Module 1
Networking & CyberSecurity Essentials

What is Penetration Testing?

A penetration testing ,colloquially known as a pentest, is an authorized simulated cyberattack on a computer system,performed to evaluate the security of the system.

- External network tests,which look for vulnerabilities and security issues in an organization's servers,hosts,devices and network systems.
- Internal network tests,which assess the damage,an attacker could do when they gain access to an organization's internal systems.
- Web application tests,which look for insecure development practices in the design coding and publishing of software or a website.
- Wireless network tests,which assess vulnerabilities in wireless systems,including wi-fi,rogue access points to weak encryption algorithm.
- Phishing penetration test,which assess employee's susceptibility to scam emails.

Career Opportunities

- Penetration Tester
- Security Auditor
- Cybersecurity Analyst
- Vulnerability Assessor
- Information Security Manager

What is Cyber Security?

The technique of protecting internet-connected systems such as computers,servers,mobile devices,electronic systems,networks and data from malicious attacks in known as cybersecurity.
We can divide cybersecurity into two parts is cyber,and the other is security.
Cyber refers to the technology that includes systems,network,programs and data.
Security is concerned with the protection of systems,networks,programs and information.

Types of Cyber Attacks

Cyber attacks can be classified into the following categories :

1. Web-Based Attacks

- Injection Attacks
- Session Attacks
- Phishing
- Brute force
- Denial of Service(DOS)
- Distributed Denial of Service(DDOS)
- Spoofing
- Man in the Middle Attack
- Dictionary Attacks
- URL Interpretation

2. System-Based Attacks

- Virus
- Worms
- Trojan Horse
- Backdoors
- Bots

What is Ethical Hacking?

The goal of ethical hacking-like criminal hacking is to find security vulnerabilities in an organization’s systems.However as the word ‘ethical’ suggests,the person conducting the attacks must have the organization’s approval before proceeding.
Why would organization ask someone to hack them?
Simple!
They understands that the best way to identify the flaws that a cyber criminal might exploit is to think like a cyber criminal themselves.

Difference between Hackers & Attackers?

A hacker is a person who breaks into a computer system.The reason for hacking can be many:installing malware,stealing or destroying data,disrupting services,and more. Hacking can also be done for ethical reasons,such as trying to find software vulnerabilities so they can be fixed.Attackers can use any means to cause havoc.
For example,an attacker may be a disgruntled insider who deletes sensitives files or disrupts the business by any means to achieve their goals.They could simply unplug a key system.

Types of Hackers

Hackers can be classified into different categories:

- Black hat hackers

Black hat hackers are also known as an unethical hackers or a security crackers.These people hack the system illegally to steal money or to achieve their own illegal goals.They find banks or other companies with weak security and steal money or credit card information.They can also modify or destroy that data as well.Black hat hacking is illegal.

- White hat hackers

They are also known as Ethical hackers or a penetration tester.White hat hackers are the good guys of the hacker world.These people use the same technique used by the black hat hackers.They also hack the system,but hey can only hack the system that they’ve permission to hack in order to test the security of the system.They focus on security and protecting IT system.White hat hacking is illegal.

- Grey hat hackers

They are hybrid between black hat hackers and white hat hackers.They can hack any system even if they don’t have permission to test the security of the system,but they’ll never steal money or damage the system.In most cases,they tell the administrator of that system.But they are also illegal because they test the security of the system that they do not have permission to test.Grey hat hacking is sometimes acted legally and sometimes not.

- Script Kiddie

It is an unskilled person who uses scripts or downloaded tools available for hacking,which are provided by other hackers

- Grey Hat Hackers

They are also amateurs in the world of hacking by they’re different from script kiddies. They care about hacking and strive to become full-blown hackers.

- Blue hat hackers

They are much like the script kiddies;are beginners in the field of hacking.If anyone makes angry a script kiddie and he/she may take revenge,then they’re considered as the blue hat hackers.

- Social Media hackers

They are the one who steals social media accounts.This can be done for revenge or gain any information about someone.

- Hacktivist

These are also called the online version of activists.They are hackers or a group of anonymous hackers who gain unauthorized access to government’s computer files and network’s for further social or political ends.

- Malicious insider/whistle blower

They could be an employee of a company or a government agency with a grudge or a strategic employee who becomes aware of any illegal activities happening within the organization and blackmail the organization for his/her personal gain.

Difference between Red Team and Blue Team?

Red Team	**Blue Team**
A red team plays the role of the attacker by trying to find vulnerabilities and break through cybersecurity defenses.	They defends against attacks and responds to incidents when they occurs.
Their activities are: ● Social Engineering ● Penetration Testing ● Intercepting communication ● Card cloning ● Making recommendation to blue team for security improvements	Their activities are: ● Digital footprint analysis ● DNS audits ● Installing and configuring firewalls and endpoint security software ● Monitoring network activities ● Using least privilege access
Red team skills: ● Software development ● Penetration testing ● Social engineering ● Threat intelligence ● Reverse engineering	Blue team skills: ● Risk assessment ● Threat intelligence ● Hardening techniques ● Monitoring and detection system

Red team jobs: ● Vulnerability assessor($80,096) ● Security Auditor($83,015) ● Ethical Hacker($98,177) ● Penetration tester($102,279) Red team certifications: ● CEH ● LPT Master ● CompTIA Pentest+ ● GPEN ● GXPN ● OSCP ● CRTOP	Blue team jobs: ● Cybersecurity Analyst($80,003) ● Incident responder($88,818) ● Threat intelligence analyst($90,257) ● Information Security Specialist($96,942) ● Security Engineer($111,630) ● Security Architect($153,160) Blue team certifications: ● CISSP ● CISA ● CompTIA Security+ ● GSEC ● GCIH ● SSCP ● CASP+

What are black box,gray box,and white box penetration testing?

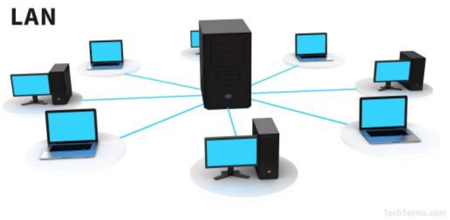
- In black box testing assignment,the penetration tester is placed in the role of the average hacker,with no internal knowledge of the target system.
- Gray box penetration tester typically have some knowledge of the network’s internals,potentially including design and architecture documentation and an account internal to the network.
- White box penetration testers are given full access to source code,architecture ,documentation and so forth .

What is network?

A network is the collection of devices like computer,networking devices and other devices which are capable to interconnect each other for the purpose of data and resource sharing, to gain control over each other , linked through medium such as cables,wireless technologies etc.

Types of network

- LAN(Local Area Network):



It is a network that covers a small geographical area such as homes,offices and groups of buildings. Example: connecting using Ethernet/internet cables.

A local area network (LAN) is a collection of devices connected together in one physical location, such as a building, office, or home. A LAN can be small or large, ranging from a home network with one user to an enterprise network with thousands of users and devices in an office or school.

A LAN comprises cables, access points, switches, routers, and other components that enable devices to connect to internal servers, web servers, and other LANs via wide area networks.

The rise of virtualization has also fueled the development of virtual LANs, which enable network administrators to logically group network nodes and partition their networks without a need for major infrastructure changes.

For example, in an office with multiple departments, such as accounting, IT support, and administration, each department's computers could be logically connected to the same switch but segmented to behave as if they are separate.

Benefits of LAN:

The advantages of a LAN are the same as those for any group of devices networked together. The devices can use a single Internet connection, share files with one another, print to shared printers, and be accessed and even controlled by one another.

Types of LAN:

In general, there are two types of LANs: client/server LANs and peer-to-peer LANs.

A client/server LAN consists of several devices (the clients) connected to a central server. The server manages file storage, application access, device access, and network traffic. A client can be any connected device that runs or accesses applications or the Internet. The clients connect to the server either with cables or through wireless connections.

Typically, suites of applications can be kept on the LAN server. Users can access databases, email, document sharing, printing, and other services through applications running on the LAN server, with read and write access maintained by a network or IT administrator. Most midsize to large business, government, research, and education networks are client/server-based LANs.

A peer-to-peer LAN doesn't have a central server and cannot handle heavy workloads like a client/server LAN can, and so they're typically smaller. On a peer-to-peer LAN, each device shares equally in the functioning of the network. The devices share resources and data through wired or wireless connections to a switch or router. Most home networks are peer-to-peer.

- WLAN(Wireless Local Area Network)

Wireless LAN

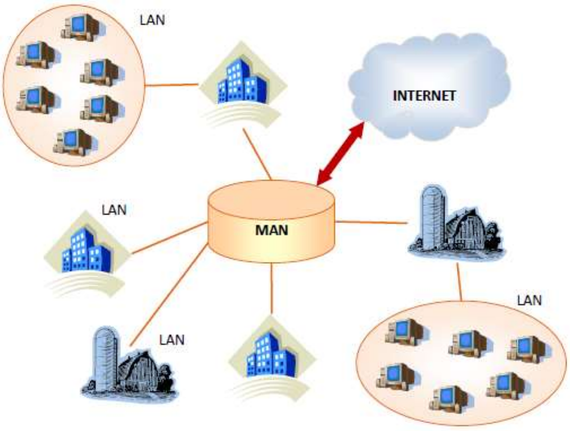
It is a group of co-located computers or other devices that form a network based on radio transmission rather than wired connection.
Ex: wifi,hotspot,bluetooth etc..

A wireless local-area network (WLAN) is a group of colocated computers or other devices that form a network based on radio transmissions rather than wired connections. A Wi-Fi network is a type of WLAN; anyone connected to Wi-Fi while reading this webpage is using a WLAN.

Benefits of a WLAN:

1. Extended reach: WLANs enable computing to happen anywhere, even when carrying high data loads and advanced web applications.
2. Device flexibility: A WLAN supports use of a wide range of devices, such as computers, phones, tablets, gaming systems, and IoT devices.
3. Easier installation and management: A WLAN requires less physical equipment than a wired network, which saves money, reduces installation time, and takes up less of a footprint in office settings.
4. Scalability: A WLAN is easy to scale. Adding users is as simple as assigning login credentials.
5. Network management: Nearly all management of a WLAN can be handled virtually. A single software interface can provide visibility, manage users, monitor network health, and collect data.

- MAN(Metropolitan Area Network)



It is an interconnection of several LANs throughout a city or municipality. Like LAN, a MAN can use various wired or wireless connectivity options,including fiber optics,Ethernet cables,wi-fi or cellular.

A metropolitan area network (MAN) is a network with a size greater than LAN but smaller than a WAN. It normally comprises networked interconnections within a city that also offers a connection to the Internet.

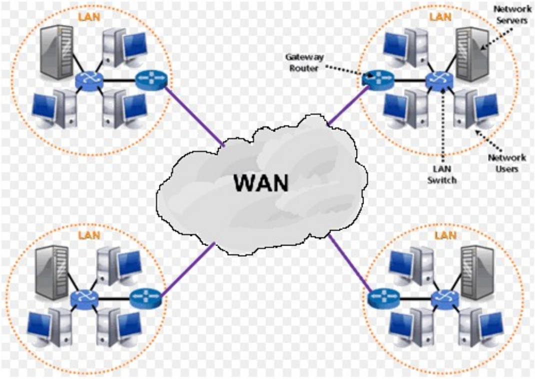
The distinguishing features of MAN are:

1. Network size generally ranges from 5 to 50 km. It may be as small as a group of buildings in a campus to as large as covering the whole city.
2. Data rates are moderate to high.
3. In general, a MAN is either owned by a user group or by a network provider who sells service to users, rather than a single organization as in LAN.
4. It facilitates sharing of regional resources.
5. They provide uplinks for connecting LANs to WANs and Internet.

Example of MAN:

1) Cable TV network
2) Telephone networks providing high-speed DSL lines
3) IEEE 802.16 or WiMAX, that provides high-speed broadband access with Internet connectivity to customer premises.

- WAN(Wide Area Network)



A WAN is the most expensive type of computer network configuration.Like a MAN, a WAN is a connection of multiple LANs belonging to the same network.Unlike MANs,however ,WANs aren't restricted to the confine's of city limits.A WAN can extend to any area of globe.
Ex: Internet
WAN connects computers together across longer physical distances.

A wide area network (WAN) is a computer network that covers a large geographical area comprising a region, a country, a continent or even the whole world. WAN includes the technologies to transmit data, image, audio and video information over long distances and among different LANs and MANs.

The distinguishing features of WAN are:

1. WANs have a large capacity, connecting a large number of computers over a large area, and are inherently scalable.
2. They facilitate the sharing of regional resources.
3. They provide uplinks for connecting LANs and MANs to the Internet.
4. Communication links are provided by public carriers like telephone networks, network providers, cable systems, satellites etc.
5. Typically, they have low data transfer rate and high propagation delay, i.e.they have low communication speed.
6. They generally have a higher bit error rate.

Example of WAN:

1) The Internet
2) 4G Mobile Broadband Systems
3) A network of bank cash dispensers.

What is Internet?

A global computer network providing a variety of information and communication facilities,consisting of interconnected network using standardized communication protocols/guidelines/regulations/rules. It is a connection of interconnected network.
Internet is used to connect the different networks of computers simultaneously. It is a public network therefore anyone can access the internet. On the internet, there are multiple users and it provides an unlimited of information to the users.

What is Intranet?

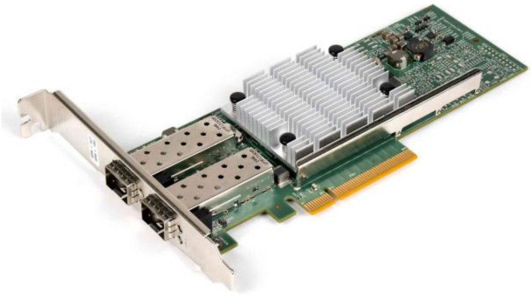
Intranet is the type of internet that is used privately. It is a private network therefore anyone can't access the intranet. On the intranet, there is a limited number of users and it provides a piece of limited information to its users.

What are Network Devices?

Network allow people to communicate,collaborate and interact in many ways.Network’s are used to access web pages,talk using IP telephones,participate in video conferences,compete in interactive gaming,shop using the internet,complete online coursework and more.

Different networking devices have different roles to play in a computer network.

- NIC(Network Interface Card)



A Network Interface Card is a computer hardware component that connects a computer to a computer network.It implements the physical layer circuitry necessary for communicating with a data link layer standard,such as Ethernet or wi-fi . Each card represents a device and can prepare ,transmit and control the flow of data on the network.

Network Interface Card (NIC) is a hardware component that is present on the computer. It is used to connect different networking devices such as computers and servers to share data over the connected network. It provides functionality such as support for I/O interrupt, Direct Memory Access (DMA) interfaces, partitioning, and data transmission.

NIC is important for us to establish a wired or wireless connection over the network.

Network Interface Card is also known as Network Interface Controller, Network Adapter, Ethernet card, Connection card, and LAN (Local Area Network) Adapter.

Functions of the Network Interface Card:

A list of functions of the Network Interface Card is given below -

1. NIC is used to convert data into a digital signal.
2. In the OSI model, NIC uses the physical layer to transmit signals and the network layer to transmit data packets.
3. NIC offers both wired (using cables) and wireless (using Wi-Fi) data communication techniques.
4. NIC is a middleware between a computer/server and a data network.
5. NIC operates on both physical as well as the data link layer of the OSI model.

Components of Network Interface Card:

Network Interface Card contains the following essential components -

1. Memory: Memory is one of the most important components of the NIC. It is used to store the data during communication.
2. Connectors : connectors are used to connect the cables to the Ethernet port.

3. Processor: Processor is used for converting the data message into a suitable form of communication.
4. Jumpers: Jumpers are the small device that is used to control the communication operations without the need of any software. It is also used to determine settings for the interrupt request line, I/O address, upper memory block, and type of transceiver.
5. Routers: To provide wireless connectivity, routers are used.
6. MAC address: MAC address is also referred to as a physical network address. It is a unique address that is present to the network interface card where ethernet packets are communicated with the computer.

Types of Network Interface Cards:

There are the following two types of NICs -

1. Ethernet NIC: Ethernet NIC was developed by Robert Metcalf in 1980. It is made by ethernet cables. This type of NIC is most widely used in the LAN, MAN, and WAN networks.

Example: TP-LINK TG-3468 Gigabit PCI Express Network Adapter.

2. Wireless Networks NIC : It is a wireless network that allows us to connect the devices without using the cables. These types of NICs are used to design a Wi-Fi connection.

Example: Intel 3160 Dual-Band Wireless Adapter

A list of advantages of NIC is given below -

1) As compared to the wireless network card, NIC provides a secure, faster, and more reliable connection.
2) NIC allows us to share bulk data among many users.
3) It helps us to connect peripheral devices using many ports of NIC.
4) Communication speed is high.
5) Network Interface cards are not expensive.
6) NICs are easy to troubleshoot.
7) Disadvantages of NIC

A list of disadvantages of NIC is given below -

1. NIC is inconvenient as compared to the wireless card.
2. For wired NIC, a hard-wired connection is required.
3. NIC needs a proper configuration to work efficiently.
4. NIC cards are not secure, so the data inside NIC is not safe.

- Router

A Router connects one network to another network.It is responsible for the delivery of packets across different networks.The destination of the IP packet might be a web server in another country or an email server on the LAN. It works on network Layer.

The router is a physical or virtual internetworking device that is designed to receive, analyze, and forward data packets between computer networks. A router examines a destination IP address of a given data packet, and it uses the headers and forwarding tables to decide the best way to transfer the packets. There are some popular companies that develop routers; such are Cisco, 3Com, HP, Juniper, D-Link, Nortel, etc. Some important points of routers are given below:

1. A router is used in LAN (Local Area Network) and WAN (Wide Area Network) environments. For example, it is used in offices for connectivity, and you can also establish the connection between distant networks such as from Bhopal to
2. It shares information with other routers in networking.
3. It uses the routing protocol to transfer the data across a network.
4. Furthermore, it is more expensive than other networking devices like switches and hubs.

- HUB

It is a multiport device that is used to connect multiple network hosts.When a host sends a data packets to a network hub,the hub copies the data packet to all of its ports connected to it.The hub is not so secure and safe.It works at physical layer.

which is used for connection of devices in a network. It works as a central connection for all the devices that are connected through a hub. The hub has numerous ports. If a packet reaches at one port, it is able to see by all the segments of the network due to a packet is copied to the other ports. A network hub has no routing tables or intelligence (unlike a network switch or router), which is used to send information and broadcast all network data across each and every connection.

Although most of the hubs can recognize network troubles or errors like collisions, broadcasting all information to the several ports can be a security risk and cause bottlenecks. The network hubs were popular in the past time as they were cheaper as compared to a switch or router. Nowadays, switches are much cheaper than a hub and provide a better solution for any network. Furthermore, a hub is no IP address, as it is a dumb device.

- Switch

It is a networking device,which is more intelligent than a hub.It does filter and forwarding which is more intelligent way.It works on the basis of the MAC address.It uses a CAM(Content Address Memory) table contains the mac address of connected devices.It works at data link layer.

Switches have a smarter job than hubs in general. A switch improves the capacity of the network. The switch keeps limited information on routing nodes in the internal network and provides links to systems such as hubs or routers. Normally LAN beaches are linked by switches. Switches will usually read incoming packets ‘ hardware addresses to transfer them to their respective destinations. Switches improve the Network’s effectiveness over hubs or routers because of the flexibility of the digital circuit. Switches also improve network protection since network control makes digital circuits easier to investigate.

You can see a switch as a system that combines some of the best routers and hubs. A switch can operate on the interface Data Link or the OSI model’s network layer. A multi-layer switch can be worked in both layers, so both a switch and a router can work. A high-performance switch adopting the same routing procedures as routers is a multilayer switch. DDoS may attack switches; flood controls can be used to prevent malicious traffic from stopping the switch. The Switch port’s protection is crucial to make sure that all unused ports are deactivated, and DHCP, ARP, and MAC Address Filtering are used to ensure stable switches.

- Bridge

Bridges link two or more hosts or network segments. Bridge processing and transfer of frames between the various bridge links are the key roles in the network architecture. For the transmission of images, you use Media Access Control (MAC) hardware. Bridges can transmit the data or block the crossing by looking at the devices’ MAC addresses connected to each line. It is also possible to connect two physical LANs with a wider theoretical LAN with bridges. Bridges only function on OSI layers Physical and Data Link. Bridges are used for dividing large networks into smaller sections through the placement between two segments of the physical network and data flow management between the two.

Bridges are in many respects like hubs, like linking LAN components to the same protocols. Yet bridges, known as frames, filter the incoming data packets to addresses before transmission. The bridge does not modify the format or content of the incoming data when it filters the data packets with the aid of a dynamic bridge table; the bridge filters and forwarded frames in the network. The initially empty bridge table preserves each LAN computer’s LAN address and each bridge interface’s addresses that link the LAN to the other LANs.

- Gateway

The transportation and session layers of the OSI model usually work in gateways. There are many guidelines and specifications for different vendors on the transport layer and above; gateways manage these. The connection between networking technologies, such as OSI and Transmission Control Protocol / Internet Protocols, such as TCP / IP, is supported by the gateway. Gateways link, thus, two or more self-contained networks with their own algorithms, protocols, topology, domain name system and policy, and network administration. Gateways handle all routing functions and more. In fact, an added translation router is a gateway. A protocol converter is called the feature that translates between different network technologies.

- Modem

Digital signals are transmitted through analog phone lines using modems (modulator demodulators). The modem converts digital signals into analog signals of various frequencies and transmits them to a modem at the receiver location. The receiving modem turns the other way and provides a digital output to a device, normally a computer, connected to a modem. In most cases, digital data is transmitted via the RS-232 standard interface to or from a serial line modem. Most cable operators use modems as final terminals to locate and remember their homes and personal clients, and many phone companies provide DSL services. All physical and data link layers are operating on modems.

- Brouter

The bridging router is also the device that combines bridge and router features. It can be used on the data connection layer or the network layer. It can route packets across networks as a router, function as a bridge, and filter network traffic in the local area.

Network Medias

It refers to the communication channels and to interconnect nodes on a computer network.They're broadly classified into guided and unguided mediums.Typical examples of network media include copper coaxial cable,copper twisted paid cables and optical fiber cables and used in wired networks and radio waves used in wireless data communication networks.

Cables

To connect two or more computers or networking devices in a network,cables are used.There are three types of network cables.

- Coaxial cables: This cable contains a conductor,insulator,braiding and sheath.The sheath covers the braiding,the braiding covers the insulation,and the insulation covers the conductor.Example:Cables in dish TV.
- Twisted paid cables : This cable is also known as Ethernet cable.This cable consists of color-coded pairs of insulated copper wires.Every two wires are twisted around each others to form pairs.Usually,there are four pairs.Each pair has one solid color and one stripped color wire.Solid colors are blue,green,brown and orange.In stripped color,the solid color is mixed with the white color. Based on how pairs are stripped in the plastic sheath,there are two types of twisted paid cables.
    1. UTP(Unshielded Twisted Pair) : All pairs are wrapped in a single plastic sheath.
    2. STP(Shielded Twisted Pair) : Each pair is wrapped with an metal shield,then all pairs are wrapped in a single outer plastic sheath.
- Fibre optic cable : The cable consists of a core,cladding buffer,and jacket.The core is made from thin strands of glass or plastic that can carry data over a long distance.The core is wrapped in the cladding,the cladding is wrapped in the buffer,and the buffer is wrapped in the jacket.The core carried the data signals in the form of light.

Network Topology

The arrangement of a network that comprised nodes and connecting lives via sender and receiver is referred to as network topology.

Mainly ,there are 6 network topologies:

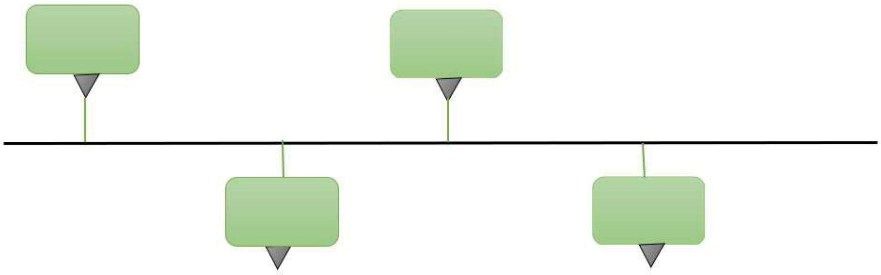
1. Bus
2. Star

3. Ring
4. Mesh
5. Tree
6. Hybrid

Bus Topology : It is a network type in which every computer and network device is connected to a single cable.It transmits the data from one to another in a single domain.

Bus topology is a specific kind of network topology in which all of the various devices in the network are connected to a single cable or line. In general, the term refers to how various devices are set up in a network.

Bus topology carries transmitted data through the cable. because data reaches each node, the node checks the destination address (MAC/IP address) to work out if it matches their address. If the address does not match with the node, the node does nothing more. But if the addresses of nodes match to address contained within data then they process on knowledge. In the bus, communication between nodes is done through a foremost network cable.



Bus Topology

Advantages of Bus Topology :

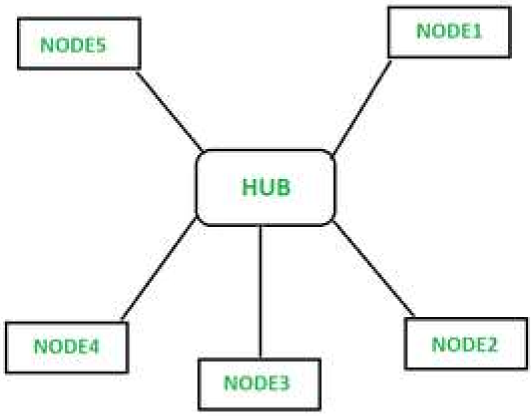
1) It is the easiest network topology for connecting peripherals or computers in a linear fashion.
2) It works very efficiently well when there is a small network.
3) The length of cable required is less than a star topology.
4) It is easy to connect or remove devices in this network without affecting any other device.
5) Very cost-effective as compared to other network topology i.e. mesh and star
6) It is easy to understand topology.
7) Easy to expand by joining the two cables together.

Disadvantages of Bus Topology :

1. Bus topology is not great for large networks.
2. Identification of problems becomes difficult if the whole network goes down.
3. Troubleshooting individual device issues is very hard.
4. Need terminators are required at both ends of the main cable.
5. Additional devices slow the network down.
6. If the main cable is damaged, the whole network fails or splits into two.
7. Packet loss is high.
8. This network topology is very slow as compared to other topologies.

Star Topology : In this,all the devices are connected to a single hub through a cable.This hub is the central node and all other nodes are connected to the central node.

Star Topology A star may be a topology for a Local Area Network (LAN) during which all nodes are individually connected to a central connection point, sort of a hub or a switch. A star takes more cable than e.g. a bus, but the benefit is that if a cable fails, just one node is going to be brought down. Each device within the network is connected to a central device called a hub. If one device wants to send data to another device, it's to first send the info to the hub then the hub transmits that data to the designated device. The number of links required to connect nodes in the star topology is N where N is the number of nodes.



Advantages of Star Topology

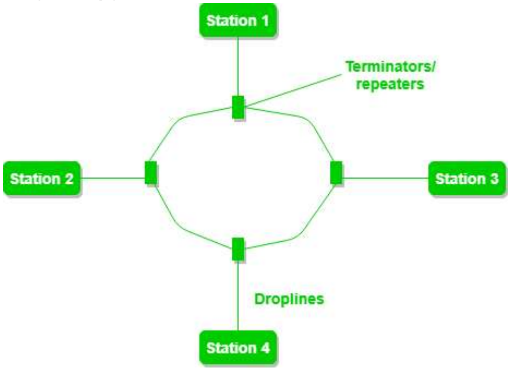
1) It is very reliable – if one cable or device fails then all the others will still work
2) It is high-performing as no data collisions can occur
3) Less expensive because each device only need one I/O port and wishes to be connected with hub with one link.
4) Easier to put in
5) Robust in nature
6) Easy fault detection because the link are often easily identified.
7) No disruptions to the network when connecting or removing devices.
8) Each device requires just one port i.e. to attach to the hub.
9) If N devices are connected to every other in star, then the amount of cables required to attach them is N. So, it's easy to line up.

Disadvantages of Star Topology

1. Requires more cable than a linear bus .
2. If the connecting network device (network switch) fails, nodes attached are disabled and can't participate in network communication.
3. More expensive than linear bus topology due to the value of the connecting devices (network switches)
4. If hub goes down everything goes down, none of the devices can work without hub.
5. Hub requires more resources and regular maintenance because it's the central system of star .
6. Extra hardware is required (hubs or switches) which adds to cost
7. Performance is predicated on the one concentrator i.e. hub.

Ring Topology : In this ,it forms a ring connecting devices with exactly two neighboring devices.

Ring Topology may be a network configuration where device connections create a circular data path. In this each device is connected to with its exactly two neighboring devices, like points on a circle which forms like a ring structure. A number of repeaters are used for Ring topology with a large number of nodes to send data and to prevent data loss repeaters are used in this network. Together, devices during a ring topology are mentioned as a hoop network. In this packets travels from one device to another until they reach the desired destination. In this data travels in unidirectional forms means in only one direction but it can also do bidirectional by having 2 connections between each Network Node, it is called Dual Ring Topology. It is used in LANs and WANs depending on the card of network in the computer.



Advantages of Ring topology :

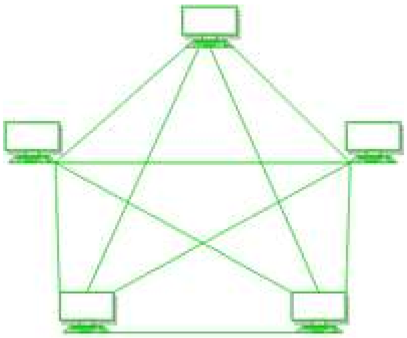
1) In this data flows in one direction which reduces the chance of packet collisions.
2) In this topology additional workstations can be added after without impacting performance of the network.
3) Equal access to the resources.
4) There is no need of server to control the connectivity among the nodes in the topology.
5) It is cheap to install and expand.
6) Minimum collision.
7) Speed to transfer the data is very high in this type of topology.
8) Due to the presence of token passing the performance of ring topology becomes better than bus topology under heavy traffic.
9) Easy to manage.
10) Ring network is extremely orderly organized where every device has access to the token and therefore the opportunity to transmit.

Disadvantages of Ring topology :

1. Due to the Uni-directional Ring, a data packet (token) must have to pass through all the nodes.
2. If one workstation shuts down, it affects whole network or if a node goes down entire network goes down.
3. It is slower in performance as compared to the bus topology
4. It is Expensive.
5. Addition and removal of any node during a network is difficult and may cause issue in network activity.
6. Difficult to troubleshoot the ring.
7. In order for all the computer to communicate with each other, all computer must be turned on.
8. Total dependence in on one cable.
9. They were not Scalable.

Mesh Topology : In this ,every device is connected to another device via a particular channel.These channels are known as links.

In mesh, all the computers are interconnected to every other during a network. Each computer not only sends its own signals but also relays data from other computers. The nodes are connected to every other completely via a dedicated link during which information is travel from nodes to nodes and there are N(N-1)/2 links in mesh if there are N nodes. Every node features a point-to-point connection to the opposite node. The connections within the mesh are often wired or wireless.



There are two types of Mesh topologies –

Fully-connected Mesh Topology
Partially-connected Mesh Topology

1. Full Mesh Topology :

All the nodes within the network are connected with every other If there are n number of nodes during a network, each node will have an n-1 number of connections. A full mesh provides an excellent deal of redundancy, but because it is prohibitively expensive to implement, it's usually reserved for network backbones.

Total number of links required for the mesh topology is [n(n-1)]/2.

2. Partial Mesh Topology :

The partial mesh is more practical as compared to the full mesh. In a partially connected mesh, all the nodes aren't necessary to be connected with one another during a network. Peripheral networks are connected using partial mesh and work with a full-mesh backbone in tandem.

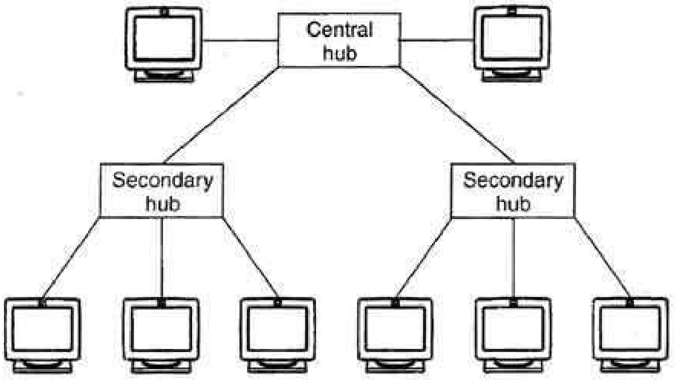
Advantages of Mesh Topology :

1) Failure during a single device won't break the network.
2) There is no traffic problem as there is a dedicated point to point links for every computer.
3) Fault identification is straightforward.
4) This topology provides multiple paths to succeed in the destination and tons of redundancy.
5) It provides high privacy and security.
6) Data transmission is more consistent because failure doesn't disrupt its processes.
7) Adding new devices won't disrupt data transmissions.
8) This topology has robust features to beat any situation.
9) A mesh doesn't have a centralized authority.

Disadvantages of Mesh Topology :

1. It’s costly as compared to the opposite network topologies i.e. star, bus, point to point topology.
2. Installation is extremely difficult in the mesh.
3. Power requirement is higher as all the nodes will need to remain active all the time and share the load.
4. Complex process.
5. The cost to implement mesh is above other selections.
6. There is a high risk of redundant connections.
7. Each node requires a further utility cost to think about.
8. Maintenance needs are challenging with a mesh.

Tree Topology : It allows more devices to be attached to a single central hub,thus it decreased the disatnce that is travelled by the signal to come to the devices.it allows the network to get isolated and also prioritze from different computers. In computer network a tree topology is also known as a star bus topology.It incorporates elements of both a bus and star topology.



Tree Topology

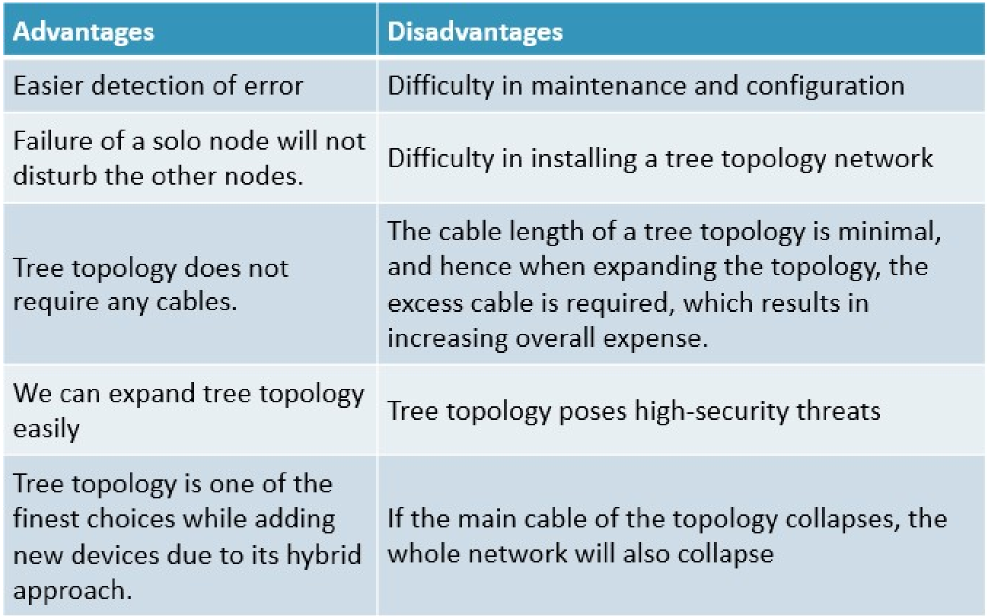
Advantages of Tree Topology

1) It allows more devices to be attached to a single central hub ,thus it decreases the distance that is traveled by the signal to come to the devices.
2) It allows the network to get isolated and also prioritize from different computers.
3) Detection of error: In a tree topology, error detection becomes more accessible. All the nodes in this topology are connected through the central hub. The hub can easily detect the node with error since all the information transmitted through the nodes passes through the hub. The node which has a mistake can be easily replaced by replacing the faulty node.
4) Sturdiness: In tree topology, if a single node gets defected, it will not affect the other nodes. The entire tree topology network is based on the main backbone cable. Hence, the failure of one node will not affect the other nodes, and the other nodes will continue to function regularly. The removal of any node does not affect the performance of the network.
5) Easy expansion: The expansion of tree topology is a straightforward method. It can be expanded even if there is no space. Since this topology follows a hierarchy pattern, many secondary nodes can be attached to it without any issue. As long as enough hubs and cables are available, the expansion won’t be a problem.
6) Device support: While adding new devices, one of the best considerable options is a tree topology. Due to its hybrid approach, various manufacturers support this network. It also allows the manufacturers to easily access the devices connected to the network for maintenance and other work.
7) Low cable requirement: Installation of a tree topology does not require any cables. There is the existence of a single cable that acts as the backbone of the network, and it runs joint for all the

segments of the network. Every tree network is allocated with a point to point wiring. This point-to-point wiring in the network ensures high bandwidth and low latency.

Disadvantages of Tree Topology

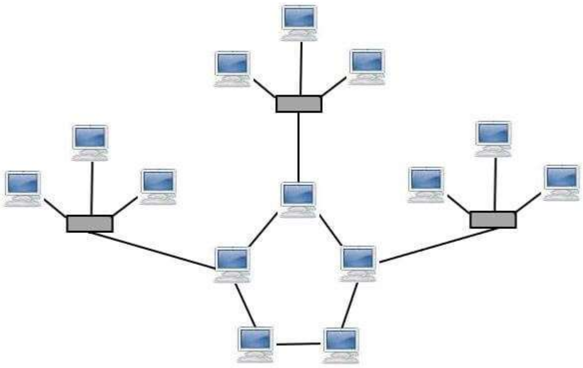
1. If the central hub get fails the entire system get failed
2. Cost is high because of cabling
3. Installing tree topology: The uses of tree topology are limited due to its difficult installation process. Tree topology includes the functions of both bus and star topology. Hence, the cabling requirement of a tree topology is massive. Due to this reason, the process of installing this topology becomes expensive and difficult to handle.
4. Security: The security of tree topology is extremely weak. In tree topology, all the computers are interconnected with each other. As a result, any computer within the network can access the data that passes through the network. Therefore, if a hacker somehow manages to take over a single workstation, they can quickly access all the data, and hence the whole network is compromised.
5. Reliability: The backbone cable of the tree topology is the main cable on which the entire network depends. If the backbone cable gets defected and fails, then the whole network will collapse. The point where the failure occurs also decides the level of loss. If the damage is restricted before a specific branch, all the segments related to that branch will face problems while functioning. On the other hand, the components which are not associated with it will continue to work usually.
6. Cost: The cable length of a tree topology is also an essential factor. While creating the point-to-point connection in tree topology, the cable length is limited to a certain point by default. This limitation later causes trouble since it makes it challenging to get wired. Regardless of this, there will be high wiring requirements if the network needs expansion, which will increase the total cost.
7. Maintenance: Maintenance and configuration of tree topology become difficult due to its large size. A lot of time is taken up for managing point-to-point connections, individual star networks, and identification of errors. This is amongst one of the major reasons why large organizations less prefer tree topology.



Advantages	Disadvantages
Easier detection of error	Difficulty in maintenance and configuration
Failure of a solo node will not disturb the other nodes.	Difficulty in installing a tree topology network
Tree topology does not require any cables.	The cable length of a tree topology is minimal, and hence when expanding the topology, the excess cable is required, which results in increasing overall expense.
We can expand tree topology easily	Tree topology poses high-security threats
Tree topology is one of the finest choices while adding new devices due to its hybrid approach.	If the main cable of the topology collapses, the whole network will also collapse

Hybrid Topology : It is the combination of all the various types of topologies.It is used when the nodes are free to take any form.It means these can be individuals such as Ring or star topology or can be combination of various topology.

A hybrid topology is a kind of network topology that is a combination of two or more network topologies, such as mesh topology, bus topology, and ring topology. Its usage and choice are dependent on its deployments and requirements like the performance of the desired network, and the number of computers, their location. The below figure is describing the structure of hybrid topology that contains more than one topology.



Advantages of Hybrid Topology:

1) This type of topology combines the benefits of different types of topologies in one topology.
2) Can be modified as per requirement.
3) It is extremely flexible.
4) It is very reliable.
5) It is easily scalable as Hybrid networks are built in a fashion which enables easy integration of new hardware components.
6) Error detecting and troubleshooting are easy.
7) Handles a large volume of traffic.
8) It is used to create large networks.
9) The speed of the topology becomes fast when two topologies are put together.

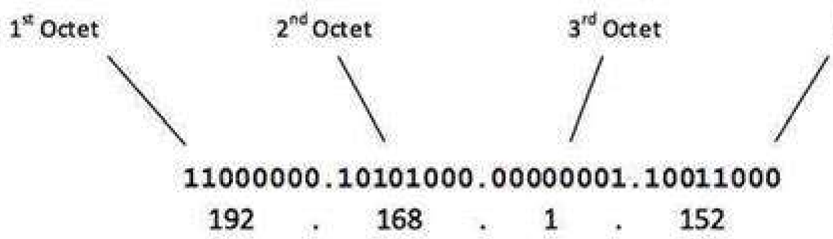
Disadvantages of Hybrid Topology :

1. It is a type of network expensive.
2. The design of a hybrid network is very complex.
3. There is a change in the hardware to connect one topology with another topology.
4. Usually, hybrid architectures are larger in scale so they require a lot of cables in the installation process.
5. Hubs which are used to connect two distinct networks are very costly. And hubs are different from usual hubs as they need to be intelligent enough to work with different architectures.
6. Installation is a difficult process.

What is IP?

IP Address stands for internet protocol Address. Computer use IP address to communicate with each other both over the internet as well as on the other networks. There are two versions of IP that currently coexist in the global internet : IPV4 & IPV6

IPV4



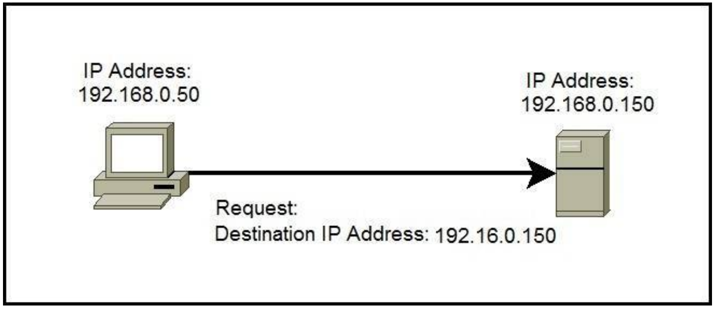
- Internet Protocol Version 4
- It defines an IP address as a 32-bit number.
- The original version of the internet protocol that was first deployed in 1983 in the ARPANET(Advanced Research Projects Agency Network),the predecessor of the internet is IPV4.
- IP address are written & displayed in human readable notations.

IPV4 Address Types:

They're categorized into three basic types- unicast address,multicast address,broadcast address.

1. Unicast Address : One-to-One trasmission

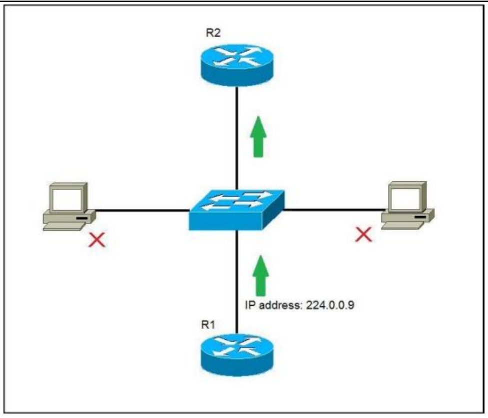
It is an address of a single interface. The IP addresses of this type are used for one-to-one communication. Unicast IP addresses are used to direct packets to a specific host. Here is an example:



In the picture above you can see that the host wants to communicate with the server. It uses the IP address of the server (192.168.0.150) to do so.

2. Multicast address : One/more sender and one/more recipient participate in data transfer traffic.

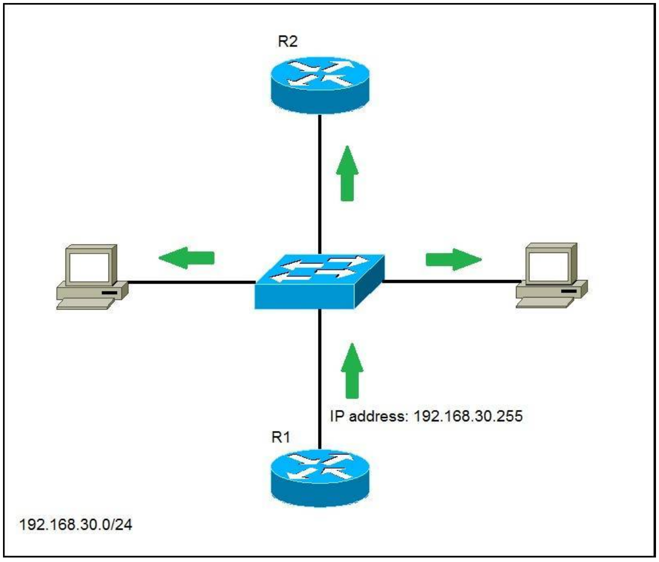
It is used for one-to-many communication. Multicast messages are sent to IP multicast group addresses. Routers forward copies of the packet out to every interface that has hosts subscribed to that group address. Only the hosts that need to receive the message will process the packets. All other hosts on the LAN will discard them. Here is an example:



R1 has sent a multicast packet destined for 224.0.0.9. This is an RIPv2 packet, and only routers on the network should read it. R2 will receive the packet and read it. All other hosts on the LAN will discard the packet.

3. Broadcast Address : Broadcasting transfer(one-to-all)

broadcast IP addresses – used to send data to all possible destinations in the broadcast domain (the one-to-everybody communication). The broadcast address for a network has all host bits on. For example, for the network 192.168.30.0 255.255.255.0 the broadcast address would be 192.168.30.255. Also, the IP address of all 1's (255.255.255.255) can be used for local broadcast. Here's an example:

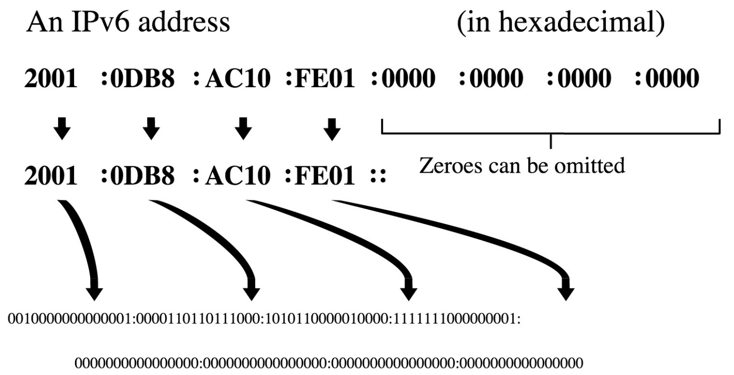


R1 has sent a broadcast packet to the broadcast IP address 192.168.30.255. All hosts in the same broadcast domain will receive and process the packet.

IPV6

The growth of the internet and the depletion of available IPV4 address,a new version of IP,using 128 bits for IP,was standardized in 1998. The IPV6 deployment has been ongoing since the mid 2000's.IPV6 address are represented as eight groups of four hexadecimal digits each separated by colons.

IPV6 was developed by Internet Engineering Task Force(IETF)



Internet Protocol Version 6 (IPv6) is a network layer protocol that allows communication and data transfers to take place over the network. IPv6 came into existence in 1998 with the sole purpose of taking over and replace the IPv4 protocol one day.

IPv4 protocol, the previous standard, consists of four number strings – each containing three digits separated by dots. A standard IPv4 address is 32-bit and looks something like 255.255.255.255, which allows 4.2 billion unique IP addresses

With wireless and network-attached devices increasing rapidly by the day, it was expected that by 2010, the internet would have exhausted all unique IPv4 addresses. To come up with a new standard of network layer protocol that allows more unique IP addresses to be created, IPv6 was standardized.

IPv6 protocol, which is 128-bits, consists of eight numbered strings, each containing four characters (alphanumeric), separated by a colon. This gives us an unbelievable amount of unique IP addresses; 340,282,366,920,938,463,463,374,607,431,768,211,456 to be precise. It also assures that we will not run out of unique IP addresses to assign to new devices anytime soon.

What are the Types of IPv6 Address?

Now that we know about what is IPv6 addresses let's take a look at their different types.

1) Unicast addresses : It identifies a unique node on a network and usually refers to a single sender or a single receiver.
2) Multicast addresses : It represents a group of IP devices and can only be used as the destination of a datagram.
3) Anycast addresses : It is assigned to a set of interfaces that typically belong to different nodes

Advantages of IPv6

1. Reliability
2. Faster Speeds
3. Stringer Security
4. Routing efficiency
5. Global Reachability
6. Enhanced Encryption
7. Higher Website Conversion
8. Improved User Experience
9. Better Customer Insights

Disadvantages of IPv6

1) Conversion:IPv4 is still very popular. People and companies are taking their time to make the switch to IPv6.
2) Communication:IPv4 and IPv6 machines cannot communicate directly with each other. They need in-between equipment to make that possible.Transition:For an individual to switch from IPv4 to IPv6, it requires immense effort and countless hours.
3) Readability:IPv6 subnetting is complicated to comprehend while remembering your IPv6 address is nearly impossible, unlike IPv4.

What is an IP address?

An IP address is a number which identifies a device within a computer network. It is part of the internet protocol standard and is being used to transfer data between a sender and a receiver.

What is an IPv4 address?

IPv4 stands for Internet Protocol Version 4, which is a standard who enables a total range of 4.2 billion addresses. It consists of four segments which are divided by dots.

Example
197.228.0.32

What is the difference between IPv4 and IPv6?

IPv6 stands for IP Version 6. This newer implementation enables a wider scope for issued addresses. In total there can be 2^128 addresses. These are generally displayed in a hexadecimal format. Since the amount of addresses within the IPv4 format is limited and more and more devices worldwide are being connected to the internet and new format had to be introduced. IPv6 enables a wider range of addresses and ensures, that new devices can be connected to the world wide web.

Example
2001:db8::211:22ff:fe33:4455

IP Classes

IP addresses are divided into five classes that are identified by the value of the first octet (the first decimal number). The system of IP address classes was developed for the purpose of Internet IP addresses assignment. The classes created were based on the network size. For example, for the small number of networks with a very large number of hosts, the Class A was created. The Class C was created for the numerous networks with the small number of hosts.

The IP address classes are:

- Class A, 0-127 – for example, 10.50.13.40. For large networks with many devices.
- Class B, 128-191 – for example, 130.5.4.77. For medium-sized networks.
- Class C, 192-223 – for example, 192.168.5.10. For small networks with the small number of hosts.
- Class D, 224-239 – for example, 224.0.0.5. For multicast addresses.
- Class E, 240-255 – for example, 241.0.0.1. Experimental/researcher.

Reserved addresses (used for special purposes):

0.0.0.0/8 – used to communicate with the network the device is on.
127.0.0.0/8 – loopback addresses.
169.254.0.0/16 – link-local addresses (APIPA).

An IP address consists of 32 bits. These bits are divided into two parts:

network bits – identify a particular network.
host bits – identify a host on the network.

What is a Loopback Address?

A loopback address is a distinct reserved IP address range that starts from 127.0.0.0 ends at 127.255.255.255 though 127.255.255.255 is the broadcast address for 127.0.0.0/8. The loopback addresses are built into the IP domain system, enabling devices to transmit and receive the data packets. The loopback address 127.0.0.1 is generally known as localhost.

TCP/IP protocol manages all the loopback addresses in the operating system. It mocks the TCP/IP server or TCP/IP client on the same system. These loopback addresses are always accessible so that the user can use them anytime for troubleshooting TCP/IP.

Whenever a protocol or program sends any data from a computer with any loopback IP address, that traffic is processed by a TCP/IP protocol stack within itself, i.e., without transmitting it to the network. That is, if a user is pinging a loopback address, they'll get the reply from the same TCP/IP stack running on their computer. So, all the data transmitted to any of the loopback addresses as the destination address will not pop up on the network.

127.0.0.1 is the most commonly used loopback address; generally, 127.0.0.1 and localhost are functionally similar, i.e., the loopback address 127.0.0.1 and the hostname localhost; are internally mapped. Though, other loopback addresses are also accessible and can be used.

IPv4 and IPv6 Loopback Addresses:

The IPv4 loopback address is 127.0.0.0/8 and the most commonly used loopback address is 127.0.0.1.
The IPv6 loopback address is ::1

Advantages of loopback address:

It is an efficient method to find a device on the network.
It can be configured as the router ID for protocols such as BGP and OSPF.
It is used as a source and destination address for testing network connectivity.
It can also be used for testing IP software.
Disadvantages:

Just like physical interfaces, it needs a unique address.

IP Types

There are mainly four types of IP addresses:

Public,
Private,
Static
Dynamic.
Among them, public and private addresses are based on their location of the network private, which should be used inside a network while the public IP is used outside of a network.

Let us see all these types of IP address in detail.

Public IP Addresses
A public IP address is an address where one primary address is associated with your whole network. In this type of IP address, each of the connected devices has the same IP address.

This type of public IP address is provided to your router by your ISP.

Private IP Addresses
A private IP address is a unique IP number assigned to every device that connects to your home internet network, which includes devices like computers, tablets, smartphones, which is used in your household.

It also likely includes all types of Bluetooth devices you use, like printers or printers, smart devices like TV, etc. With a rising industry of internet of things (IoT) products, the number of private IP addresses you are likely to have in your own home is growing.

Dynamic IP address:
Dynamic IP addresses always keep changing. It is temporary and are allocated to a device every time it connects to the web. Dynamic IPs can trace their origin to a collection of IP addresses that are shared across many computers.

Dynamic IP addresses are another important type of internet protocol addresses. It is active for a specific amount of time; after that, it will expire.

Static IP Addresses
A static IP address is an IP address that cannot be changed. In contrast, a dynamic IP address will be assigned by a Dynamic Host Configuration Protocol (DHCP) server, which is subject to change. Static IP address never changes, but it can be altered as part of routine network administration.

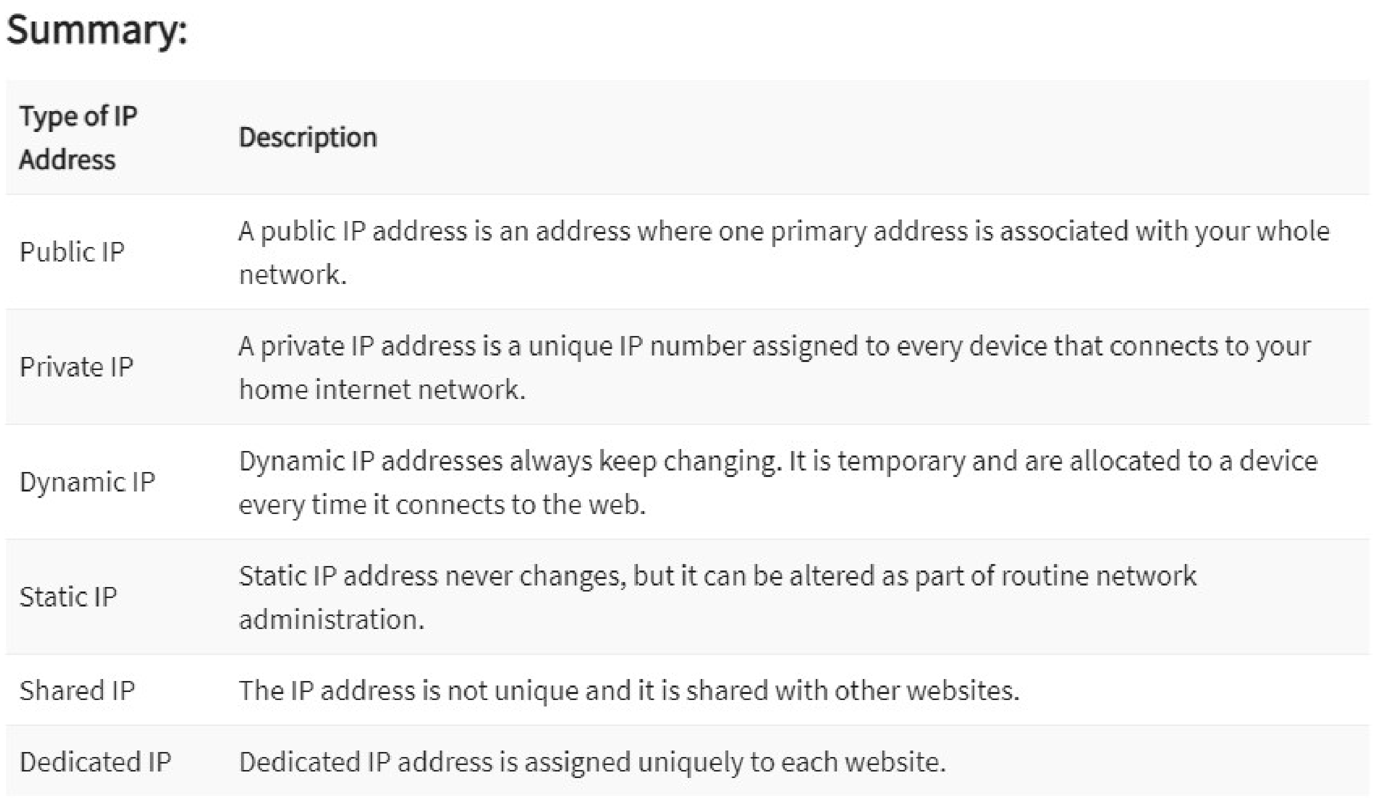
Static IP addresses are consistent, which is assigned once, that stays the same over the years. This type of IP also helps you procure a lot of information about a device.

Types of Website IP Addresses

Two types of website IP Addresses are 1) Share IP Address 2) Dedicated IP Address

Shared IP Addresses:
Shared IP address is used by small business websites that do not yet get many visitors or have many files or pages on their site. The IP address is not unique and it is shared with other websites.

Dedicated IP Addresses:
Dedicated IP address is assigned uniquely to each website. Dedicated IP addresses helps you avoid any potential backlists because of bad behavior from others on your server. The dedicated IP address also gives you the option of pulling up your website using the IP address alone, instead of your domain name. It also helps you to access your website when you are waiting on a domain transfer.



Summary:

Type of IP Address	Description
Public IP	A public IP address is an address where one primary address is associated with your whole network.
Private IP	A private IP address is a unique IP number assigned to every device that connects to your home internet network.
Dynamic IP	Dynamic IP addresses always keep changing. It is temporary and are allocated to a device every time it connects to the web.
Static IP	Static IP address never changes, but it can be altered as part of routine network administration.
Shared IP	The IP address is not unique and it is shared with other websites.
Dedicated IP	Dedicated IP address is assigned uniquely to each website.

What is a protocol ?

A network protocol is an established set of rules that determine how data is transmitted between different devices in the same network.
Essentially it allows connected devices to communicate with each other regardless of any difference in their internal process,structure or design.

Types of Protocol

- TCP
- POP
- HTTP
- SMTP
- SSL
- FTP

HTTP:

1. Hyper Text Transfer Protocol
2. It is an application layer protocol for transmitting hypermedia documents such as HTML.
3. It was designed for communicating between web browsers and web servers,but it can also be used for other purposes.
4. HTTP is one of the most commonly used application-level protocol used for hyper-text data distribution, collaboration, and hypertext information system.
5. HTTP is abbreviated as Hypertext Transfer Protocol, an application layer protocol used primarily with the WWW (World Wide Web) in the client-server model where a web browser is a client communicating with the webserver which is hosting the website. Since 1990, this has become the foundation for data communication. HTTP is a standard and stateless protocol that is used for different purposes as well using extensions for request methods, error codes, as well as headers.
6. HTTP is a communication protocol which is employed for delivering data (usually HTML files, multimedia files, etc.) on the World Wide Web through its default TCP port 80. However, there are other ports also which can be implemented for this function. HTTP has two different versions, HTTP/1.0, which is the old one and the newest HTTP/1.1. In its older version, a separate connection was required. In the case of a new version, the same connection can be recycled several times.

Steps involved in HTTP request:

A necessary HTTP request has the following steps:

- Initially, a link to the HTTP server gets opened.
- Then a request is sent.
- It does some processing on the server.
- Once the request processing is done, the response is sent back from the server.
- Finally, the connection is closed.

Architecture of HTTP

The HTTP is meant for request/response depending on a client-server architecture where the user requests information through a web browser to the web server, which then responds to the requested data.

Web Client: The client of this client-server architecture asks for a request to a specific server through the HTTP (TCP/IP connection) as a request method in the form of a URL. It also contains a MIME-like message that contains request modifier and client information.

Web Server: This accepts the request and process with a response by a status line, together with the version of the message's protocol as well as the success or error code, followed by a MIME-like message having server information, some metadata, and possible the entity-body content holding the requested information.

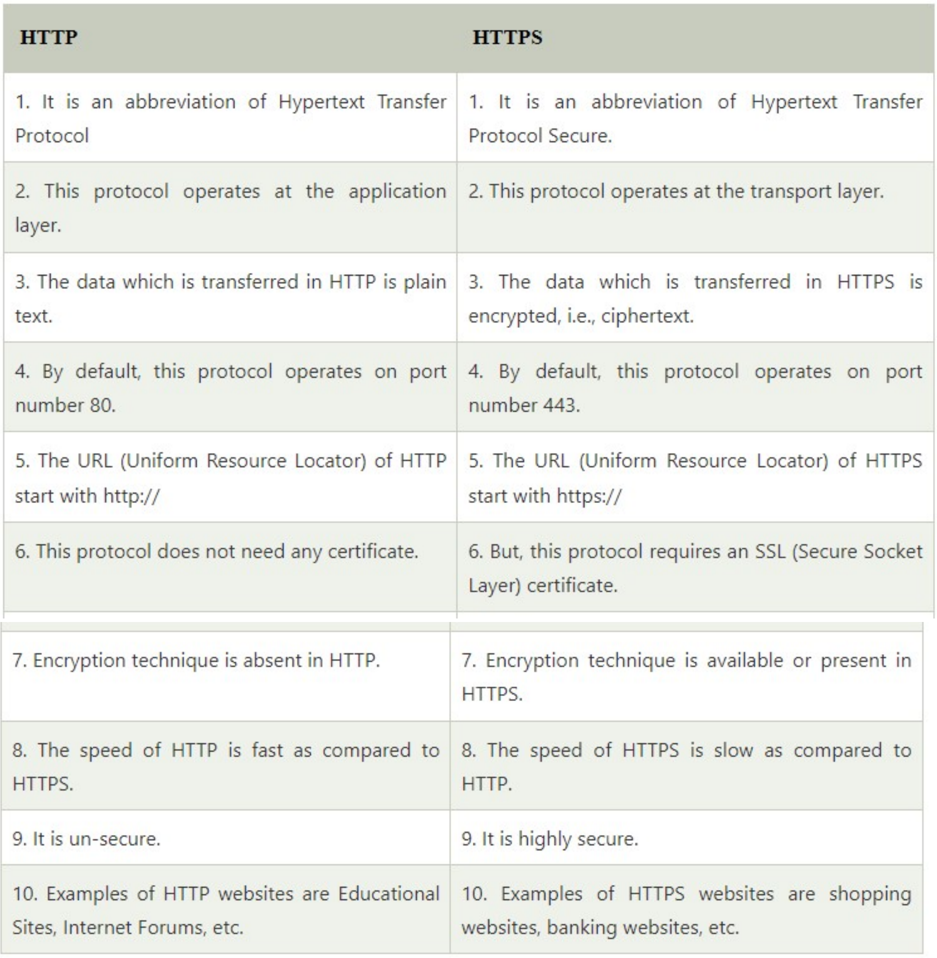
Feature of HTTP

- **HTTP is connection less:** An HTTP request is initiated by the browser (HTTP client) as per the user's request for information. The server will process the request and launch back with a response which the client waits for.
- **HTTP is simple:** HTTP/2 does the encapsulation of HTTP messages into frames; i.e., HTTP is typically designed to be plain and human-readable.
- **HTTP is extensible/customized:** HTTP can be integrated with new functionality by providing a simple agreement between a client and a server.
- **HTTP is stateless, but not sessionless:** HTTP is stateless, which means there is no connection among two requests being consecutively carried out on the same connection. However, when the core of HTTP is itself a stateless one, HTTP cookies provide in making use of stateful sessions. Through the concept of header extensibility, HTTP cookies can be incorporated into the workflow, making session creation on each HTTP request for sharing the same content.

HTTPS

1. Hypertext Transfer Protocol Secure
2. It is an extension of the hypertext transfer protocol
3. It is used for secure communication over a computer network and is widely used on internet.
4. HTTPS is an abbreviation of Hypertext Transfer Protocol Secure. It is a secure extension or version of HTTP. This protocol is mainly used for providing security to the data sent between a website and the web browser. It is widely used on the internet and used for secure communications. This protocol uses the 443 port number for communicating the data.
5. This protocol is also called HTTP over SSL because the HTTPS communication protocols are encrypted using the SSL (Secure Socket Layer).
6. By default, it is supported by various web browsers.
7. Those websites which need login credentials should use the HTTPS protocol for sending the data.

Difference between HTTP and HTTPS



HTTP	HTTPS
1. It is an abbreviation of Hypertext Transfer Protocol	1. It is an abbreviation of Hypertext Transfer Protocol Secure.
2. This protocol operates at the application layer.	2. This protocol operates at the transport layer.
3. The data which is transferred in HTTP is plain text.	3. The data which is transferred in HTTPS is encrypted, i.e., ciphertext.
4. By default, this protocol operates on port number 80.	4. By default, this protocol operates on port number 443.
5. The URL (Uniform Resource Locator) of HTTP start with http://	5. The URL (Uniform Resource Locator) of HTTPS start with https://
6. This protocol does not need any certificate.	6. But, this protocol requires an SSL (Secure Socket Layer) certificate.
7. Encryption technique is absent in HTTP.	7. Encryption technique is available or present in HTTPS.
8. The speed of HTTP is fast as compared to HTTPS.	8. The speed of HTTPS is slow as compared to HTTP.
9. It is un-secure.	9. It is highly secure.
10. Examples of HTTP websites are Educational Sites, Internet Forums, etc.	10. Examples of HTTPS websites are shopping websites, banking websites, etc.

Advantages of HTTPS:

Following are the advantages or benefits of a Hypertext Transfer Protocol Secure (HTTPS):

- The main advantage of HTTPS is that it provides high security to users.
- Data and information are protected. So, it ensures data protection.
- SSL technology in HTTPS protects the data from third-party or hackers. And this technology builds trust for the users who are using it.
- It helps users by performing banking transactions.

Disadvantages of HTTPS:

Following are the disadvantages or limitations of a Hypertext Transfer Protocol Secure (HTTPS):

- The big disadvantage of HTTPS is that users need to purchase the SSL certificate.
- The speed of accessing the website is slow because there are various complexities in communication.
- Users need to update all their internal links.

SSH

1. Secure shell
2. It is a network communication protocol that enables two computers to communicate and share data
3. SSH(Secure Shell) is access credential that is used in the SSH Protocol. In other words, it is a cryptographic network protocol that is used for transferring encrypted data over network. It allows you to connect to a server, or multiple servers, without having you to remember or enter your password for each system that is to login remotely from one system into another.

It always comes in key pair:

- Public key – Everyone can see it, no need to protect it. (for encryption function)
- Private key – Stays in computer, must be protected. (for decryption function)

Key pairs can be of the following types:

- User Key – If public key and private key remain with the user.
- Host Key – If public key and private key are on a remote system.
- Session key – Used when large amount of data is to be transmitted.

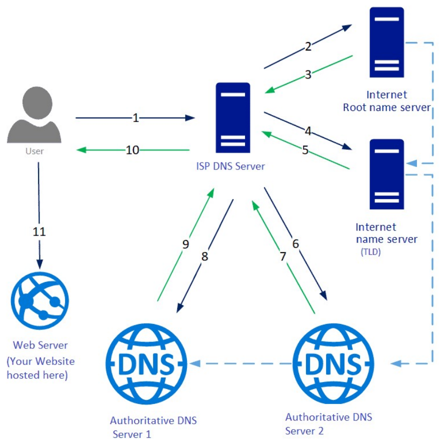
FTP

1. It is a standard communication protocol used for the transfer of computer files from a server to a client on a computer network.
2. File transfer protocol (FTP) is an Internet tool provided by TCP/IP. The first feature of FTP is developed by Abhay Bhushan in 1971. It helps to transfer files from one computer to another by providing access to directories or folders on remote computers and allows software, data, text file to be transferred between different kinds of computers. The end-user in the connection is known as localhost and the server which provides data is known as the remote host.

The goals of FTP are:

- It encourages the direct use of remote computers.
- It shields users from system variations (operating system, directory structures, file structures, etc.)
- It promotes sharing of files and other types of data.

DNS

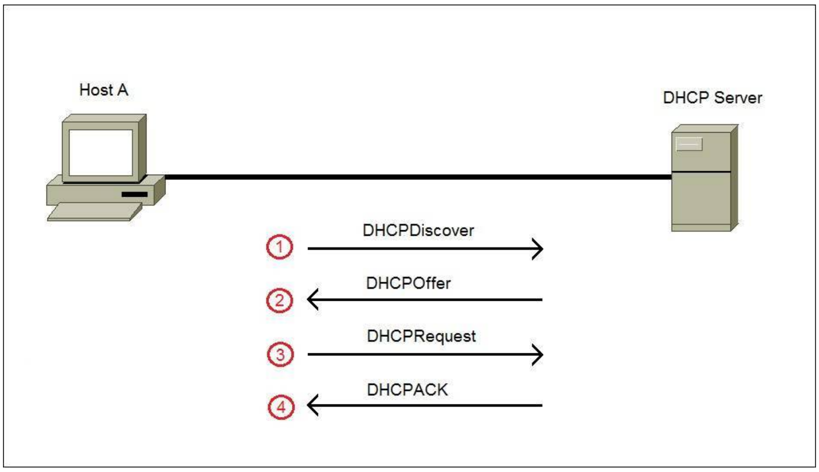


1. It is the hierarchical and decentralized naming system used to identify computer reachable through the internet or other IP network.
2. The Domain Name System (DNS) turns domain names into IP addresses, which browsers use to load internet pages. Every device connected to the internet has its own IP address, which is used by other devices to locate the device. DNS servers make it possible for people to input normal words into their browsers, such as Fortinet.com, without having to keep track of the IP address for every website.

DHCP

1) Dynamic Host Configuration Protocol
2) It is a client/server protocol that automatically provides an ip host with its IP address and other realted configuration information such as the subnet mask & default gateway.
3) DHCP (Dynamic Host Configuration Protocol) is a protocol that provides quick, automatic, and central management for the distribution of IP addresses within a network. It's also used to configure the subnet mask, default gateway, and DNS server information on the device.

How DHCP Works?



a) A DHCP server issues unique IP addresses and automatically configures other network information. In most homes and small businesses, the router acts as the DHCP server. In large networks, a single computer might take on that role. To make this work, a device (the client) requests an IP address from a router (the host). Then, the host assigns an available IP address so that the client can communicate on the network.
b) When a device is turned on and connected to a network that has a DHCP server, it sends a request to the server, called a DHCPDISCOVER request.

c) After the DISCOVER packet reaches the DHCP server, the server holds on to an IP address that the device can use, then offers the client the address with a DHCPOFFER packet.

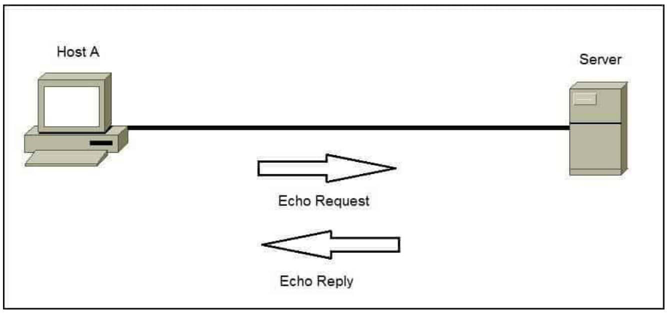
d) Once the offer has been made for the chosen IP address, the device responds to the DHCP server with a DHCPREQUEST packet to accept it. Then, the server sends an ACK to confirm that the device has that specific IP address and to define the amount of time that the device can use the address before getting a new one.

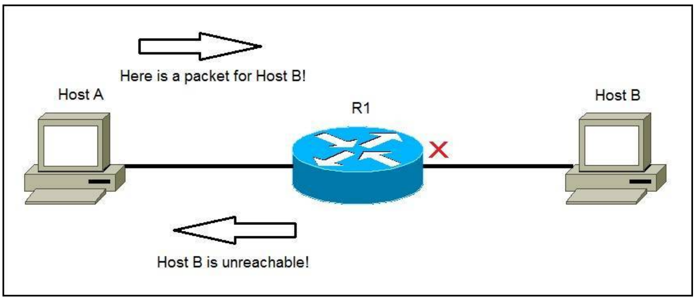
e) If the server decides that the device cannot have the IP address, it will send a NACK.

What is DHCP snooping?
DHCP snooping is a layer two security technology that stops any DHCP traffic that it defines as unacceptable. The snooping technology, built into the network switch operating system, prevents unauthorized DHCP servers from offering IP addresses to DHCP clients.

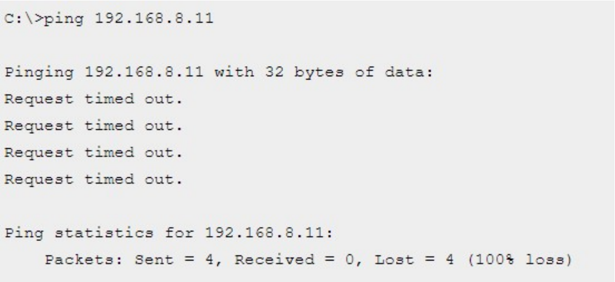
What is DHCP relay?
A relay agent is a host that forwards DHCP packets between clients and servers. A network administrator can use relay agents to forward requests and replies between clients and servers not on the same physical subnet.

ICMP





1. Internet Control Manage Protocol
2. It is a protocol that devices within a network use to communicate problem with data transmission.
3. ICMP (Internet Control Message Protocol) is a network layer protocol that reports errors and provides information related to IP packet processing. ICMP is used by network devices to send error messages indicating, for example, that a requested service is not available or that a host isn't reachable
4. ICMP is commonly used by network tools such as ping or traceroute. Consider the following example that illustrates how ping can be used to test the reachability of a host:
5. Host A wants to test whether it can reach Server over the network. Host A will start the ping utility that will send ICMP Echo Request packets to Server. If Server is reachable, it will respond with ICMP Echo Reply packets. If Host A receives no response from Server, there might be a problem on the network.
6. One other common ICMP message is the Destination unreachable message. Here is an example:
7. Host A sends a packet to Host B. Because the Host B is down, the router will send an ICMP Destination host unreachable message to Host A, informing it that the destination host is unreachable, e.g.:

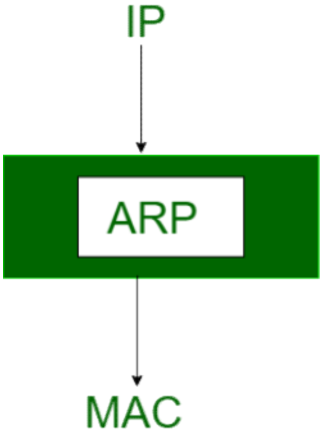


```
C:\>ping 192.168.8.11

Pinging 192.168.8.11 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.8.11:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss)
```

NOTE
ICMP messages are encapsulated in IP datagrams, which means that they don't use higher level protocols (such as TCP or UDP) for transmission.

ARP

1) Address Resolution Protocol
2) It is a protocol or procedure that connects an ever-changing IP address to a fixed physical machine address,also known as MAC address,in a LAN.
3) Most of the computer programs/applications use logical address (IP address) to send/receive messages, however, the actual communication happens over the physical address (MAC address) i.e from layer 2 of the OSI model. So our mission is to get the destination MAC address which helps in communicating with other devices. This is where ARP comes into the picture, its functionality is to translate IP address to physical addresses.



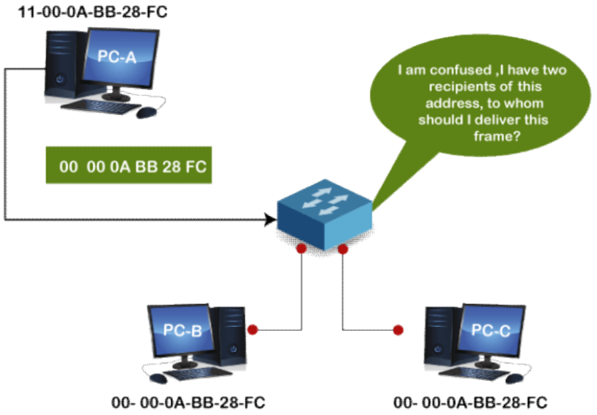
4) The acronym ARP stands for Address Resolution Protocol which is one of the most important protocols of the Network layer in the OSI model.
5) Note: ARP finds the hardware address, also known as Media Access Control (MAC) address, of a host from its known IP address.

MAC

1. Media Access Control
2. It is a unique identifier assigned to a network interface card for use as a network address in communication within a network segment.
3. MAC address is the physical address, which uniquely identifies each device on a given network. To make communication between two networked devices, we need two addresses: IP address and MAC address. It is assigned to the NIC (Network Interface card) of each device that can be connected to the internet.
4. It stands for Media Access Control, and also known as Physical address, hardware address, or BIA (Burned In Address).
5. It is globally unique; it means two devices cannot have the same MAC address. It is represented in a hexadecimal format on each device, such as 00:0a:95:9d:67:16.
6. It is 12-digit, and 48 bits long, out of which the first 24 bits are used for OUI(Organization Unique Identifier), and 24 bits are for NIC/vendor-specific.
7. It works on the data link layer of the OSI model.
8. It is provided by the device's vendor at the time of manufacturing and embedded in its NIC, which is ideally cannot be changed.
9. The ARP protocol is used to associate a logical address with a physical or MAC address.

Why should the MAC address be unique in the LAN network?
If a LAN network has two or more devices with the same MAC address, that network will not work.

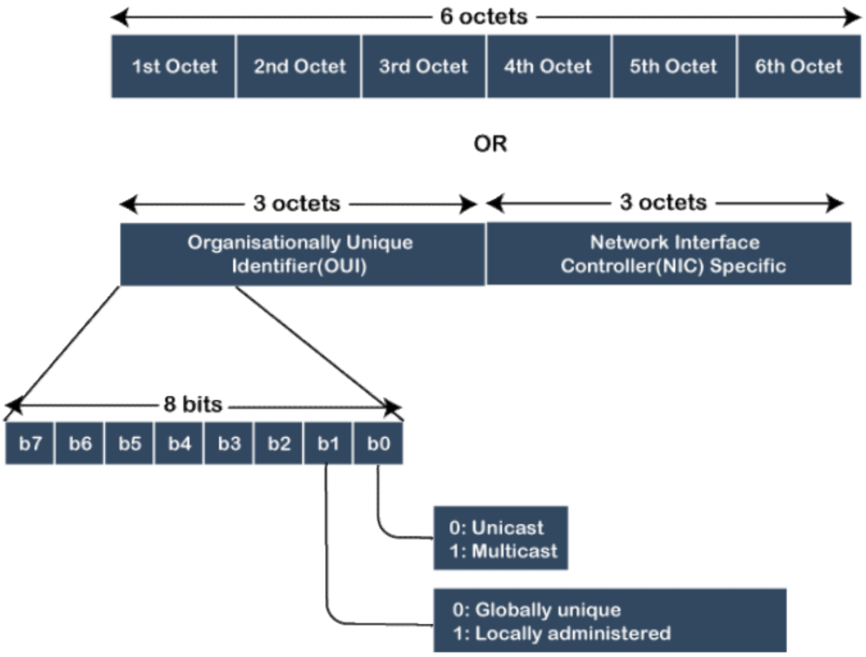
Suppose three devices A, B, and C are connected to a network through a switch. The MAC addresses of these devices are 11000ABB28FC, 00000ABB28FC, and 00000ABB28FC, respectively. The NIC of devices B and C have the same MAC address. If device A sends a data frame to the address 00000ABB28FC, the switch will fail to deliver this frame to the destination, as it has two recipients of this data frame.


11-00-0A-BB-28-FC
PC-A
00 00 0A BB 28 FC
I am confused ,I have two recipients of this address, to whom should I deliver this frame?
PC-B
PC-C
00- 00-0A-BB-28-FC
00- 00-0A-BB-28-FC

Format of MAC address

As we have already discussed in the above section, we cannot assign the MAC address to the device's NIC; it is preconfigured by the manufacturers. So, let's understand how it is configured and what format is selected.

It is 12 digits or 6-byte hexadecimal number, which is represented in colon-hexadecimal notation format. It is divided into six octets, and each octet contains 8 bits.
The first three octets are used as the OUI or Organisationally Unique Identifier. These MAC prefixes are assigned to each organization or vendor by the IEEE Registration Authority Committee.
Some example of OUI of known vendors are:
CC:46:D6 - Cisco
3C:5A:B4 - Google, Inc.
3C:D9:2B - Hewlett Packard
00:9A:CD - HUAWEI TECHNOLOGIES CO.,LTD



Reason to have both IP and MAC addresses.
As we already had the IP address to communicate a computer to the internet, why we need the MAC address. The answer to this question is that every mac address is assigned to the NIC of a hardware device that helps to identify a device over a network.

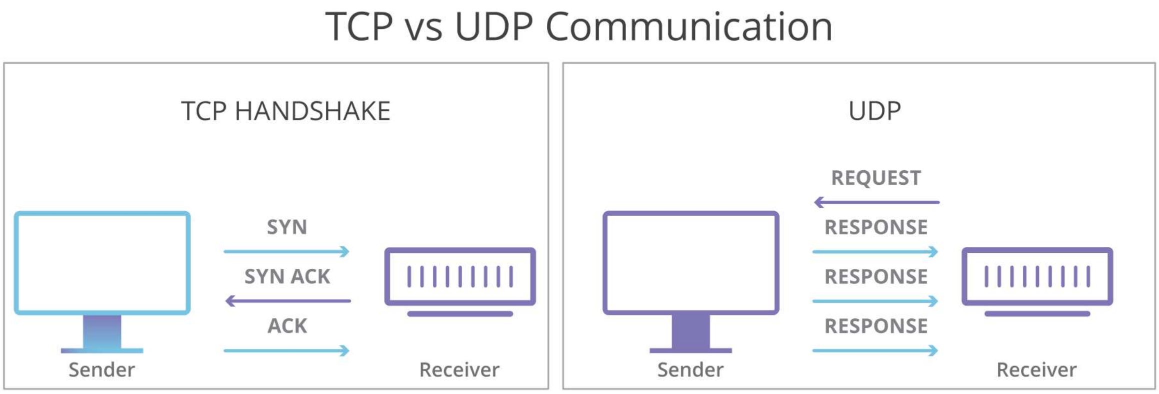
When we request a page to load on the internet, the request is responded and sent to our IP address.

Both MAC and IP addresses are operated on different layers of the internet protocol suite. The MAC address works on layer 2 and helps identify the devices within the same broadcast network (such as the router). On the other hand, the IP addresses are used on layer 3 and help identify the devices on different networks.

We have the IP address to identify the device through different networks, we still need a MAC address to find the devices on the same network.

TCP v/s UPD

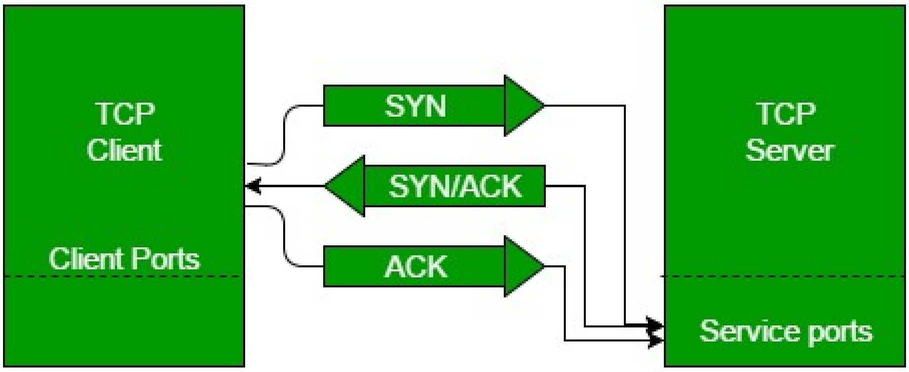
TCP	UDP
1) Transmission Control Protocol 2) It is a standard way of communication that enables application programs and computing devices to exchange messages over a network. 3) TCP stands for Transmission Control Protocol. It is a transport layer protocol that facilitates the transmission of packets from source to destination. It is a connection-oriented protocol that means it establishes the connection prior to the communication that occurs between the computing devices in a network. This protocol is used with an IP protocol, so together, they are referred to as a TCP/IP. 4) The main functionality of the TCP is to take the data from the application layer. Then it divides the data into a several packets, provides numbering to these packets, and finally transmits these packets to the destination. The TCP, on the other side, will reassemble the packets and transmits them to the application layer. As we know that TCP is a connection-oriented protocol, so the connection will remain established until the communication is not completed between the sender and the receiver.	1. User Datagram Protocol 2. It refers to a protocol used for communication throughout the internet. 3. It is specifically chosen for time-sensitive application like gaming,streaming,live or dns lookup. 4. The User Datagram Protocol, or UDP, is a communication protocol used across the Internet for especially time-sensitive transmissions such as video playback or DNS lookups. It speeds up communications by not formally establishing a connection before data is transferred. This allows data to be transferred very quickly, but it can also cause packets to become lost in transit — and create opportunities for exploitation in the form of DDoS attacks.
5)	5.



TCP Three way Handshake

This could also be seen as a way of how TCP connection is established. Before getting into the details, let us look at some basics. TCP stands for Transmission Control Protocol which indicates that it does something to control the transmission of the data in a reliable way.

The process of communication between devices over the internet happens according to the current TCP/IP suite model(stripped out version of OSI reference model). The Application layer is a top pile of a stack of TCP/IP models from where network referenced applications like web browsers on the client-side establish a connection with the server. From the application layer, the information is transferred to the transport layer where our topic comes into the picture. The two important protocols of this layer are – TCP, UDP(User Datagram Protocol) out of which TCP is prevalent(since it provides reliability for the connection established). However, you can find an application of UDP in querying the DNS server to get the binary equivalent of the Domain Name used for the website.



TCP provides reliable communication with something called Positive Acknowledgement with Re-transmission(PAR). The Protocol Data Unit(PDU) of the transport layer is called a segment. Now a device using PAR resend the data unit until it receives an acknowledgement. If the data unit received at the receiver’s end is damaged(It checks the data with checksum functionality of the transport layer that is used for Error Detection), the receiver discards the segment. So the sender has to resend the data unit for which positive acknowledgement is not received. You can realize from the above mechanism that three segments are exchanged between sender(client) and receiver(server) for a reliable TCP connection to get established.

Let us delve into how this mechanism works :

Step 1 (SYN): In the first step, the client wants to establish a connection with a server, so it sends a segment with SYN(Synchronize Sequence Number) which informs the server that the client is likely to start communication and with what sequence number it starts segments with
Step 2 (SYN + ACK): Server responds to the client request with SYN-ACK signal bits set. Acknowledgement(ACK) signifies the response of the segment it received and SYN signifies with what sequence number it is likely to start the segments with
Step 3 (ACK): In the final part client acknowledges the response of the server and they both establish a reliable connection with which they will start the actual data transfer

TCP Flags

TCP flags are used to indicate a particular state during a TCP conversation. TCP flags can be used for troubleshooting purposes or to control how a particular connection is handled.

TCP flags are various types of flag bits present in the TCP header. Each of them has its own significance. They initiate connections, carry data, and tear down connections. The commonly used TCP flags are syn, ack, rst, fin, urg, psh. We will discuss the details later.

TCP Flags List

- SYN (synchronize): Packets that are used to initiate a connection.
- ACK (acknowledgment): Packets that are used to confirm that the data packets have been received, also used to confirm the initiation request and tear down requests
- RST (reset): Signify the connection is down or maybe the service is not accepting the requests
- FIN (finish): Indicate that the connection is being torn down. Both the sender and receiver send the FIN packets to gracefully terminate the connection
- PSH (push): Indicate that the incoming data should be passed on directly to the application instead of getting buffered
- URG (urgent): Indicate that the data that the packet is carrying should be processed immediately by the TCP stack

3 Additional TCP Flags

These CWR ECE NS TCP flags are not commonly used.

CWR (congestion window has been reduced). Indicates that the sending host has received a TCP segment with the ECE flag set. The congestion window is an internal variable maintained by TCP to manage the size of the send window.
ECE (TCP peer is ECN-capable).
Indicates that a TCP peer is ECN-capable during the TCP 3-way handshake and to indicate that a TCP segment was received on the connection with the ECN field in the IP header set to 11.
NS (1 bit): ECN-nonce – concealment protection

Protocols & Ports

A network protocol is an established set of rules that determine how data is transmitted between different devices in the same network.Essentially,it allows connected devices to communicate with each other,regardless of any differences in their internal process,structure or design.
A port in networking is a software defined number associated to a network protocol that receives or transmits communication for a specific service.So IP address+port defines address of the particular service on the particular system.Thus ranging is 0-65535. Port no 0 is reserved & cannot be used.
Ports are divided into three:

1. The well known port
   a) 0-1023
   b) These are allocated to server services by the internet assigned number authority(IANA).
   c) Ex: Web server normally use port 80
   d) SMTP-port 25
2. Registered port
   a) 1024-49151
   b) These can be registered for services with IANA & should be treated as semi-reserved.
   c) User written programs should not use these.

3. Dynamic port/private port
    a) 49125-65535
    b) Free to use in client program
    c) When a web browser connects to a web server the browser will allocate itself a port in this range .
    d) Also known as ephemeral ports

What is the difference between a port number and a protocol number?

You can think of a **port** as a phone extension, with the computer's IP address being like its phone number. You can call the number (IP address) to talk to the computer, then dial the extension (port) to talk to a specific application. An application needs to be listening on a port in order to communicate.

A **protocol** is just the language that the two applications on either end of a conversation agree to speak in. If your application is sending streams of bytes to my application, my application needs to know how to interpret those bytes.

A protocol is an agreement on how to interpret data and how to respond to messages. They generally specify message formats and legal messages. Examples of protocols include:

- TCP/IP

- HTTP

- SSH

A port is part of socket end point in TCP and UDP. They allow the operating system to distinguish which TCP or UDP service on the host should receive incoming messages.

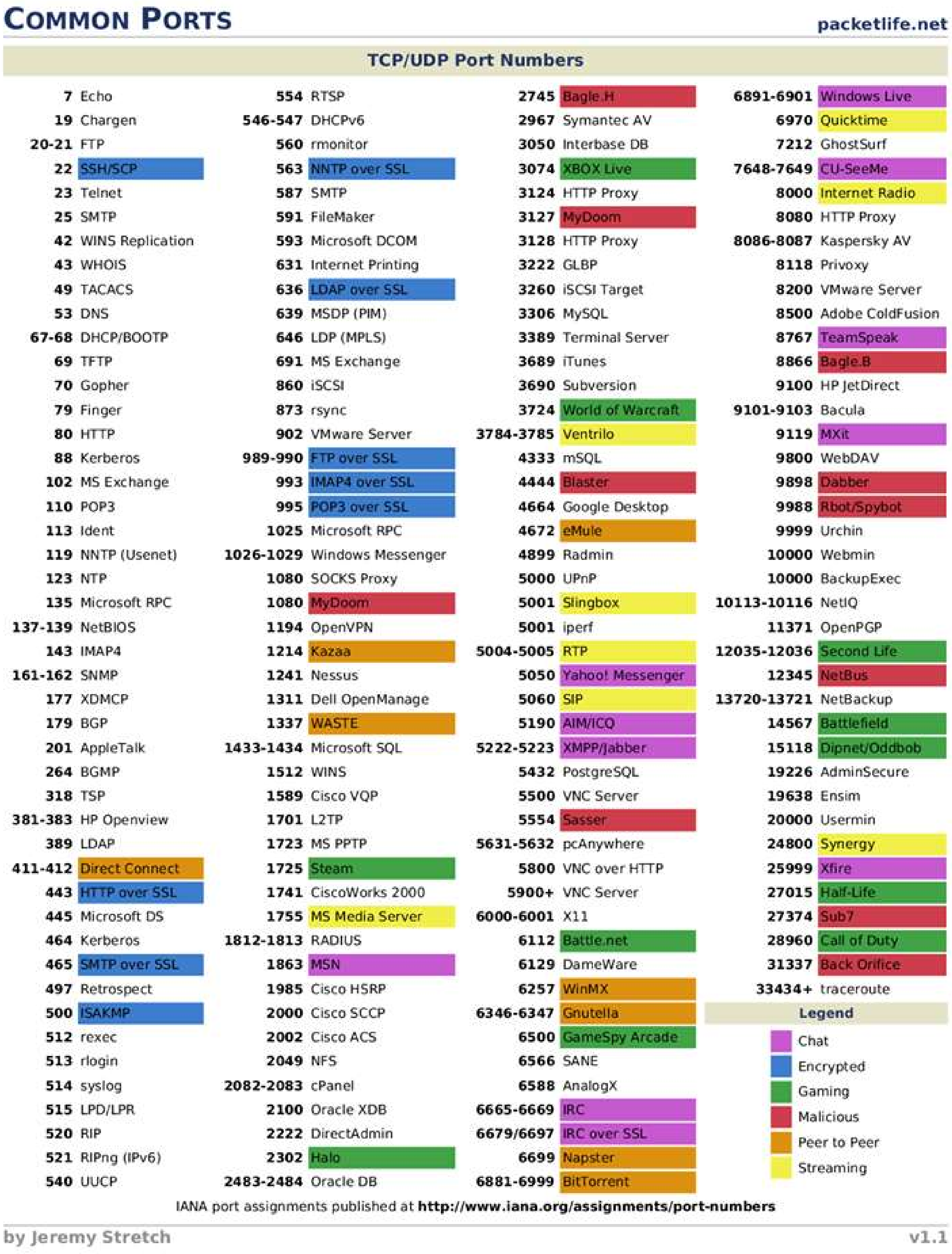
The confusion generally arises because, a number of ports are reserved (eg. port 80) and are generally listened to by severs expecting a particular protocol (HTTP in the case of port 80). While messages send to port 80 are generally expected to be HTTP messages, there is nothing stopping an non-HTTP server from listening on port 80 or an HTTP server from listening on an alternative port (for example 8080 or 8088).

A protocol is a specification for how two devices should exchange data in a way that they can both understand. A port is kind of a numbered 'tag' that helps a computer decide who should receive an incoming piece of data.

Many protocols have a port that they run on by default; this makes it easier to discover them or configure applications that use them. But that's not a hard rule; they could always listen on a different port, as long as anyone contacting them knew about the change.

In Simple port means to whom you communicate. & Protocol means how to communicate or way of communication.

A port is just a channel that you select for the communication, and the protocol determines how the communication is done. A certain protocol usually uses a specific port, like port 80 for HTTP, port 21 for FTP.



Common Ports

packetlife.net

TCP/UDP Port Numbers

7	Echo
19	Chargen
20-21	FTP
22	🟦 SSH/SCP
23	Telnet
25	SMTP
42	WINS Replication
43	WHOIS
49	TACACS
53	DNS
67-68	DHCP/BOOTP
69	TFTP
70	Gopher
79	Finger
80	HTTP
88	Kerberos
102	MS Exchange
110	POP3
113	Ident
119	NNTP (Usenet)
123	NTP
135	Microsoft RPC
137-139	NetBIOS
143	IMAP4
161-162	SNMP
177	XDMCP
179	BGP
201	AppleTalk
264	BGMP
318	TSP
381-383	HP Openview
389	LDAP
411-412	🟧 Direct Connect
443	🟦 HTTP over SSL
445	Microsoft DS
464	Kerberos
465	🟦 SMTP over SSL
497	Retrospect
500	🟦 ISAKMP
512	rexec
513	rlogin
514	syslog
515	LPD/LPR
520	RIP
521	RIPng (IPv6)
540	UUCP
554	RTSP
546-547	DHCPv6
560	rmonitor
563	🟦 NNTP over SSL
587	SMTP
591	FileMaker
593	Microsoft DCOM
631	Internet Printing
636	🟦 LDAP over SSL
639	MSDP (PIM)
646	LDP (MPLS)
691	MS Exchange
860	iSCSI
873	rsync
902	VMware Server
989-990	🟦 FTP over SSL
993	🟦 IMAP4 over SSL
995	🟦 POP3 over SSL
1025	Microsoft RPC
1026-1029	Windows Messenger
1080	SOCKS Proxy
1080	🟥 MyDoom
1194	OpenVPN
1214	🟧 Kazaa
1241	Nessus
1311	Dell OpenManage
1337	🟧 WASTE
1433-1434	Microsoft SQL
1512	WINS
1589	Cisco VQP
1701	L2TP
1723	MS PPTP
1725	🟩 Steam
1741	CiscoWorks 2000
1755	🟨 MS Media Server
1812-1813	RADIUS
1863	🟪 MSN
1985	Cisco HSRP
2000	Cisco SCCP
2002	Cisco ACS
2049	NFS
2082-2083	cPanel
2100	Oracle XDB
2222	DirectAdmin
2302	🟩 Halo
2483-2484	Oracle DB
2745	🟥 Bagle.H
2967	Symantec AV
3050	Interbase DB
3074	🟩 XBOX Live
3124	HTTP Proxy
3127	🟥 MyDoom
3128	HTTP Proxy
3222	GLBP
3260	iSCSI Target
3306	MySQL
3389	Terminal Server
3689	iTunes
3690	Subversion
3724	🟩 World of Warcraft
3784-3785	🟨 Ventrilo
4333	mSQL
4444	🟥 Blaster
4664	Google Desktop
4672	🟧 eMule
4899	Radmin
5000	UPnP
5001	🟨 Slingbox
5001	iperf
5004-5005	🟨 RTP
5050	🟪 Yahoo! Messenger
5060	🟨 SIP
5190	🟪 AIM/ICQ
5222-5223	🟪 XMPP/Jabber
5432	PostgreSQL
5500	VNC Server
5554	🟥 Sasser
5631-5632	pcAnywhere
5800	VNC over HTTP
5900+	VNC Server
6000-6001	X11
6112	🟩 Battle.net
6129	DameWare
6257	🟧 WinMX
6346-6347	🟧 Gnutella
6500	🟩 GameSpy Arcade
6566	SANE
6588	AnalogX
6665-6669	🟪 IRC
6679/6697	🟪 IRC over SSL
6699	🟧 Napster
6881-6999	🟧 BitTorrent
6891-6901	🟪 Windows Live
6970	🟨 Quicktime
7212	GhostSurf
7648-7649	🟪 CU-SeeMe
8000	🟨 Internet Radio
8080	HTTP Proxy
8086-8087	Kaspersky AV
8118	Privoxy
8200	VMware Server
8500	Adobe ColdFusion
8767	🟪 TeamSpeak
8866	🟥 Bagle.B
9100	HP JetDirect
9101-9103	Bacula
9119	🟪 MXit
9800	WebDAV
9898	🟥 Dabber
9988	🟥 Rbot/Spybot
9999	Urchin
10000	Webmin
10000	BackupExec
10113-10116	NetIQ
11371	OpenPGP
12035-12036	🟩 Second Life
12345	🟥 NetBus
13720-13721	NetBackup
14567	🟩 Battlefield
15118	🟩 Dipnet/Oddbob
19226	AdminSecure
19638	Ensim
20000	Usermin
24800	🟨 Synergy
25999	🟪 Xfire
27015	🟩 Half-Life
27374	🟥 Sub7
28960	🟩 Call of Duty
31337	🟥 Back Orifice
33434+	traceroute

Legend

🟪	Chat
🟦	Encrypted
🟩	Gaming
🟥	Malicious
🟧	Peer to Peer
🟨	Streaming

IANA port assignments published at **http://www.iana.org/assignments/port-numbers**

by Jeremy Stretch

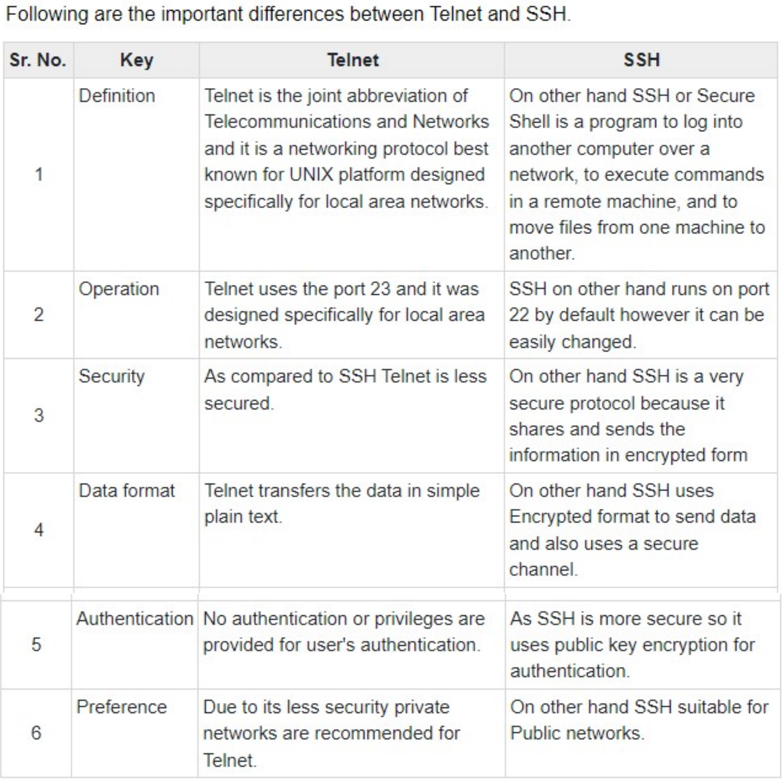
v1.1

what is telnet?

TELNET stands for TErminaL NETwork. It is a type of protocol that enables one computer to connect to local computer. It is a used as a standard TCP/IP protocol for virtual terminal service which is given by ISO. Computer which starts connection known as the local computer. Computer which is being connected to i.e. which accepts the connection known as remote computer. When the connection is established between local and remote computer. During telnet operation whatever that is being performed on the remote computer will be displayed by local computer. Telnet operates on client/server principle. Local computer uses telnet client program and the remote computers uses telnet server program.

The main task of the internet is to provide services to users. For example, users want to run different application programs at the remote site and transfers a result to the local site. This requires a client-server program such as FTP, SMTP. But this would not allow us to create a specific program for each demand.
The better solution is to provide a general client-server program that lets the user access any application program on a remote computer. Therefore, a program that allows a user to log on to a remote computer.
A popular client-server program Telnet is used to meet such demands. Telnet is an abbreviation for Terminal Network.
Telnet provides a connection to the remote computer in such a way that a local terminal appears to be at the remote side.

Difference between telnet & ssh?



Following are the important differences between Telnet and SSH.

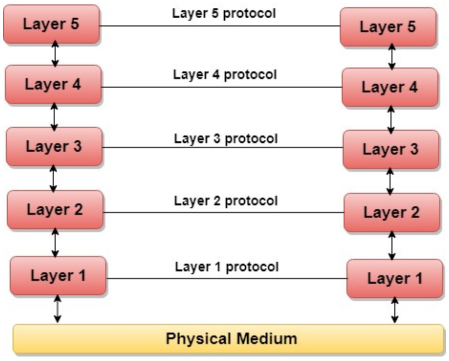
Sr. No.	Key	Telnet	SSH
1	Definition	Telnet is the joint abbreviation of Telecommunications and Networks and it is a networking protocol best known for UNIX platform designed specifically for local area networks.	On other hand SSH or Secure Shell is a program to log into another computer over a network, to execute commands in a remote machine, and to move files from one machine to another.
2	Operation	Telnet uses the port 23 and it was designed specifically for local area networks.	SSH on other hand runs on port 22 by default however it can be easily changed.
3	Security	As compared to SSH Telnet is less secured.	On other hand SSH is a very secure protocol because it shares and sends the information in encrypted form
4	Data format	Telnet transfers the data in simple plain text.	On other hand SSH uses Encrypted format to send data and also uses a secure channel.
5	Authentication	No authentication or privileges are provided for user's authentication.	As SSH is more secure so it uses public key encryption for authentication.
6	Preference	Due to its less security private networks are recommended for Telnet.	On other hand SSH suitable for Public networks.

Network Models

A communication subsystem is a complex piece of Hardware and software. Early attempts for implementing the software for such subsystems were based on a single, complex, unstructured program with many interacting components. The resultant software was very difficult to test and modify. To overcome such problem, the ISO has developed a layered approach. In a layered approach, networking concept is divided into several layers, and each layer is assigned a particular task. Therefore, we can say that networking tasks depend upon the layers.

Layered Architecture

- The main aim of the layered architecture is to divide the design into small pieces.
- Each lower layer adds its services to the higher layer to provide a full set of services to manage communications and run the applications.
- It provides modularity and clear interfaces, i.e., provides interaction between subsystems.
- It ensures the independence between layers by providing the services from lower to higher layer without defining how the services are implemented. Therefore, any modification in a layer will not affect the other layers.
- The number of layers, functions, contents of each layer will vary from network to network. However, the purpose of each layer is to provide the service from lower to a higher layer and hiding the details from the layers of how the services are implemented.
- The basic elements of layered architecture are services, protocols, and interfaces.
  - Service: It is a set of actions that a layer provides to the higher layer.
  - Protocol: It defines a set of rules that a layer uses to exchange the information with peer entity. These rules mainly concern about both the contents and order of the messages used.
  - Interface: It is a way through which the message is transferred from one layer to another layer.
- In a layer n architecture, layer n on one machine will have a communication with the layer n on another machine and the rules used in a conversation are known as a layer-n protocol.

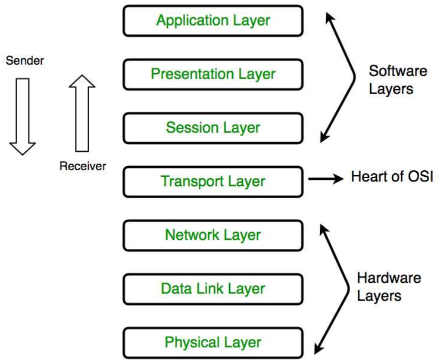


Why do we require Layered architecture?

- Divide-and-conquer approach: Divide-and-conquer approach makes a design process in such a way that the unmanageable tasks are divided into small and manageable tasks. In short, we can say that this approach reduces the complexity of the design.
- Modularity: Layered architecture is more modular. Modularity provides the independence of layers, which is easier to understand and implement.
- Easy to modify: It ensures the independence of layers so that implementation in one layer can be changed without affecting other layers.
- Easy to test: Each layer of the layered architecture can be analyzed and tested individually.

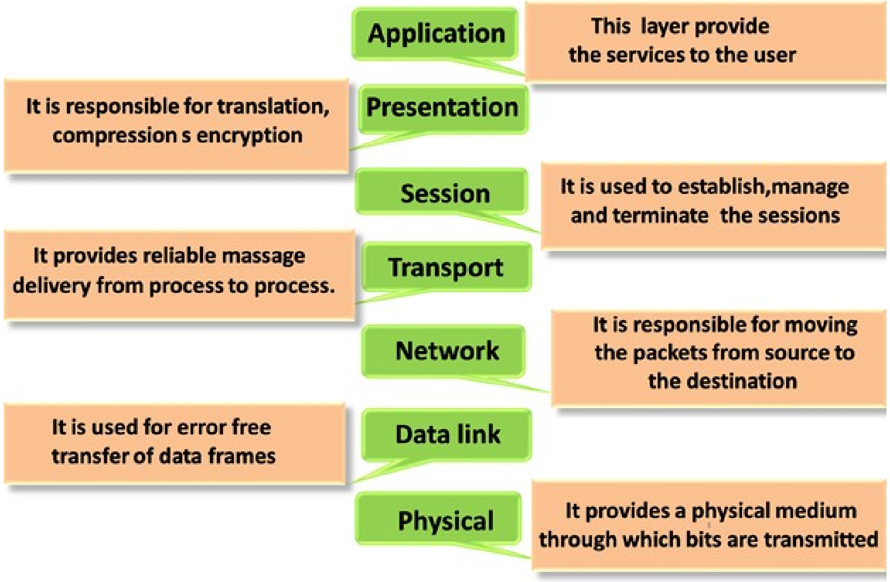
OSI MODEL

1. OSI stands for Open System Interconnection is a reference model that describes how information from a software application in one computer moves through a physical medium to the software application in another computer.
2. OSI consists of seven layers, and each layer performs a particular network function.
3. OSI model was developed by the International Organization for Standardization (ISO) in 1984, and it is now considered as an architectural model for the inter-computer communications.
4. OSI model divides the whole task into seven smaller and manageable tasks. Each layer is assigned a particular task.
5. Each layer is self-contained, so that task assigned to each layer can be performed independently.



Characteristics of OSI Model

1) The OSI model is divided into two layers: upper layers and lower layers.
2) The upper layer of the OSI model mainly deals with the application related issues, and they are implemented only in the software. The application layer is closest to the end user. Both the end user and the application layer interact with the software applications. An upper layer refers to the layer just above another layer.
3) The lower layer of the OSI model deals with the data transport issues. The data link layer and the physical layer are implemented in hardware and software. The physical layer is the lowest layer of the OSI model and is closest to the physical medium. The physical layer is mainly responsible for placing the information on the physical medium.


Application
This layer provide the services to the user
Presentation
It is responsible for translation, compression s encryption
Session
It is used to establish,manage and terminate the sessions
Transport
It provides reliable massage delivery from process to process.
Network
It is responsible for moving the packets from source to the destination
Data link
It is used for error free transfer of data frames
Physical
It provides a physical medium through which bits are transmitted

PHYSICAL LAYER

The lowest layer of the OSI reference model is the physical layer. It is responsible for the actual physical connection between the devices. The physical layer contains information in the form of bits. It is responsible for transmitting individual bits from one node to the next. When receiving data, this layer will get the signal received and convert it into 0s and 1s and send them to the Data Link layer, which will put the frame back together.
The functions of the physical layer are as follows:

- Bit synchronization: The physical layer provides the synchronization of the bits by providing a clock. This clock controls both sender and receiver thus providing synchronization at bit level.
- Bit rate control: The Physical layer also defines the transmission rate i.e. the number of bits sent per second.
- Physical topologies: Physical layer specifies the way in which the different, devices/nodes are arranged in a network i.e. bus, star, or mesh topology.
- Transmission mode: Physical layer also defines the way in which the data flows between the two connected devices. The various transmission modes possible are Simplex, half-duplex and full-duplex.

DATA LINK LAYER(DLL0 - LAYER 2

The data link layer is responsible for the node-to-node delivery of the message. The main function of this layer is to make sure data transfer is error-free from one node to another, over the physical layer. When a packet arrives in a network, it is the responsibility of DLL to transmit it to the Host using its MAC address. Data Link Layer is divided into two sublayers:

1. Logical Link Control (LLC)
2. Media Access Control (MAC)

The packet received from the Network layer is further divided into frames depending on the frame size of NIC(Network Interface Card). DLL also encapsulates Sender and Receiver’s MAC address in the header.

The Receiver’s MAC address is obtained by placing an ARP(Address Resolution Protocol) request onto the wire asking “Who has that IP address?” and the destination host will reply with its MAC address.

The functions of the Data Link layer are :

- Framing: Framing is a function of the data link layer. It provides a way for a sender to transmit a set of bits that are meaningful to the receiver. This can be accomplished by attaching special bit patterns to the beginning and end of the frame.
- Physical addressing: After creating frames, the Data link layer adds physical addresses (MAC address) of the sender and/or receiver in the header of each frame.
- Error control: Data link layer provides the mechanism of error control in which it detects and retransmits damaged or lost frames.
- Flow Control: The data rate must be constant on both sides else the data may get corrupted thus, flow control coordinates the amount of data that can be sent before receiving acknowledgement.
- Access control: When a single communication channel is shared by multiple devices, the MAC sub-layer of the data link layer helps to determine which device has control over the channel at a given time.

NETWORK LAYER - LAYER 3

The network layer works for the transmission of data from one host to the other located in different networks. It also takes care of packet routing i.e. selection of the shortest path to transmit the packet, from the number of routes available. The sender & receiver's IP addresses are placed in the header by the network layer.

The functions of the Network layer are :

- Routing: The network layer protocols determine which route is suitable from source to destination. This function of the network layer is known as routing.
- Logical Addressing: In order to identify each device on internetwork uniquely, the network layer defines an addressing scheme. The sender & receiver's IP addresses are placed in the header by the network layer. Such an address distinguishes each device uniquely and universally.

TRANSPORT LAYER - LAYER 4

The transport layer provides services to the application layer and takes services from the network layer. The data in the transport layer is referred to as Segments. It is responsible for the End to End Delivery of the complete message. The transport layer also provides the acknowledgement of the successful data transmission and re-transmits the data if an error is found.

At sender's side: Transport layer receives the formatted data from the upper layers, performs Segmentation, and also implements Flow & Error control to ensure proper data transmission. It also adds Source and Destination port numbers in its header and forwards the segmented data to the Network Layer. Generally, this destination port number is configured, either by default or manually. For example, when a web application makes a request to a web server, it typically uses port number 80, because this is the default port assigned to web applications. Many applications have default ports assigned.

At receiver's side: Transport Layer reads the port number from its header and forwards the Data which it has received to the respective application. It also performs sequencing and reassembling of the segmented data.

The functions of the transport layer are as follows:

- Segmentation and Reassembly: This layer accepts the message from the (session) layer, and breaks the message into smaller units. Each of the segments produced has a header associated with it. The transport layer at the destination station reassembles the message.
- Service Point Addressing: In order to deliver the message to the correct process, the transport layer header includes a type of address called service point address or port address. Thus by specifying this address, the transport layer makes sure that the message is delivered to the correct process.

The services provided by the transport layer :

A. Connection-Oriented Service: It is a three-phase process that includes

– Connection Establishment
– Data Transfer
– Termination / disconnection

In this type of transmission, the receiving device sends an acknowledgement, back to the source after a packet or group of packets is received. This type of transmission is reliable and secure.

B. Connectionless service: It is a one-phase process and includes Data Transfer. In this type of transmission, the receiver does not acknowledge receipt of a packet. This approach allows for much faster communication between devices. Connection-oriented service is more reliable than connectionless Service.

* Data in the Transport Layer is called as Segments.
** Transport layer is operated by the Operating System. It is a part of the OS and communicates with the Application Layer by making system calls.
Transport Layer is called as Heart of OSI model.

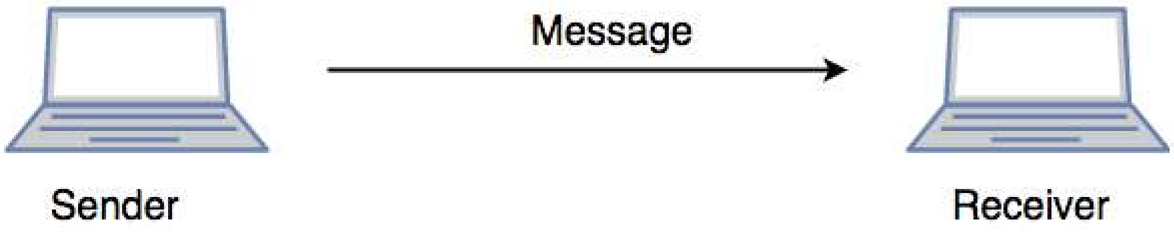
SESSION LAYER-LAYER 5

This layer is responsible for the establishment of connection, maintenance of sessions, authentication, and also ensures security.
The functions of the session layer are :

- Session establishment, maintenance, and termination: The layer allows the two processes to establish, use and terminate a connection.
- Synchronization: This layer allows a process to add checkpoints which are considered synchronization points into the data. These synchronization points help to identify the error so that the data is re-synchronized properly, and ends of the messages are not cut prematurely and data loss is avoided.
- Dialog Controller: The session layer allows two systems to start communication with each other in half-duplex or full-duplex.

**All the below 3 layers(including Session Layer) are integrated as a single layer in the TCP/IP model as “Application Layer”.
**Implementation of these 3 layers is done by the network application itself. These are also known as Upper Layers or Software Layers.

Scenario:
Let us consider a scenario where a user wants to send a message through some Messenger application running in his browser. The “Messenger” here acts as the application layer which provides the user with an interface to create the data. This message or so-called Data is compressed, encrypted (if any secure data), and converted into bits (0’s and 1’s) so that it can be transmitted.



PRESENTATION LAYER-LAYER 6

The presentation layer is also called the Translation layer. The data from the application layer is extracted here and manipulated as per the required format to transmit over the network.
The functions of the presentation layer are :

- Translation: For example, ASCII to EBCDIC.
- Encryption/ Decryption: Data encryption translates the data into another form or code. The encrypted data is known as the ciphertext and the decrypted data is known as plain text. A key value is used for encrypting as well as decrypting data.

- Compression: Reduces the number of bits that need to be transmitted on the network.

APPLICATION LAYER-LAYER 7

At the very top of the OSI Reference Model stack of layers, we find the Application layer which is implemented by the network applications. These applications produce the data, which has to be transferred over the network. This layer also serves as a window for the application services to access the network and for displaying the received information to the user.

Example: Application – Browsers, Skype Messenger, etc.
The functions of the Application layer are :

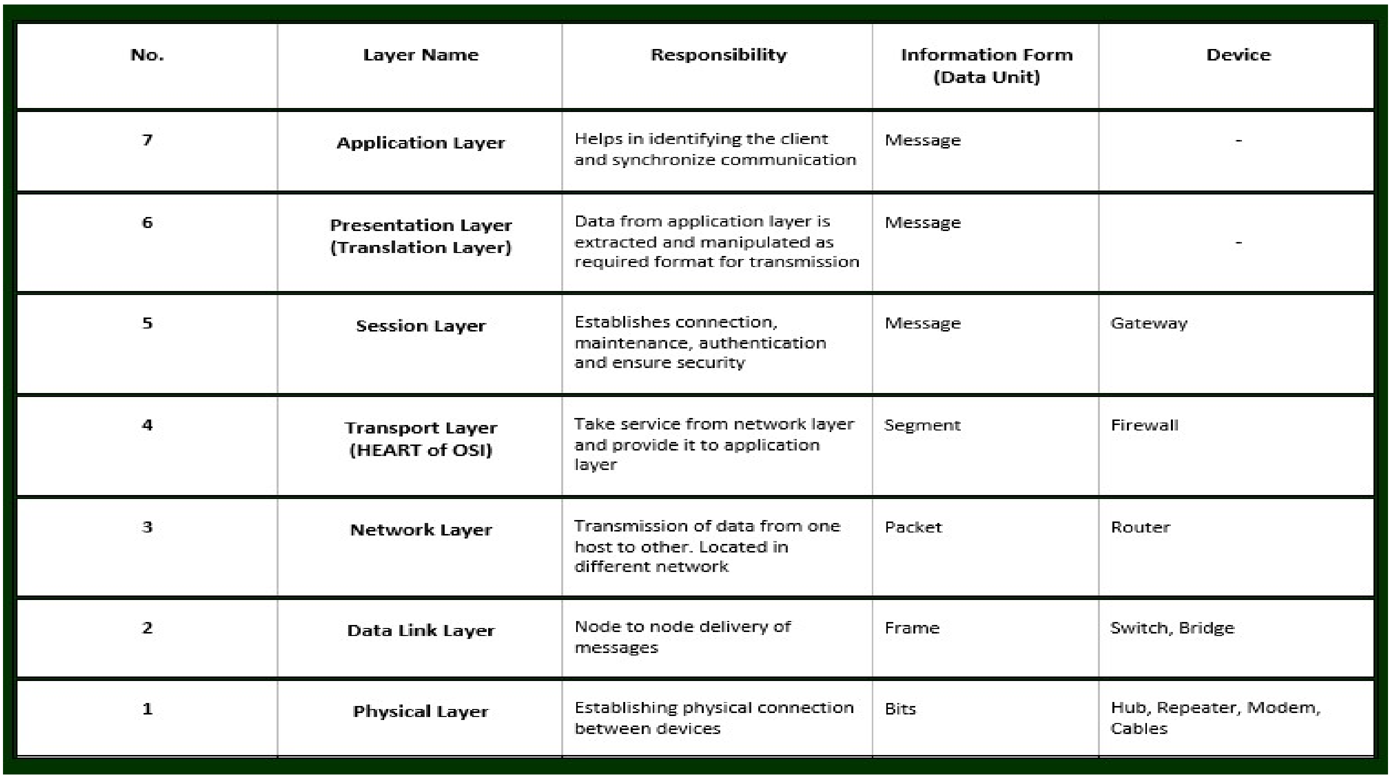
- Network Virtual Terminal
- FTAM-File transfer access and management
- Mail Services
- Directory Services

NOTES:

* Hub, Repeater, Modem, Cables are Physical Layer devices.
** Network Layer, Data Link Layer, and Physical Layer are also known as Lower Layers or Hardware Layers.
* Packet in Data Link layer is referred to as Frame.
** Data Link layer is handled by the NIC (Network Interface Card) and device drivers of host machines.
*** Switch & Bridge are Data Link Layer devices.
* Segment in Network layer is referred to as Packet.
** Network layer is implemented by networking devices such as routers.
Note: In transport layer,The sender needs to know the port number associated with the receiver's application.
**Application Layer is also called Desktop Layer.
***example for session layer IS NETBIOS protocol

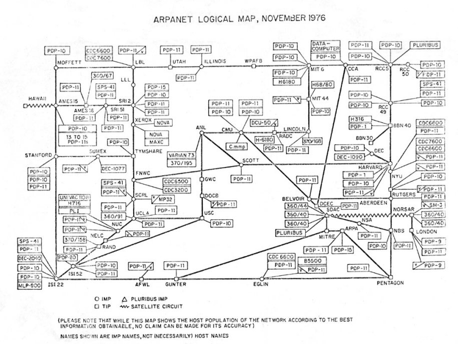
OSI model acts as a reference model and is not implemented on the Internet because of its late invention. The current model being used is the TCP/IP model.

OSI model in a nutshell



No.	Layer Name	Responsibility	Information Form (Data Unit)	Device
7	**Application Layer**	Helps in identifying the client and synchronize communication	Message	-
6	**Presentation Layer (Translation Layer)**	Data from application layer is extracted and manipulated as required format for transmission	Message	-
5	**Session Layer**	Establishes connection, maintenance, authentication and ensure security	Message	Gateway
4	**Transport Layer (HEART of OSI)**	Take service from network layer and provide it to application layer	Segment	Firewall
3	**Network Layer**	Transmission of data from one host to other. Located in different network	Packet	Router
2	**Data Link Layer**	Node to node delivery of messages	Frame	Switch, Bridge
1	**Physical Layer**	Establishing physical connection between devices	Bits	Hub, Repeater, Modem, Cables

ARPANET LOGICAL MAP

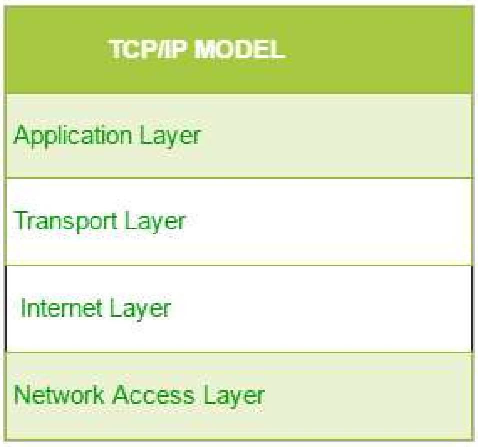

ARPANET LOGICAL MAP, NOVEMBER 1976
○ IMP
△ PLURIBUS IMP
□ TIP
SATELLITE CIRCUIT
(PLEASE NOTE THAT WHILE THIS MAP SHOWS THE HOST POPULATION OF THE NETWORK ACCORDING TO THE BEST INFORMATION OBTAINABLE, NO CLAIM CAN BE MADE FOR ITS ACCURACY)
NAMES SHOWN ARE IMP NAMES, NOT (NECESSARILY) HOST NAMES

TCP/IP Model

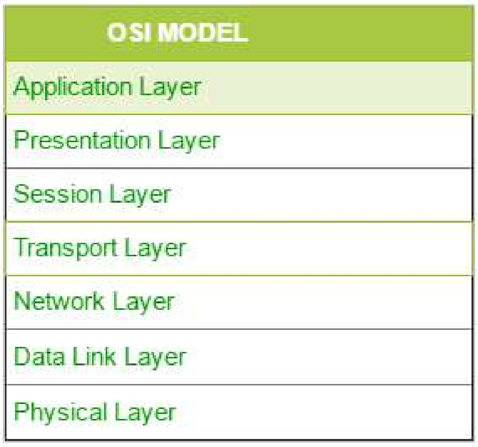
The OSI Model we just looked at is just a reference/logical model. It was designed to describe the functions of the communication system by dividing the communication procedure into smaller and simpler components. But when we talk about the TCP/IP model, it was designed and developed by Department of Defense (DoD) in 1960s and is based on standard protocols. It stands for Transmission Control Protocol/Internet Protocol. The TCP/IP model is a concise version of the OSI model. It contains four layers, unlike seven layers in the OSI model. The layers are:

- Process/Application Layer
- Host-to-Host/Transport Layer
- Internet Layer
- Network Access/Link Layer

The diagrammatic comparison of the TCP/IP and OSI model is as follows

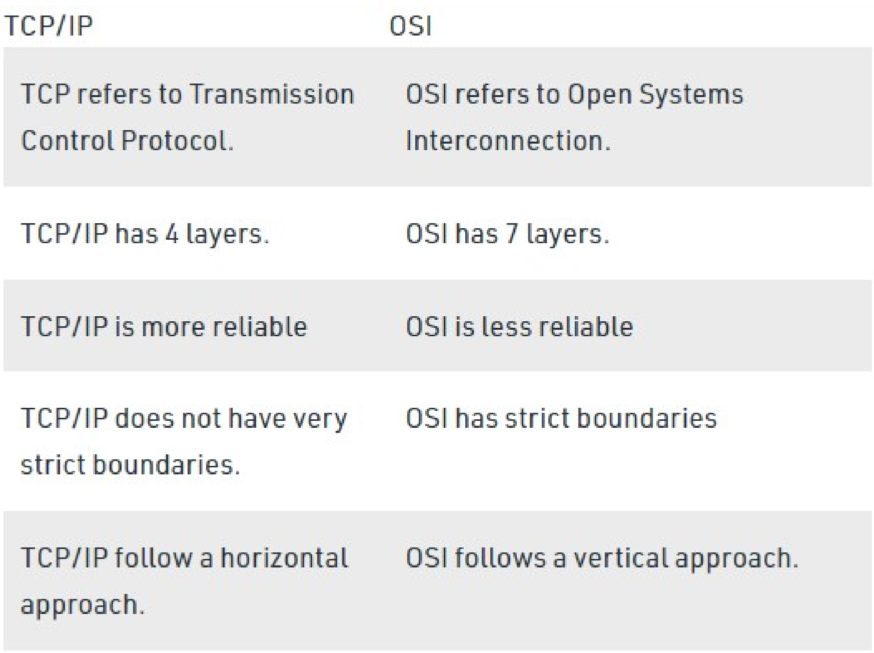


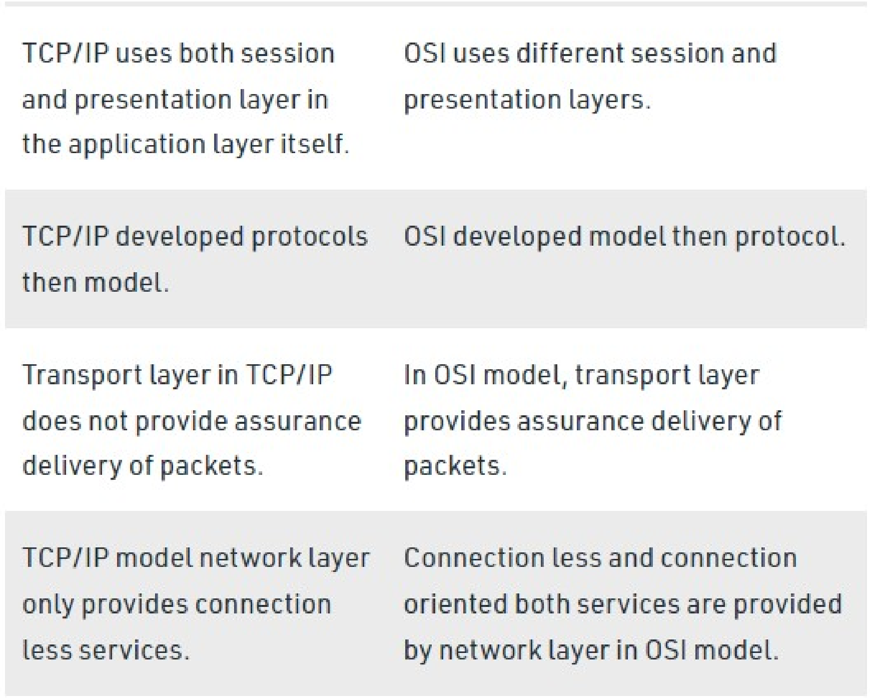
TCP/IP MODEL
Application Layer
Transport Layer
Internet Layer
Network Access Layer



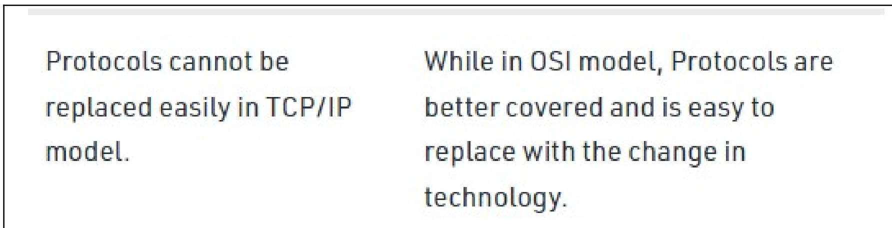
OSI MODEL
Application Layer
Presentation Layer
Session Layer
Transport Layer
Network Layer
Data Link Layer
Physical Layer

Difference between TCP/IP and OSI Model





TCP/IP	OSI
TCP refers to Transmission Control Protocol.	OSI refers to Open Systems Interconnection.
TCP/IP has 4 layers.	OSI has 7 layers.
TCP/IP is more reliable	OSI is less reliable
TCP/IP does not have very strict boundaries.	OSI has strict boundaries
TCP/IP follow a horizontal approach.	OSI follows a vertical approach.
TCP/IP uses both session and presentation layer in the application layer itself.	OSI uses different session and presentation layers.
TCP/IP developed protocols then model.	OSI developed model then protocol.
Transport layer in TCP/IP does not provide assurance delivery of packets.	In OSI model, transport layer provides assurance delivery of packets.
TCP/IP model network layer only provides connection less services.	Connection less and connection oriented both services are provided by network layer in OSI model.



Protocols cannot be replaced easily in TCP/IP model.	While in OSI model, Protocols are better covered and is easy to replace with the change in technology.

The first layer is the Process layer on the behalf of the sender and Network Access layer on the behalf of the receiver. During this article, we will be talking on the behalf of the receiver.

1. Network Access Layer –
This layer corresponds to the combination of Data Link Layer and Physical Layer of the OSI model. It looks out for hardware addressing and the protocols present in this layer allows for the physical transmission of data.
We just talked about ARP being a protocol of Internet layer, but there is a conflict about declaring it as a protocol of Internet Layer or Network access layer. It is described as residing in layer 3, being encapsulated by layer 2 protocols.

2. Internet Layer –
This layer parallels the functions of OSI's Network layer. It defines the protocols which are responsible for logical transmission of data over the entire network. The main protocols residing at this layer are :

- IP – stands for Internet Protocol and it is responsible for delivering packets from the source host to the destination host by looking at the IP addresses in the packet headers. IP has 2 versions:
- IPv4 and IPv6. IPv4 is the one that most of the websites are using currently. But IPv6 is growing as the number of IPv4 addresses are limited in number when compared to the number of users.
- ICMP – stands for Internet Control Message Protocol. It is encapsulated within IP datagrams and is responsible for providing hosts with information about network problems.
- ARP – stands for Address Resolution Protocol. Its job is to find the hardware address of a host from a known IP address. ARP has several types: Reverse ARP, Proxy ARP, Gratuitous ARP and Inverse ARP.

3. Host-to-Host Layer –
This layer is analogous to the transport layer of the OSI model. It is responsible for end-to-end communication and error-free delivery of data. It shields the upper-layer applications from the complexities of data. The two main protocols present in this layer are :

- Transmission Control Protocol (TCP) – It is known to provide reliable and error-free communication between end systems. It performs sequencing and segmentation of data. It also has acknowledgment feature and controls the flow of the data through flow control mechanism. It is a very effective protocol but has a lot of overhead due to such features. Increased overhead leads to increased cost.
- User Datagram Protocol (UDP) – On the other hand does not provide any such features. It is the go-to protocol if your application does not require reliable transport as it is very cost-effective. Unlike TCP, which is connection-oriented protocol, UDP is connectionless.

4. Application Layer –
This layer performs the functions of top three layers of the OSI model: Application, Presentation and Session Layer. It is responsible for node-to-node communication and controls user-interface specifications. Some of the protocols present in this layer are: HTTP, HTTPS, FTP, TFTP, Telnet, SSH, SMTP, SNMP, NTP, DNS, DHCP, NFS, X Window, LPD. Have a look at Protocols in Application Layer for some information about these protocols. Protocols other than those present in the linked article are :

- HTTP and HTTPS – HTTP stands for Hypertext transfer protocol. It is used by the World Wide Web to manage communications between web browsers and servers. HTTPS stands for HTTP-Secure. It is a combination of HTTP with SSL(Secure Socket Layer). It is efficient in cases where the browser need to fill out forms, sign in, authenticate and carry out bank transactions.
- SSH – SSH stands for Secure Shell. It is a terminal emulations software similar to Telnet. The reason SSH is more preferred is because of its ability to maintain the encrypted connection. It sets up a secure session over a TCP/IP connection.
- NTP – NTP stands for Network Time Protocol. It is used to synchronize the clocks on our computer to one standard time source. It is very useful in situations like bank transactions. Assume the following situation without the presence of NTP. Suppose you carry out a transaction, where your computer reads the time at 2:30 PM while the server records it at 2:28 PM. The server can crash very badly if it’s out of sync.

What is Data Encapsulation and de-encapsulation in networking?

Whenever we send the data from one node to another in a computer network. The data is encapsulated at the sender's side, while it is de-encapsulated at the receiver's end. Actually, the encapsulation of data at various layers of the implementing model(OSI or TCP/IP) adds various functionalities and features to the data transmission. The most important feature that it adds is the security and reliability of data transmission between two nodes in a network.

In this , we will mainly learn what is encapsulation. We will also learn the encapsulation and de-encapsulation process in the OSI and TCP/IP models in detail. So, now let us learn these things one by one.

Data Encapsulation

Data Encapsulation is the process in which some extra information is added to the data item to add some features to it. We use either the OSI or the TCP/IP model in our network, and the data transmission takes place through various layers in these models. Data encapsulation adds the protocol information to the data so that data transmission can take place in a proper way. This information can either be added in the header or the footer of the data.

The data is encapsulated on the sender’s side, starting from the application layer to the physical layer. Each layer takes the encapsulated data from the previous layer and adds some more information to encapsulate it and some more functionalities with the data. These functionalities may include proper data sequencing, error detection and control, flow control, congestion control, routing information, etc.

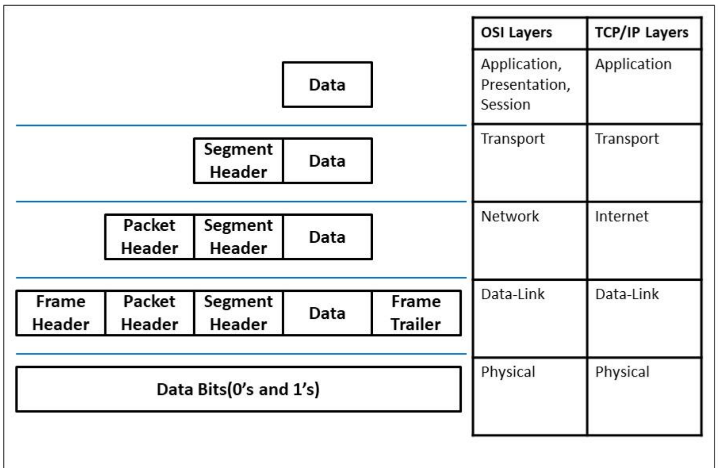
Data De-encapsulation

Data De-encapsulation is the reverse process of data encapsulation. The encapsulated information is removed from the received data to obtain the original data. This process takes place at the receiver’s end. The data is de-encapsulated at the same layer at the receiver’s end to the encapsulated layer at the sender’s end. The added header and trailer information are removed from the data in this process.

The below diagram shows how header and footer are added and removed from the data in the process of encapsulation and de-encapsulation respectively.

The data is encapsulated in every layer at the sender’s side and also de-encapsulated in the same layer at the receiver’s end of the OSI or TCP/IP model. Actually, we use different terms for the encapsulated form of the data that is described in the below-mentioned diagram.

Now, we will learn the whole process of encapsulation and de-encapsulation in the OSI and TCP/IP model step-by-step as mentioned in the below picture.



OSI Layers	TCP/IP Layers
Application, Presentation, Session	Application
Transport	Transport
Network	Internet
Data-Link	Data-Link
Physical	Physical

Encapsulation and De-encapsulation Process

Encapsulation Process (At sender's side)

Step 1: The Application, Presentation, and Session layer in the OSI model, or the Application layer in the TCP/IP model takes the user data in the form of data streams, encapsulates it and forwards the data to the Transport layer. It does not necessarily add any header or footer to the data. But it is application-specific and can add the header if needed.

Step 2: The Transport layer (in the OSI or TCP/IP model) takes the data stream from the upper layers, and divide it into multiple pieces. The Transport layer encapsulates the data by adding the appropriate header to each piece. These data pieces are now called as data segments. The header contains the sequencing information so that the data segments can be reassembled at the receiver's end.

Step 3: The Network layer (in the OSI model) or the Internet layer (in the TCP/IP model) takes the data segments from the Transport layer and encapsulate it by adding an additional header to the data segment. This data header contains all the routing information for the proper delivery of the data. Here, the encapsulated data is termed as a data packet or datagram.

Step 4: The Data-Link layer (in the OSI or TCP/IP model) takes the data packet or datagram from the Network layer and encapsulate it by adding an additional header and footer to the data packet or datagram. The header contains all the switching information for the proper delivery of the data to the appropriate hardware components, and the trailer contains all the information related to error detection and control. Here, the encapsulated data is termed as a data frame.

Step 5: The Physical layer (in the OSI or TCP/IP model) takes the data frames from the Data-Link layer and encapsulate it by converting it to appropriate data signals or bits (corresponding to the physical medium).

De-Encapsulation Process (At receiver's side)

Step 1: The Physical layer (in the OSI or TCP/IP model) takes the encapsulated data signals or bits from the sender, and de-encapsulate it in the form of a data frame to be forwarded to the upper layer, i.e., the Data-Link layer.

Step 2: The Data-Link layer (in the OSI or TCP/IP model) takes the data frames from the Physical layer. It de-encapsulates the data frames and checks the frame header whether the data frame is switched to the correct hardware or not. If the frame is switched to the incorrect destination, it is discarded, else it checks the trailer information. If there is any error in the data, data retransmission is requested, else it is de-encapsulated and the data packet is forwarded to the upper layer.

Step 3: The Network layer (in the OSI model) or the Internet layer (in the TCP/IP model) takes the data packet or datagram from the Data-Link layer. It de-encapsulates the data packets and checks the packet header whether the packet is routed to the correct destination or not. If the packet is routed to the incorrect destination, the packet is discarded, else it is de-encapsulated and the data segment is forwarded to the upper layer.

Step 4: The Transport layer (in the OSI or TCP/IP model) takes the data segments from the network layer and de-encapsulate it. It first checks the segment header and then reassembles the data segments to form data streams, and these data streams are then forwarded to the upper layers.

Step 5: The Application, Presentation, and Session layer in the OSI model, or the Application layer in the TCP/IP model takes encapsulated data from the Transport layer, de-encapsulate it, and the application-specific data is forwarded to the applications.

What is Subnetting?

Subnetting is the practice of dividing a network into two or smaller networks. It increases routing efficiency, which helps to enhance the security of the network and reduces the size of the broadcast domain.

IP Subnetting designates high-order bits from the host as part of the network prefix. This method divides a network into smaller subnets.

It also helps you to reduce the size of the routing tables, which is stored in routers. This method also helps you to extend the existing IP address base & restructures the IP address.

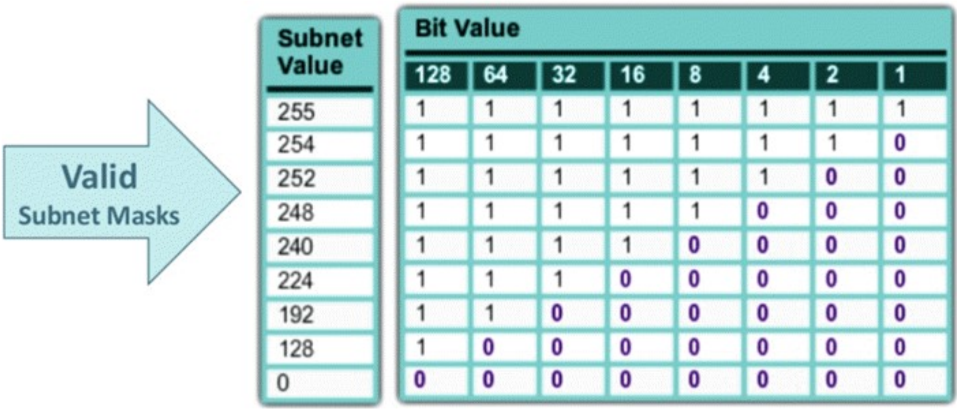
Why Use Subnetting?

Here are important reasons for using Subnetting:

1. It helps you to maximise IP addressing efficiency.
2. Extend the life of IPV4.
3. Public IPV4 Addresses are scarce.
4. IPV4 Subnetting reduces network traffic by eliminating collision and broadcast traffic and thus improves overall performance.
5. This method allows you to apply network security policies at the interconnection between subnets.
6. Optimized IP network performance.
7. Facilitates spanning of large geographical distances.
8. Subnetting process helps to allocate IP addresses that prevent large numbers of IP network addresses from remaining unused.
9. Subnets are usually set up geographically for specific offices or particular teams within a business that allows their network traffic to stay within the location.

What is Subnet Mask?

A subnet mask is a 32 bits address used to distinguish between a network address and a host address in IP address. A subnet mask identifies which part of an IP address is the network address and the host address. They are not shown inside the data packets traversing the Internet. They carry the destination IP address, which a router will match with a subnet.
Subnet mask is used to differnetiate network & host ID


Valid
Subnet Masks

Subnet Value	Bit Value							
	128	64	32	16	8	4	2	1
255	1	1	1	1	1	1	1	1
254	1	1	1	1	1	1	1	0
252	1	1	1	1	1	1	0	0
248	1	1	1	1	1	0	0	0
240	1	1	1	1	0	0	0	0
224	1	1	1	0	0	0	0	0
192	1	1	0	0	0	0	0	0
128	1	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0

Two types of subnet masks are:

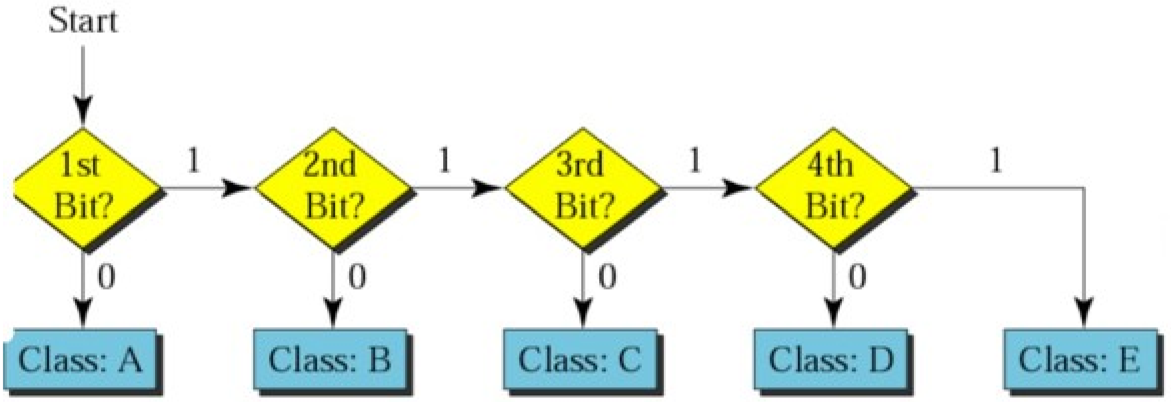
- The default Subnet Mask is the number of bits which is reserved by the address class. Using this default mask will accommodate a single network subnet in the relative class.
- A Custom Subnet Mask can be defined by an administrator to accommodate many Network

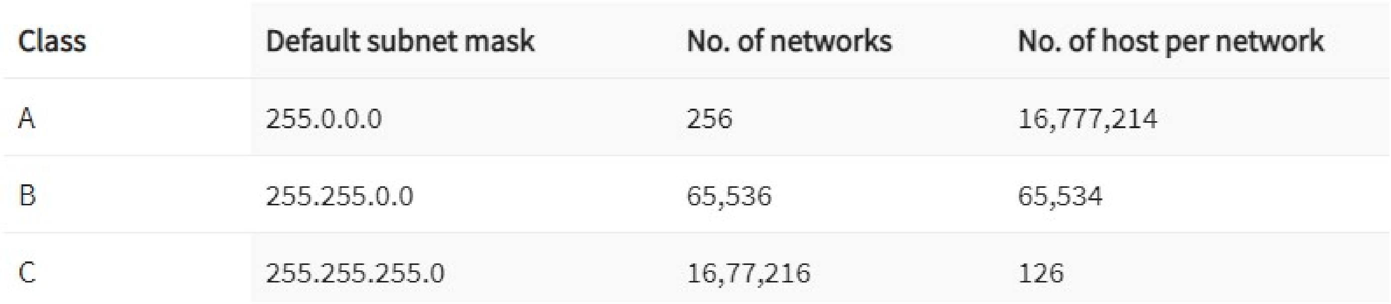
How to Use a Subnet Mask?

The subnet mask is used by the router to cover up the network address. It shows which bits are used to identify the subnet.

Every network has its own unique address, Like here, class B network has network address 172.20.0.0, which has all zeroes in the host portion of the address.

Example IP address: 11000001. Here 1st and 2nd bits are 1, and the 3rd bit is 0; hence, it is class C.





Class	Default subnet mask	No. of networks	No. of host per network
A	255.0.0.0	256	16,777,214
B	255.255.0.0	65,536	65,534
C	255.255.255.0	16,77,216	126

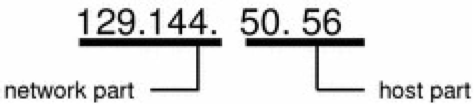
- IP subnetting is the practice of dividing a network into two or smaller networks.
- Subnetting helps you to maximize IP addressing efficiency.
- A subnet mask is a 32 bits address used to distinguish between a network address and a host address in IP address.
- The subnet mask is used by the router to cover up the network address. It shows which bits are used to identify the subnet.
- Subnet mask is used to differnetiate network & host ID

Parts of the IP Address

Each network running TCP/IP must have a unique network number, and every machine on it must have a unique IP address. It is important to understand how IP addresses are constructed before you register your network and obtain its network number.

The IP address is a 32-bit number that uniquely identifies a network interface on a machine. An IP address is typically written in decimal digits, formatted as four 8-bit fields separated by periods. Each 8-bit field represents a byte of the IP address. This form of representing the bytes of an IP address is often referred to as the **dotted-decimal format**.

The bytes of the IP address are further classified into two parts: the network part and the host part.



Network Part

This part specifies the unique number assigned to your network. It also identifies the class of network assigned.

Host Part

This is the part of the IP address that you assign to each host. It uniquely identifies this machine on your network. Note that for each host on your network, the network part of the address will be the same, but the host part must be different.

Subnet Number (Optional)

Local networks with large numbers of hosts are sometimes divided into subnets. If you choose to divide your network into subnets, you need to assign a subnet number for the subnet. You can maximize the efficiency of the IP address space by using some of the bits from the host number part of the IP address as a network identifier. When used as a network identifier, the specified part of the address becomes the subnet number. You create a subnet number by using a netmask, which is a bit mask that selects the network and subnet parts of an IP address.

What is the Default Gateway?

A default gateway is a node that is present in the computer network that serves as a forwarding host to another network when the destination IP address of a packet does not match with any route.

Functions

The functions of default gateway are explained below −

- The major function of the default gateway is to pass the information to another router when the current packet does not know the destination.
- It is a node or a router in the network that connects the host to remote network components.

- Whenever a packet needs to be transmitted to another network, the packet must pass through the default gateway and the default gateway identifies the destination route and forwards the packet on that route. It is considered as an exit point for the packets in the network.

Find PC’s default gateway IP address

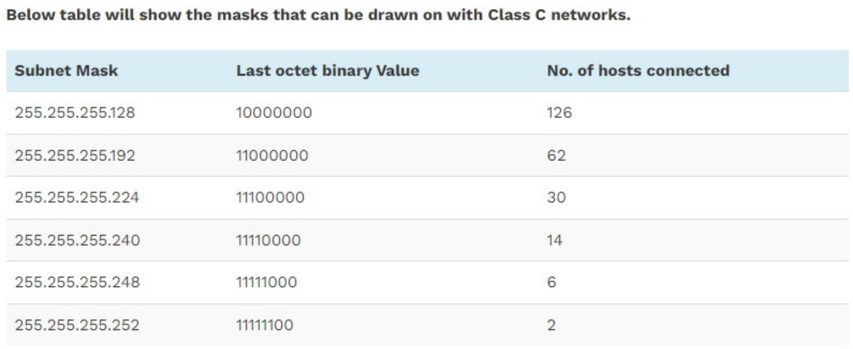
You can find your PC’s default gateway IP address by following the steps given below −

1. By using the Command Prompt window, type “ipconfig” then press “Enter/Return” on your keyboard.
2. We can see a lot of information generated in this window.
3. Just scroll up and we can see “Default Gateway” with the device's IP address (e.g., 192.168.255.1) listed to the right of it.
4. When a default gateway is not configured on a host, the packet will be dropped. Packet won't leave the host at all. Default gateway should always be configured for the packet to reach the destination.
5. If default gateway is incorrectly configured, what situation may occur is explained below −
6. The host cannot communicate with other hosts in the local network.
7. The switch will not forward packets initiated by the host.
8. The host will have to use ARP to determine the correct address of the default gateway.
9. The host cannot communicate with hosts in other networks. A ping from the host to 168.0.0.1 would not be successful.
10. When a host needs to send a message to another host located on the same network it can forward the message directly.
11. When a host needs to send a message to a remote network, it must use the router also called as default gateway.
12. This is because the data link from the address of the remote destination on the host cannot be used directly.
13. Instead the IP packet has to be sent to the router and the router will forward the packet towards its destination.

What is “network ID” and “host ID” in IP Addresses?

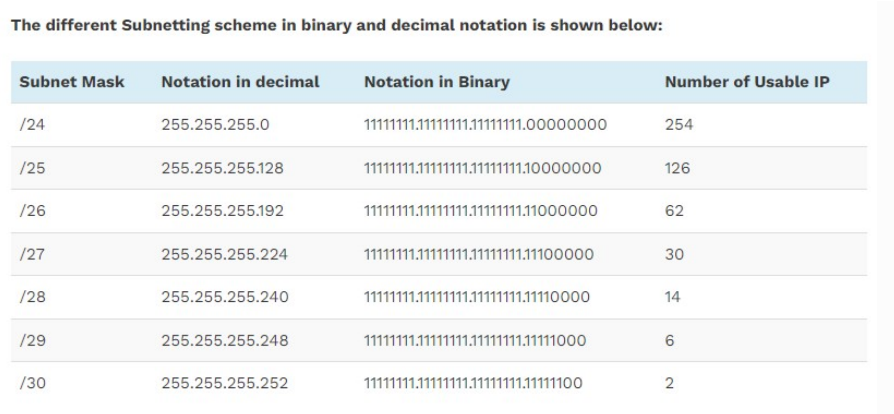
IP addresses are divided into 5 classes namely, Class A, Class B, Class C, Class D, and Class E. This concept came in around the 1980s. Where

- Class A is generally used for big networks such as the ISP networks.
- Class B is used for medium to large networks like some big organizations.
- Class C addresses are generally used for smaller networks.
- Class D addresses are used for Multicasting.
- Class E addresses are reserved addresses and they are used for experimental purposes.



Below table will show the masks that can be drawn on with Class C networks.

Subnet Mask	Last octet binary Value	No. of hosts connected
255.255.255.128	10000000	126
255.255.255.192	11000000	62
255.255.255.224	11100000	30
255.255.255.240	11110000	14
255.255.255.248	11111000	6
255.255.255.252	11111100	2



The different Subnetting scheme in binary and decimal notation is shown below:

Subnet Mask	Notation in decimal	Notation in Binary	Number of Usable IP
/24	255.255.255.0	11111111.11111111.11111111.00000000	254
/25	255.255.255.128	11111111.11111111.11111111.10000000	126
/26	255.255.255.192	11111111.11111111.11111111.11000000	62
/27	255.255.255.224	11111111.11111111.11111111.11100000	30
/28	255.255.255.240	11111111.11111111.11111111.11110000	14
/29	255.255.255.248	11111111.11111111.11111111.11111000	6
/30	255.255.255.252	11111111.11111111.11111111.11111100	2

Binary to decimal conversion

To find decimal value of a number ,just add the numbers where true value occurs under the table values.ie,where 1 occur.
10101100.10110000.00110101.01010001

128	64	32	16	8	4	2	1
1	0	1	0	1	1	0	0
1	0	1	1	0	0	0	0
0	0	1	1	0	1	0	1
0	1	0	1	0	0	0	1

first : 128+32+8+4 : 172
second:128+32+16 : 176
third: 32+16+4+1:53
forth:64+16+1:81
IP : 172.176.53.81

Decimal to Binary Conversion

To find the binary value, just check the octect can subtrated from the below table values, If yes ,put 1 or else 0.

IP : 172.176.53.81

128	64	32	16	8	4	2	1
1	0	1	0	1	1	0	0
1	0	1	1	0	0	0	0
0	0	1	1	0	1	0	1
0	1	0	1	0	0	0	1

NAT vs PAT difference

Network Address Translation (NAT) and Port Address Translation (PAT) both map IP addresses on an internal network to IP addresses on an external network. Which method of address translation you use depends on the types of networks that you are translating and the number of available IP addresses that you have.

If you are connecting a site in the 10.10.10.0 network to a site in the 10.10.20.0 network, you could use NAT to translate 10.10.10.0 IP addresses to available 10.10.20.0 IP addresses so that hosts on the 10.10.10.0 network can access data and use network resources on the 10.10.20.0 network. However, for this scenario to work, you must have an address pool that contains enough available IP addresses on the 10.10.20.0 network to accommodate every host on the 10.10.10.0 network, because NAT requires a one-to-one relationship when translating IP addresses.

PAT attempts to use the original source port number of the internal host to form a unique, registered IP address and port number combination. For example, two hosts that have been assigned the IP addresses 10.10.10.100 and 10.10.10.101, respectively, could send traffic to and receive traffic from the Internet by using the single public IP address 123.45.67.89. If that port number is already allocated, PAT searches for an available alternate source port number. Therefore, the host at IP address 10.10.10.100 could access the Internet by using the public IP address and source port combination of 123.45.67.89:10000. Meanwhile, the host at IP address 10.10.10.101 could access the Internet by using the IP address and source port combination of 123.45.67.89:10001.

If you are connecting a site in the 10.10.10.0 network to the Internet, you must translate host IPs on that network to a registered IP address that is routable over the Internet. In order to use traditional NAT in this scenario, you would need to purchase a registered IP address for each host on your internal network. Alternatively, you could use PAT to translate all the IP addresses on the internal network to a single, shared IP address that connects to the Internet. PAT, which is also known as NAT overloading, uses 16-bit source port numbers to map and track traffic between an internal host and the Internet.

As you can see, the first letter in each acronym denotes the difference between NAT (Network Address Translation) and PAT (Port Address Translation), which should make it easier for you to remember which does what. Just remember that both NAT and PAT use at least one IP address and that PAT is also referred to as NAT overloading because it uses one IP address for all clients to multiple ports, whereas standard NAT uses a one-to-one IP address relationship per client.