Table of Contents

[**Computer Networks 3**](#_7xprc2xttylu)

[Network 3](#_elq9l5hdsr1k)

[The Internet 3](#_8szeozjav457)

[The History of Computer Networks 3](#_bja8qo9ua33u)

[Need for Computer Network 4](#_q0oz8w8nxjd2)

[**Protocol 4**](#_jxa2l5km185p)

[Types of Protocol 5](#_9lpcgtknklu0)

[How network protocol works 5](#_no9erzcmxj93)

[1. The OSI Model (Open Systems Interconnection model) 5](#_3mth7zy1joi)

[There are Seven Layers of the OSI model. 5](#_aq7givn342mb)

[2. The TCP/IP Model (Transmission Control Protocol / Internet Protocol) 7](#_mnxrymib7bed)

[There are Four Layers of the TCP/IP Model 8](#_g8v01pu8ebm1)

[Functions of Network Layer 8](#_7gxft0udfck9)

[Network Layer Protocolk 8](#_5dktw9ghkm62)

[1. Internet Protocol(IP):- Internet Protocol is used to help uniquely identify each device on the network. Internet protocol is responsible for transferring the data from one node to another node in the network. 9](#_y4sl4tmdzhna)

[2. ARP (Address Resolution Protocol) 9](#_h8xg6mw59qcs)

[Types of ARP Entries 10](#_jbf6ijo9vgse)

[3. RARP (Reversed Address Resolution Protocol) 10](#_dfsvv0vx2cky)

[4. ICMP (Internet Control Message Protocol) 10](#_rk4av6mg9xwt)

[5. IGMP (Internet Group Message Protocol) 11](#_1ftooc1l3bjv)

[**Network Connectivity Devices 11**](#_i1zlvos755m0)

[**Types of Network 12**](#_j3bo94ouw0hr)

[1. Client-Server Network: 12](#_6wajej3htqpo)

[Types of Client-Server Network 12](#_d81sx8uperbg)

[2. Peer-to-Peet Network: 13](#_prxtt28kihp6)

[**Classification Of Network 13**](#_rllsi0yoffvm)

[1. PAN (Personal Area Network) 13](#_c5ysnh71hxkz)

[Two Types of PAN 14](#_2a2qst159xzq)

[2) LAN (Local Area Network) 14](#_p5eioewqquwz)

[3) MAN (Metropolitan Area Network) 14](#_s8qkv4mosudy)

[Uses of Metropolitan Area Network 14](#_4qaecxieqr5k)

[4) WAN(Wide Area Network) 15](#_t600706zhx2f)

[Examples of Wide Area Network 15](#_3vw6vdpctqxx)

[5) Global Area Network (GAN) 15](#_7r9x2pjbo1gn)

[**Transmission Medium 16**](#_wh8qb2gsbqt9)

[Transmission mediums are classified into the following types. 16](#_s3sfr6pfmph3)

[1) Guided Media 16](#_f5whkikrpi97)

[There are three major types of Guided Media. 16](#_5wh4ejodrpf1)

[2) UnGuided Media: 18](#_wf8ma7ey5my8)

[There are Three types of Signals transmitted through unguided media 18](#_wdsgdb2b8lin)

[**Impairment Causes in the Transmission of Network 18**](#_do8wi78728h5)

[There are three causes of Transmission Impairment 19](#_fw98gf3hk0g3)

[1. Attenuation: 19](#_gdlgvh162ylz)

[2. Distortion: 19](#_7nypd9nx5sfd)

[3. Noise: 19](#_9ffk4rc734ps)

[**Routing 20**](#_ghltq9d4sn81)

[Types of Routing 20](#_ogkc4suzfti1)

[1. Static Routing 20](#_garxlzdvprvx)

[2. Dynamic Routing 20](#_ntewyzove07s)

[**STP (Spanning Tree Protocol) 21**](#_jc6z5rtxn7wg)

[How Spanning Tree Protocol Works 21](#_hbzvton18fp6)

[**TTL (Time to Live Protocol) 21**](#_2206kxl0vglj)

[How Time-To-Live (TTL) Work? 21](#_4wp2sf8cknt)

[VLAN 22](#_dcowor1camm5)

# Computer Networks

* A computer network is a telecommunications network, which allows digital devices(nodes) to exchange data between each other using either wired or wireless connections to share resources(h/w or s/w) i.e. Internet.
* A collection of autonomous computers interconnected by a single technology.

## Network

A group or system of interconnected things.

## The Internet

The network of the network is called the internet.

## The History of Computer Networks

The history of modern computer networking technology goes back to 1969 when ARPANET (Advanced Research Projects Agency Network) became the first connected computer network. It implemented the TCP/IP protocol suite, which later became the Internet. ARPANET was developed by the Advanced Research Projects Agency (ARPA), a subset of the US Department of Defense.

The first computer network was created by connecting four host computers of four main universities in America. This network was not for personal communication but for communication between the army and the organization.

By 1980, there were 213 nodes in the ARPANET system. Over the next few years, ARPANET grew rapidly and began to be connected to other networks, Bob Kahn invented the TCP/IP protocol for networks and developed it, with the help of Vint Cerf, in 1978. Gradually more development took place and today it has become the largest network in the world, which we know by the name of the Internet.

## Need for Computer Network

1. **To share Computer Files: -** To sharing of files and data is the most vital feature of a computer network. When there was no computer network, the floppy disk was physically carried to move files from one computer to another.
2. **To share Hardware Devices: -** Users can share hardware devices such as printers, scanners, CD-ROM drives, hard drives, etc.
3. **Application Sharing: -** Applications can be shared over the network, and this allows to implementation of client/server applications.
4. **Communication:** The network allows individuals and groups to communicate and collaborate, whether through email, instant messaging, video conferencing, or other means.
5. **Resources Sharing: -** Networks enable multiple users to share resources such as printers, data storage devices, and other hardware and software resources. This can help to reduce costs, increase efficiency, and improve productivity.
6. **Gaming: -** Network also helps to play games with other people.
7. **Access Information: -** Networks enable access to a diverse set of services and information, such as the Internet, database servers, and cloud-based services for computing.
8. **E-Commerce:-** E-Commerce stands for Electronic commerce. We can sell products and services online through the internet to any corner of the world and can buy online 24X7 from anywhere in the world.
9. **Entertainment: -** Millions of people use computer networks or the internet for entertainment.
10. **Voice over IP: -** It is also known as VOIP. It is a protocol used for telecommunications. VoIP is a technology that allows you to make voice calls using a broadband Internet connection instead of a regular phone line.
11. **To reduce the cost of data transfer: -** If you share data and files using a computer network, then it costs very little. It is cheaper than other method.

# Protocol

Network Protocol is the set of standard 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 communication exchange must accept and follow protocol conventions. In-network support for protocols can be built into software, hardware, or both.

Without network protocols, computers and other devices wouldn’t know how to engage with each other.

## Types of Protocol

TCP/IP, IP, FTP, HTTP, ICMP, SFTP, Telnet, etc

## How network protocol works

### The OSI Model (Open Systems Interconnection model)

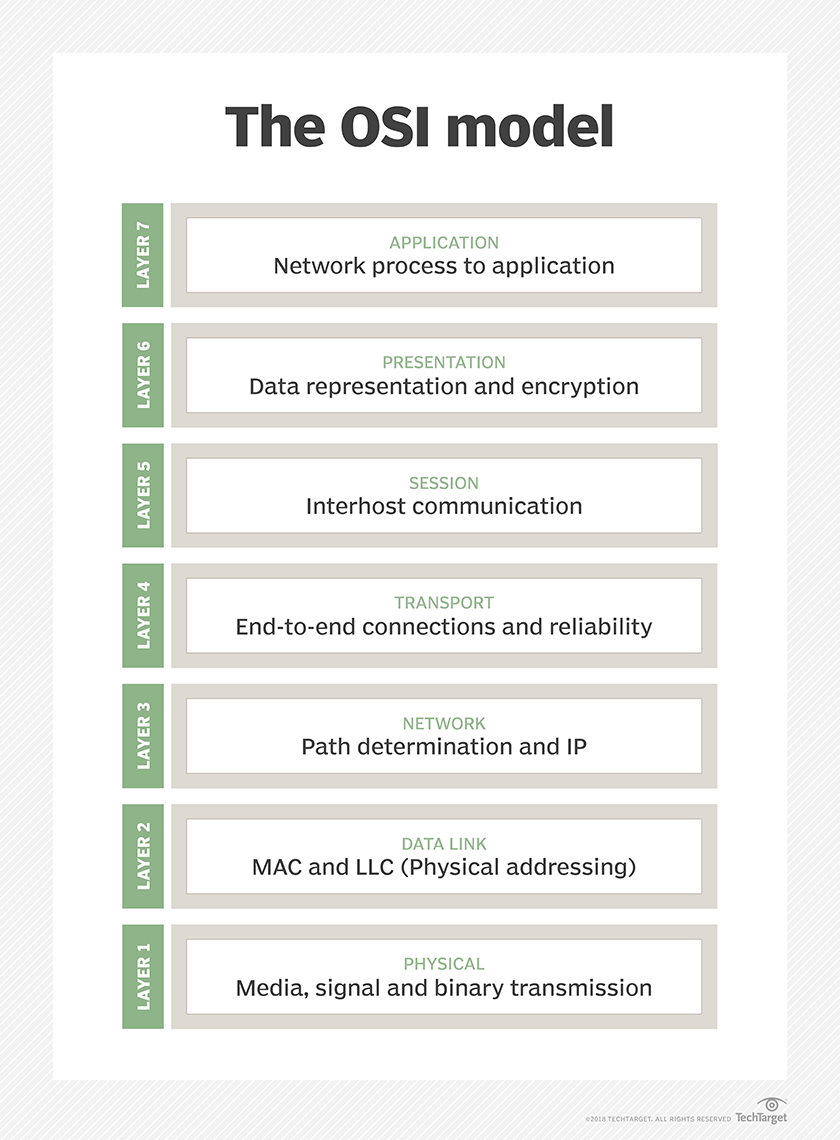
Network protocol breaks large processes into discrete, narrowly defined functions and tasks across every network level.

#### There are Seven Layers of the OSI model.

1. **Application Layer: -** The application layer, which is the top layer of the network, oversees relaying user application requests to lower levels. File transfer, email, remote login, data entry, and other common applications take place at this layer.
2. **Presentation Layer: -** The presentation layer is also known as the *translation layer* because it retrieves the data from the application layer and formats it for transmission over the network. In addition Presentation Layer is in charge of managing file-level security and transforming data to network standards. It checks and converts in which format we send the data that is receiver understandable. It encrypts the data to move faster data in the network.
3. **Session Layer: -** The session layer establishes a connection between two workstations that need to communicate until the data does not reach to receiver. If half data is received by the receiver and the remaining data is going to the receiver, then the session layer again starts sending the data from the session layer it can’t create a new session for that remaining data.
4. **Transport Layer: -** The transport layer transfers services from the network layer to the application layer and breaks data into data segments for error checking at the network segment level. This also ensures that a fast host on a network doesn't overtake a slower one.

There are two protocols used:

1. TCP:- When we establish the connection then send the data using TCP protocol. In this, we have a notification from the receiver side that the data has been received or not.
2. UDP: - When we don’t establish the connection fastly send the data using UDP protocol. When we use UDP we don’t know whether the data is received by the receiver or not.
3. **Network Layer: -**  It stores the IP address of the sender and the IP address of the receiver all the works of routers perform at this layer. It checks from which path we send the data which reaches to receiver fastly. Additionally, it divides up segments from the transport layer into error-free packets.
4. **Data Link Layer: -**  It converts the data into frames. 1) It checks the data and sends the error-free data to onwards. 2) It maintains the speed of both the sender and the receiver. 3) it also picks the physical address of the hardware. CRC algorithm is used here.
5. **Physical Layer: -**  The physical layer is the initial layer that physically connects two interoperable systems. It controls simplex or duplex modem transmission and transfers data in bits. Additionally, it oversees the hardware that connects the network interface card (NIC) to the network, including the wiring, cable terminators, topography, and voltage levels.



### 2. The TCP/IP Model (Transmission Control Protocol / Internet Protocol)

A set of cooperating network protocols is called a *protocol suite*. The Transmission Control Protocol/Internet Protocol (TCP/IP) suite, is typically used in client-server models and peer-to-peer support.

Developed by ARPANET.

#### **There are Four Layers of the TCP/IP Model**

1. **Application layer.** This is the topmost layer of the TCP/IP model and is responsible for providing users with access to network resources. Some of the protocols included in this layer are HTTPS, Simple Mail Transfer Protocol (SMTP), and FTP.
2. **Transport layer.** This layer ensures that segments are transmitted correctly via the communication channel. The network link between the source and destination systems is also established at this layer. The port number assigned here.
3. **Internet layer**. Also known as the *network layer*, the internet layer receives and sends packets for the network. This layer comprises IP, Address Resolution Protocol (ARP), and Internet Control Message Protocol (ICMP).
4. **Network access layer**. The network access layer of TCP/IP combines the physical and data-link layers of the OSI model. It deals with Layer 1 concerns, such as energy, bits, and the media used to transport them, such as copper, fiber, and wireless. Additionally, it deals with Layer 2 difficulties, including bit conversion into protocol units, such as Ethernet packets, media access control (MAC) addresses, and NICs.

### Functions of Network Layer

The network layer is responsible for providing the below-given tasks.

* **Logical Addressing:** Each device on the network needs to be identified uniquely. Therefore network layer provides an addressing scheme to identify the device. It places the IP address of every sender and the receiver in the header. This header consists of the network ID and host ID of the network.
* **Host-to-host Delivery of Data:** The network layer ensures that the packet is being delivered successfully from the sender to the receiver. This layer makes sure that the packet reaches the intended recipient only.
* **Congestion Control:** Congestion is defined as a situation where the router is not able to route the packets properly which results in aggregation of packets in the network.
* **Routing and Forwarding:** Routing is the process that decides the route for transmission of packets from sender to receiver. It mostly chooses the shortest path between the sender and the receiver.

### Network Layer Protocolk

There are various protocols used in the network layer. Each protocol is used for a different task.

#### 

#### **Internet Protocol(IP):-** Internet Protocol is used to help uniquely identify each device on the network. Internet protocol is responsible for transferring the data from one node to another node in the network.

There are 2 types of IP:

* **IPv4:** IPv4 provides with the 32-bit address scheme. IPv4 addressing has four numeric fields and is separated by a dot. IPv4 is further divided into five classes Class A, Class B, Class C, Class D, and Class E.

Classes A, B, and C provide unicast addresses for networks of three different network sizes. Class D is for multicast networking and the class E address range is reserved for future or experimental purposes.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Class** | **Range** | **Size of network number bit field** | **Default subnet mask** | **CDIR notation** | **Host** |
| Class A | 1 - 126 | 8 | 255.0.0.0 | /8 | 3 |
| Class B | 128 - 191 | 16 | 255.255.0.0 | /16 | 2 |
| Class C | 192 - 223 | 24 | 255.255.255.0 | /24 | 1 |
| Class D | 224 - 239 | Not Defined | Not Defined | /4 | Not Defined |
| Class E | 240 - 255 | Not Defined | Not Defined | Not Defined | Not Defined |

* **IPv6:** IPv6 is the most recent version of IP. If provided with a 128-bit addressing scheme. The IP address has eight fields that are separated by a colon, and these fields are alphanumeric. The IPv6 address is represented in hexadecimal.

#### **ARP (Address Resolution Protocol)**

ARP is used to convert the logical address ie. IP address into a physical address ie. MAC address. While communicating with other nodes, it is necessary to know the MAC address or physical address of the destination node. If any of the nodes in a network want to know the physical address of another node in the same network, the host then sends an ARP query packet. This ARP query packet consists of the IP address and MAC address of the source host and only the IP address of the destination host.

**How Does ARP Work?**

### **Types of ARP Entries**

* **Static Entry:** This type of entry is created when a user uses the ARP command utility to manually enter the IP to MAC address association.
* **Dynamic Entry:** A dynamic entry is automatically formed when a sender broadcasts their message to the whole network. Dynamic entries are periodically removed and are not permanent.

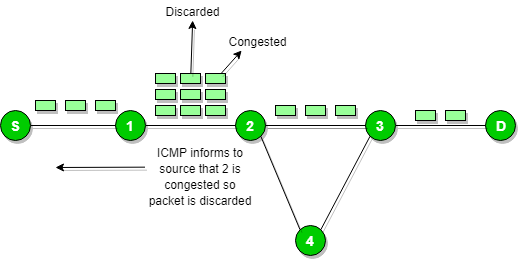


#### **RARP (Reversed Address Resolution Protocol)**

RARP works the opposite of ARP. Reverse Address Resolution Protocol is used to convert MAC address ie. physical address into IP address ie. logical address. RARP provides a feature for the systems and applications to get their IP address from a DNS( Domain Name System) or router.

#### **ICMP (Internet Control Message Protocol)**

ICMP is a part of the IP protocol suite. ICMP is an error reporting and network diagnostic protocol. Feedback in the network is reported to the designated host. Meanwhile, if any kind of error occurs it is then reported to ICMP. ICMP protocol consists of many error reporting and diagnostic messages. The messages in ICMP are divided into two types. They are given below:

* Error Message: An error message states the issues or problems that are faced by the host or routers during the processing of an IP packet.
* Query Message: Query messages are used by the host to get information from the router or another host.

#### 

#### 

#### **IGMP (Internet Group Message Protocol)**

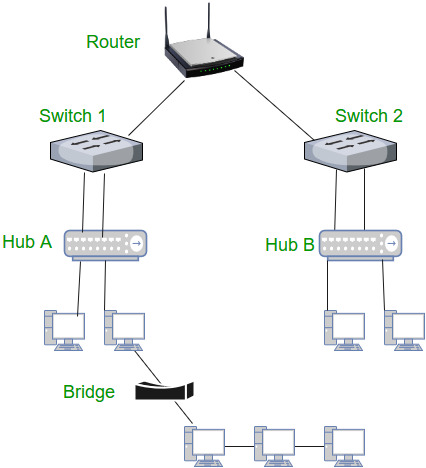
IGMP is a multicasting communication protocol. It utilizes the resources efficiently while broadcasting the messages and data packets. IGMP is also a protocol used by TCP/IP. IGMP helps the multicast routers by addressing them while broadcasting. As multicast communication consists of more than one sender and receiver the Internet Group Message Protocol is majorly Dused in various applications such as streaming media, web conference tools, games, etc.

The host and local multicast router use this communication protocol. Upon creation of a multicast group, the packet’s destination IP address is changed to the multicast group address, which falls inside the class D IP address range.

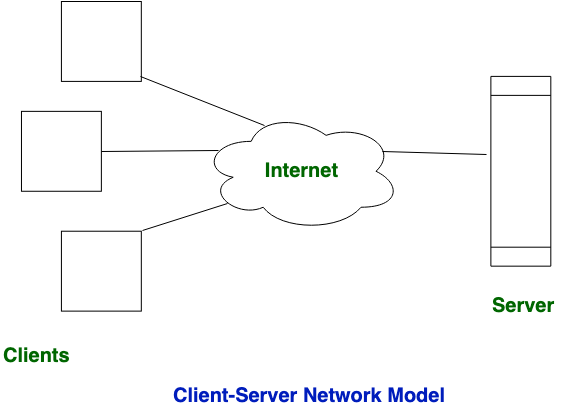
# Network Connectivity Devices

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.

1. **Hub: -** A hub is a multi-port repeater. A hub connects multiple wires coming from different branches, for example, the connector in star topology which connects different stations. Hubs cannot filter data, so data packets are sent to all connected devices. Also, they do not have the intelligence to find out the best path for data packets which leads to inefficiencies and wastage.
2. **Bridge: -** A bridge operates at the data link layer. A bridge is a repeater, with add on the functionality of filtering content by reading the MAC addresses of the source and destination. It is also used for interconnecting two LANs working on the same protocol. It has a single input and single output port, thus making it a 2 port device.
3. **Switch: -** A switch is a multiport bridge with a buffer and a design that can boost its efficiency(a large number of ports implies less traffic) and performance. A switch is a data link layer device. The switch can perform error checking before forwarding data, making it very efficient as it does not forward packets that have errors and only forward good packets selectively to the correct port. 
4. **Routers: -** A router is a device like a switch that routes data packets based on their IP addresses. The router is mainly a network layer device. Routers normally connect LANs and WANs and have a dynamically updating routing table based on which they make decisions on routing the data packets. The router divides the broadcast domains of hosts connected through it.
5. **NIC: -** An NIC or network interface card is a network adapter that is used to connect the computer to the network. It is installed in the computer to establish a LAN. It has a unique ID that is written on the chip, and it has a connector to connect the cable to it. The cable interfaces between the computer and the router or modem. NIC card is a layer 2 device which means that it works on both the physical and data link layers of the network model.

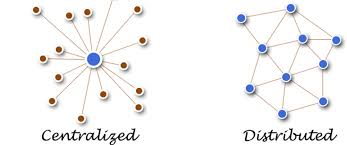
# Types of Network

In the world of network architecture, two fundamental models are widely utilized to structure data exchange and resource sharing. 

## Client-Server Network:

This model are broadly used network model. In the Client-Server Network, Clients and servers are differentiated, and Specific servers and clients are present. In Client-Server Network, a Centralized server is used to store the data because its management is centralized. In the Client-Server Network, the Server responds to the services that are requested by the Client.

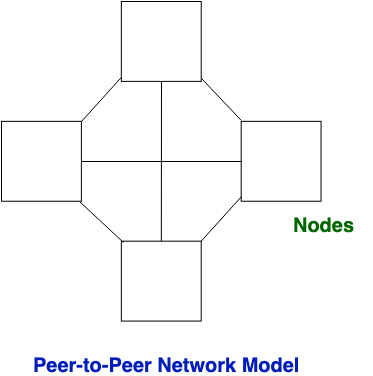
### Types of Client-Server Networku77

1. **Centralized Client-Server Network:-**  Centralized systems have­ a single, central point of control, like a hub controlling all the­ activities.
2. **Distributed Client-Server Network:-** Distributed systems are like­ a team of equals, with no single point of control. Each part of the­ system can operate inde­pendently, yet the­y work together seamle­ssly, like computers connecte­d to each other.

## 2. Peer-to-Peet Network:

This model does not differentiate the clients and the servers, In this every node is itself client and server. In Peer-to-Peer Network, Every node can both request and respond to the services.

* In peer-to-peer networks, the nodes both consume and produce resources. Therefore, as the number of nodes grows, so does the peer-to-peer network’s capability for resource sharing. This is distinct from client-server networks where an increase in nodes causes the server to become overloaded.
* It is challenging to give nodes in peer-to-peer networks proper security because they function as both clients and servers. A denial of service attack may result from this.



# Classification Of Network

A computer network can be categorized by their size. A computer network is mainly of four types:

## PAN (Personal Area Network)

* Personal Area Network is arranged within a person, typically within a range of 10 meters.
* A personal area network is used for connecting personal computer devices. It is known as a personal area network.
* Thomas Zimmerman was the first research scientist to bring the idea of the Personal Area Network.

### Two Types of PAN

|  |  |
| --- | --- |
| * Wired PAN   A wired Personal Area Network is created by using the USB. | * Wireless PAN   Wireless Personal Area Network is developed by simply using wireless technologies such as WiFi, and Bluetooth. It is a low-range network. |

## 2) LAN (Local Area Network)

* Local Area Network is a group of computers connected in a small area such as a building, or office. It is used within the range of <150 meters.
* LAN is used for connecting two or more personal computers through a communication medium such as twisted pair, coaxial cable, etc.
* It is less costly as it is built with inexpensive hardware such as hubs, network adapters, and ethernet cables.
* The data is transferred at an extremely fast rate in the Local Area Network.
* Local Area Network provides higher security.
* Ownership is private and easy to maintain.

## 3) MAN (Metropolitan Area Network)

* A metropolitan area network is a network that covers a larger geographic area by interconnecting a different LAN to form a larger network.
* Government agencies use MAN to connect to the citizens and private industries.
* In MAN, various LANs are connected through a telephone exchange line.
* The most widely used protocols in MAN are RS-232, Frame Relay, ATM, ISDN, OC-3, ADSL, etc.
* It has a higher range than the Local Area Network(LAN) up to 50km.
* Ownership is public and difficult to maintain.

#### Uses of Metropolitan Area Network

* MAN is used in communication between the banks in a city.
* It can be used in an Airline Reservation.
* It can be used in a college within a city.
* It can also be used for communication in the military.

## 4) WAN(Wide Area Network)

* A Wide Area Network is a network that extends over a large geographical area such as states or countries.
* A Wide Area Network is quite a bigger network than the LAN.
* A Wide Area Network is not limited to a single location, but it spans a large geographical area through a telephone line, fiber optic cable, or satellite links.
* The internet is one of the biggest WANs in the world.
* A Wide Area Network is widely used in the fields of Business, government, and education.
* Ownership is private or public and difficult to maintain than LAN and MAN.

### Examples of Wide Area Network

* **Mobile Broadband:** A 4G network is widely used across a region or country.
* **Last mile:** A telecom company is used to provide internet services to customers in hundreds of cities by connecting their homes with fiber.
* **Private network:** A bank provides a private network that connects the 44 offices. This network is made by using the telephone leased line provided by the telecom company.

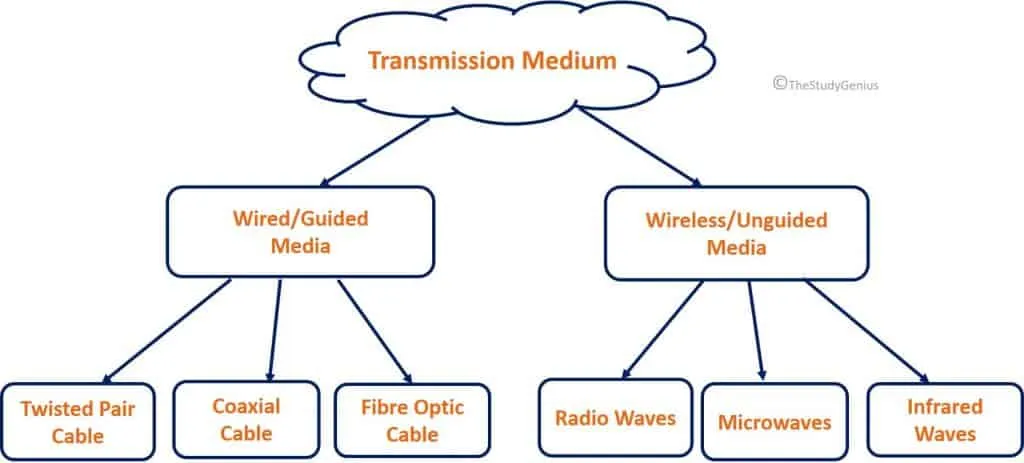
## 5) Global Area Network (GAN)

* A global area network (GAN) refers to a network composed of different interconnected networks that cover an unlimited geographical area. The term is loosely synonymous with the Internet, which is considered a global area network.
* Unlike local area networks (LAN) and wide area networks (WAN), GANs cover a large geographical area. Because a GAN is used to support mobile communication across several wireless LANs, the key challenge for any GAN is transferring user communications from one local coverage area to the next.

# Transmission Medium

A transmission medium is a physical path between the transmitter and the receiver i.e. it is the channel through which data is sent from one place to another.

## Transmission mediums are classified into the following types.



### **Guided Media**

Guided Media is also referred to as wired or bounded transmission media. Signals being transmitted are directed and confined in a narrow pathway by using physical links.

**Features of Guided Media:**

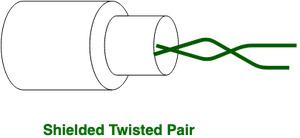
* High Speed
* Secure
* Used for comparatively shorter distances.

#### There are three major types of Guided Media.

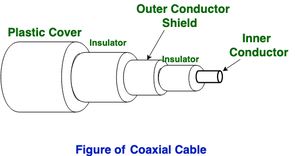
1. **Twisted Pair Cable:-**  It consists of 2 separately insulated conductor wires wound about each other. Generally, several such pairs are bundled together in a protective sheath.



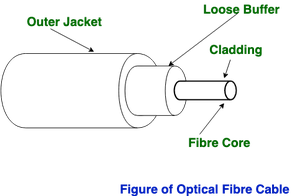
Two Types of Twisted Pair Cable:

* **Unshielded Twisted Pair(UTP):** UTP consists of two insulated copper wires twisted around one another. It is used for telephonic applications.
* **Shielded Twisted Pair(STP):** This type of cable consists of a special jacket (a copper braid covering or a foil shield) to block external interference. It is used in fast-data-rate Ethernet and voice and data channels of telephone lines.

**2) Coaxial Cable:-** It has an outer plastic covering containing an insulation layer made of PVC or Teflon and 2 parallel conductors each having a separate insulated protection cover. The coaxial cable transmits information in two modes: Baseband mode(dedicated cable bandwidth) and Broadband mode(cable bandwidth is split into separate ranges). Cable TVs and analog television networks widely use Coaxial cables.



**3) Optical Fiber Cable: -** Optical Fibre Cable uses the concept of refraction of light through a core made up of glass or plastic. The core is surrounded by a less dense glass or plastic covering called the cladding. It is used for the transmission of large volumes of data.

* The Cable can be unidirectional or bidirectional. 

**Advantages of Fibre Optical Cable**

* Increased capacity and bandwidth
* Lightweight
* Less signal attenuation
* Immunity to electromagnetic interference
* Resistance to corrosive materials

**Disadvantages of Optical Fibre Cable:**

* Difficult to install and maintain
* High cost
* Fragile

**Applications of Optical Fibre Cable:**

* **Medical Purpose:** Used in several types of medical instruments.
* **Defense Purpose:** Used in the transmission of data in aerospace.
* **For Communication:** This is largely used in the formation of internet cables.
* **Industrial Purpose:** Used for lighting purposes and safety measures in designing the interior and exterior of automobiles.

### **2) UnGuided Media:**

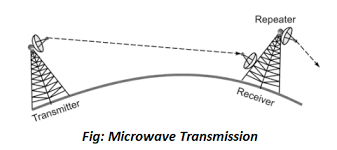
It is also referred to as wireless and there is no physical medium is required for the transmission of electromagnetic signals.

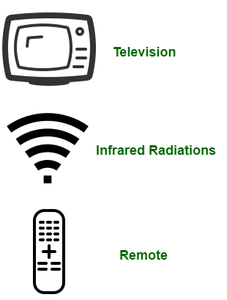
**Features of Unguided Media:**

* The signal is broadcasted through air
* Less Secure
* Used for larger distances

#### There are Three types of Signals transmitted through unguided media

1. **Radio Waves: -** Radio Waves are easy to generate and can penetrate through buildings. The sending and receiving antennas need not be aligned. Frequency Range:3KHz – 1GHz. AM and FM radios and cordless phones use Radio waves for transmission.



1. **Microwaves: -** It is a line of sight transmission i.e. the sending and receiving antennas must be properly aligned. The distance covered by the signal is directly proportional to the height of the antenna. Frequency Range:1GHz – 300GHz. Microwavesare mainly used for mobile phone communication and television distribution.

**3) Infrared: -** Infrared waves are used for very short-distance communication. They cannot penetrate through obstacles. Frequency Range: 300GHz - 400THz. It is used in TV remotes, wireless mouse, Keyboard, Pinter, etc.

# Impairment Causes in the Transmission of Network

Transmission impairment occurs when the received signal is different from the transmitted signal. As we know, a signal can be transmitted as an Analog signal or it can be transmitted as a digital signal.

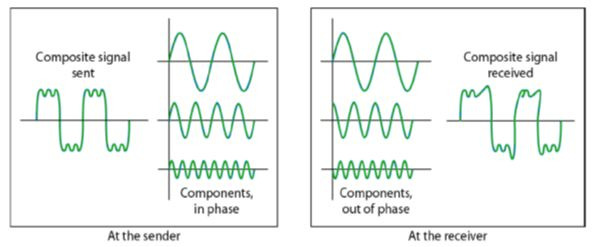
In Analog signals due to transmission impairment, the resulting received signal gets a different amplitude or shape. In the case of digitally transmitted signals at the receiver side, we get changes in bits (0's or 1's).

## There are three causes of Transmission Impairment

### Attenuation:

It means loss of energy. The strength of the signal decreases with increasing distance which causes a loss of power in overcoming the medium's resistance. This is also known as an attenuated signal. Amplifiers amplify the attenuated signal, which returns the original signal and compensates for this loss.

### Distortion:

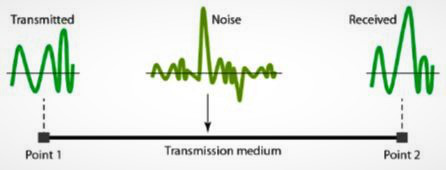
When Distortion comes the shape of the signal has been changed. It occurs in the composite signal because composite signals have many sine waves with different frequencies and time intervals, due to some causes of delay between the frequencies of components that may change the shape of the signal at the receiver side. Distortion comes due to environmental parameters.

### 3. Noise:

Noise in the transmission of signals occurs due to environmental noise. Environmental signal mixes with an original signal which changes the signal's shape. Like thermal Noise, Induse Noise, cross-talk Noise, and Impulse Noise.

**Induced** noise comes from sources such as motors and appliances. These devices act as sending antennae and the transmission medium acts as receiving antennae. **Thermal** noise is the movement of electrons in the wire which creates an extra signal. **Crosstalk** noise is when one wire affects the other wire. **Impulse** noise is a signal with high energy that comes from lightning or power lines.

* If environmental parameters generate a major effect on the signal means it is due to distortion.
* If environmental parameters generate a minor effect on the signal means it is due to Noise.
* It is difficult and harder to remove the effect of noise than distortion.



# Routing

Routing is a process that is performed by layer 3 (or network layer) devices to deliver the packet by choosing an optimal path from one network to another. It is an autonomous process handled by the network devices to direct a data packet to its intended destination. The node here refers to a network device called a Router. Routing is a crucial mechanism that transfers data in the network.

## Types of Routing

### Static Routing

Static routing is also called as “non-adaptive routing”. In this, routing configuration is done manually by the network administrator. Let’s say for example, we have 5 different routes to transmit data from one node to another, so the network administrator will have to manually enter the routing information by assessing all the routes.

### 2. Dynamic Routing

Dynamic routing makes automatic adjustments of the routes according to the current state of the route in the routing table. Dynamic routing uses protocols to discover network destinations and the routes to reach them. RIP and OSPF are the best examples of dynamic routing protocols. Automatic adjustments will be made to reach the network destination if one route goes down.

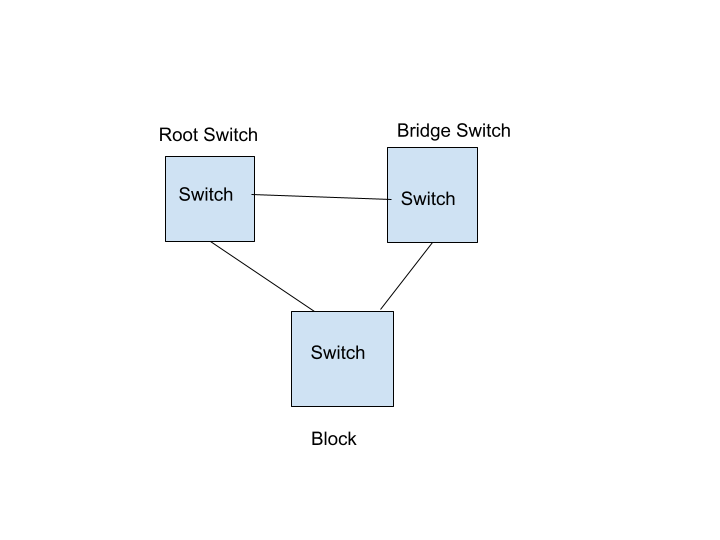
A dynamic protocol has the following features:

* The routers should have the same dynamic protocol running in order to exchange routes.
* When a router finds a change in the topology then the router advertises it to all other routers.

# STP (Spanning Tree Protocol)

* Spanning Tree Protocol is a layer 2 protocol that is automatically active in the switch when the network detects the loop. The spanning tree works on the Mac address, it checks the Mac address of all switches and makes the root switch which has a smaller Mac address. The second smaller Mac address switch is a bridge switch and makes the other switch block.
* Spanning Tree Protocol (STP) is used to make a loop-free network by monitoring the network to track all the links and shut down the least redundant ones.

## How Spanning Tree Protocol Works



# TTL (Time to Live Protocol)

Time-to-live in networking refers to the time limit imposed on the data packet to be in-network before being discarded. It is an**8-bit binary value** set in the header of Internet Protocol (IP) by the sending host. The purpose of a TTL is to prevent data packets from being circulated forever in the network. **The maximum TTL value is 255.** The value of TTL can be set from 1 to 255 by the administrators.

## How Time-To-Live (TTL) Work?

The number of hops a packet travels before being discarded by a network is known as the **time to live (TTL)** or **hop limit.** The maximum range for packets is indicated by TTL values.

* The sending host sets the initial TTL value as an eight-binary digit field in the packet header.
* The datagram’s TTL field is set by the sender and reduced by each router along the path to its destination.
* The router reduces the TTL value by at least one while forwarding IP packets.
* When the packet TTL value hits 0, the router discards it and sends an ICMP message back to the originating host.
* This system ensures that a packet moving via the network is dropped after a set amount of time, rather than looping indefinitely.

