)

**Protocol**

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.

## Unique Identifiers of Network

**Hostname:**Each device in the network is associated with a unique device name known as Hostname. (Type “hostname” in terminal for displaying the hostname of your machine).

**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. Type “ipconfig” in the command prompt 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](https://www.geeksforgeeks.org/introduction-of-mac-address-in-computer-network/) is the unique identifier of each host and is associated with its [NIC (Network Interface Card)](https://www.geeksforgeeks.org/nic-full-form/). 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.

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

**Other Related Concepts**

**DNS Server:** [DNS](https://www.geeksforgeeks.org/domain-name-system-dns-in-application-layer/) 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](https://www.geeksforgeeks.org/how-address-resolution-protocol-arp-works/) 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](https://www.geeksforgeeks.org/what-is-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.

**2. Goals of Networks**

-------------------------------------------------------------------------------------------------------

Computer Network means an interconnection of autonomous (standalone) computers for information exchange. The connecting media could be a copper wire, optical fiber, microwave, or satellite.

**Networking Elements –** The computer network includes the following networking elements:

1. At least two computers
2. Transmission medium either wired or wireless
3. Protocols or rules that govern the communication
4. Network software such as Network Operating System

**Network Criteria:**

The criteria that have to be met by a computer network are:

**1. Performance –** It is measured in terms of transit time and response time

* Transit time is the time for a message to travel from one device to another
* Response time is the elapsed time between an inquiry and a response.

Performance is dependent on the following factors:

* The number of users
* Type of transmission medium
* Capability of connected network
* Efficiency of software
* Bandwidth
* Network topology
* Network protocols
* Distance
* Network congestion
* Network hardware

**2. Reliability –** It is measured in terms of

* Frequency of failure
* Recovery from failures
* Robustness during catastrophe
* Quality of service (QoS)
* Reducing single points of failure
* Capacity planning
* Network architecture

**3. Security –** It means protecting data from unauthorized access.

**4. Network topology -**it is another crucial factor to consider when designing a computer network. It refers to the way in which computers, devices, and links are arranged in a network. Common topologies include **bus, star, ring, mesh, and hybrid**, each with its own advantages and disadvantages in terms of cost, scalability, reliability, and performance. The choice of topology depends on the specific needs and constraints of the network. Other important criteria that must be met by a computer network include performance, reliability, and security.

**Goals of Computer Networks:** The following are some important goals of computer networks:

1. **Resource Sharing –** Many organization has a substantial number of computers in operations, which are located apart. Ex. A group of office workers can share a common printer, fax, modem, scanner, etc.
2. **High Reliability –** If there are alternate sources of supply, all files could be replicated on two or more machines. If one of them is not available, due to hardware failure, the other copies could be used.
3. **Inter-process Communication –** Network users, located geographically apart, may converse in an interactive session through the network. In order to permit this, the network must provide almost error-free communications.
4. **Flexible access –** Files can be accessed from any computer in the network. The project can be begun on one computer and finished on another.
5. **Security** – Computer networks must be secure to protect against unauthorized access, data breaches, and other security threats. This includes implementing measures such as firewalls, antivirus software, and encryption to ensure the confidentiality, integrity, and availability of data.
6. **Performance**– Computer networks must provide high performance and low latency to ensure that applications and services are responsive and available when needed. This requires optimizing network infrastructure, bandwidth utilization, and traffic management.
7. **Scalability-** Computer networks must be designed to scale up or down as needed to accommodate changes in the number of users, devices, and data traffic. This requires careful planning and management to ensure the network can meet current and future needs.

Other goals include Distribution of processing functions, Centralized management, and allocation of network resources, Compatibility of dissimilar equipment and software, Good network performance, Scalability, Saving money, Access to remote information, Person to person communication, etc.