TOP 50

INTERVIEW QUESTIONS

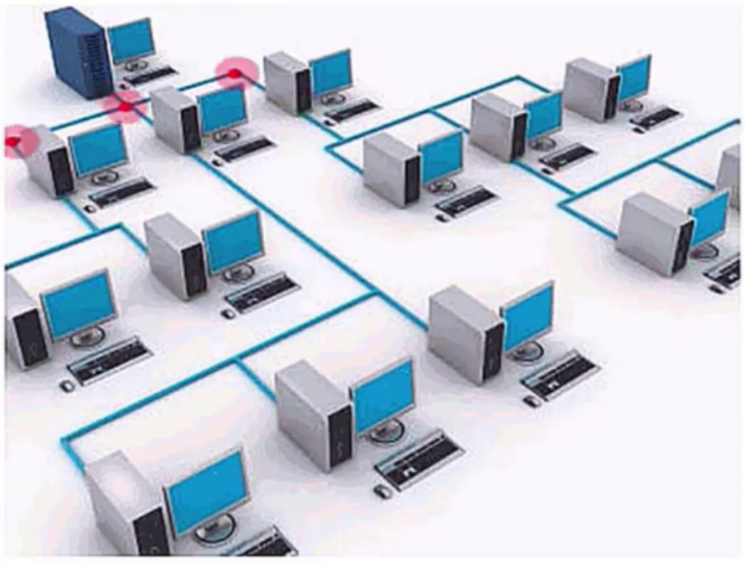
For Computer Networking

www.acenetworker.com

What is a Network?

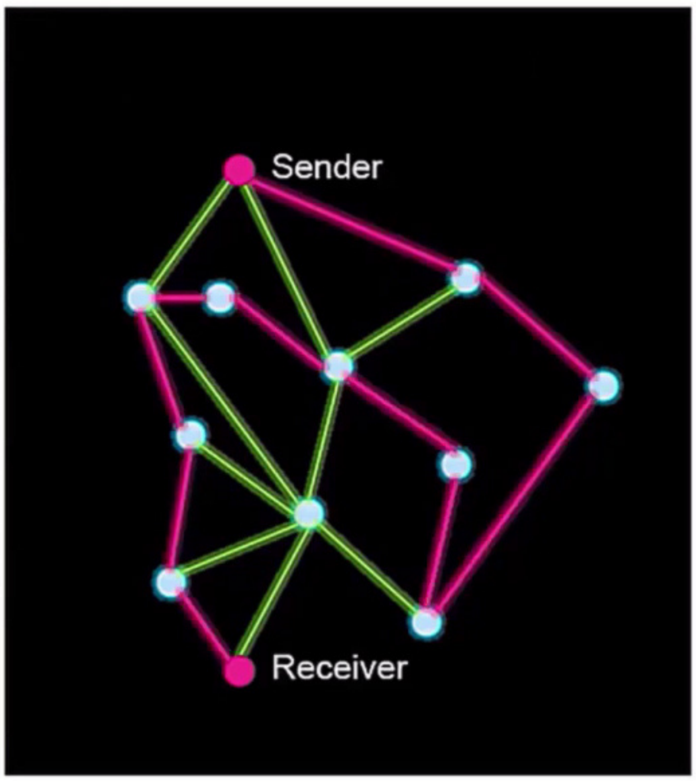
Network is defined as a group of devices connected to each other using a transmission medium.

for example: A computer network is a group of computers connected with each other to communicate and share information and resources like hardware, data, and software.



What is a node and link?

A network is a connection setup of two or more computers directly connected by some physical mediums like optical fiber or coaxial cable.
This physical medium of connection is known as a link, and the computers that it is connected are known as nodes.

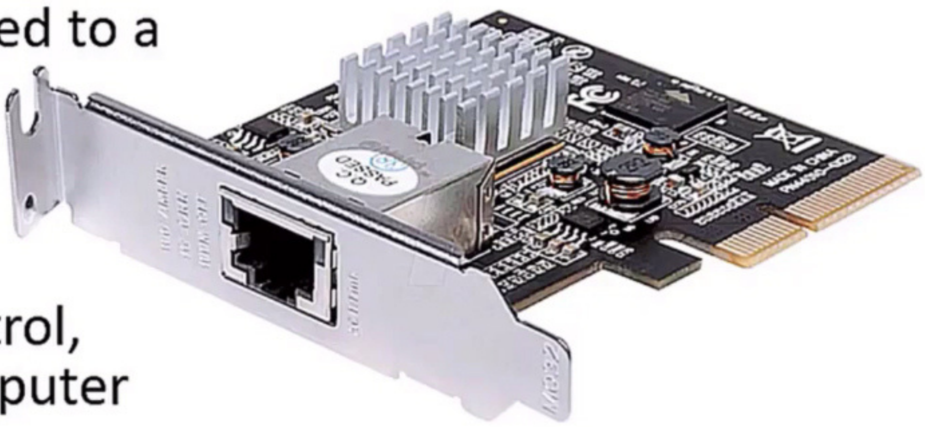


What is NIC?

NIC stands for Network Interface Card. It is also known as Network Adapter or Ethernet Card. It is in the form of an add-in card and is installed on a computer so that the computer can be connected to a network.

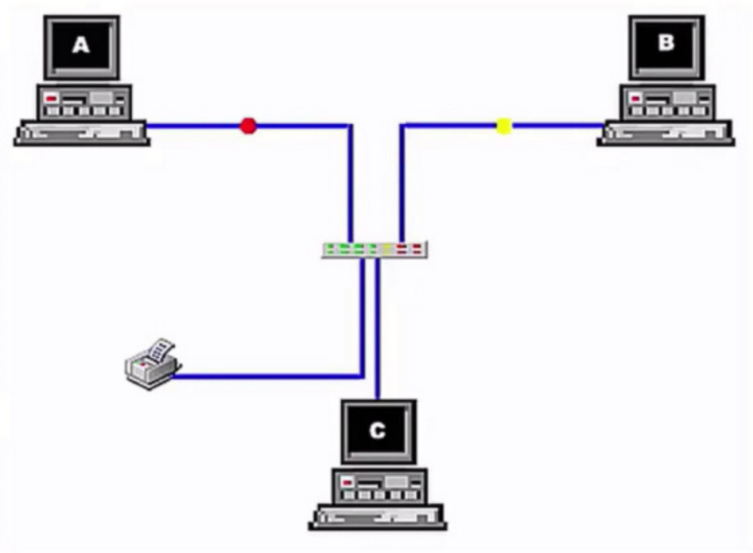
Each NIC has a MAC address.

MAC stands for Media Access Control, which helps in identifying the computer on a network.



What are network devices?

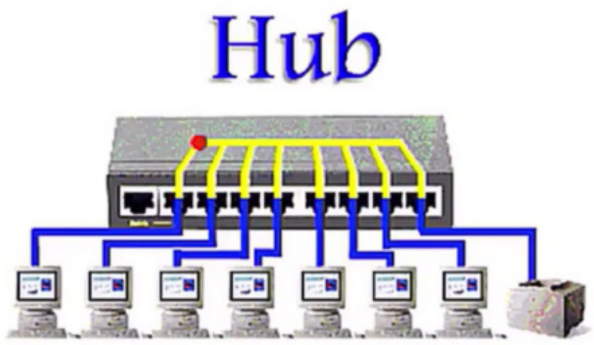
Network devices, or networking hardware, are physical devices that are required for communication and interaction between hardware on a computer network.



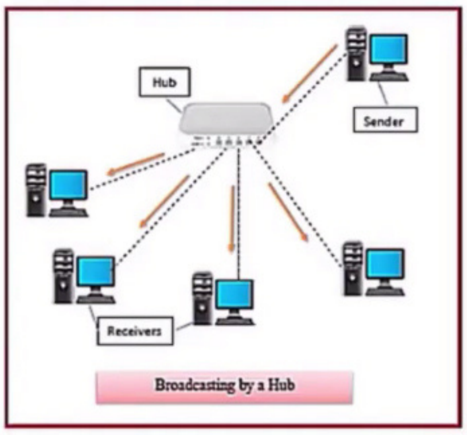
These devices are used for creating a network, maintaining a network and to extend our computer network.

What is a Hub?

Hubs are networking devices operating at a physical layer of the OSI model that are used to connect multiple devices in a network. They are generally used to connect computers in a LAN.



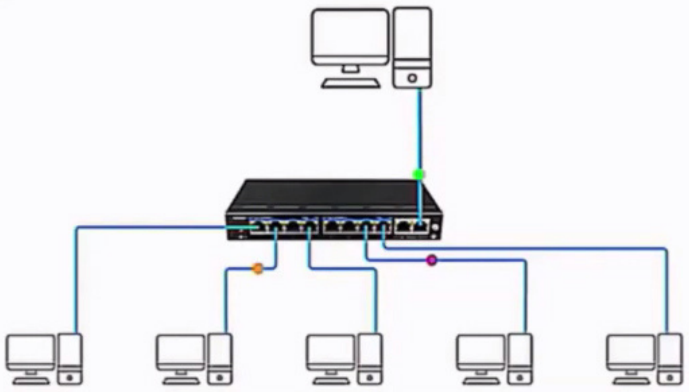
A hub has many ports in it. A computer which intends to be connected to the network is plugged in to one of these ports. When a data frame arrives at a port, it is broadcast to every other port, without considering whether it is destined for a particular destination device or not.



A hub cannot filter data. It is a non-intelligent network device that sends message to all ports.

What is a Switch?

Switch is a network device that has multiple ports that are used to connect devices and create a network.



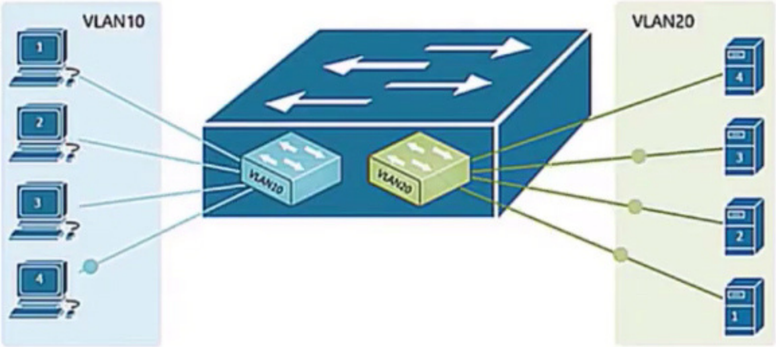
It works on a layer 2 (data-link layer) of the OSI model and has multiple ports, whichever PC connects to the in ports connects that computer to the network.

A switch can actually learn the physical addresses of the devices, that are connected to it and it stores these physical addresses (called MAC address) in its table.

It is an intelligent device because it has a memory where it maintains the table called CAM table (Content Accessible Memory), and stores the port number and MAC addresses of all devices, which helps to identify every device on a network.

What is Layer 2 switch and layer 3 switch?

Network switches can operate at either in OSI layer 2 (the data link layer) or in layer 3 (the network layer).



Layer 2 switches forward data based on the destination MAC address, while layer 3 switches forward data based on the destination IP address. Some switches can do both.

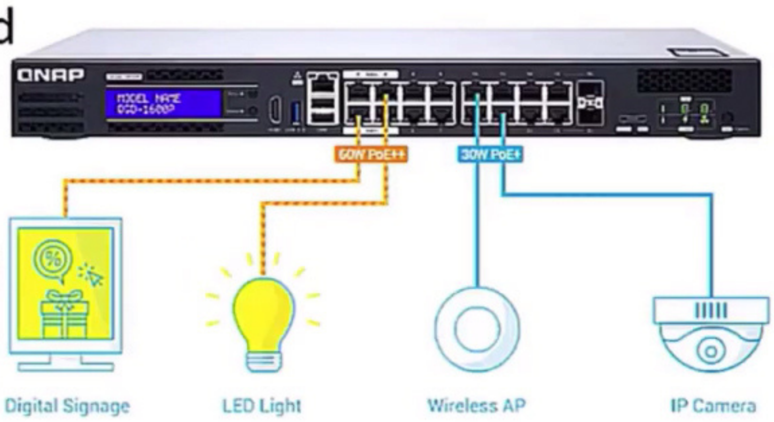
Layer 2 switches are used to reduce the traffic on local network, whereas layer 3 switches are mainly used to create VLANs.

Layer 2 switches can communicate within a network only. Layer 3 switches can communicate within or outside network.

Most switches, however, are layer 2 switches. Layer 2 switches most often connect to the devices in their networks using Ethernet cables. Ethernet cables are physical cables that plug into devices via Ethernet ports

What is an unmanaged switch and managed switch?

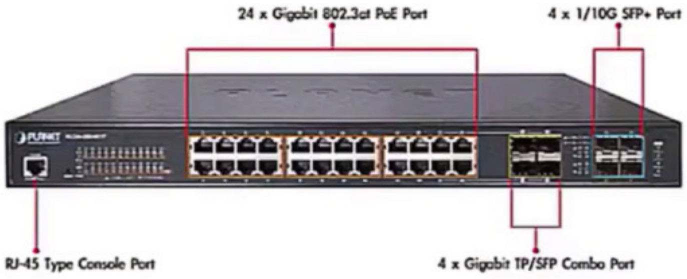
An unmanaged switch simply creates more Ethernet ports on a LAN, so that more local devices can access the Internet. Unmanaged switches pass data back and forth based on device MAC addresses.



A managed switch fulfills the same function for much larger networks, and offers network administrators much more control over how traffic is prioritized. They also enable administrators to set up Virtual LANs to further subdivide a local network into smaller chunks.

What is PoE Switch?

Power over Ethernet switches are used in PoE Gigabit Ethernets. PoE technology combine data and power transmission over the same cable so that devices connected to it can receive both electricity as well as data over the same line. PoE switches offer greater flexibility and simplifies the cabling connections



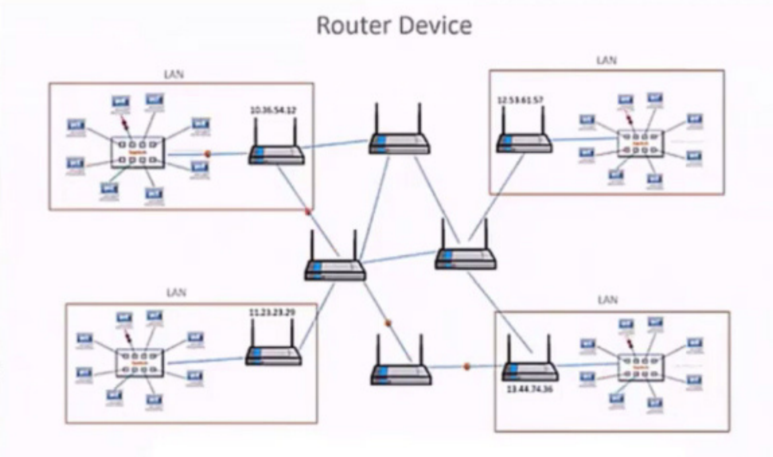
Which are the different factors that affect the performance of a network?

The following factors affect the performance of a network:

- Large number of users
- Transmission medium types
- Hardware
- Software

What is a Router?

The router is a network device that connects two or more network segments. It is used to transfer information from the source to the destination.



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

What is the difference between the Internet, Intranet, and Extranet?

The terminologies Internet, Intranet, and Extranet are used to define how the applications in the network can be accessed. They use similar TCP/IP technology but differ in terms of access levels for each user inside the network and outside the network.

Internet: Applications are accessed by anyone from any location using the web.

Intranet: It allows limited access to users in the same organization.

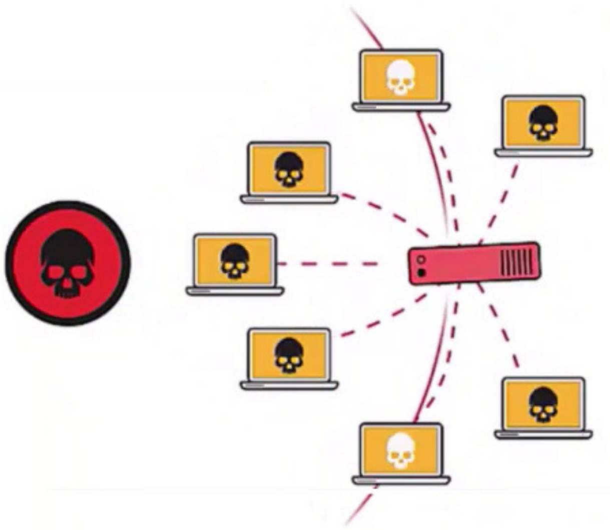
Extranet: External users are allowed or provided with access to use the network application of the organization.

What are some of the security challenges associated with routers?

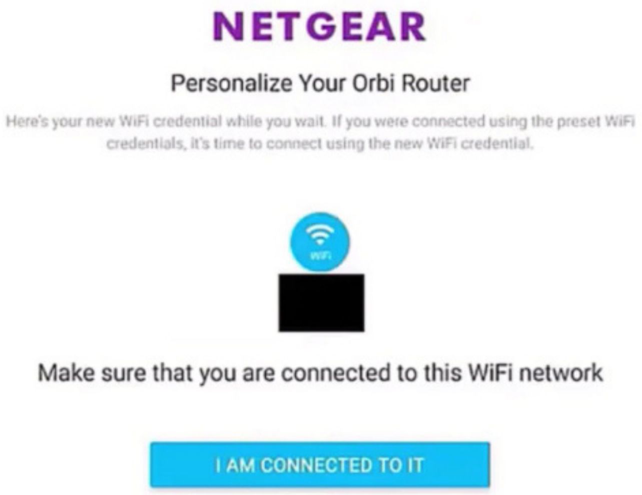
Vulnerability exploits: All hardware-based routers come with automatically installed software known as firmware that helps the router perform its functions. Like any other piece of software, router firmware often contains vulnerabilities that cyber attackers can exploit, and router vendors periodically issue updates to patch these vulnerabilities. For this reason, router firmware needs to be updated regularly. Unpatched routers can be compromised by attackers, enabling them to monitor traffic or use the router as part of a botnet.

DDoS attacks:

Small and large organizations often are the targets of distributed denial-of-service attacks directed at their network infrastructure.
Unmitigated network layer DDoS attacks can overwhelm routers or cause them to crash, resulting in network downtime



Administrative credentials:
All routers come with a set of admin credentials for performing administrative functions. These credentials are set to default values, such as "admin" as the username and "admin" as the password. The username and password should be reset to something more secure as soon as possible: attackers are aware of the common default values for these credentials and can use them to gain control of the router remotely if they are not reset.



Personalize Your Orbi Router

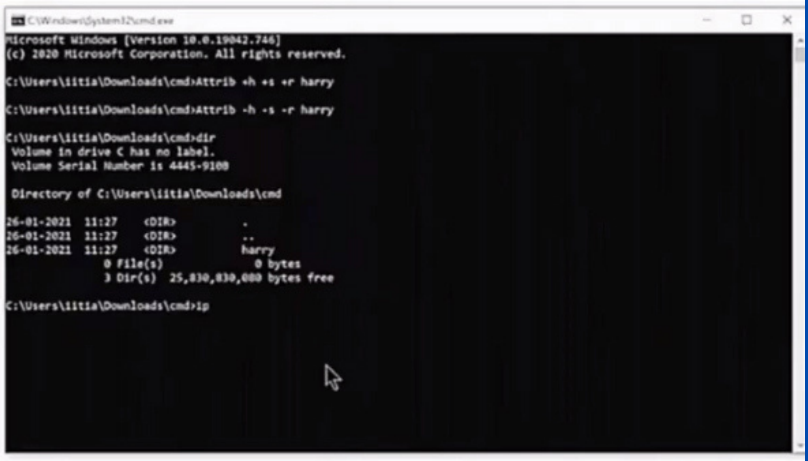
Here's your new WiFi credential while you wait. If you were connected using the preset WiFi credentials, it's time to connect using the new WiFi credential.

[redacted]

Make sure that you are connected to this WiFi network

What are IPConfig and Ifconfig commands?

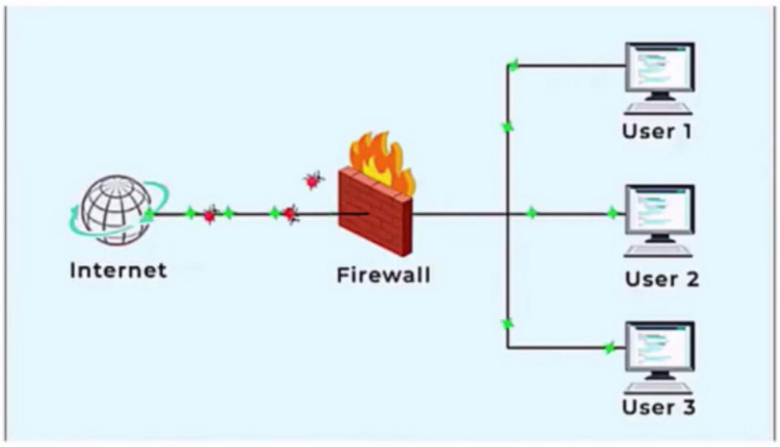
Ipconfig stands for Internet Protocol Configuration and this command is used on Microsoft Windows to view and configure the network interface.
The command Ipconfig is useful for displaying all TCP/IP network summary information currently available on a network. It also helps to modify the DHCP protocol and DNS setting.
Ifconfig (Interface Configuration) is a command that is used on Linux, Mac, and UNIX operating systems. It is used to configure, control the TCP/IP network interface parameters from CLI i.e. Command Line Interface. It allows you to see the IP addresses of these network interfaces.



```
Microsoft Windows [Version 10.0.19042.746]
(c) 2020 Microsoft Corporation. All rights reserved.

C:\Users\iitia\Downloads\cmd>Attrib +h +s +r harry

C:\Users\iitia\Downloads\cmd>Attrib -h -s -r harry

C:\Users\iitia\Downloads\cmd>dir
 Volume in drive C has no label.
 Volume Serial Number is 4445-9100

 Directory of C:\Users\iitia\Downloads\cmd

26-01-2021  11:27    <DIR>          .
26-01-2021  11:27    <DIR>          ..
26-01-2021  11:27    <DIR>          harry
               0 File(s)              0 bytes
               3 Dir(s)  25,830,830,080 bytes free

C:\Users\iitia\Downloads\cmd>ip
```

What is a firewall?

Firewall is a network security system that is used to protect computer networks from unauthorized access. It prevents malicious access from outside to the computer network. A firewall can also be built to grant limited access to outside users.



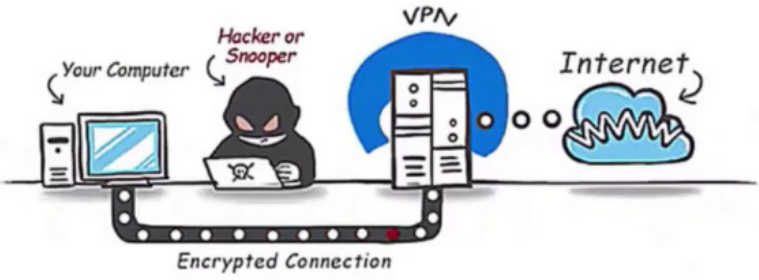
The firewall consists of a hardware device, software program or a combined configuration of both. All the messages that route through the firewall are examined by specific security criteria and the messages which meet the criteria are successfully traversed through the network or else those messages are blocked.

Firewalls can be installed just like any other computer software and later can be customized as per the need and have some control over the access and security features.

"Windows Firewall" is an inbuilt Microsoft Windows application that comes along with the operating system. This "Windows Firewall" also helps to prevent viruses, worms, etc.

What is a VPN?

VPN stands for **"Virtual Private Network"** and describes the opportunity to establish a protected network connection when using public networks. VPNs encrypt your internet traffic and disguise your online identity. This makes it more difficult for third parties to track your activities online and steal data. The encryption takes place in real time. VPNs are used to connect offices remotely and are less expensive when compared to WAN connections. VPNs are used for secure transactions and confidential data can be transferred between multiple offices. VPN keeps company information secure against any potential intrusion.



The different types of VPN's are:

Access VPN: Access VPN is used to provide connectivity to remote mobile users and telecommuters. It serves as an alternative to dial-up connections or ISDN (Integrated Services Digital Network connections. It is a low-cost solution and provides a wide range of connectivity.

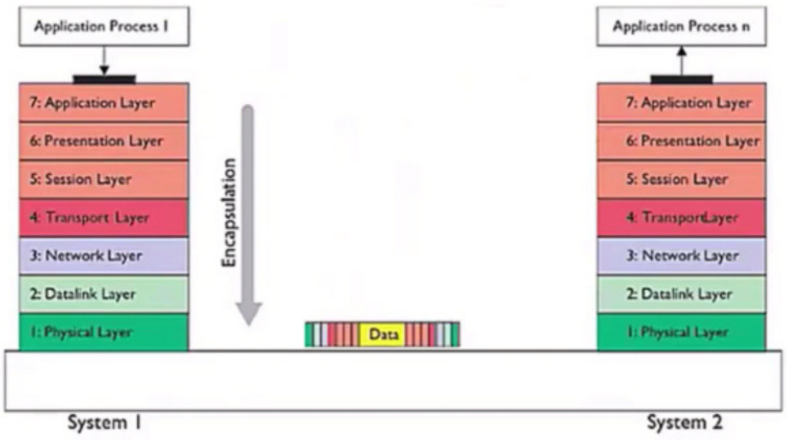
Site-to-Site VPN: A Site-to-Site or Router-to-Router VPN is commonly used in large companies having branches in different locations to connect the network of one office to another in different locations.

Intranet VPN: Intranet VPN is useful for connecting remote offices in different geographical locations using shared infrastructure (internet connectivity and servers) with the same accessibility policies as a private WAN (wide area network).

Extranet VPN: Extranet VPN uses shared infrastructure over an intranet, suppliers, customers, partners, and other entities and connects them using dedicated connections

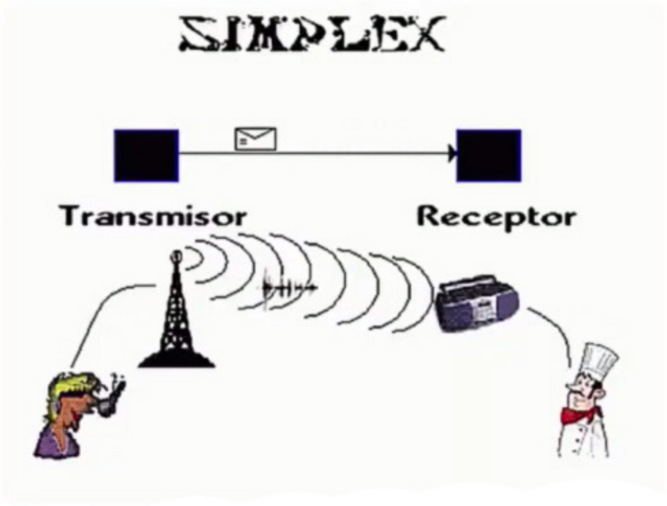
What is data encapsulation?

Data encapsulation is the process of breaking down information into smaller, manageable chunks before it is transmitted across the network. In this process that the source and destination addresses are attached to the headers, along with parity checks.

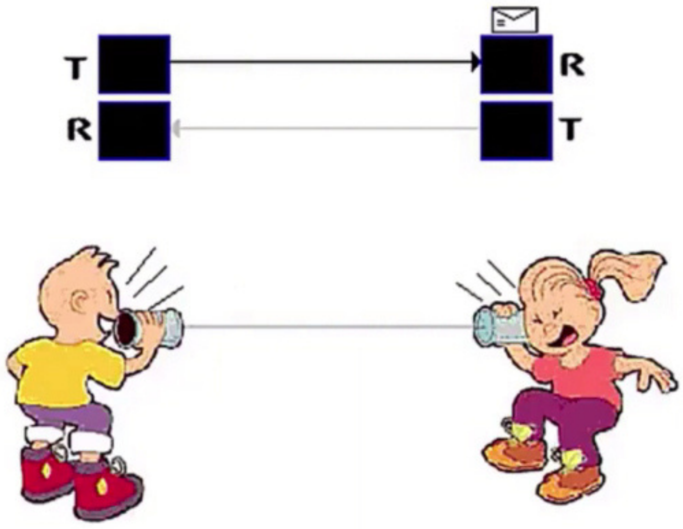


How many types of modes are used in data transferring through networks?

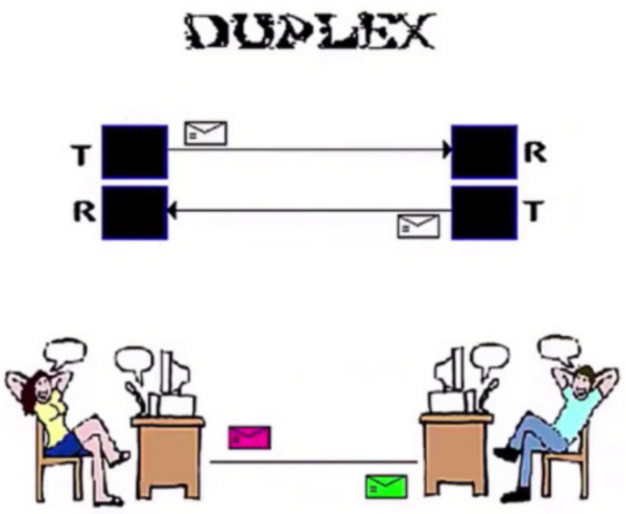
Simplex:
Data transferring which takes place only in one direction is called Simplex. In Simplex mode, the data gets transferred either from sender to receiver or from receiver to sender. For Example, Radio signal, the print signal given from computer to printer, etc.



Half Duplex:
Data transferring can happen in both directions but not at the same time. Alternatively, the data is sent and received. For Example, Browsing through the internet, a user sends the request to the server and later the server processes the request and sends back the web page.



Full Duplex:
Data transferring happens in both directions that too simultaneously. For Example, Communication through telephone, etc.

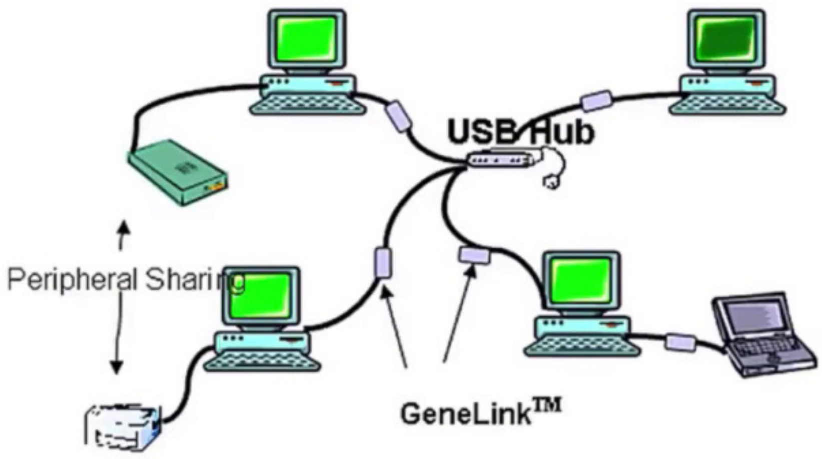


What do you mean by network topology?

Network topology is a physical layout of the computer network and it defines how the computers, devices, cables, etc are connected to each other.

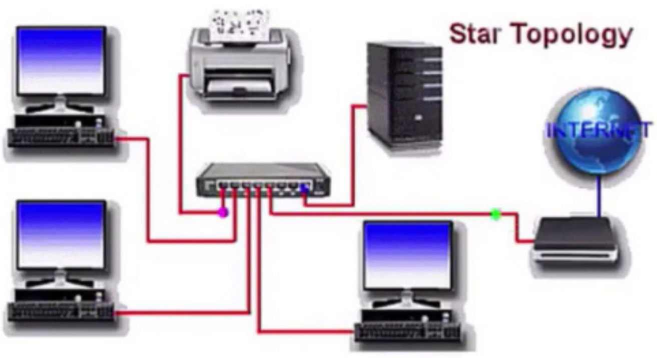
Different types of topologies are:

- Point to point topology
- Daisy chain Topology
- Bus Topology
- Star Topology
- Ring Topology
- Mesh Topology
- Tree Topology, and Hybrid Topology



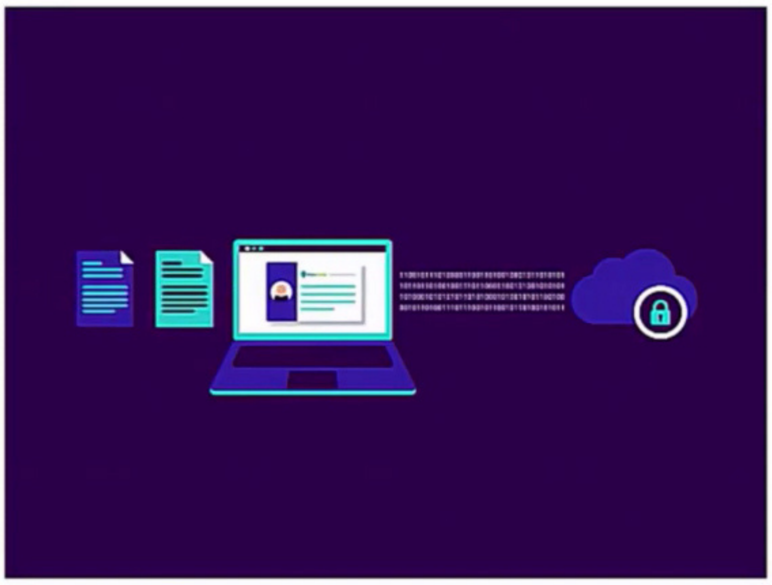
What is Star topology?

In Star Topology, there is a central controller or hub to which every node or device is connected through a cable. In this topology, the devices are not linked to each other. If a device needs to communicate with the other, then it has to send the signal or data to the central hub or switch. And then the hub sends the same data to the destination device.



The advantage of the star topology is that if a link breaks then only that particular link is affected. The whole network remains undisturbed. The main disadvantage of the star topology is that all the devices of the network are dependent on a single point , hub or switch. If the centralized management device like hub or switch gets failed, then the whole network gets down.

What is Data Encryption?



Data encryption is a process that helps us to protect data by converting it into data into an unreadable format using different devices and techniques. The converted text is known as “cipher text,” which ensures data integrity. The cipher text is transformed into a readable format through a decryption key. Cyphers can be of many types, like block ciphers that convert text into a fixed-sized message, stream ciphers that generate a continuous stream of symbols, etc.

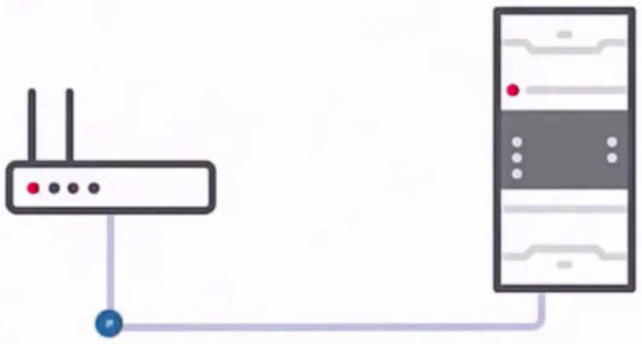
The conversion of data into cipher text, which is only accessible through a specific decryption key, ensures data integrity. Since the data is converted into an unreadable format with encryption, it eliminates the chances of data snooping or data theft.

Data encryption remains a reliable form of data storage and transport. It works as an extra layer of security in transmitting your confidential data. It can be used to increase the security level of individual files, devices, machines, or a hard disk and protect them from counterfeit activities, attacks, or malicious actors.

The following are the main types of data encryption:
Symmetric Encryption
Asymmetric Encryption
Public Key Infrastructure

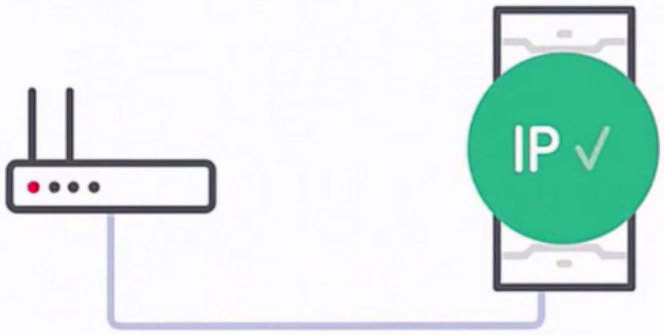
What is DHCP?

DHCP stands for Dynamic Host Configuration Protocol.
It is a standard protocol that allows a server to dynamically distribute IP addressing and configuration information to clients. Normally the DHCP server provides the client with at least this basic information



- IP Address
- Subnet Mask
- Default Gateway

When a new device is added to the network, it broadcasts a message stating that it is new to the network. Then the message is transmitted to all the devices of the network. Only the DHCP server will react to the message and assigns a new IP address to the newly added device of the network. With the help of DHCP, IP management became very easy.

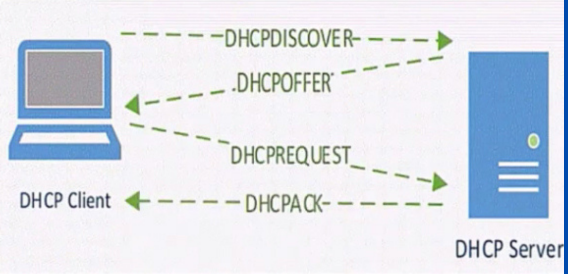


Define IEEE in the Networking?

IEEE stands for the Institute of Electrical and Electronic Engineer. This is used to design or develop standards that are used for networking.
Eg: IEEE 802.11, which is a standard for wireless networks

Explain how DHCP works?

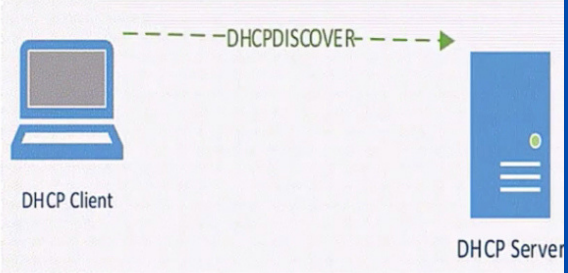
When a host needs an IP configuration, it connects to a DHCP server and requests for an IP configuration. A DHCP server contains several pre-configured IP configurations. When DHCP Server receives a DHCP request from a DHCP client, it provides an IP configuration to the client from all available IP configurations.



This entire process goes through the four steps: they are, **Discover, Offer, Request, and Acknowledgment**.

DHCP discovery:

When we start a device, it checks whether a valid IP configuration is available or not. If the valid IP configuration is not available, the device generates a special message known as the DHCP DISCOVER message and broadcasts this message on the local LAN segment.

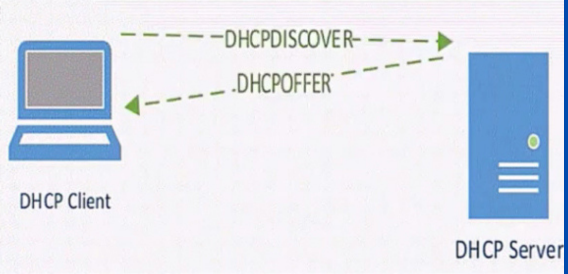


To broadcast DHCP DISCOVER messages, the device uses the 0.0.0.0 and 255.255.255.255 as the source address and destination address, respectively.

The 0.0.0.0 and 255.255.255.255 are two special addresses. Any device, whether it has a valid IP configuration or not, can use these addresses to send local broadcast messages.

DHCP offer:

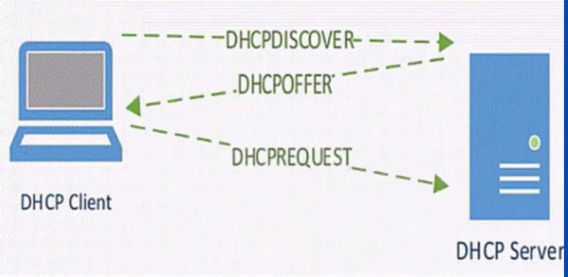
Since the client sends the DHCP DISCOVER message to the local broadcast address, if a DHCP server is configured on the local network, it will also receive the message and can reply to the DHCP DISCOVER message. In reply to the DHCPDISCOVER message, a DHCP server sends a DHCP OFFER message to the client.



The DHCP OFFER message contains protocol specific information and an IP configuration. An IP configuration typically includes the following important information: the IP address for the client, the subnet mask of the proposed IP address, the IP address of the default gateway, the DNS domain name, the DNS server address or addresses, and the TFTP server address or addresses.

DHCP request:

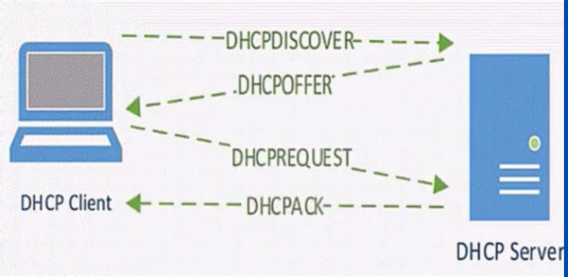
All hosts in the local network receive the DHCP OFFER message. The host that sent the DHCP DISCOVER message accepts the DHCP OFFER message. Except the original host, all other hosts ignore the DHCP OFFER. Depending on the number of DHCP servers, a host may receive multiple DHCP OFFER messages. If a host receives multiple DHCP OFFER messages, it accepts only one message and tells the corresponding server with a DHCP REQUEST message that it wants to use the offered IP configuration.



The DHCP REQUEST message contains a Transaction ID field. Just like hosts use the client ID field of the DHCP OFFER message to know whether the message is intended for them or not, DHCP servers use the Transaction ID field of the DHCP REQUEST message to know whether their offer has been accepted or not.

DHCP acknowledgment:

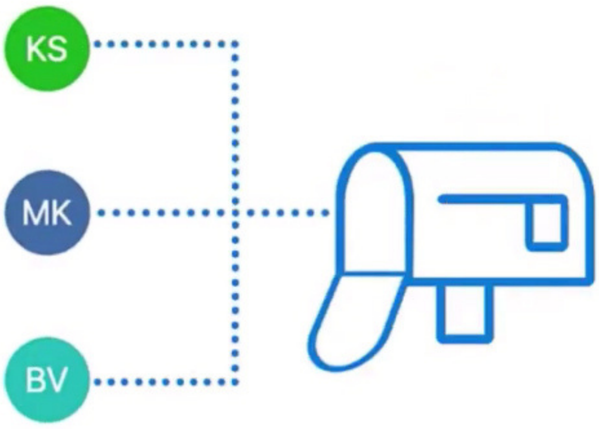
When the DHCP server receives a DHCP REQUEST message from the client, the configuration process enters its final stage. In this stage, the server sends a DHCP ACKnowledge message to the client.



The DHCP ACKnowledge message is an acknowledgment to the client indicating that the DHCP server has received the DHCP REQUEST message of the client, and the client can use the offered IP configuration.

What is an email client?

Email client is a desktop application that enables configuring one or more email addresses to receive, read, compose and send emails from that email address through the desktop interface. It provides a central interface for receiving, composing and sending emails of configured email address.



examples are: microsoft outlook, mozilla thunderbird, etc

What is an email server?

A mail server (sometimes also referred to an e-mail server) is a server that handles and delivers e-mail over a network, usually over the Internet. A mail server can receive e-mails from client computers and deliver them to other mail servers. A mail server can also deliver e-mails to client computers. A client computer is normally the computer where you read your e-mails, for example your computer at home or in your office. Also an advanced mobile phone or Smartphone, with e-mail capabilities, can be regarded as a client computer in these circumstances.

MAIL SERVER
MAIL SERVER

Mail servers can be broken down into two main categories: outgoing mail servers and incoming mail servers. Outgoing mail servers uses **SMTP** protocol which stands for Simple Mail Transfer Protocol.
Incoming mail servers uses **POP3** or **IMAP4** protocols which stands for Post office protocol version 3 and Internet Message Access Protocol respectively.

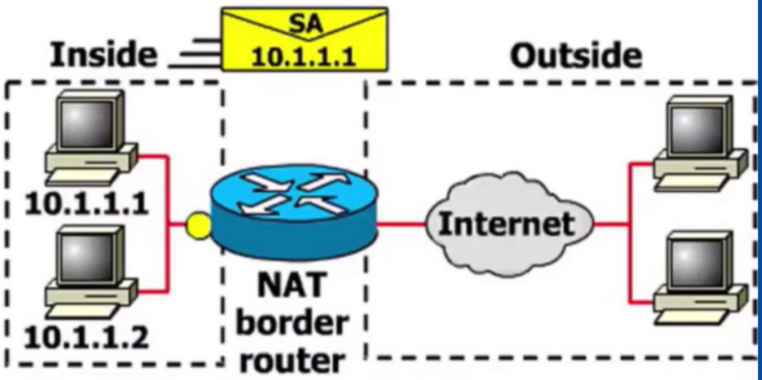
MAIL SERVER
MAIL SERVER

What is NAT?

NAT stands for network address translation. It's a way to map multiple local private addresses to a public one before transferring the information. Organizations that want multiple devices to employ a single IP address use NAT.

There are three different types of NATs

- Static NAT
- Dynamic NAT
- PAT, it stands for port address translation

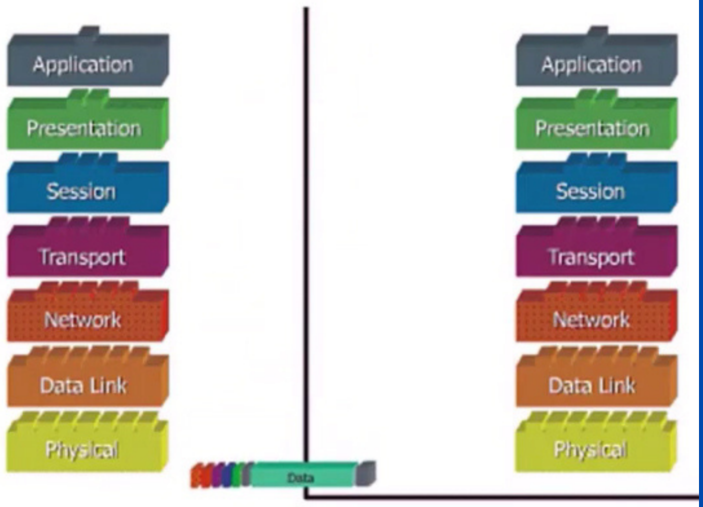


What is OSI Model?

OSI stands for Open Systems Interconnect. OSI Model is a reference model for data communication, it describes how the data is transferred from one device to another device. It is made up of 7 layers, with each layer defining a particular aspect of how network devices connect and communicate with one another. One layer may deal with the physical media used, while another layer dictates how data is transmitted across the network.

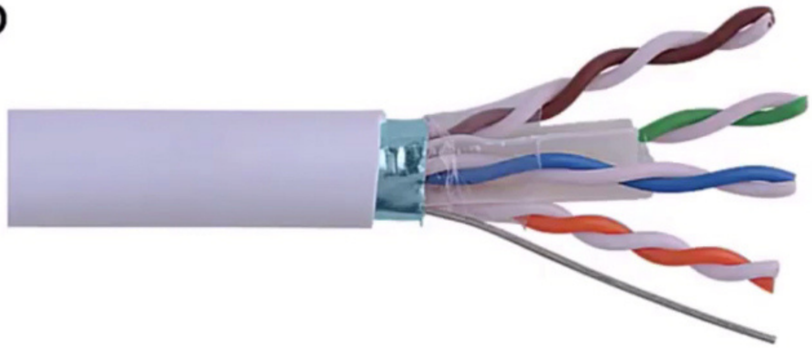
The 7 layers of OSI Model are:

- Physical Layer
- Data-link Layer
- Network Layer
- Transport Layer
- Session Layer
- Presentation Layer
- Application Layer



What is the purpose of cables being shielded and having twisted pairs?

The primary purpose of this is to prevent crosstalk. Crosstalk is electromagnetic interference or noise that can affect data being transmitted across cables.



What is ICMP?

ICMP stands for Internet Control Message Protocol. It provides messaging and communication for protocols within the TCP IP stack. This is also the protocol that manages error messages that are used by network tools such as PING

ECHO REQUEST

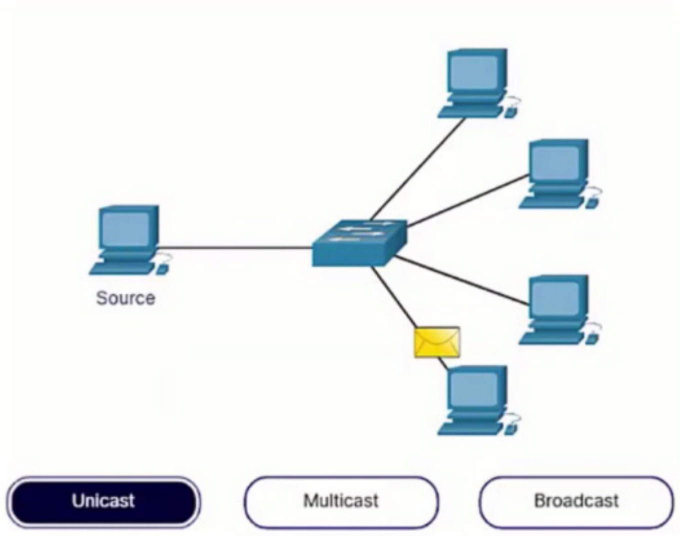
What are Unicasting, Multicasting, Broadcasting, and Anycasting?

Unicasting: If the message is sent to a single node from the source then it is known as unicasting. This is commonly used in networks to establish a new connection.

Multicasting: If the message is sent to a subset of nodes from the source then it is known as multicasting. Used to send the same data to multiple receivers.

Broadcasting: If the message is sent to all the nodes in a network from a source then it is known as broadcasting. DHCP and A R P in the local network use broadcasting.

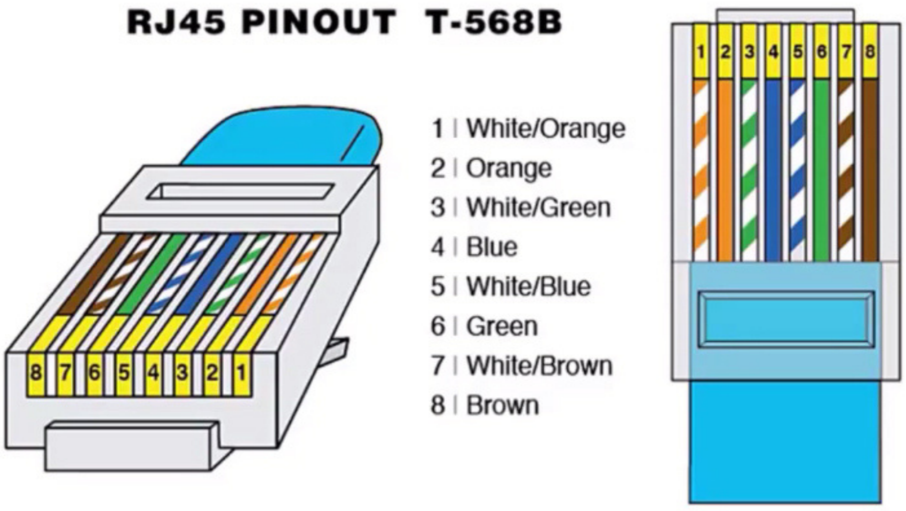
Anycasting: If the message is sent to any of the nodes from the source then it is known as anycasting. It is mainly used to get the content from any of the servers in the Content Delivery System.



What is the standard color sequence of a straight-through cable?

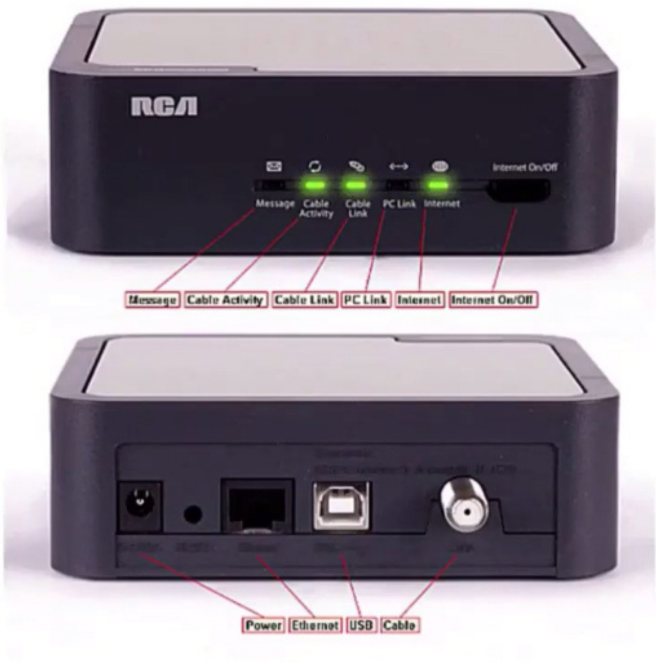
The color sequence for straight through cable is:

Orange white
orange
green white
blue
blue white
green
brown white
brown.



What is Modem? What are the advantages of a Modem?

A modem stands for modulator-demodulator.
A modem is a device that modulates an analog signal to digital information. It also decodes carrier signals to demodulates the transmitted information. The main aim of the Modem is to produce a signal that can be transmitted easily and decoded to reproduce the digital data in its original form. Modems are also used for transmitting analog signals, from LED to radio.



Here, are the advantages of Modem:

- More useful in connecting LAN with the Internet
- Speed depends on the cost
- The Modem is the most widely used data communication roadway.

What is the difference between a straight-through and crossover cable?

A straight-through cable is used to connect to dissimilar functionaliy devices like, computers to a switch, hub, or router.

A crossover cable is used to connect to similar functionality devices such as, PC to PC, or Hub to the Hub.

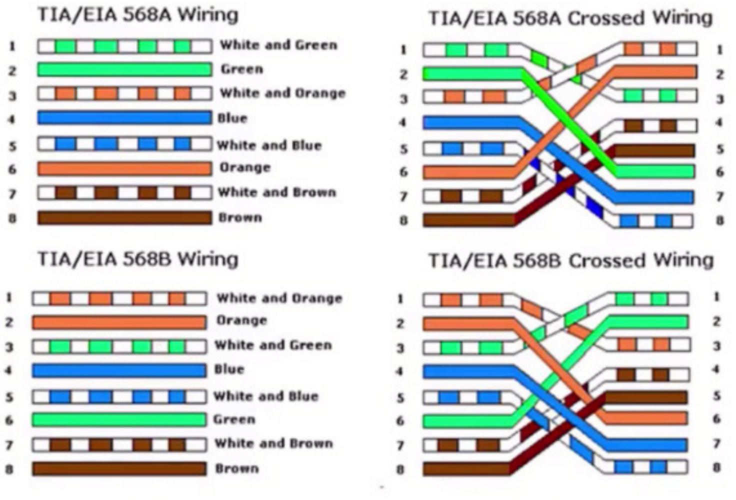


Figure A

Shows the Pin Out of Straight through Cables

Figure B

Shows the Pin Out of Crossover Cables

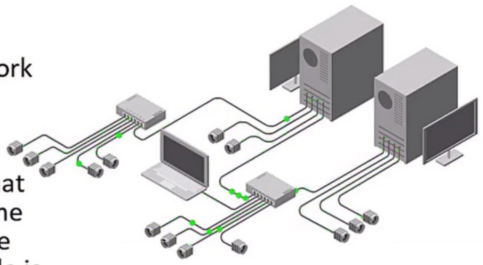
What are the maximum networks and hosts in class A, B, and C network?

For Class A, there are 126 possible networks and 16,777,214 hosts.

For Class B, there are 16,384 possible networks and 65,534 hosts.

For Class C, there are 2,097,152 possible networks and 254 hosts

What is Ethernet, Types along with speeds and IEEE standards?



Ethernet is the traditional technology for connecting devices in a wired local area network or wide area network. It enables devices to communicate with each other via a protocol.

Ethernet describes how network devices format and transmit data so other devices on the same LAN or campus network can recognize, receive and process the information. An Ethernet cable is the physical, encased wiring over which the data travels.

Compared to wireless LAN technology, Ethernet is typically less vulnerable to disruptions. It can also offer a greater degree of network security and control than wireless technology because devices must connect using physical cabling. This makes it difficult for outsiders to access network data or hijack bandwidth for unsanctioned devices.

The Different Types of Ethernet Networks are:

Ethernet
Fast Ethernet
Gigabit Ethernet
10 Gigabit Ethernet.

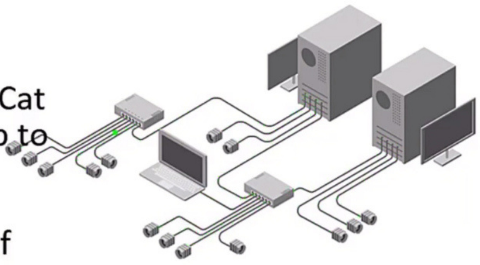
The speeds of different Ethernet networks are:

Ethernet - 10 MBPS
Fast Ethernet - 100 MBPS.
Gigabit Ethernet - 1,000 MBPS.
10 Gigabit Ethernet - 10,000 MBPS.

IEEE Standard for Ethernet is:

IEEE 802.3 - 10 Base T [100 meters].

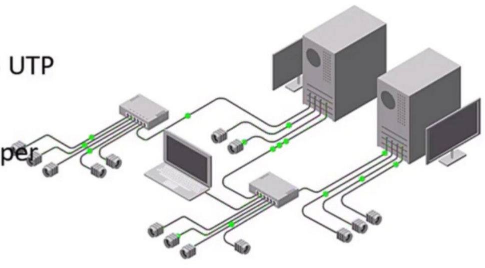
IEEE standard for fast Ethernet is



- IEEE 802u - 100 base TX. It uses Cat 5, 5 e, or 6 UTP wiring. It supports up to 100 meters long.

- 100 base FX which is a version of fast Ethernet which uses multi-mode fiber optical cable and supports up to 412 meters.

IEEE standard for Gigabit Ethernet is:



- IEEE 802.ab - 1000 base T that uses cat 5 UTP wiring and supports up to 100 meters long.

- IEEE 802.3z - 1000 base CX that uses copper cabling and supports up to 25 meters long.

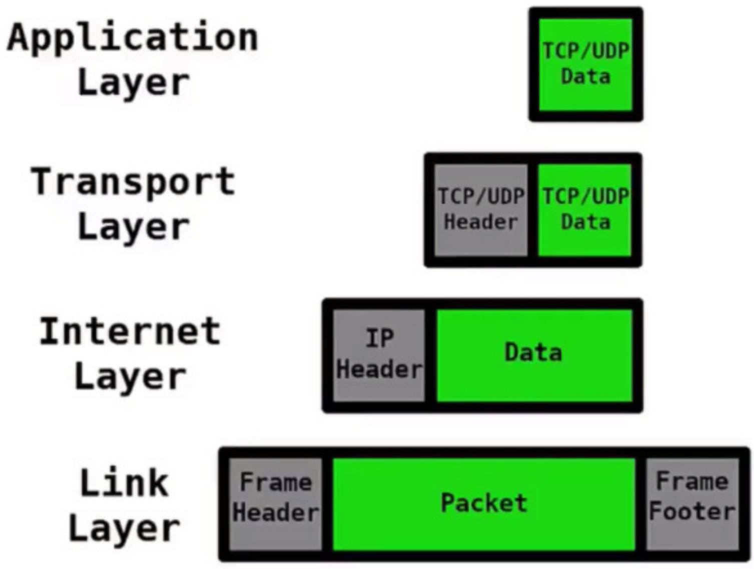
- IEEE 802.3Z - 1000 base SX that uses multimode fiber optical cable.

- IEEE 802.3Z - 1000 base LX that uses single mode fiber optical cable.

IEEE standard for 10 gigabit Ethernet is:

- IEEE 802.3.an - 10G Base T.

What is TCP/IP?



The TCP IP model is a part of the Internet Protocol Suite. This model acts as a communication protocol for computer networks and connects hosts on the Internet.

It is a concise version of the OSI Model and comprises four layers in its structure.

it was Developed during the 1970s.

US Department of Defense declared TCP IP as the standard for all military computer networking in March 1982.

In 1983, this structured protocol was adopted by ARPANET as a standard protocol

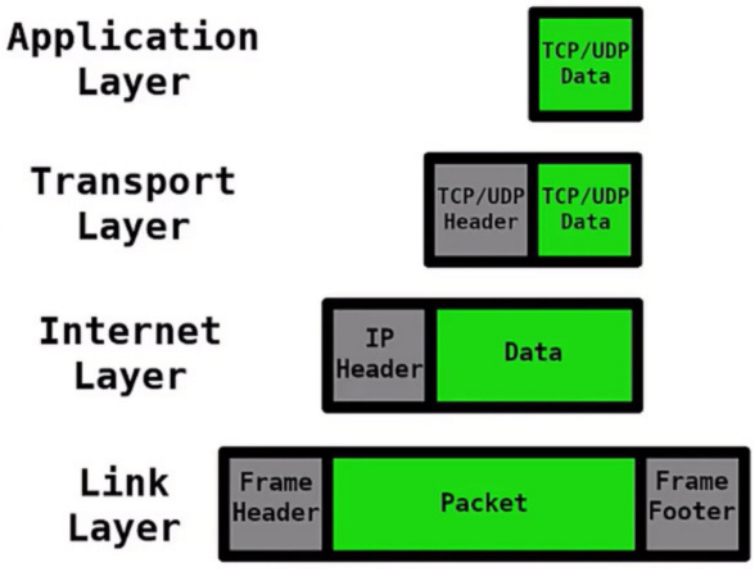
Later on other Computer and IT companies had also adapted the TCP IP model as their standard communication protocol

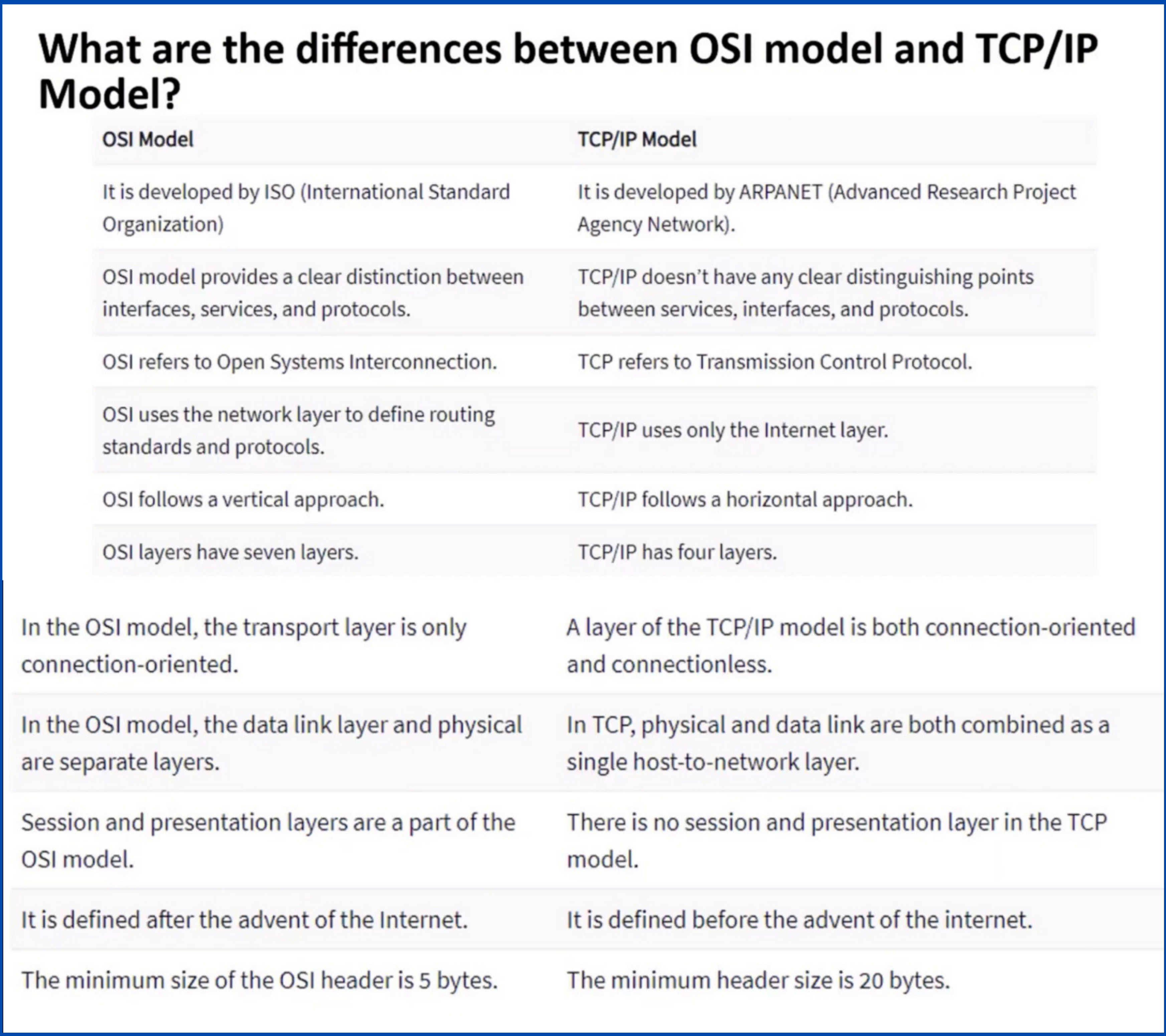
In 1989, the University of California has accepted the TCP IP code for public domain.

Unlike the OSI model which comprises seven layers, the TCP IP model is structured with four different layers.

These tour layers are:

Application Layer
Host to Host Layer
Internet Layer
Network Access Layer

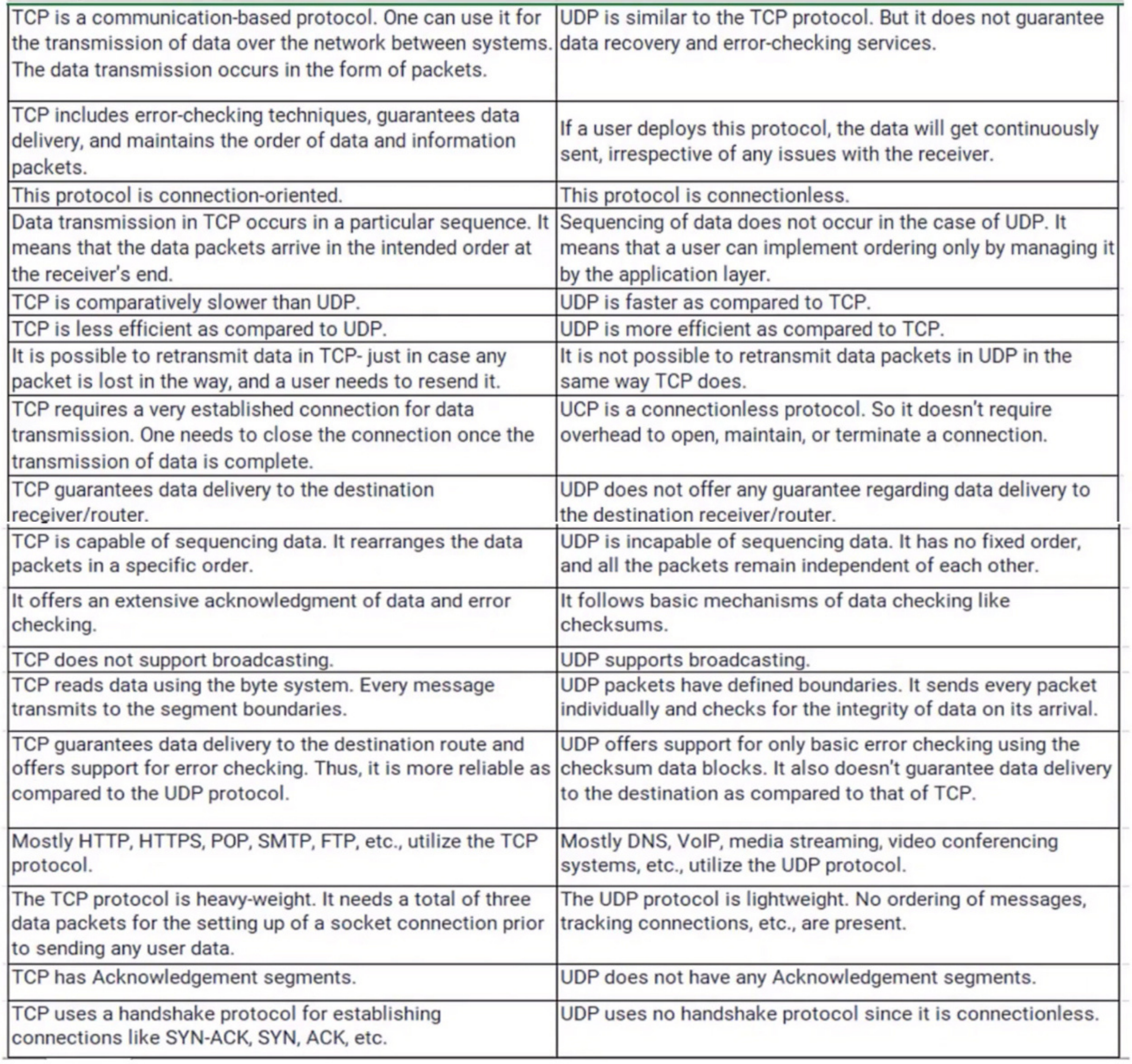




What are the differences between OSI model and TCP/IP Model?

OSI Model	TCP/IP Model
It is developed by ISO (International Standard Organization)	It is developed by ARPANET (Advanced Research Project Agency Network).
OSI model provides a clear distinction between interfaces, services, and protocols.	TCP/IP doesn't have any clear distinguishing points between services, interfaces, and protocols.
OSI refers to Open Systems Interconnection.	TCP refers to Transmission Control Protocol.
OSI uses the network layer to define routing standards and protocols.	TCP/IP uses only the Internet layer.
OSI follows a vertical approach.	TCP/IP follows a horizontal approach.
OSI layers have seven layers.	TCP/IP has four layers.
In the OSI model, the transport layer is only connection-oriented.	A layer of the TCP/IP model is both connection-oriented and connectionless.
In the OSI model, the data link layer and physical are separate layers.	In TCP, physical and data link are both combined as a single host-to-network layer.
Session and presentation layers are a part of the OSI model.	There is no session and presentation layer in the TCP model.
It is defined after the advent of the Internet.	It is defined before the advent of the internet.
The minimum size of the OSI header is 5 bytes.	The minimum header size is 20 bytes.

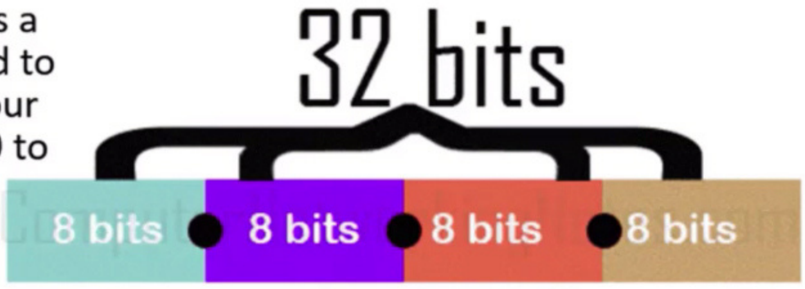
Compare TCP and UDP



TCP is a communication-based protocol. One can use it for the transmission of data over the network between systems. The data transmission occurs in the form of packets.	UDP is similar to the TCP protocol. But it does not guarantee data recovery and error-checking services.
TCP includes error-checking techniques, guarantees data delivery, and maintains the order of data and information packets.	If a user deploys this protocol, the data will get continuously sent, irrespective of any issues with the receiver.
This protocol is connection-oriented.	This protocol is connectionless.
Data transmission in TCP occurs in a particular sequence. It means that the data packets arrive in the intended order at the receiver's end.	Sequencing of data does not occur in the case of UDP. It means that a user can implement ordering only by managing it by the application layer.
TCP is comparatively slower than UDP.	UDP is faster as compared to TCP.
TCP is less efficient as compared to UDP.	UDP is more efficient as compared to TCP.
It is possible to retransmit data in TCP- just in case any packet is lost in the way, and a user needs to resend it.	It is not possible to retransmit data packets in UDP in the same way TCP does.
TCP requires a very established connection for data transmission. One needs to close the connection once the transmission of data is complete.	UCP is a connectionless protocol. So it doesn't require overhead to open, maintain, or terminate a connection.
TCP guarantees data delivery to the destination receiver/router.	UDP does not offer any guarantee regarding data delivery to the destination receiver/router.
TCP is capable of sequencing data. It rearranges the data packets in a specific order.	UDP is incapable of sequencing data. It has no fixed order, and all the packets remain independent of each other.
It offers an extensive acknowledgment of data and error checking.	It follows basic mechanisms of data checking like checksums.
TCP does not support broadcasting.	UDP supports broadcasting.
TCP reads data using the byte system. Every message transmits to the segment boundaries.	UDP packets have defined boundaries. It sends every packet individually and checks for the integrity of data on its arrival.
TCP guarantees data delivery to the destination route and offers support for error checking. Thus, it is more reliable as compared to the UDP protocol.	UDP offers support for only basic error checking using the checksum data blocks. It also doesn't guarantee data delivery to the destination as compared to that of TCP.
Mostly HTTP, HTTPS, POP, SMTP, FTP, etc., utilize the TCP protocol.	Mostly DNS, VoIP, media streaming, video conferencing systems, etc., utilize the UDP protocol.
The TCP protocol is heavy-weight. It needs a total of three data packets for the setting up of a socket connection prior to sending any user data.	The UDP protocol is lightweight. No ordering of messages, tracking connections, etc., are present.
TCP has Acknowledgement segments.	UDP does not have any Acknowledgement segments.
TCP uses a handshake protocol for establishing connections like SYN-ACK, SYN, ACK, etc.	UDP uses no handshake protocol since it is connectionless.

What is IP address in Networking?

IP address stands for Internet Protocol address and is a unique identifying number for each device connected to the network. An IP address is expressed as a set of four numbers with each number in the set ranging from 0 to 255.
for example – 192.152.1.21.

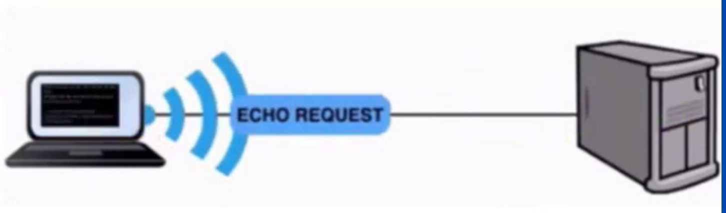


IP addresses are not random strings of numbers. They are allocated by the Internet Assigned Numbers Authority (IANA) to help maintain the internet's security. It was developed in the 1970s and formed the foundation of the internet protocol suite. All the devices connected over the same network can find, send or exchange information with the other connected device using the IP Address protocol. There are two main versions of the IP addresses – IPv4 and IPv6.

What is Ping in Networking?

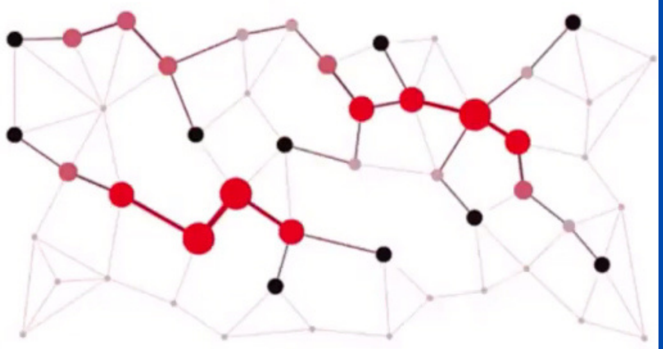
A Ping is a software utility used to verify the reachability of a specific IP address on a network. It was first developed by Michael Muss, in 1983 to quickly test various points of the network and get a response. It works by sending Internet Control Message Protocol echo requests to the host of a destination computer and then waiting for an echo reply. The ping is initiated several times to get responses echoed back to the source provides important information such as –

- consistency in the network connection
- bytes sent and received
- approximate duration of the round-trip time
- packets sent, received, or lost



What is Routing in Networking?

Routing is a process of selecting a path for traffic across one or more networks. Network routing protocols use metrics to determine the optimal path for data packet delivery. For example, in the case of packet-switching networks such as the internet, routing helps to determine the best paths for IP packets to travel from source to their destination.

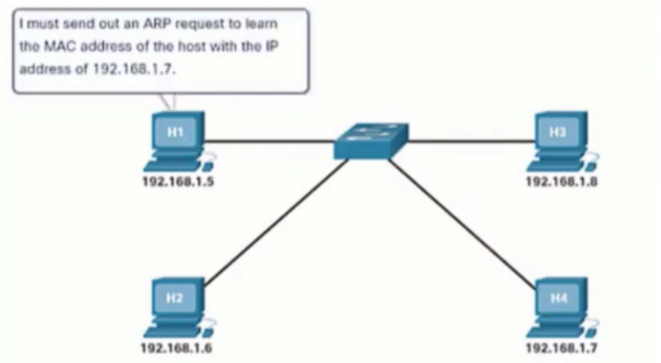


Routing is performed by layer 3 or network layer for the process of most efficient path determination. It can be classified into three categories –

- Static routing
- Dynamic routing
- Default routing

What is ARP?

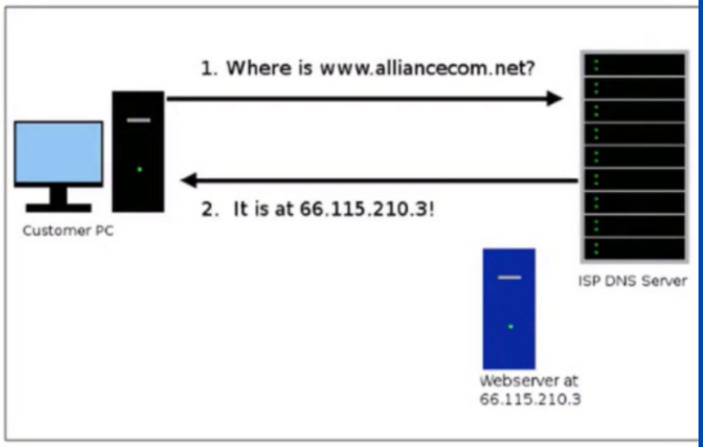
The ARP stands for Address Resolution Protocol which is a communication protocol used to find the MAC address of a host from its IP address. It is an important protocol in networking used to convert a 32-bit Internet Protocol address, typically for IPv4, to a 48-bit MAC address in a LAN.


I must send out an ARP request to learn the MAC address of the host with the IP address of 192.168.1.7.
H1
192.168.1.5
H3
192.168.1.8
H2
192.168.1.6
H4
192.168.1.7

What is DNS?

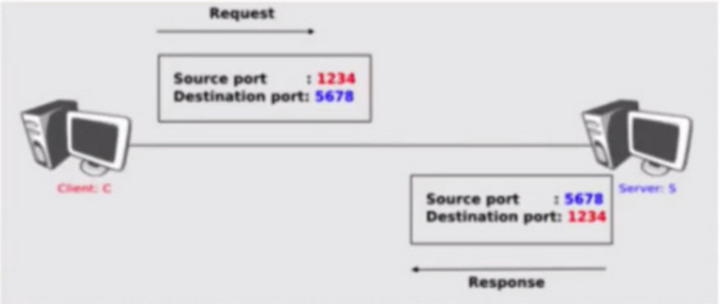
DNS stands for Domain Name System, which, at its most basic, works like the phone book for the internet. You can think of DNS like your smartphone's contact list, which matches contact's names with their phone numbers and email addresses.

DNS is a hierarchical host naming system connected to the internet or any private network. The process involves converting the domain names of participating entities or hosts to a computer-friendly IP address. DNS has been one of the foundations of the functionality of the internet since 1985. Though we don't realise it, we use DNS to check our emails or while browsing on our smartphones every day. Whenever you connect to the internet, the DNS server that you use is automatically established by your network provider.



What is Port in Networking?

A Port is a communication endpoint in networking through which information flows from a program on the computer to another computer on the network. Think of a port as a docking point where all private boats are docked.
Ports are numbered, and each port is associated with a distinct service. They allow computers to differentiate between different kinds of incoming and outgoing traffic over the same network connection. Some ports are reserved for specific protocols, such as HTTP uses port 80, FTP uses port 21, emails received on a local computer use TCP port 25. Each host can have 65535 ports per IP address, and the use of these ports is managed by IANA (Internet Assigned Numbers Authority).



What is Bandwidth?

The network bandwidth refers to the maximum transfer capacity of a wired or wireless network communication. In other words, it is a measure of the amount of data that can be sent and received at a time. While bandwidth is traditionally expressed in bits per second, modern network links with greater capacity are often measured in megabits or gigabits per second. For example, having 5 Mbps bandwidth means you can receive up to 5 megabits of data per second.

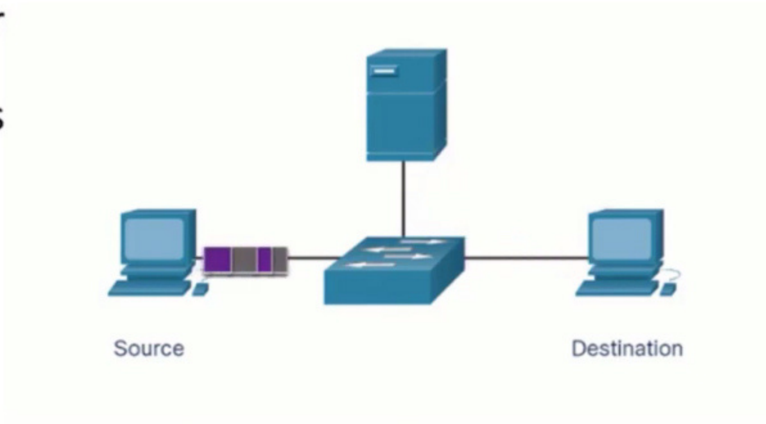
The more bandwidth a connection has, the more data it can send or receive at a given time.

What is Switching?

Switching is a process of exchanging information or data between different computer networks or a network segment using multiple layers of the OSI model. Adding a switch to the network helps reduce traffic congestion and increase network performance.

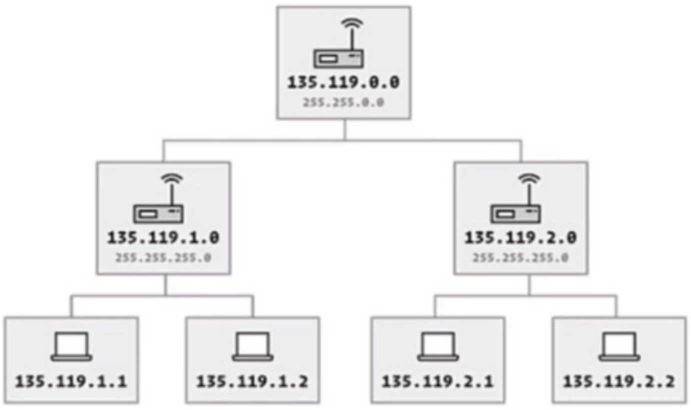
Communication takes place through network switching in three phases –

- By establishing a dedicated circuit link between the sender and the receiver through nodes or switching centres
- Transfer of data once the circuit is established
- Once the communication is complete, the circuit disconnects.



What is Subnetting?

Subnetting is a process of partitioning a bigger network into smaller networks. The primary purpose of subnetting is to reduce network congestion by splitting into subnets or subnetworks, thereby creating a resilient computer network. Creating a subnet allows you to limit the network traffic and avoid backlogs. Subnetting works by dividing broadcast domains to reduce the load imparted on the network. It is crucial for large organisations and businesses to have full control over traffic and improve network speed and performance. Subnetting also enhances network security as the division between each subnet allows enterprises to enforce access controls.


135.119.0.0
255.255.0.0
135.119.1.0
255.255.255.0
135.119.2.0
255.255.255.0
135.119.1.1
135.119.1.2
135.119.2.1
135.119.2.2