./

Learning Report – Networking



|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Ver. Rel. No.** | **Release Date** | **Prepared. By** | **Reviewed By** | **Approved By** | **Remarks/Revision Details** |
| 1 | 30/01/2021 | Prathviraj  (99003123) |  |  |  |

**Document History**

Table of Contents

[ACTIVITY 1: 5](#_Toc63069862)

[Advantages and Disadvantages of mobile towers near residence: 5](#_Toc63069863)

[Advantages: - 5](#_Toc63069864)

[Disadvantages: - 6](#_Toc63069865)

[ACTIVITY 2 7](#_Toc63069866)

[OSI layers & its Functions 7](#_Toc63069867)

[ Layer 1 - Physical 7](#_Toc63069868)

[ Layer 2 – Data Link 7](#_Toc63069869)

[ Layer 3 - Network 7](#_Toc63069870)

[ Layer 4 – Transport 7](#_Toc63069871)

[ Layer 5 - Session 8](#_Toc63069872)

[ Layer 6 - Presentation 8](#_Toc63069873)

[ Layer 7 - Application 8](#_Toc63069874)

[ACTIVITY 3 9](#_Toc63069875)

[COMPONENTS OF NETWORKING 9](#_Toc63069876)

[Hub: - 9](#_Toc63069877)

[Switches: 10](#_Toc63069878)

[Routers: 10](#_Toc63069879)

[Bridges: 10](#_Toc63069880)

[NETWORKING PROTOCOLS 12](#_Toc63069881)

[Gateway: 12](#_Toc63069882)

[Transmission Control Protocol (TCP) 12](#_Toc63069883)

[User Datagram Protocol (UDP) 13](#_Toc63069884)

[Internet Protocol (IP) 13](#_Toc63069885)

[Types of WLAN Protocols 15](#_Toc63069886)

[Key Differences Between LAN, MAN and WAN: 16](#_Toc63069887)

[Wired technologies 18](#_Toc63069888)

[Wireless technologies 20](#_Toc63069889)

[Types of Topology 21](#_Toc63069890)

[1. Mesh Topology 21](#_Toc63069891)

[2. Star Topology 21](#_Toc63069892)

[3. Bus Topology 22](#_Toc63069893)

[4. Ring Topology 22](#_Toc63069894)

[5. Hybrid Topology 22](#_Toc63069895)

[What is IPv4? 22](#_Toc63069896)

[Drawback of IPv4: 23](#_Toc63069897)

[What Is IPv6? 23](#_Toc63069898)

[Address format 24](#_Toc63069899)

[Understanding Sub netting In Ipv4 24](#_Toc63069900)

**Table of Figures**

[Figure 1: OSI LAYERS 9](file:///D:\Networking\Networkking_99003123_Prathviraj.docx#_Toc63069901)

[Figure 2: BRIDGE 10](#_Toc63069902)

[Figure 3: Networking Devices 11](#_Toc63069903)

# ACTIVITY 1:

# Advantages and Disadvantages of mobile towers near residence:

## Advantages: -

1. **Income:** The telecommunication companies and service providers pay rents upto Rs. 30,000 or sometimes more when competition is high among them, for the installation of the towers. This is good source of income for the property owners and institutions.
2. **Frequency:** Radiation of mobile towers is insignificant with small area covered. It’s frequency is minute, hence there is no need to worry about health hazards.
3. **Rules and regulation:** The proper authorization of the mobile towers is a must nowadays due to the strict rules directed by the government. A large number of unauthorized towers have been sealed over last few years and people responsible are fined heavily.
4. **Revenue:** If a new tower has to be added to the area, it is probably better to be the landowner receiving revenue from it than being on a neighboring property and having to look at it while receiving nothing.
5. **Low Maintenance Tenants:** Unlike commercial tenants or residential tenants, there is no maintenance burden (or very little) when it comes to cell tower tenants. They maintain their own lease area.
6. **Transferable Asset:** In most cases, the lease can be sold in the future. Lease buyout companies typically pay 15 times the annual lease rate or more for a lease buyout. Where else can you sell a lease for that multiple of annual income?
7. **Highest and Best Use:** This is an appraisal term which means that it is rare that landowners to receive more income from other non-cell tower uses on the same property. The typical land lease is 2,500 to 5,000 square feet. In many cases, there aren’t other uses that would pay the same lease rate for that limited space.

## Disadvantages: -

1. **Electromagnetic radiations:** If you go for expert advice, they would tell you that living within 50m of a mobile tower is like being stuck in a microwave oven for the entire day. The electromagnetic radiations are cancerous elements that are straightforward lethal for health.
2. **Unauthorized constructions:** Out of all the mobile phone towers in metropolitan cities, a shocking 45% of them are illegal. They did not follow the norms that are set for the purpose and ignorantly put the lives of people at risk of cancer and other disastrous ailments.
3. **Birds on the go:** The most notable effect of mobile tower radiation has been seen on birds. The numbers of local birds like sparrows have started to dwindle from the residential areas where mobile towers have been installed. The mobile towers are known to emit microwaves that are found to damage bird eggs and embryos as they cause thinning of the skulls of chicks as well as eggshells.
4. **On children and unborn:** Children have thinner skulls and are hence known to be more affected by radiation from mobile phone towers. The same applies for pregnant woman carrying an underdeveloped child. The penetration of radiation is easier on them and the effect could be really disastrous if not kept under check. Children these days are known to have less concentration power – one of the effects of having cellular towers in residential areas, near schools and hospitals.
5. **Other issues:**

* While cancer is the biggest threat to people living in the vicinity of a mobile phone tower, there are other health issues too. People in the area experience sleep disorders, fatigue, headache, memory loss, depression, hearing problems, joint pains, skin diseases, and even cardiovascular problems.
* Mobile phone towers make air toxic. There are indicative studies to prove that the electromagnetic radiation is harmful to the people living in the 300-meter radius of the towers.
* According to established norms, the radiation level of 600 milli watts per meter square (mw/m. sq.) is considered safe. But mobile phone towers emit electromagnetic rays above the safe limit.
* Some cell phone companies set up unauthorized towers, also called as “camouflage towers”, which looks like a palm tree, street light, chimney or water tanks. These are illegal and does not follow any norms to be followed since they are unauthorized.

# ACTIVITY 2

# OSI layers & its Functions

## Layer 1 - Physical

At the bottom of our OSI bean dip we have the Physical Layer, which represents the electrical and physical representation of the system. This can include everything from the cable type, radio frequency link (as in an 802.11 wireless systems), as well as the layout of pins, voltages and other physical requirements. When a networking problem occurs, many networking pros go right to the physical layer to check that all of the cables are properly connected and that the power plug hasn’t been pulled from the router, switch or computer.

## Layer 2 – Data Link

The Data Link Layer provides node-to-node data transfer (between two directly connected nodes), and also handles error correction from the physical layer. Two sublayers exist here as well - the Media Access Control (MAC) layer and the Logical Link Control (LLC) layer. In the networking world, most switches operate at Layer 2. But it's not that simple. Some switches also operate at Layer 3 in order to support virtual LANs that may span more than one switch subnet, which requires routing capabilities.

## Layer 3 - Network

Here at the Network Layer is where you’ll find most of the router functionality that most networking professionals care about and love. In its most basic sense, this layer is responsible for packet forwarding, including routing through different routers. You might know that your Boston computer wants to connect to a server in California, but there are millions of different paths to take. Routers at this layer help do this efficiently.

## Layer 4 – Transport

The Transport Layer deals with the coordination of the data transfer between end systems and hosts. How much data to send, at what rate, where it goes, etc. The best known example of the Transport Layer is the Transmission Control Protocol (TCP), which is built on top of the Internet Protocol (IP), commonly known as TCP/IP. TCP and UDP port numbers work at Layer 4, while IP addresses work at Layer 3, the Network Layer.

## Layer 5 - Session

When two devices, computers or servers need to “speak” with one another, a session needs to be created, and this is done at the Session Layer**.** Functions at this layer involve setup, coordination (how long should a system wait for a response, for example) and termination between the Chrome, Firefox, Safari, etc.) TelNet, and FTP, are examples of communications  that rely  on Layer 7.

## Layer 6 - Presentation

The Presentation Layer represents the area that is independent of data representation at the application layer. In general, it represents the preparation or translation of application format to network format, or from network formatting to application format. In other words, the layer “presents” data for the application or the network. A good example of this is encryption and decryption of data for secure transmission - this happens at Layer 6.

## Layer 7 - Application

To further our bean dip analogy, the Application Layer is the one at the top--it’s what most users see. In the OSI model, this is the layer that is the “closest to the end user”. It receives information directly from users and displays incoming data it to the user. Oddly enough, applications themselves do not reside at the application layer. Instead the layer facilitates communication through lower layers in order to establish connections with applications at the other end.

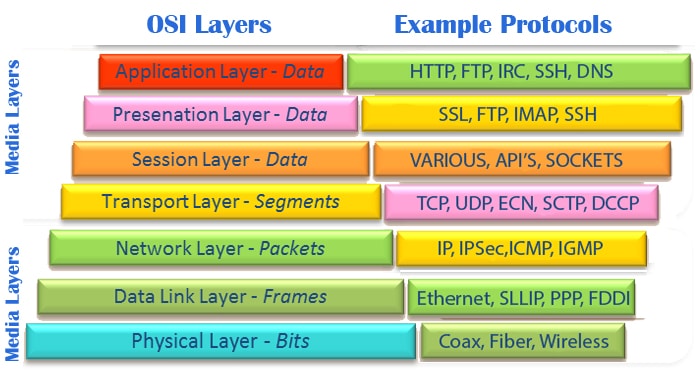


Figure 1: OSI LAYERS

# ACTIVITY 3

# COMPONENTS OF NETWORKING

## Hub: -

A hub is a physical layer networking device which is used to connect multiple devices in a network. They are generally used to connect computers in a LAN.

A hub has many ports in it. A computer which intends to be connected to the network is plugged in to one of these ports. When a data frame arrives at a port, it is broadcast to every other port, without considering whether it is destined for a particular destination or not.

## Switches:

A switch is a data link layer networking device which connects devices in a network and uses packet switching to send and receive data over the network.

Like a hub, a switch also has many ports, to which computers are plugged in. However, when a data frame arrives at any port of a network switch, it examines the destination address and sends the frame to the corresponding device(s). Thus, it supports both unicast and multicast communications.

## Routers:

Routers are networking devices operating at layer 3 or a network layer of the OSI model. They are responsible for receiving, analysing, and forwarding data packets among the connected computer networks. When a data packet arrives, the router inspects the destination address, consults its routing tables to decide the optimal route and then transfers the packet along this route.

## Bridges:

A bridge is a network device that connects multiple LANs (local area networks) together to form a larger LAN. The process of aggregating networks is called network bridging. A bridge connects the different components so that they appear as parts of a single network. Bridges operate at the data link layer of the OSI model and hence also referred as Layer 2 switches.

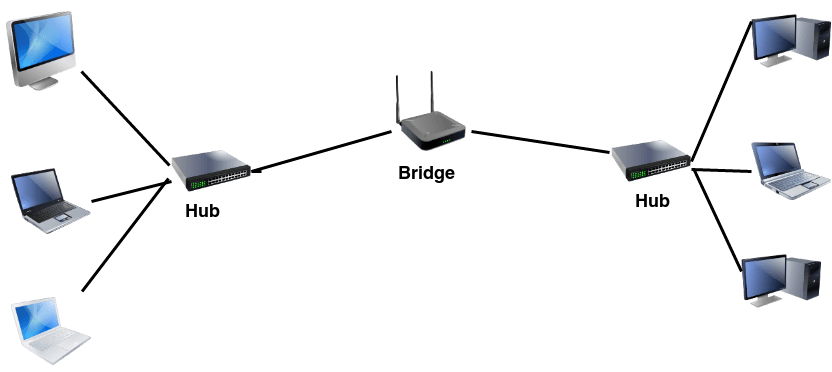


Figure 2: BRIDGE

The following diagram shows all the components in the networking devices:

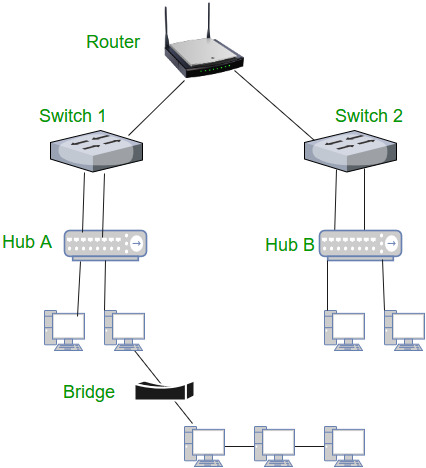


Figure 3: Networking Devices

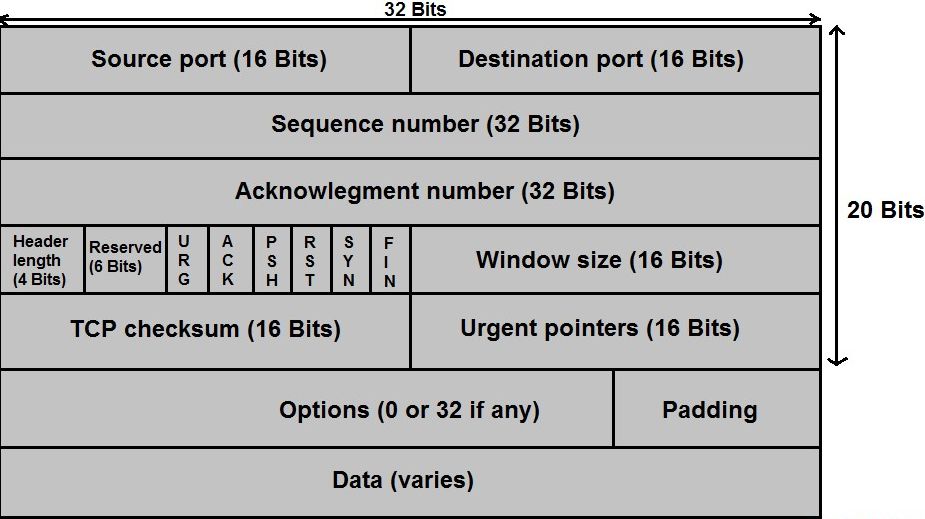
# NETWORKING PROTOCOLS

## Gateway:

A gateway is a network node that forms a passage between two networks operating with different transmission protocols. The most common type of gateways, the network gateway operates at layer 3, i.e. network layer of the OSI (open systems interconnection) model. However, depending upon the functionality, a gateway can operate at any of the seven layers of OSI model. It acts as the entry – exit point for a network since all traffic that flows across the networks should pass through the gateway. Only the internal traffic between the nodes of a LAN does not pass through the gateway.

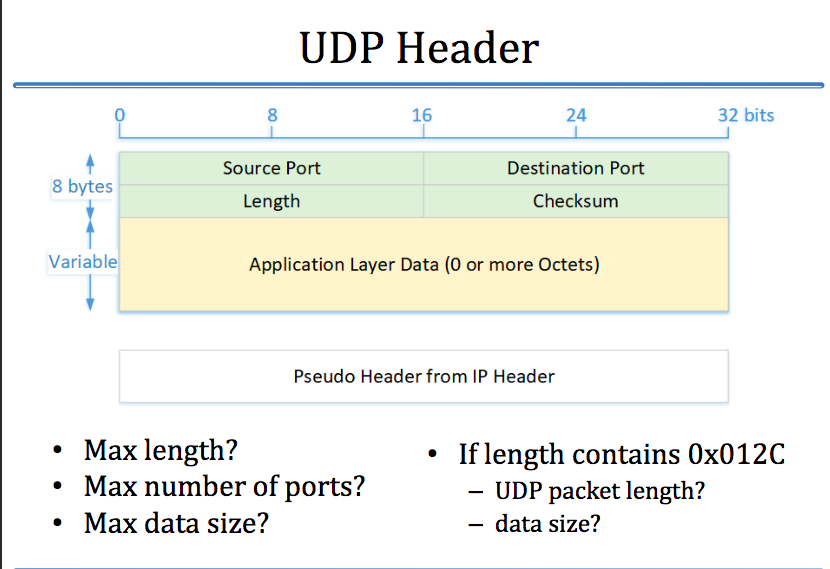
## Transmission Control Protocol (TCP)

In terms of the OSI model, TCP is a transport-layer protocol. It provides a reliable virtual-circuit connection between applications; that is, a connection is established before data transmission begins. Data is sent without errors or duplication and is received in the same order as it is sent. No boundaries are imposed on the data; TCP treats the data as a stream of bytes.



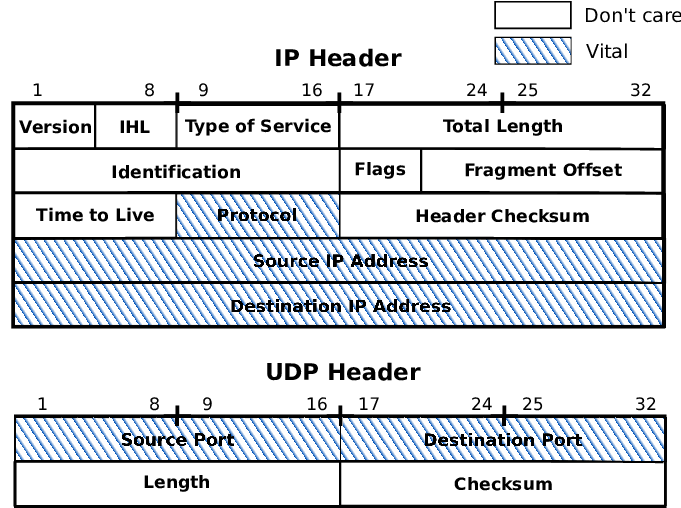
## User Datagram Protocol (UDP)

UDP is also a transport-layer protocol and is an alternative to TCP. It provides an unreliable datagram connection between applications. Data is transmitted link by link; there is no end-to-end connection. The service provides no guarantees. Data can be lost or duplicated, and datagrams can arrive out of order.



## Internet Protocol (IP)

It is a protocol defined in the TCP/IP model used for sending the packets from source to destination. The main task of IP is to deliver the packets from source to the destination based on the IP addresses available in the packet headers. IP defines the packet structure that hides the data which is to be delivered as well as the addressing method that labels the datagram with a source and destination information.



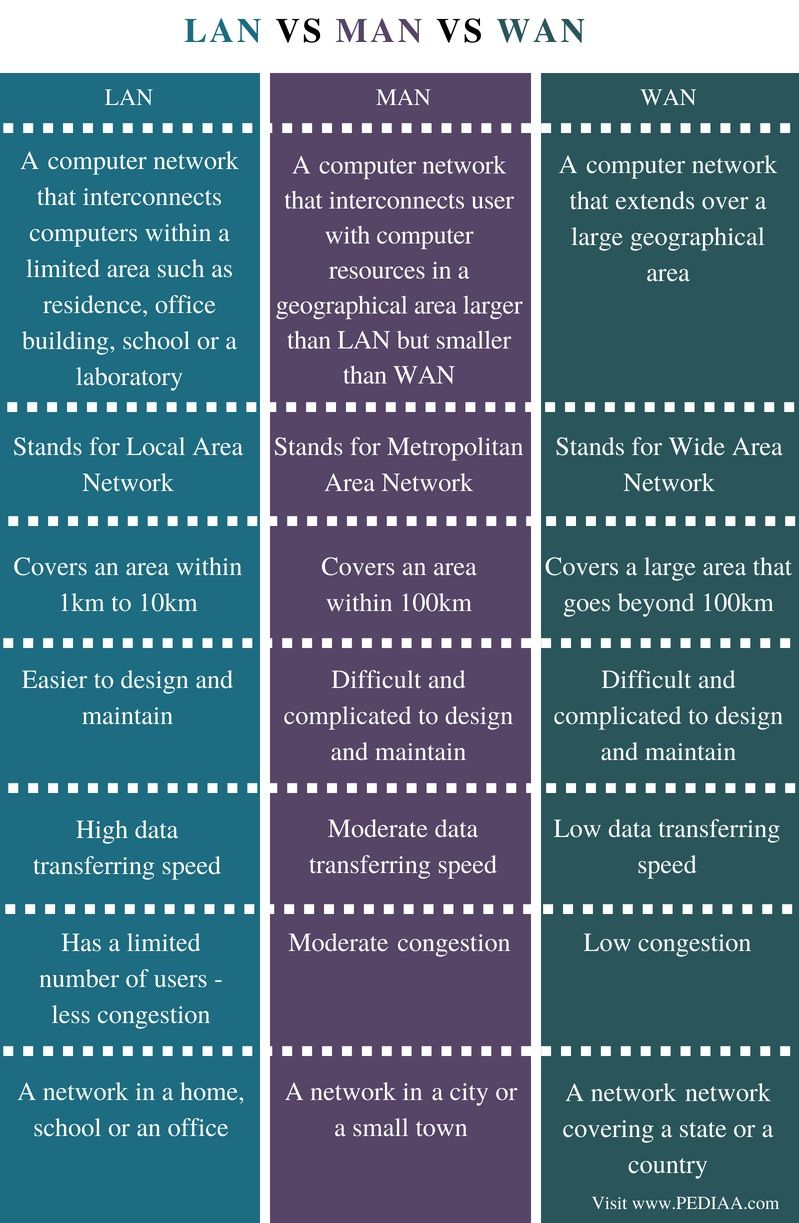
## Types of WLAN Protocols

IEEE 802.11 or WiFi has a number of variations, the main among which are −

* **802.11a Protocol**− This protocol supports very high transmission speeds of 54Mbps. It has a high frequency of 5GHz range, due to which signals have difficulty in penetrating walls and other obstructions. It employs Orthogonal Frequency Division Multiplexing (OFDM).
* **802.11b Protocol** − This protocol operates within the frequency range of 2.4GHz and supports 11Mbps speed. It facilitates path sharing and is less vulnerable to obstructions. It uses Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) with Ethernet protocol.
* **802.11g Protocol** − This protocol combines the features of 802.11a and 802.11b protocols. It supports both the frequency ranges 5GHz (as in 802.11a standard) and 2.4GHz (as in 802.11b standard). Owing to its dual features, 802.11g is backward compatible with 802.11b devices. 802.11g provides high speeds, varying signal range, and resilience to obstruction. However, it is more expensive for implementation.
* **802.11n Protocol** − Popularly known as Wireless N, this is an upgraded version of 802.11g. It provides very high bandwidth up to 600Mbps and provides signal coverage. It uses Multiple Input/Multiple Output (MIMO), having multiple antennas at both the transmitter end and receiver ends. In case of signal obstructions, alternative routes are used. However, the implementation is highly expensive.

## Key Differences Between LAN, MAN and WAN:

1. The geographical area covered by LAN is small, whereas, MAN covers relatively large and WAN covers the greatest of all.
2. LAN is confined to schools, hospitals or buildings, whereas, MAN connects small towns or Cities and on the other hand, WAN covers Country or a group of Countries.
3. Devices used for transmission of data are-  
   LAN: WiFi, Ethernet Cables.  
   MAN: Modem and Wire/Cable  
   WAN: Optic wires, Microwaves, Satellites.
4. LAN’s transmit data at a faster rate than MAN and WAN.
5. Maintenance of LAN is easier than that of MAN and WAN.
6. The bandwidth available for transmission is higher in LAN than MAN and WAN.
7. Data transmission errors and noise are least in LAN, moderate in MAN and high in WAN.



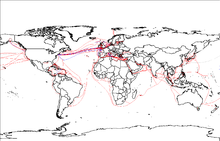
## Wired technologies

[](https://en.wikipedia.org/wiki/File:Fibreoptic.jpg)

Fiber optic cables are used to transmit light from one computer/network node to another

The orders of the following wired technologies are, roughly, from slowest to fastest transmission speed.

* [*Coaxial cable*](https://en.wikipedia.org/wiki/Coaxial_cable) is widely used for cable television systems, office buildings, and other work-sites for local area networks. The cables consist of copper or aluminum wire surrounded by an insulating layer (typically a flexible material with a high dielectric constant), which itself is surrounded by a conductive layer. The insulation helps minimize interference and distortion. Transmission speed ranges from 200 million bits per second to more than 500 million bits per second.
* [*ITU-T*](https://en.wikipedia.org/wiki/ITU-T)[*G.hn*](https://en.wikipedia.org/wiki/G.hn) technology uses existing [home wiring](https://en.wikipedia.org/wiki/Home_wiring) ([coaxial cable](https://en.wikipedia.org/wiki/Ethernet_over_coax), phone lines and [power lines](https://en.wikipedia.org/wiki/Power_line_communication)) to create a high-speed (up to 1 Gigabit/s) local area network.
* [*Signal traces*](https://en.wikipedia.org/wiki/Signal_trace) on [printed circuit boards](https://en.wikipedia.org/wiki/Printed_circuit_board) are common for board-level serial communication, particularly between certain types integrated circuits, a common example being [SPI](https://en.wikipedia.org/wiki/Serial_Peripheral_Interface_Bus).
* [*Ribbon cable*](https://en.wikipedia.org/wiki/Ribbon_cable) (untwisted and possibly unshielded) has been a cost-effective media for serial protocols, especially within metallic enclosures or rolled within copper braid or foil, over short distances, or at lower data rates. Several serial network protocols can be deployed without shielded or twisted pair cabling, that is, with "flat" or "ribbon" cable, or a hybrid flat/twisted ribbon cable, should [EMC](https://en.wikipedia.org/wiki/Electromagnetic_compatibility), length, and [bandwidth](https://en.wikipedia.org/wiki/Bandwidth_(computing)) constraints permit: [RS-232](https://en.wikipedia.org/wiki/RS-232),[[6]](https://en.wikipedia.org/wiki/Network_topology#cite_note-6) [RS-422](https://en.wikipedia.org/wiki/RS-422), [RS-485](https://en.wikipedia.org/wiki/RS-485),[[7]](https://en.wikipedia.org/wiki/Network_topology#cite_note-7) [CAN](https://en.wikipedia.org/wiki/CAN_Bus),[[8]](https://en.wikipedia.org/wiki/Network_topology#cite_note-8) [GPIB](https://en.wikipedia.org/wiki/IEEE-488), [SCSI](https://en.wikipedia.org/wiki/SCSI),[[9]](https://en.wikipedia.org/wiki/Network_topology#cite_note-9) etc.
* [*Twisted pair*](https://en.wikipedia.org/wiki/Twisted_pair)*wire* is the most widely used medium for all telecommunication.[[10]](https://en.wikipedia.org/wiki/Network_topology#cite_note-10) Twisted-pair cabling consist of copper wires that are twisted into pairs. Ordinary telephone wires consist of two insulated copper wires twisted into pairs. Computer network cabling (wired [Ethernet](https://en.wikipedia.org/wiki/Ethernet) as defined by [IEEE 802.3](https://en.wikipedia.org/wiki/IEEE_802.3)) consists of 4 pairs of copper cabling that can be utilized for both voice and data transmission. The use of two wires twisted together helps to reduce [crosstalk](https://en.wikipedia.org/wiki/Crosstalk_(electronics)) and [electromagnetic induction](https://en.wikipedia.org/wiki/Electromagnetic_induction). The transmission speed ranges from 2 million bits per second to 10 billion bits per second. Twisted pair cabling comes in two forms: unshielded twisted pair (UTP) and shielded twisted-pair (STP). Each form comes in several category ratings, designed for use in various scenarios.

[](https://en.wikipedia.org/wiki/File:World_map_of_submarine_cables.png)

2007 map showing submarine optical fiber telecommunication cables around the world.

* An [*optical fiber*](https://en.wikipedia.org/wiki/Optical_fiber) is a glass fiber. It carries pulses of light that represent data. Some advantages of optical fibers over metal wires are very low transmission loss and immunity from electrical interference. Optical fibers can simultaneously carry multiple wavelengths of light, which greatly increases the rate that data can be sent, and helps enable data rates of up to trillions of bits per second. Optic fibers can be used for long runs of cable carrying very high data rates, and are used for [undersea cables](https://en.wikipedia.org/wiki/Undersea_cables) to interconnect continents.

Price is a main factor distinguishing wired- and wireless-technology options in a business. Wireless options command a price premium that can make purchasing wired computers, printers and other devices a financial benefit. Before making the decision to purchase hard-wired technology products, a review of the restrictions and limitations of the selections is necessary. Business and employee needs may override any cost considerations.

## Wireless technologies

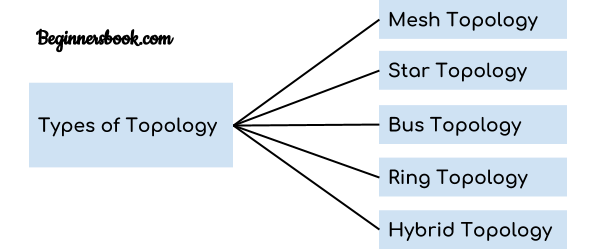
[](https://en.wikipedia.org/wiki/File:Wireless_network.jpg)

Personal computers are very often connected to networks using wireless links

*Main article:*[*Wireless network*](https://en.wikipedia.org/wiki/Wireless_network)

* *Terrestrial*[*microwave*](https://en.wikipedia.org/wiki/Microwave) – Terrestrial microwave communication uses Earth-based transmitters and receivers resembling satellite dishes. Terrestrial microwaves are in the low gigahertz range, which limits all communications to line-of-sight. Relay stations are spaced approximately 50 km (30 mi) apart.
* [*Communications satellites*](https://en.wikipedia.org/wiki/Communications_satellite) – Satellites communicate via microwave radio waves, which are not deflected by the Earth's atmosphere. The satellites are stationed in space, typically in [geostationary orbit](https://en.wikipedia.org/wiki/Geostationary_orbit) 35,786 km (22,236 mi) above the equator. These Earth-orbiting systems are capable of receiving and relaying voice, data, and TV signals.
* [*Cellular*](https://en.wikipedia.org/wiki/Cellular_network)*and PCS systems* use several radio communications technologies. The systems divide the region covered into multiple geographic areas. Each area has a low-power transmitter or radio relay antenna device to relay calls from one area to the next area.
* *Radio and*[*spread spectrum*](https://en.wikipedia.org/wiki/Spread_spectrum)*technologies* – Wireless local area networks use a high-frequency radio technology similar to digital cellular and a low-frequency radio technology. Wireless LANs use spread spectrum technology to enable communication between multiple devices in a limited area. [IEEE 802.11](https://en.wikipedia.org/wiki/IEEE_802.11) defines a common flavor of open-standards wireless radio-wave technology known as [Wi-Fi](https://en.wikipedia.org/wiki/Wi-Fi).
* [*Free-space optical communication*](https://en.wikipedia.org/wiki/Free-space_optical_communication) uses visible or invisible light for communications. In most cases, [line-of-sight propagation](https://en.wikipedia.org/wiki/Line-of-sight_propagation) is used, which limits the physical positioning of communicating devices.

## Types of Topology

There are five types of topology in computer networks:  


1. Mesh Topology  
2. Star Topology  
3. Bus Topology  
4. Ring Topology  
5. Hybrid Topology

### 1. Mesh Topology

In mesh topology each device is connected to every other device on the network through a dedicated point-to-point link. When we say dedicated it means that the link only carries data for the two connected devices only. Lets say we have n devices in the network then each device must be connected with (n-1) devices of the network. Number of links in a mesh topology of n devices would be n(n-1)/2.

### 2. Star Topology

In star topology each device in the network is connected to a central device called hub. Unlike Mesh topology, star topology doesn’t allow direct communication between devices, a device must have to communicate through hub. If one device wants to send data to other device, it has to first send the data to hub and then the hub transmit that data to the designated device.

### 3. Bus Topology

In bus topology there is a main cable and all the devices are connected to this main cable through drop lines. There is a device called tap that connects the drop line to the main cable. Since all the data is transmitted over the main cable, there is a limit of drop lines and the distance a main cable can have.

### 4. Ring Topology

In ring topology each device is connected with the two devices on either side of it. There are two dedicated point to point links a device has with the devices on the either side of it. This structure forms a ring thus it is known as ring topology. If a device wants to send data to another device then it sends the data in one direction, each device in ring topology has a repeater, if the received data is intended for other device then repeater forwards this data until the intended device receives it.

### 5. Hybrid Topology

A combination of two or more topology is known as hybrid topology. For example a combination of star and mesh topology is known as hybrid topology.

## What is IPv4?

IPv4 is a version 4 of IP. It is a current version and the most commonly used IP address. It is a 32-bit address written in four numbers separated by 'dot', i.e., periods. This address is unique for each device.

For example, **66.94.29.13**

The above example represents the IP address in which each group of numbers separated by periods is called an Octet. Each number in an octet is in the range from 0-255. This address can produce 4,294,967,296 possible unique addresses.

In today's computer network world, computers do not understand the IP addresses in the standard numeric format as the computers understand the numbers in binary form only. The binary number can be either 1 or 0. The IPv4 consists of four sets, and these sets represent the octet. The bits in each octet represent a number.

Each bit in an octet can be either 1 or 0. If the bit the 1, then the number it represents will count, and if the bit is 0, then the number it represents does not count.

# Drawback of IPv4:

Currently, the population of the world is 7.6 billion. Every user is having more than one device connected with the internet, and private companies also rely on the internet. As we know that IPv4 produces 4 billion addresses, which are not enough for each device connected to the internet on a planet. Although the various techniques were invented, such as variable- length mask, network address translation, port address translation, classes, inter-domain translation, to conserve the bandwidth of IP address and slow down the depletion of an IP address. In these techniques, public IP is converted into a private IP due to which the user having public IP can also use the internet. But still, this was not so efficient, so it gave rise to the development of the next generation of IP addresses, i.e., IPv6.

## What Is IPv6?

IPv4 produces 4 billion addresses, and the developers think that these addresses are enough, but they were wrong. IPv6 is the next generation of IP addresses. The main difference between IPv4 and IPv6 is the address size of IP addresses. The IPv4 is a 32-bit address, whereas IPv6 is a 128-bit hexadecimal address. IPv6 provides a large address space, and it contains a simple header as compared to IPv4.

It provides transition strategies that convert IPv4 into IPv6, and these strategies are as follows:

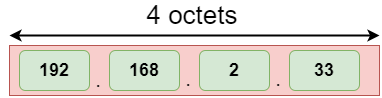
* **Dual stacking:** It allows us to have both the versions, i.e., IPv4 and IPv6, on the same device.
* **Tunneling:** In this approach, all the users have IPv6 communicates with an IPv4 network to reach IPv6.
* **Network Address Translation:** The translation allows the communication between the hosts having a different version of IP.

This hexadecimal address contains both numbers and alphabets. Due to the usage of both the numbers and alphabets, IPv6 is capable of producing over 340 undecillion (3.4\*1038) addresses.

IPv6 is a 128-bit hexadecimal address made up of 8 sets of 16 bits each, and these 8 sets are separated by a colon. In IPv6, each hexadecimal character represents 4 bits. So, we need to convert 4 bits to a hexadecimal number at a time

### Address format

**The address format of IPv4:**



## Understanding Sub netting In Ipv4

Why do we have to subnet a network?

The reason we have to subnet is to proficiently disseminate IP addresses with the consequence of less wastage. This carries us to different inquiries, for example, for what reason do we have to break a single IP address block, and for what reason is the least wastage so significant? Would we be able to just assign a Class A, B, or C address block to a network of any size? To address these inquiries, we will go more inside and out with this subject with the help of real-life examples and scenarios.

How about we assume that you are a network administrator at a company and one day the IT chief allocates a new assignment to you? Sounds fun, so let’s move forward. The task is to update the IP scheme of the organization. He has additionally advised you to utilize an address class that is appropriate for the organization's size and to guarantee that there is insignificant wastage of IP addresses.

The main thing you chose to do was draw a high-level network diagram demonstrating each branch, which shows the number of hosts per branch office and the Wide Area Network (WAN) joins between each branch router:

As should be obvious from the above network diagram, each building has a branch router, and every router is associated with another through a WAN connection. Each branch area has an alternate number of host devices that require an IP address for network correspondence. Now you will follow the following steps to reach your goals:

Step 1 – determining the appropriate class of IP addresses

Step 2 – making subnets (subnetworks)

Step 3 – relegating each network a suitable subnet and computing the ranges

Step 4 – Variable Length Subnet Masking (VLSM) and sub netting a subnet