Physical layer in the OSI model plays the role of interacting with actual hardware and signaling mechanism. Physical layer is the only layer of OSI network model which actually deals with the physical connectivity of two different stations. This layer defines the hardware equipment, cabling, wiring, frequencies, pulses used to represent binary signals etc.

Physical layer provides its services to Data-link layer. Data-link layer hands over frames to physical layer. Physical layer converts them to electrical pulses, which represent binary data.The binary data is then sent over the wired or wireless media.

Signals

When data is sent over physical medium, it needs to be first converted into electromagnetic signals. Data itself can be analog such as human voice, or digital such as file on the disk.Both analog and digital data can be represented in digital or analog signals.

* **Digital Signals**

Digital signals are discrete in nature and represent sequence of voltage pulses. Digital signals are used within the circuitry of a computer system.

* **Analog Signals**

Analog signals are in continuous wave form in nature and represented by continuous electromagnetic waves.

Transmission Impairment

When signals travel through the medium they tend to deteriorate. This may have many reasons as given:

* **Attenuation**

For the receiver to interpret the data accurately, the signal must be sufficiently strong.When the signal passes through the medium, it tends to get weaker.As it covers distance, it loses strength.

* **Dispersion**

As signal travels through the media, it tends to spread and overlaps. The amount of dispersion depends upon the frequency used.

* **Delay distortion**

Signals are sent over media with pre-defined speed and frequency. If the signal speed and frequency do not match, there are possibilities that signal reaches destination in arbitrary fashion. In digital media, this is very critical that some bits reach earlier than the previously sent ones.

* **Noise**

Random disturbance or fluctuation in analog or digital signal is said to be Noise in signal, which may distort the actual information being carried. Noise can be characterized in one of the following class:

* + **Thermal Noise**

Heat agitates the electronic conductors of a medium which may introduce noise in the media. Up to a certain level, thermal noise is unavoidable.

* + **Intermodulation**

When multiple frequencies share a medium, their interference can cause noise in the medium. Intermodulation noise occurs if two different frequencies are sharing a medium and one of them has excessive strength or the component itself is not functioning properly, then the resultant frequency may not be delivered as expected.

* + **Crosstalk**

This sort of noise happens when a foreign signal enters into the media. This is because signal in one medium affects the signal of second medium.

* + **Impulse**

This noise is introduced because of irregular disturbances such as lightening, electricity, short-circuit, or faulty components. Digital data is mostly affected by this sort of noise.

Transmission Media

The media over which the information between two computer systems is sent, called transmission media. Transmission media comes in two forms.

* **Guided Media**

All communication wires/cables are guided media, such as UTP, coaxial cables, and fiber Optics. In this media, the sender and receiver are directly connected and the information is send (guided) through it.

* **Unguided Media**

Wireless or open air space is said to be unguided media, because there is no connectivity between the sender and receiver. Information is spread over the air, and anyone including the actual recipient may collect the information.

Channel Capacity

The speed of transmission of information is said to be the channel capacity. We count it as data rate in digital world. It depends on numerous factors such as:

* **Bandwidth:**  The physical limitation of underlying media.
* **Error-rate:**  Incorrect reception of information because of noise.
* **Encoding:**  The number of levels used for signaling.

Multiplexing

Multiplexing is a technique to mix and send multiple data streams over a single medium. This technique requires system hardware called multiplexer (MUX) for multiplexing the streams and sending them on a medium, and de-multiplexer (DMUX) which takes information from the medium and distributes to different destinations.

For any networking to be effective, raw stream of data is to be transported from one device to other over some medium. Various transmission media can be used for transfer of data. These transmission media may be of two types −

* **Guided** − In guided media, transmitted data travels through cabling system that has a fixed path. For example, copper wires, fibre optic wires, etc.
* **Unguided** − In unguided media, transmitted data travels through free space in form of electromagnetic signal. For example, radio waves, lasers, etc.

Each transmission media has its own advantages and disadvantages in terms of bandwidth, speed, delay, cost per bit, ease of installation and maintenance, etc. Let’s discuss some of the most commonly used media in detail.

## Twisted Pair Cable

Copper wires are the most common wires used for transmitting signals because of good performance at low costs. They are most commonly used in telephone lines. However, if two or more wires are lying together, they can interfere with each other’s signals. To reduce this electromagnetic interference, pair of copper wires are twisted together in helical shape like a DNA molecule. Such twisted copper wires are called **twisted pair**. To reduce interference between nearby twisted pairs, the twist rates are different for each pair.



Up to 25 twisted pair are put together in a protective covering to form twisted pair cables that are the backbone of telephone systems and Ethernet networks.

### Advantages of twisted pair cable

Twisted pair cable are the oldest and most popular cables all over the world. This is due to the many advantages that they offer −

* Trained personnel easily available due to shallow learning curve
* Can be used for both analog and digital transmissions
* Least expensive for short distances
* Entire network does not go down if a part of network is damaged

### Disadvantages of twisted pair cable

With its many advantages, twisted pair cables offer some disadvantages too −

* Signal cannot travel long distances without repeaters
* High error rate for distances greater than 100m
* Very thin and hence breaks easily
* Not suitable for broadband connections

## Shielding twisted pair cable

To counter the tendency of twisted pair cables to pick up noise signals, wires are shielded in the following three ways −

* Each twisted pair is shielded.
* Set of multiple twisted pairs in the cable is shielded.
* Each twisted pair and then all the pairs are shielded.

Such twisted pairs are called **shielded twisted pair (STP) cables**. The wires that are not shielded but simply bundled together in a protective sheath are called **unshielded twisted pair (UTP) cables**. These cables can have maximum length of 100 metres.

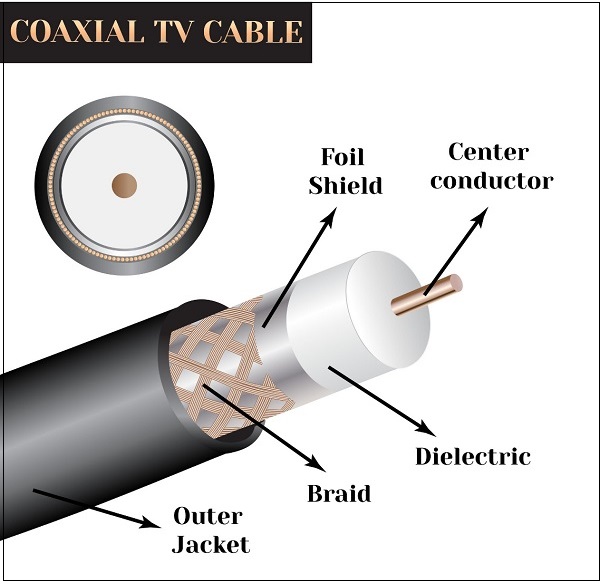
Shielding makes the cable bulky, so UTP are more popular than STP. UTP cables are used as the last mile network connection in homes and offices.

## Coaxial Cable

**Coaxial cables** are copper cables with better **shielding** than twisted pair cables, so that transmitted signals may travel longer distances at higher speeds. A coaxial cable consists of these layers, starting from the innermost −

* Stiff copper wire as **core**
* **Insulating material** surrounding the core
* Closely woven braided mesh of **conducting material**surrounding the **insulator**
* Protective **plastic sheath** encasing the wire

Coaxial cables are widely used for **cable TV** connections and **LANs**.



### Advantages of Coaxial Cables

These are the advantages of coaxial cables −

* Excellent noise immunity
* Signals can travel longer distances at higher speeds, e.g. 1 to 2 Gbps for 1 Km cable
* Can be used for both analog and digital signals
* Inexpensive as compared to fibre optic cables
* Easy to install and maintain

### Disadvantages of Coaxial Cables

These are some of the disadvantages of coaxial cables −

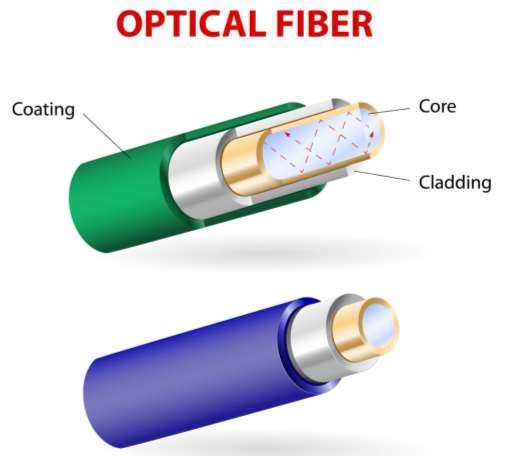
* Expensive as compared to twisted pair cables
* Not compatible with twisted pair cables

## Optical Fibre

Thin glass or plastic threads used to transmit data using light waves are called **optical fibre**. Light Emitting Diodes (LEDs) or Laser Diodes (LDs) emit light waves at the **source**, which is read by a **detector** at the other end. **Optical fibre cable** has a bundle of such threads or fibres bundled together in a protective covering. Each fibre is made up of these three layers, starting with the innermost layer −

* **Core** made of high quality **silica glass** or **plastic**
* **Cladding** made of high quality **silica glass** or **plastic**, with a lower refractive index than the core
* Protective outer covering called **buffer**

Note that both core and cladding are made of similar material. However, as **refractive index** of the cladding is lower, any stray light wave trying to escape the core is reflected back due to **total internal reflection**.



Optical fibre is rapidly replacing copper wires in telephone lines, internet communication and even cable TV connections because transmitted data can travel very long distances without weakening. **Single node** fibre optic cable can have maximum segment length of 2 kms and bandwidth of up to 100 Mbps. **Multi-node** fibre optic cable can have maximum segment length of 100 kms and bandwidth up to 2 Gbps.

### Advantages of Optical Fibre

Optical fibre is fast replacing copper wires because of these advantages that it offers −

* High bandwidth
* Immune to electromagnetic interference
* Suitable for industrial and noisy areas
* Signals carrying data can travel long distances without weakening

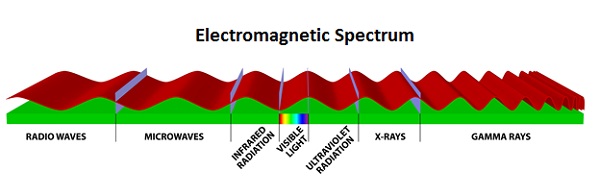
### Disadvantages of Optical Fibre

Despite long segment lengths and high bandwidth, using optical fibre may not be a viable option for every one due to these disadvantages −

* Optical fibre cables are expensive
* Sophisticated technology required for manufacturing, installing and maintaining optical fibre cables
* Light waves are unidirectional, so two frequencies are required for full duplex transmission

## Infrared

Low frequency infrared waves are used for very short distance communication like TV remote, wireless speakers, automatic doors, hand held devices etc. Infrared signals can propagate within a room but cannot penetrate walls. However, due to such short range, it is considered to be one of the most secure transmission modes.



## Radio Wave

Transmission of data using radio frequencies is called **radio-wave transmission**. We all are familiar with radio channels that broadcast entertainment programs. Radio stations transmit radio waves using **transmitters**, which are received by the receiver installed in our devices.

Both transmitters and receivers use antennas to radiate or capture radio signals. These radio frequencies can also be used for **direct voice communication** within the **allocated range**. This range is usually 10 miles.



### Advantages of Radio Wave

These are some of the advantages of radio wave transmissions −

* Inexpensive mode of information exchange
* No land needs to be acquired for laying cables
* Installation and maintenance of devices is cheap

### Disadvantages of Radio Wave

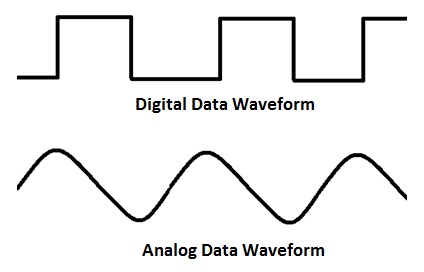
These are some of the disadvantages of radio wave transmissions −

* Insecure communication medium
* Prone to weather changes like rain, thunderstorms, etc.

Hardware devices that are used to connect computers, printers, fax machines and other electronic devices to a network are called **network devices**. These devices transfer data in a fast, secure and correct way over same or different networks. Network devices may be inter-network or intra-network. Some devices are installed on the device, like NIC card or RJ45 connector, whereas some are part of the network, like router, switch, etc. Let us explore some of these devices in greater detail.

Modem

Modem is a device that enables a computer to send or receive data over telephone or cable lines. The data stored on the computer is digital whereas a telephone line or cable wire can transmit only analog data.



The main function of the modem is to convert digital signal into analog and vice versa. Modem is a combination of two devices − **modulator** and **demodulator**. The **modulator** converts digital data into analog data when the data is being sent by the computer. The **demodulator** converts analog data signals into digital data when it is being received by the computer.

Types of Modem

Modem can be categorized in several ways like direction in which it can transmit data, type of connection to the transmission line, transmission mode, etc.

Depending on direction of data transmission, modem can be of these types −

* **Simplex** − A simplex modem can transfer data in only one direction, from digital device to network (modulator) or network to digital device (demodulator).
* **Half duplex** − A half-duplex modem has the capacity to transfer data in both the directions but only one at a time.
* **Full duplex** − A full duplex modem can transmit data in both the directions simultaneously.

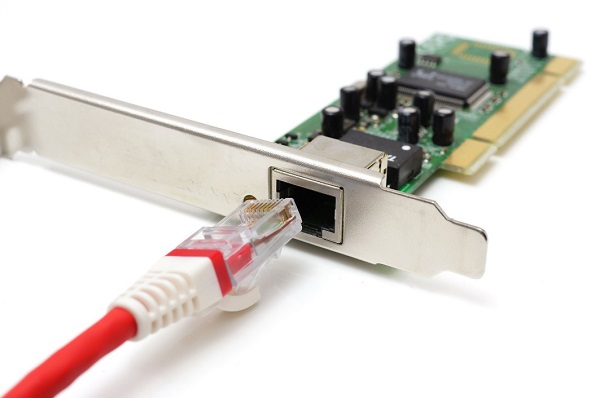
RJ45 Connector

RJ45 is the acronym for **Registered Jack 45. RJ45 connector**is an 8-pin jack used by devices to physically connect to **Ethernet** based **local area networks (LANs)**. **Ethernet** is a technology that defines protocols for establishing a LAN. The cable used for Ethernet LANs are twisted pair ones and have **RJ45 connector pins** at both ends. These pins go into the corresponding socket on devices and connect the device to the network.



Ethernet Card

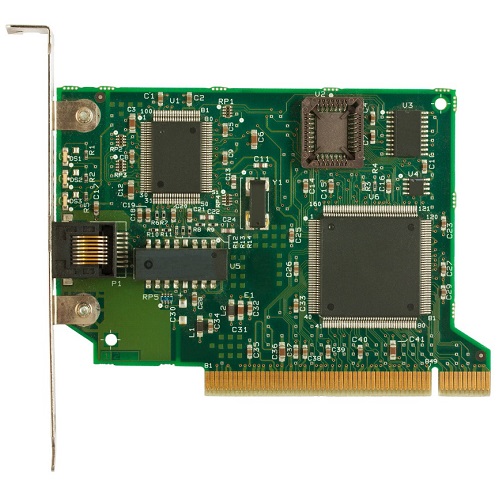
**Ethernet card**, also known as **network interface card (NIC)**, is a hardware component used by computers to connect to **Ethernet LAN** and communicate with other devices on the LAN. The earliest **Ethernet cards** were external to the system and needed to be installed manually. In modern computer systems, it is an internal hardware component. The NIC has **RJ45 socket**where network cable is physically plugged in.



**Ethernet card speeds** may vary depending upon the protocols it supports. Old Ethernet cards had maximum speed of **10 Mbps**. However, modern cards support fast Ethernets up to a speed of **100 Mbps**. Some cards even have capacity of **1 Gbps**.

Router

A **router** is a **network layer** hardware device that transmits data from one LAN to another if both networks support the same set of protocols. So a **router** is typically connected to at least two LANs and the **internet service provider** (ISP). It receives its data in the form of **packets**, which are **data frames** with their **destination address** added. Router also strengthens the signals before transmitting them. That is why it is also called **repeater**.



Routing Table

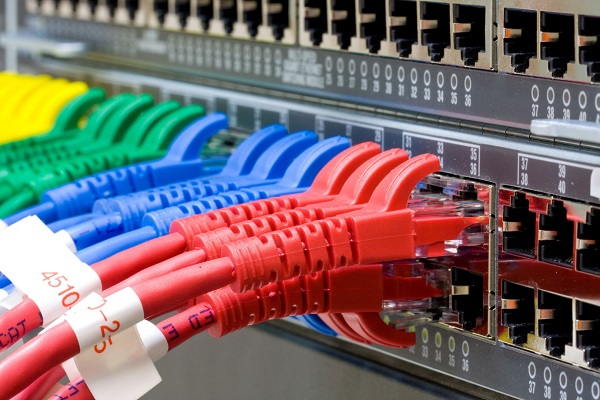
A router reads its routing table to decide the best available route the packet can take to reach its destination quickly and accurately. The routing table may be of these two types −

* **Static** − In a static routing table the routes are fed manually. So it is suitable only for very small networks that have maximum two to three routers.
* **Dynamic** − In a dynamic routing table, the router communicates with other routers through protocols to determine which routes are free. This is suited for larger networks where manual feeding may not be feasible due to large number of routers.

Switch

**Switch** is a network device that connects other devices to **Ethernet** networks through **twisted pair** cables. It uses **packet switching** technique to **receive, store** and **forward data packets** on the network. The switch maintains a list of network addresses of all the devices connected to it.

On receiving a packet, it checks the destination address and transmits the packet to the correct port. Before forwarding, the packets are checked for collision and other network errors. The data is transmitted in full duplex mode



Data transmission speed in switches can be double that of other network devices like hubs used for networking. This is because switch shares its maximum speed with all the devices connected to it. This helps in maintaining network speed even during high traffic. In fact, higher data speeds are achieved on networks through use of multiple switches.

Gateway

**Gateway** is a network device used to connect two or more dissimilar networks. In networking parlance, networks that use different protocols are **dissimilar networks**. A gateway usually is a computer with multiple **NICs** connected to different networks. A gateway can also be configured completely using software. As networks connect to a different network through gateways, these gateways are usually hosts or end points of the network.



**Gateway** uses **packet switching** technique to transmit data from one network to another. In this way it is similar to a **router**, the only difference being router can transmit data only over networks that use same protocols.

Wi-Fi Card

**Wi-Fi** is the acronym for **wireless fidelity. Wi-Fi technology**is used to achieve **wireless connection** to any network. **Wi-Fi card** is a **card** used to connect any device to the local network wirelessly. The physical area of the network which provides internet access through Wi-Fi is called **Wi-Fi hotspot**. Hotspots can be set up at home, office or any public space. Hotspots themselves are connected to the network through wires.

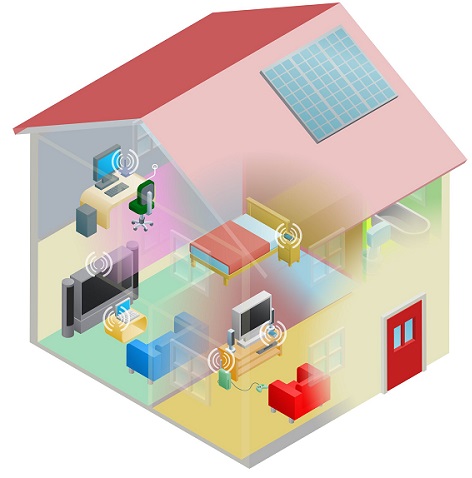


A **Wi-Fi card** is used to add capabilities like **teleconferencing, downloading** digital camera images, **video chat**, etc. to old devices. Modern devices come with their in-built **wireless network adapter**.

Networks can be categorized depending on size, complexity, level of security, or geographical range. We will discuss some of the most popular topologies based on geographical spread.

PAN

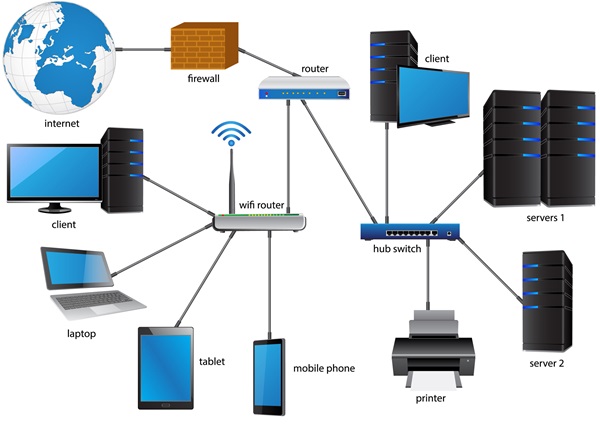
PAN is the acronym for Personal Area Network. PAN is the interconnection between devices within the range of a person’s private space, typically within a range of 10 metres. If you have transferred images or songs from your laptop to mobile or from mobile to your friend’s mobile using Bluetooth, you have set up and used a personal area network.



A person can connect her laptop, smart phone, personal digital assistant and portable printer in a network at home. This network could be fully Wi-Fi or a combination of wired and wireless.

LAN

LAN or Local Area Network is a wired network spread over a single site like an office, building or manufacturing unit. LAN is set up to when team members need to share software and hardware resources with each other but not with the outside world. Typical software resources include official documents, user manuals, employee handbook, etc. Hardware resources that can be easily shared over the network include printer, fax machines, modems, memory space, etc. This decreases infrastructure costs for the organization drastically.



A LAN may be set up using wired or wireless connections. A LAN that is completely wireless is called Wireless LAN or WLAN.

MAN

MAN is the acronym for Metropolitan Area Network. It is a network spread over a city, college campus or a small region. MAN is larger than a LAN and typically spread over several kilometres. Objective of MAN is to share hardware and software resources, thereby decreasing infrastructure costs. MAN can be built by connecting several LANs.



The most common example of MAN is cable TV network.

WAN

WAN or Wide Area Network is spread over a country or many countries. WAN is typically a network of many LANs, MANs and WANs. Network is set up using wired or wireless connections, depending on availability and reliability.



The most common example of WAN is the Internet.

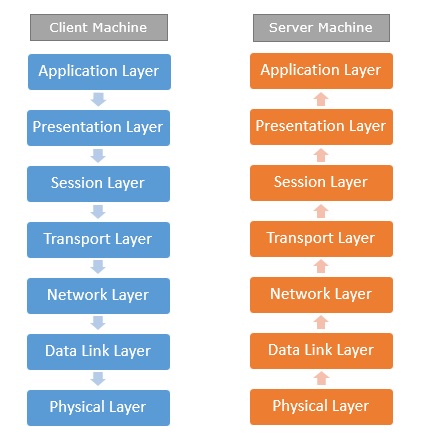
**Network Protocols** are a set of rules governing exchange of information in an easy, reliable and secure way. Before we discuss the most common protocols used to transmit and receive data over a network, we need to understand how a network is logically organized or designed. The most popular model used to establish open communication between two systems is the **Open Systems Interface (OSI) model** proposed by ISO.

OSI Model

OSI model is not a **network architecture** because it does not specify the exact services and protocols for each layer. It simply tells what each layer should do by defining its input and output data. It is up to network architects to implement the layers according to their needs and resources available.

These are the seven layers of the OSI model −

* **Physical layer** −It is the first layer that physically connects the two systems that need to communicate. It transmits data in bits and manages simplex or duplex transmission by modem. It also manages Network Interface Card’s hardware interface to the network, like cabling, cable terminators, topography, voltage levels, etc.
* **Data link layer** − It is the firmware layer of Network Interface Card. It assembles datagrams into frames and adds start and stop flags to each frame. It also resolves problems caused by damaged, lost or duplicate frames.
* **Network layer** − It is concerned with routing, switching and controlling flow of information between the workstations. It also breaks down transport layer datagrams into smaller datagrams.
* **Transport layer** − Till the session layer, file is in its own form. Transport layer breaks it down into data frames, provides error checking at network segment level and prevents a fast host from overrunning a slower one. Transport layer isolates the upper layers from network hardware.
* **Session layer** − This layer is responsible for establishing a session between two workstations that want to exchange data.
* **Presentation layer** − This layer is concerned with correct representation of data, i.e. syntax and semantics of information. It controls file level security and is also responsible for converting data to network standards.
* **Application layer** − It is the topmost layer of the network that is responsible for sending application requests by the user to the lower levels. Typical applications include file transfer, E-mail, remote logon, data entry, etc.



It is not necessary for every network to have all the layers. For example, network layer is not there in broadcast networks.

When a system wants to share data with another workstation or send a request over the network, it is received by the application layer. Data then proceeds to lower layers after processing till it reaches the physical layer.

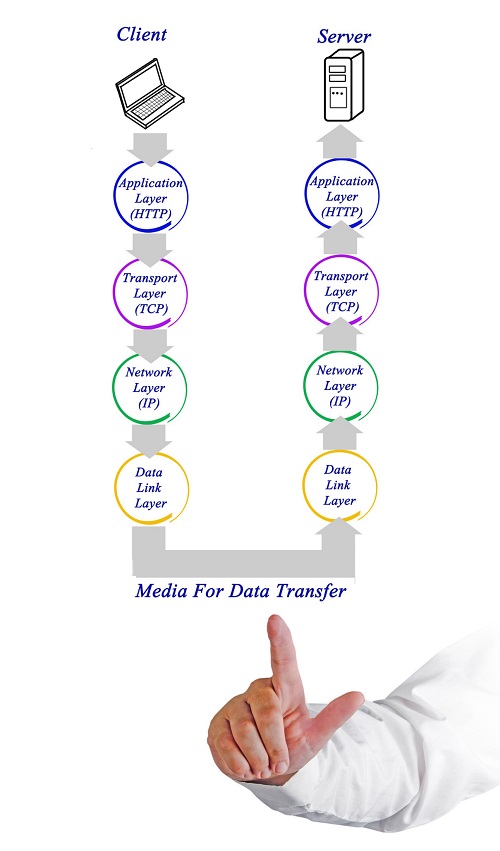
At the physical layer, the data is actually transferred and received by the physical layer of the destination workstation. There, the data proceeds to upper layers after processing till it reaches application layer.

At the application layer, data or request is shared with the workstation. So each layer has opposite functions for source and destination workstations. For example, data link layer of the source workstation adds start and stop flags to the frames but the same layer of the destination workstation will remove the start and stop flags from the frames.

Let us now see some of the protocols used by different layers to accomplish user requests.

TCP/IP

TCP/IP stands for **Transmission Control Protocol/Internet Protocol**. TCP/IP is a set of layered protocols used for communication over the Internet. The communication model of this suite is client-server model. A computer that sends a request is the client and a computer to which the request is sent is the server.



TCP/IP has four layers −

* **Application layer** − Application layer protocols like HTTP and FTP are used.
* **Transport layer** − Data is transmitted in form of datagrams using the Transmission Control Protocol (TCP). TCP is responsible for breaking up data at the client side and then reassembling it on the server side.
* **Network layer** − Network layer connection is established using Internet Protocol (IP) at the network layer. Every machine connected to the Internet is assigned an address called IP address by the protocol to easily identify source and destination machines.
* **Data link layer** − Actual data transmission in bits occurs at the data link layer using the destination address provided by network layer.

TCP/IP is widely used in many communication networks other than the Internet.

FTP

As we have seen, the need for network came up primarily to facilitate sharing of files between researchers. And to this day, file transfer remains one of the most used facilities.The protocol that handles these requests is **File Transfer Protocol** or **FTP**.

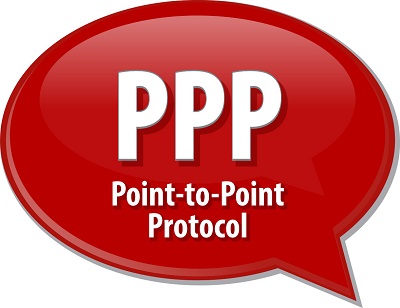


Using FTP to transfer files is helpful in these ways −

* Easily transfers files between two different networks
* Can resume file transfer sessions even if connection is dropped, if protocol is configure appropriately
* Enables collaboration between geographically separated teams

PPP

Point to Point Protocol or PPP is a data link layer protocol that enables transmission of TCP/IP traffic over serial connection, like telephone line.



To do this, PPP defines these three things −

* A framing method to clearly define end of one frame and start of another, incorporating errors detection as well.
* Link control protocol (LCP) for bringing communication lines up, authenticating and bringing them down when no longer needed.
* Network control protocol (NCP) for each network layer protocol supported by other networks.

Using PPP, home users can avail Internet connection over telephone lines.

## GPRS

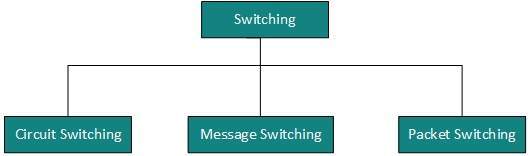
GPRS stands for General Packet Radio Services. It is a packet based wireless communication technology that charges users based on the volume of data they send rather than the time duration for which they are using the service. This is possible because GPRS sends data over the network in packets and its throughput depends on network traffic. As traffic increases, service quality may go down due to congestion, hence it is logical to charge the users as per data volume transmitted.

GPRS is the mobile communication protocol used by second (2G) and third generation (3G) of mobile telephony. It pledges a speed of 56 kbps to 114 kbps, however the actual speed may vary depending on network load.

Switching

Switching is a mechanism by which data/information sent from source towards destination which are not directly connected. Networks have interconnecting devices, which receives data from directly connected sources, stores data, analyze it and then forwards to the next interconnecting device closest to the destination.

Switching can be categorized as:



Switching is process to forward packets coming in from one port to a port leading towards the destination. When data comes on a port it is called ingress, and when data leaves a port or goes out it is called egress. A communication system may include number of switches and nodes. At broad level, switching can be divided into two major categories:

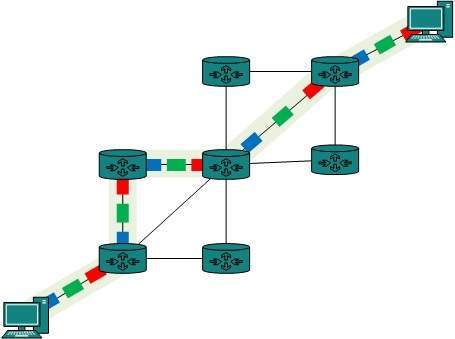
* **Connectionless:** The data is forwarded on behalf of forwarding tables. No previous handshaking is required and acknowledgements are optional.
* **Connection Oriented:**  Before switching data to be forwarded to destination, there is a need to pre-establish circuit along the path between both endpoints. Data is then forwarded on that circuit. After the transfer is completed, circuits can be kept for future use or can be turned down immediately.

Circuit Switching

When two nodes communicate with each other over a dedicated communication path, it is called circuit switching.There 'is a need of pre-specified route from which data will travels and no other data is permitted.In circuit switching, to transfer the data, circuit must be established so that the data transfer can take place.

Circuits can be permanent or temporary. Applications which use circuit switching may have to go through three phases:

* Establish a circuit
* Transfer the data
* Disconnect the circuit

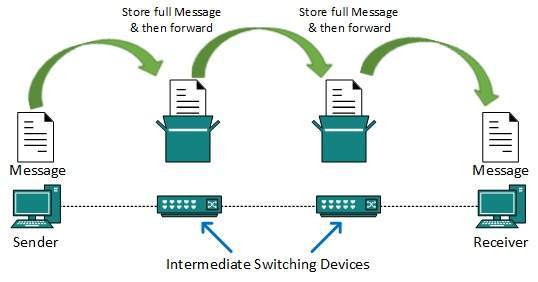


Circuit switching was designed for voice applications. Telephone is the best suitable example of circuit switching. Before a user can make a call, a virtual path between caller and callee is established over the network.

Message Switching

This technique was somewhere in middle of circuit switching and packet switching. In message switching, the whole message is treated as a data unit and is switching / transferred in its entirety.

A switch working on message switching, first receives the whole message and buffers it until there are resources available to transfer it to the next hop. If the next hop is not having enough resource to accommodate large size message, the message is stored and switch waits.



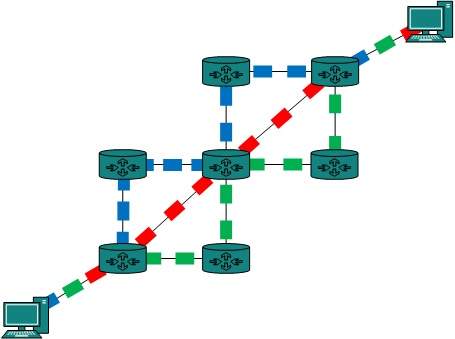
This technique was considered substitute to circuit switching. As in circuit switching the whole path is blocked for two entities only. Message switching is replaced by packet switching. Message switching has the following drawbacks:

* Every switch in transit path needs enough storage to accommodate entire message.
* Because of store-and-forward technique and waits included until resources are available, message switching is very slow.
* Message switching was not a solution for streaming media and real-time applications.

Packet Switching

Shortcomings of message switching gave birth to an idea of packet switching. The entire message is broken down into smaller chunks called packets. The switching information is added in the header of each packet and transmitted independently.

It is easier for intermediate networking devices to store small size packets and they do not take much resources either on carrier path or in the internal memory of switches.



Packet switching enhances line efficiency as packets from multiple applications can be multiplexed over the carrier. The internet uses packet switching technique. Packet switching enables the user to differentiate data streams based on priorities. Packets are stored and forwarded according to their priority to provide quality of service.