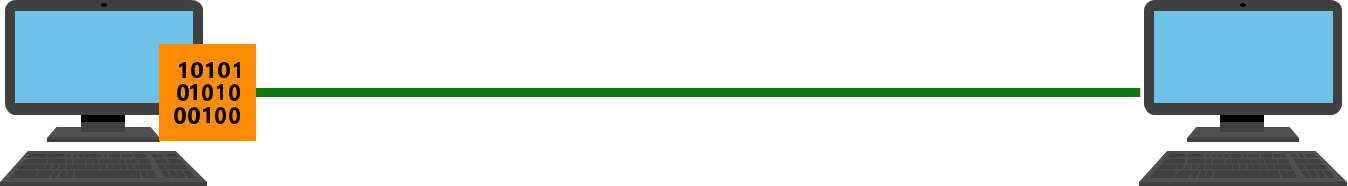
Networking Fundamentals

Network: A network is two devices connected to each other with a physical medium, such as wires or radio signals

The connection allows those two devices to exchange data

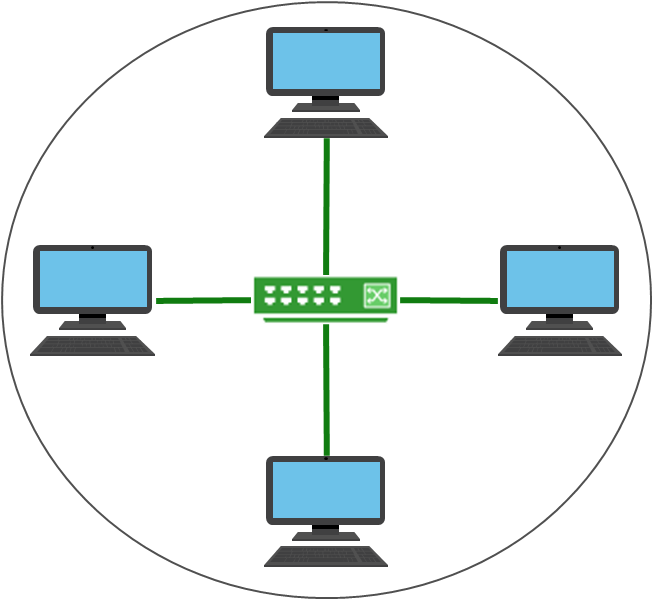


Purpose of Networking:

* communication and collaboration
* sharing information and resources (Files and Printers)
* organizing data
* saving costs
* Different Types Of Networks

How Networks are Organized:

* Networks are organized based on their geographic location
* A Local Area Network, or LAN, is a group of computers or devices that:
  + 1. are confined to a small geographic area, such as a single building
    2. share a common communication medium, such as cabled or wireless connections
    3. are connected to a central connecting device, like a hub, switch, or router

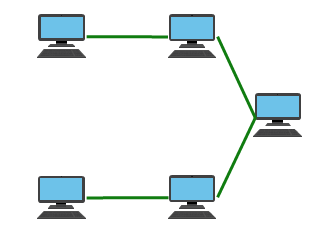


Network Topologies: A **network topology** defines the physical connections of hosts in a network.

Different types of topologies:

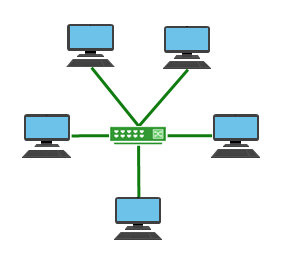
1. Bus
2. Star
3. Ring
4. Mesh
5. Tree (Bus + Star)

Bus Topology: All devices are connected via copper cable in a line. Data has to pass on from one host to another in a bus fashion.

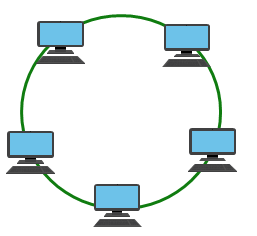


Star Topology: Each host is connected to a central connecting device with twisted-pair cabling. The central connecting device can be a hub, a switch, or a router. This is the most commonly used topology.

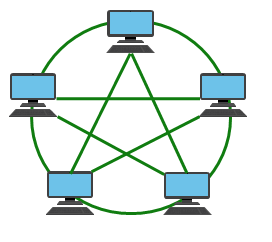
* Layer-1 device such as hub or repeater
* Layer-2 device such as switch or bridge
* Layer-3 device such as router or gateway



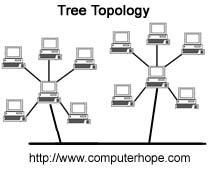
Ring Topology: In the [ring network](http://searchcio-midmarket.techtarget.com/definition/ring-network) topology, the workstations are connected in a closed loop configuration. Adjacent pairs of workstations are directly connected. Other pairs of workstations are indirectly connected, the data passing through one or more intermediate nodes.



Mesh Topology: Each computer connects to every other computer in a LAN. There won't be any central connecting device. The Setup is fault-tolerant and allows data to be sent via multiple pathways if one path fails.



Tree Topology: A tree topology is also known as a **star bus topology**. It incorporates elements of both a [bus topology](http://www.computerhope.com/jargon/b/bustopol.htm) and a [star topology](http://www.computerhope.com/jargon/s/startopo.htm). Below is an example network diagram of a tree topology, in which the central nodes of two star networks are connected to one another in a bus fashion. The switches of the star topologies is connected to main cable called back bone cable where in it will connect to router.



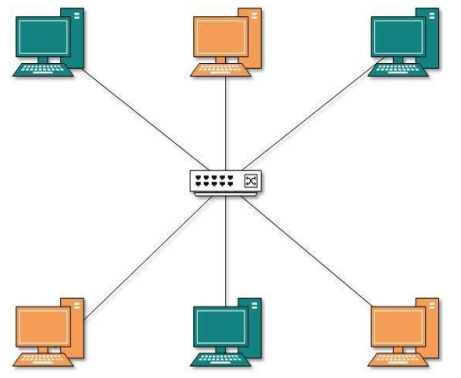
Different Types of Networks:

* **Local-area network** (LAN): The computers are geographically close together (that is, in the same building).
* **Wide-area network** (WAN): The computers are farther apart and are connected by telephone lines or radio waves.
* **Metropolitan-area networ**k (MAN): A data network designed for a town or city.
* **Home-area network** (HAN):  A network contained within a user's home that connects a person's digital devices.
* **Virtual private networ**k (VPN):  A network that is constructed by using public network — usually the Internet — to connect to a private network, such as a company's internal network.
* **Storage area network** (SAN): A high-speed network of storage devices that also connects those storage devices with servers.

VLAN (Virtual LAN): In VLAN, a physical single LAN which is connected to switch can be divided logically into sub networks or subnet's which in turn called Virtual LAN (VLAN).

Usually in a LAN all the devices connected to switch can communicate to each other. But whereas in VLAN the logically divided devices will act as one VLAN. One VLAN group cannot communicate to other VLAN directly using switch an additional Layer-3 router is required for communication.

From the below diagram we can two groups one is blue and orange. Communication across the VLAN groups is possible only through router.



The purpose of the VLAN is to control the network traffic and security.

Ethernet: is a way of connecting computers together in a [local area network](https://simple.wikipedia.org/wiki/Local_area_network) or LAN using cable called Ethernet cable. Ethernet cables are made of copper wires transmit data in the form of electrical pulses.

[Higher level network protocols](https://www.lifewire.com/definition-of-protocol-network-817949) like [**Internet Protocol (IP)**](https://www.lifewire.com/definition-of-internet-protocol-817974) use Ethernet as their transmission medium. Data travels over Ethernet inside protocol units called *frames.*



IP Address: An Internet Protocol address is an identifier assigned to each computer and other device (e.g., printer, [router](https://en.wikipedia.org/wiki/Router_(computing)), [mobile device](https://en.wikipedia.org/wiki/Mobile_device), etc.) connected to a [TCP/IP network](https://en.wikipedia.org/wiki/TCP/IP_network) that is used to locate and identify the node in communications with other nodes on the network.

IP addresses are usually written and displayed in [human-readable](https://en.wikipedia.org/wiki/Human-readable) notations, such as 172.16.254.1 in IPv4, and 2001:db8:0:1234:0:567:8:1 in IPv6.

An IP address always consists of 4 numbers separated by periods, with the numbers having a possible range of 0 through 255.

An example of how an IP address appears is: **192.168.1.10**

This representation of an IP address is called **decimal notation** and is what is generally used by humans to refer to an IP address for readability purposes.

Private IP Address: The address which is been used for internal communication with in the LAN. When the private IP address try to connect outside world i.e Internet the NAT will translate the private IP into Public IP for the communication.

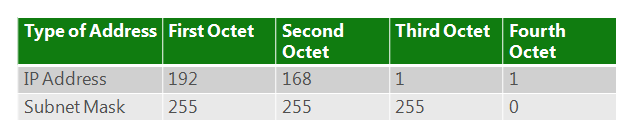
Public IP Address: The IP adresss which is issued by the ISP to communicate the outside world.

Subnet: A LAN network which is sub divided into logical units to form a subnetwork is called subnet.

Subnet is a way to partitioning network into logical segments to form subnets for greater ease of administration. When subnets are properly implemented, both the performance and [security of networks](https://www.lifewire.com/introduction-to-computer-network-security-817989) can be improved.

Subnet Mask:

* A group of four numbers that define a computer’s network
* **NOTE:** All of the 255s in a subnet mask collectively refer to the network portion, whereas the 0s refer to the host portion



Routing Table:

Subnet Vs VLAN:

Virtual local area networks (VLANs) allow us to create different logical and physical networks; whereas IP subnetting simply allows us to create logical networks through the same physical network.

Host in a Network: Desktop PCs, laptops, cell phones, servers, routers and so on.

A host can be any device that has an IP address – an address used to send and receive data in a network.

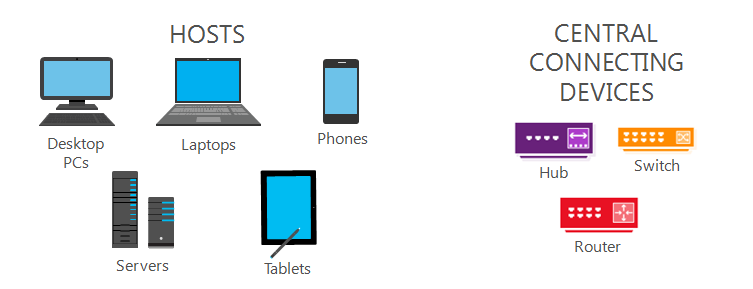
IP addresses help identify devices and the networks where they are located.

Central Connecting Devices:

* Hubs, switches, and routers act as central connecting devices
* Central connecting devices are responsible for:

1. connecting hosts
2. Transmitting data

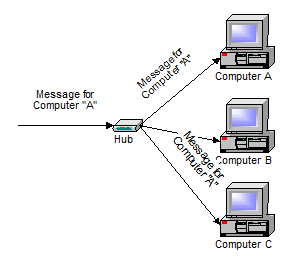
* Different central connecting devices perform these functions in different ways.



Hub Vs Switch Vs Router: Hubs, switches, and routers are all devices that let you connect one or more computers to other computers, networked devices, or even other networks. Each has two or more connectors called ports into which you plug in the cables to make the connection.

Hub or LAN Hub: A **hub** is typically the least expensive, least intelligent, and least complicated of the three. Its job is very simple – anything that comes in one port is sent out to the other ports as well.

If a message is sent to computer A, the same data is replicated and delivered to other computers on the network i.e. computer B and computer C.



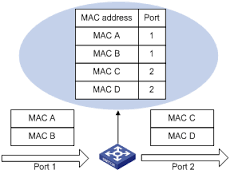
Hubs wastes lots of bandwidth on the network and creates lots of un necessary traffic.

Data has a security threat on hub, we are trying to send to one intended host but the data is replicated and delivered to all the hosts that is connected on the hub.

Switch or LAN Switch:

* Hosts send data to a switch
* Switches direct data to its intended destination
* Unlike hubs, switches can send and receive data simultaneously
* Switches are the most common device used to connect hosts to a network

In switch, communication between hosts happen with the help of MAC address. Every host connected in a network (Ethernet or LAN) will have a unique MAC Address. The switch will have MAC address table and it will make a lookup on MAC address for communicating with other hosts by routing the traffic to intended ports.

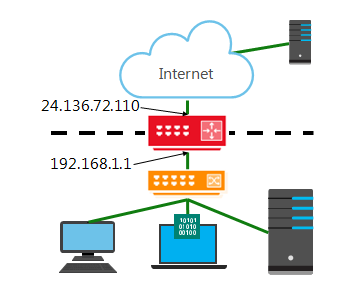


Routers: A router is a device that forwards data packets along networks. A router is connected to at least two networks and is located at gateways, the places where two or more networks connect.

It also routes the data that it’s being asked to handle. Many routers today are, in fact, little computers dedicated to the task of routing network traffic.

As far as simple traffic routing is concerned, a router operates exactly as a switch, learning the location of the computers on its connections and routing traffic only to those computers.

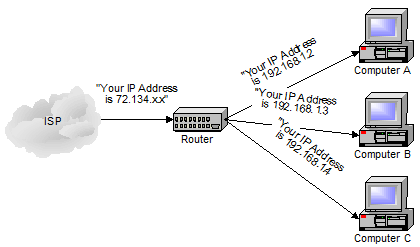
Routers are at the edge of LANs and they act as a gateway to other networks



Yellow device is switch and Red is Router in the above Diagram.

Here **24.136.72.100** is **Public IP** which is assigned by ISP and **192.168.1.1** is **Local IP** which is assigned by DHCP for communication within the LAN.

Consumer grade routers perform at minimum two additional and important  
tasks: DHCP and NAT.



DHCP – Dynamic Host Configuration Protocol: is the way dynamic IP addresses are assigned. A device asks for an IP address to be assigned to it from “upstream” and a DHCP server responds with an IP address assignment. A router connected to your ISP-provided internet connection will typically ask your ISP’s server for an IP address; this will be your IP address on the internet. Your local computers, on the other hand, will ask the router for an IP address and these addresses are local to your network.

DHCP Software's are pre built on Modern Routers and how ever this can be installed on a separate server.

NAT – Network Address Translation: is the way that the router *translates* the IP addresses of packets that cross the internet/local network boundary. When computer “A” sends a packet out, the IP address that it’s “from” is that of computer “A” – 192.168.1.2 in the example above. When the router passes that on to the internet, it replaces the local IP address with the internet IP address assigned by the ISP. It also keeps track, so that if a response comes back from somewhere on the internet, the router knows to do the translation in reverse - replace the internet IP address **(Public IP)** with the **local IP** address for machine “A” and then send that response packet on to machine “A”.

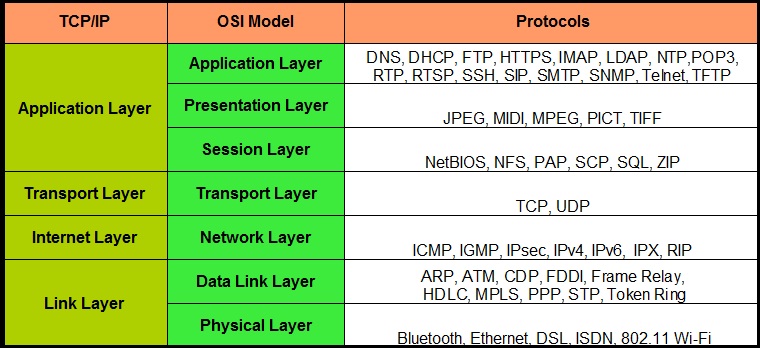
A side effect of NAT is that machines on the internet cannot initiate communications to local machines – they can only respond to communications initiated by those local machines.

Port: Always port number is associated with an IP address (192.168.30.4:8080) and belongs to any device (Computer, Server, Printer) that is connect on a network. Each application (mysql, web server, FTP, SSH) on a machine/computer will listen the requests from port numbers and each application will have its own dedicated port number. Different client request can be catered and served based on the port number and hence conflict won’t arise in the network. Port numbers range is from 0 – 65535.

Socket: Combination of IP address and port number (192.168.30.4:8080) which is used for communicating with end point machines.

OSI Model and its corresponding Protocols

Below is the comparison of TCP/IP Model and OSI Model



1. **Physical Layer:**

This layer deals with the physical connection between the two devices which are trying to communicate. Which means the patch cable connecting two computers is the Physical layer of the OSI model. The first thing while troubleshooting a network problem is to check for physical layer connection. 95% of time this will solve your problem.

2. **Data-link Layer:**

Computers usually store the logical address of the recipient. Now the data it is about to send will be addressed to the logical address but cannot be sent directly to it, because the logical address is just for the understanding of the computer. We work with physical address. So, we need a device which translates the logical address into physical address and this process takes place in data-link layer with the help of [Switches](https://www.geekstarts.info/network-switch/). Encapsulation of data into frames takes place in this layer.

3. **Network Layer:**

The network layer is the most critical layer of OSI model. In this layer, basic questions like which protocols to be used? The best route to destination? Or the shortest path to the recipient? [Routers](https://www.geekstarts.info/router/) work in the Network Layer. Network layer is also responsible for encapsulating segments into packets.

4. **Transport Layer:**

This is where http comes into the picture. A connection is established with the recipient using the TCP protocol. A number is assigned to each packet. Now, Transport layer determines the number of packet to be sent at a time and packets to be sent to avoid congestion. It basically deals with how much information should be transported in one go.

5. **Session Layer:**

When you connect to a web server or login into one, the server starts a session between your machine and the web server. A token is used to recognize each session, usually a number which is unique. Creating a new session is like creating a new identity. The web server will then find you by your session id. Apache and Php config files usually define how to create a session.  
Sessions play an important role during online transactions and in e-commerce websites. Http is a stateless protocol, hence when you move from one page to another, you will lose your data as http doesn’t care about which data was with you before. Sessions makes sure your data is intact irrespective of which protocol or page you’re on.

6. **Presentation Layer:**

Every webpage has texts, images, videos, html files. Presentation layer recognizes these common formats and displays them. This is where your Operating System comes into picture. If you don’t have audio driver and you try to play a song, the presentation layer will tell you it can’t do so because of absence of audio drivers.

7. **Application Layer:**

Students usually consider Firefox or Chrome or Internet Explorer as Application Layer. These browsers are not the application layers. The common protocols used by these browsers are application layer. This is where the data is actually shown to the users via the browsers. But the common protocols used by the browsers and applications like Skype or Yahoo Messenger are application layer.

To troubleshoot any problem, we can simply put our  understanding of OSI model into use.

If you have understood each layer and know its working, we can find our any problem within few minutes. Once we know the problem, we can then start working on it