COMPUTER NETWORKS

MODULE 1:

Welcome to all to the IT(information technology) world of telephones, mobile phones, smart phones, computers, tablets, etc.

First we think about the answers for these question!! Like:

How is the telephone from my home or office connected to all the telephones in world?
What happens in the background When I dial a number , speak ……using telephones/mobile numbers???
How is the cell phone (mobile phone) is connected to all the mobile / telephones in the world ???
How do millions of telephones worldwide 'communicate' simultaneously???
How is the Desktop Computer from my home /office connected to www.google.com ???
What happens in the background when I type www.google.com and get the first (home) page on my computer???

Further knowing answer for these questions ICT picture comes in our mind, Core technology enabler for whole lot of Information technology services / applications is Information communication technology.

Why Computer networks or Information communication technology?

Because Information Communication Technology is an Evergreen & Ever growing Technology domain.

Needs of ICT professionals in the industry:

We divides ICT industry into two parts:

ICT Products	**ICT Human resources**
Servers	Researchers
Routers	Product developers
Switches	Solution architects
Gateways	Deployment professionals
Firewalls	Management and maintenance professionals
Multiplexers	Marketing and sales professionals
Modems	

ICT professionals:

1. Telecom carriers/service providers like: BSNL, Reliance, Airtel, Vodafone, Idea
2. Internet service providers like: Airtel, BSNL, Reliance, Vodafone, Tata
3. System integrators like: Wipro, Infosys, IBM, Acccenture
4. Large enterprises like: Hindustan lever, Maruti Udyog, TVS Motors, OIL, Power grid corporation, Electric utility companies
5. All most all the companies like: Google, Microsoft, Face-book, TCS, Accenture, Infosys, Wipro
6. Product development companies like: CISCO, Lucent, Intel, Motorola, D-link, Juniper, HP
7. All Engineering institutions like: To teach subjects related to ICT

In day today life we are using internet like social-media, browser etc. Both "client" and "server" refer to computers that are used for different purposes. A client is a small computer that accesses a server through a network. For example, in an organization, an employee logs in to the client machine to access the files and applications running on a server machine.

Basically, whole IT(information technology) is built on ICT(Information communication technology).

How IT and ICT related?? Means, it encompasses the use of computers, networks, computer-software and other electronic devices for the management and communication of information. ITC focuses more on how digital technologies assist users in handling information.

Computer Networks:

In simplest form, A network is a collection and connection of entities located over geographical points to supply products or services from one end to other end. A communication network is a set of equipment and facilities that provides transfer of information service between users located at various geographical points.

Basically, Network is known as proper communication between sender and receiver in any medium using some protocol. A computer network is a set of computers sharing resources located on or provided by network nodes. Computers use common communication protocols over digital interconnections to communicate with each other.

Sender ----->media----> Receiver

Example: Newspaper distribution network

Newspaper Publishing house ---> Distributor ---> agent ---> newspaper boy ---> newspaper reader.

So, network is nothing but a collection and connection of entities to provide a specific service. Today's Internet is a multi-media network, we can send any type of information through the internet (i.e. anything that can be represented as 0s and 1s).

Components of data communication: Sender, receiver , transmission medium, message, protocol.

Sender: The sender is the device that sends the data message. It can be a computer, workstation, telephone handset, video camera, and so on.

Receiver: The receiver is the device that receives the message. It can be a computer, workstation, telephone handset, television, and so on.

Transmission Medium: The transmission medium is the physical path by which a message travels from sender to receiver. Some examples of transmission media include twisted-pair wire, coaxial cable, fiber-optic cable, and radio waves.

Message: The message is the information (data) to be communicated. Popular forms of information include text, numbers, pictures, audio, and video.

Protocol: A protocol is a set of rules used to communicate between sender and receiver. Without a protocol, two devices may be connected but not communicating, just as a person speaking Kannada cannot be understood by a person who speaks only Hindi.

Different types of communications: Text, images, audio, and video.

Internet Service Provider (ISP): ISP is a business that provides the service to connect your computer to the Internet.

Note that an ISP is not directly connected to server of each and every website. It is just a part of the network.

Internet is the indirect connectivity between numerous networks.

Aspects:

1. Connectivity: Examples how various phones are connected with others like 5G, 4G etc.
2. Processing Communication.

Broadcasting:

Broadcasting is a group communication, where a sender sends data to receivers simultaneously. This is an all − to − all communication model where each sending device transmits data to all other devices in the network domain.

Example: Browsing information through chrome using network. Means in between computer and google server are not connected directly, so for connection it will use ISP to ISP connection.

Hubs:

If we want to connect multiple computer to single single node at a time then we use hubs. And it’s a single layer device.

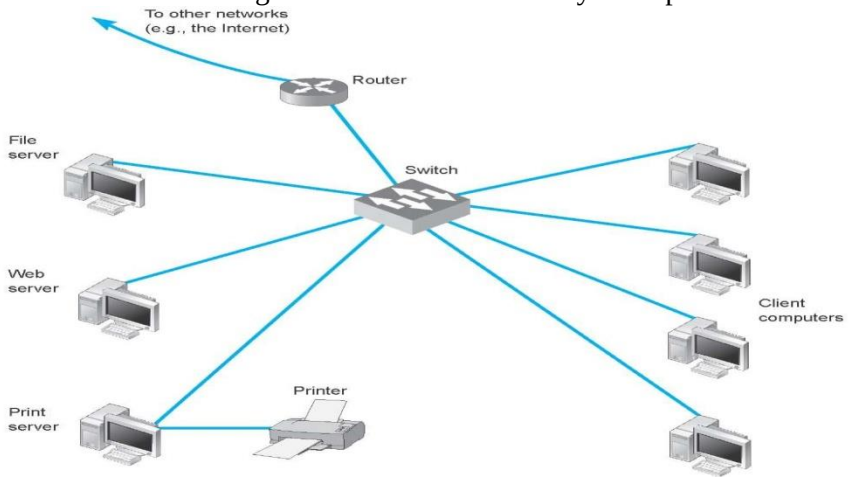
Switches:

Switch helps to connect between two different hubs. And it’s two layer device.

Routers:

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. And it's three layer device. Routers are used to route information from one end to another end. Every ISP utilizes a network of routers to connect to internet.

Local Area Network (LAN): It is a collection of devices connected together in one physical location, such as a building, office, or home.
For example, in college with multiple departments, such as ECE, CSE, ME and CE, each department's computers could be logically connected to the same switch but segmented to behave as if they are separate.



Flow of data packets: Entity(device) -> Hub -> Switch -> Router -> ……..-> entity(device)

Transmission link:

Transmission link is used to connecting routers. This comprises of telephone cables, coaxial cables, fiber optic cables. There is difference between link and media. Media comprises of everything between two entities while links are just the connecting parts of the network. The data is transmitted through the transmission links in the form of 1s and 0s.

Mode Of Communication types:

1. Simplex mode: the communication is unidirectional, as on a one-way street. Only one of the two devices on a link can transmit; the other can only receive.
For example, Keyboards and traditional monitors. The key-board can only introduce input; the monitor can only accept output. The simplex mode can use the entire capacity of the channel to send data in one direction.

2.Half-duplex mode: In half-duplex mode, each station can both transmit and receive, but not at the same time. When one device is sending, the other can only receive, and vice versa.
For example, a one-lane road with traffic allowed in both directions. When cars are traveling in one direction, cars going the other way must wait. In a half-duplex transmission, the entire capacity of a channel is taken over by whichever of the two devices is transmitting at the time. Walkie-talkies and CB (citizens band) radios are both half-duplex systems. The half-duplex mode is used in cases where there is no need for communication in both directions at the same time; the entire capacity of the channel can be utilized for each direction.

3.Full-duplex mode: In full-duplex, both stations can transmit and receive simultaneously.
For example, a two-way street with traffic flowing in both directions at the same time. In full-duplex mode, signals going in one direction share the capacity of the link with signals going in the other direction. This sharing can occur in two ways: Either the link must contain two physically separate transmission paths, one for sending and the other for receiving; or the capacity of the channel is divided between signals travelling in both directions.
One common example of full-duplex communication is the telephone network. When two people are communicating by a telephone line, both can talk and listen at the same time.

Difference between Connection Oriented communication and Connection less communication:

Connection oriented communication	Connection less communication
Establish a dedicated connection before data sending	Doesn't establish a dedicated connection before data sending
More reliable	Faster compare to connection oriented
Performs handshaking	Doesn't performs handshaking
Data is delivered in the same order the sender has sent them	No guarantee that the data is delivered in order
Performs flow control and error checking	Doesn't performs flow control and error checking
It is preferred by long and steady communication.	It is preferred by bursty communication.

Information communication networks traditional categories into two types:

1. Telecom Networks: These are primarily for only voice communications
2. Computer Networks: These are primarily for data communications like text, image, video using computers

Once upon a time, only telephones were used for voice communication, only computers were used for data(text, image, video) communication, only radio was used for audio broadcasting, only TVs were used for video broadcasting. But today's computers, smart phones connected to INTERENT because of this we using these three services like voice, text and video.

Telecom Networks:

1.Traditional: These are called wired phones/landline phones
2. Modern: These are called wireless phones/mobile phones(2G, 3G, 4G, 5G)

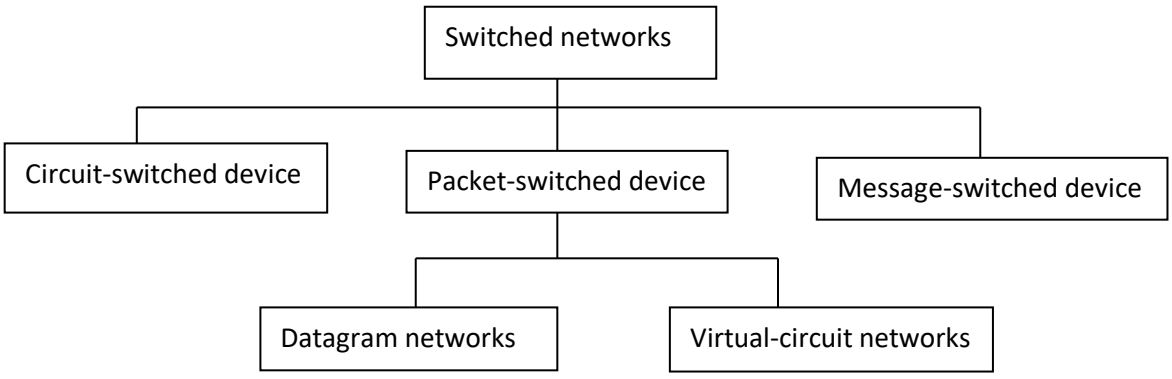
Telecom Networks are systems of interconnected communication devices and equipment that enable people to communicate with each other over long distances. These networks use various technologies and protocols to facilitate the transmission of voice, data, and video signals between devices, including smart phones, computers, and other communication devices. Telecom networks play a critical role in modern society, providing essential communication services to individuals, businesses, and organizations. They enable people to communicate with each other across vast distances, enabling global communication and facilitating international trade and commerce.

Telecom Networks are made up of various components, including transmission systems, switching systems, and network management systems. These components work together to ensure that communication signals are transmitted and delivered efficiently and securely.

Basic elements:

1.Switches
2. Multiplexer
3. Transmission line

Switched Networks:



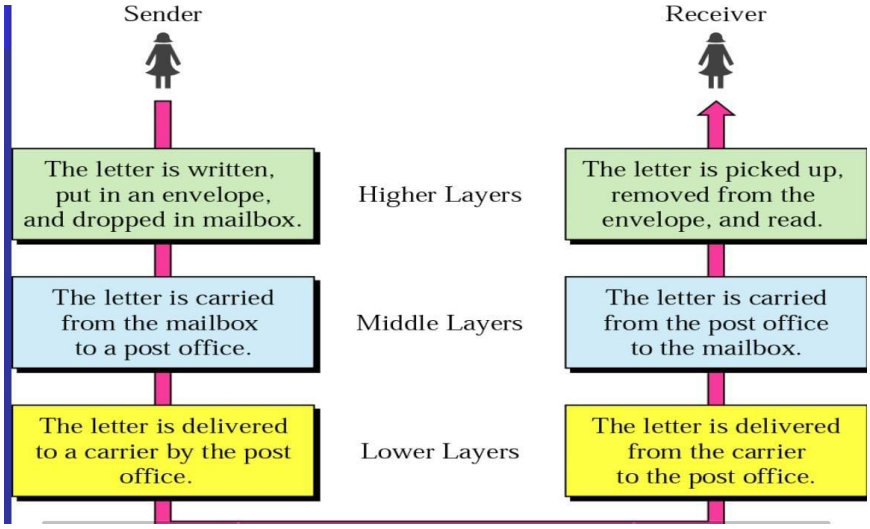
Switched networks: Switching is the technique by which nodes control or switch data to transmit it between specific points on a network. In message switching the entire message is transmitted without any break from one node to another. There is no direct link present between the sender and the receiver in message switching.

Circuit-switched device: A circuit-switched network consists of a set of switches connected by physical links. A connection between two stations is a dedicated path made of one or more links. However, each connection uses only one dedicated channel on each link. Each link is normally divided into n channels by using FDM or TDM. It is made of a set of switches connected by physical links, in which each link is divided into n channels. In circuit switching, the resources need to be reserved during the setup phase, the resources remain dedicated for the entire duration of data transfer until the teardown phase.

Packet-switched device: The routing and transferring of data by means of addressed packets so that a channel is occupied during the transmission of the packet only, and upon completion of the transmission the channel is made available for the transfer of other traffic.

Message-switched device: Message switching is a switching mechanism in which a message is sent as a single unit and routed to intermediary nodes where it is stored and forwarded. The message-switching approach does not provide a dedicated path between the sender and receiver. In message switching, end-users communicate by sending and receiving messages that include the entire data to be shared. Messages are the smallest individual unit. Also, the sender and receiver are not directly connected. Several intermediate nodes transfer data and ensure that the message reaches its destination. Message-switched data networks are hence called hop-by-hop systems.

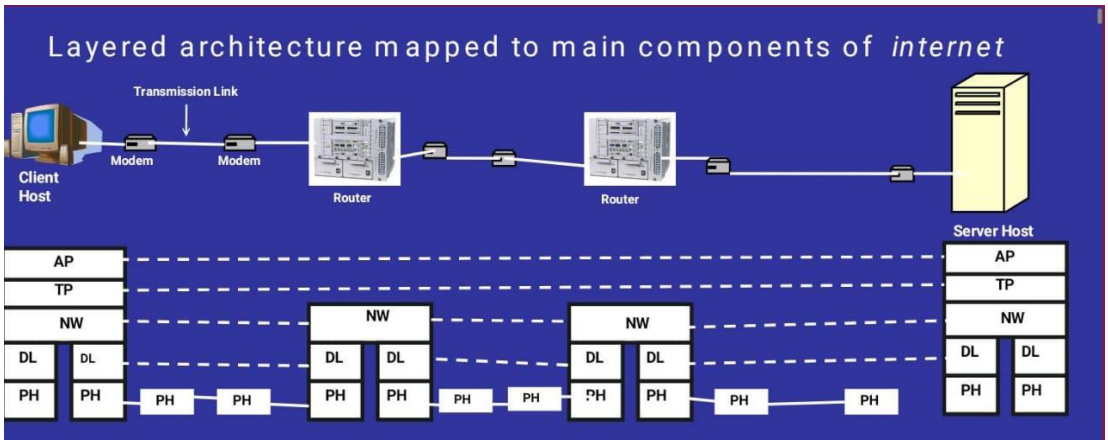
Layered Archicture:



For example, In higher layer the sender written a letter, put in an envelope, and dropped in mailbox. Then letter enters to middle layer which is carried by mailbox to a post office. When it comes to lower layers which is carried by post office. Now latter is transform through media without effecting to letter or matter which is present in latter. After from reciver side, in lower layer they will collect the letter from the carrier. Then letter is carried by post office to the mailbox. Now in higher layer, the letter is picked up, removed from the envelope, and received by receiver.

So that, benefits of layering is simplify the process of network design, network management, product development and providing flexibility to modify network, develop network.

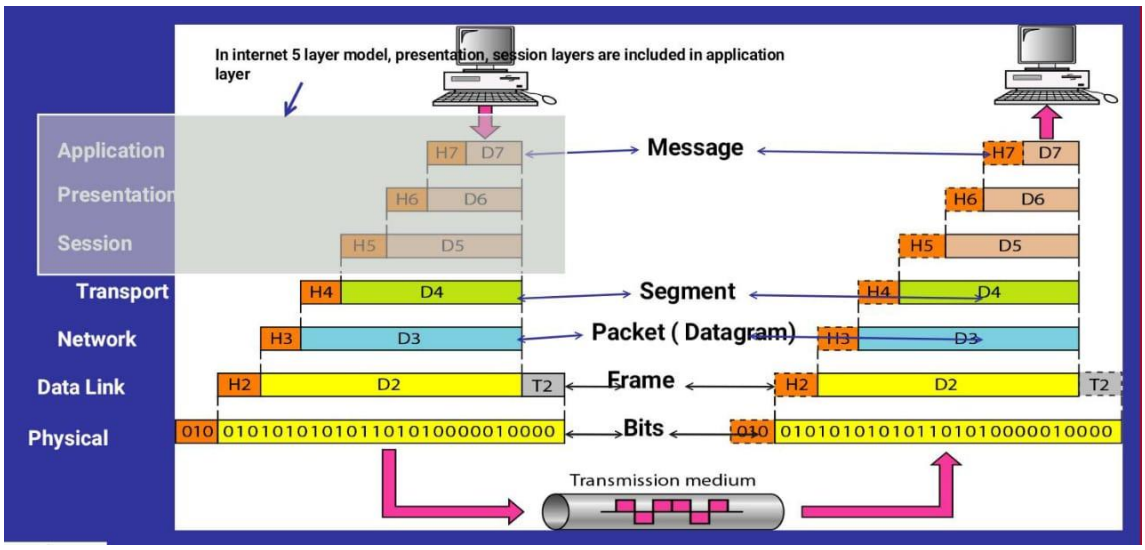
Main components of internet:



Let us assume that server communicates with computer, we have five communicating devices in this communication: server host (server), the switch in link 1, the router, the switch in link 2, and the client host (computer). Each device is involved with a set of layers depending on the role of the device in the internet. The two hosts are involved in all five layers; the server host needs to create a message in the application layer and send it down the layers so that it is physically sent to the client host. The client host needs to receive the communication at the physical layer and then deliver it through the other layers to the application layer.

The router is involved in only three layers; there is no transport or application layer in a router as long as the router is used only for routing. Although a router is always involved in one network layer, it is involved in n combinations of link and physical layers in which n is the number of links the router is connected to. The reason is that each link may use its own data-link or physical protocol.

A switch in a link, however, is involved only in two layers, data-link and physical. Although each switch in the above figure has two different connections, the connections are in the same link, which uses only one set of protocols. This means that, unlike a router, a switch is involved only in one data-link and one physical layer.



At the application layer, the data to be exchanged is referred to as a message. A message normally does not contain any header or trailer, but if it does, we refer to the whole as the message. The message is passed to the transport layer.

The transport layer takes the message as the payload, the load that the transport layer should take care of. It adds the transport layer header to the payload, which contains the identifiers of the source and destination application programs that want to communicate plus some more information that is needed for the end-to- end delivery of the message, such as information needed for flow, error control, or congestion control. The result is the transport-layer packet, which is called the segment (in TCP) and the user datagram (in UDP). The transport layer then passes the packet to the network layer.

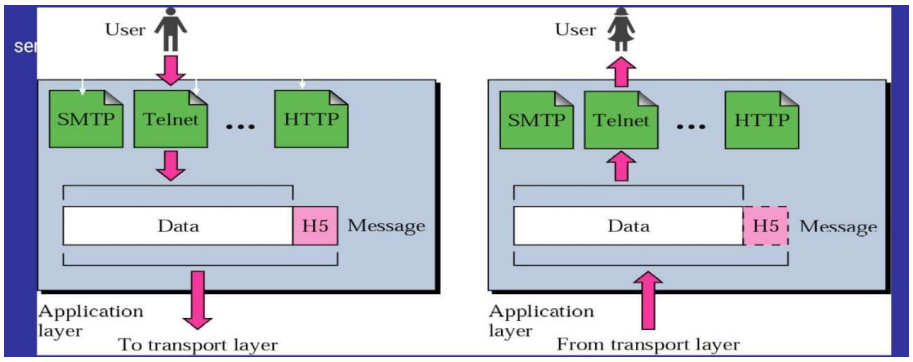
The network layer takes the transport-layer packet as data or payload and adds its own header to the payload. The header contains the addresses of the source and destination hosts and some more information used for error checking of the header, fragmentation information, and so on. The result is the network layer packet, called a datagram. The network layer then passes the packet to the data-link layer.

The data-link layer takes the network-layer packet as data or payload and adds its own header, which contains the link-layer addresses of the host or the next hop (the router). The result is the link-layer packet, which is called a frame. The frame is passed to the physical layer for transmission.

At the destination host, each layer only encapsulates the packet received, removes the payload, and delivers the payload to the next-higher layer protocol until the message reaches the application layer. It is necessary to say that encapsulation in the host involves error checking.

Key responsibilities of every layer:

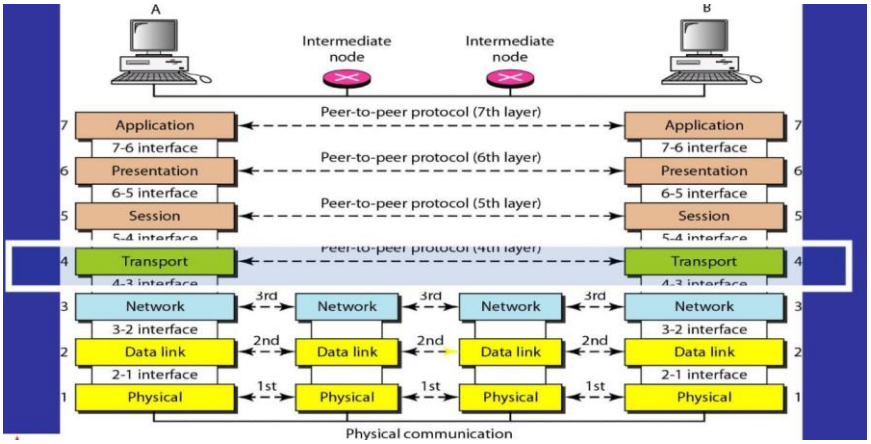
1. Application layer:



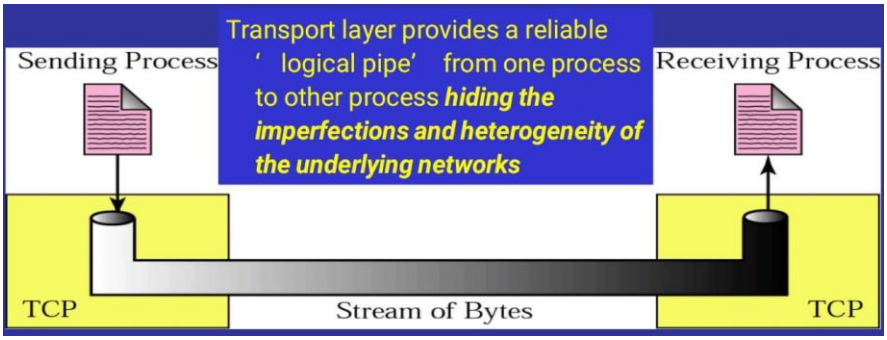
The logical connection between the two application layers is end- to-end. The two application layers exchange messages between each other as though there were a bridge between the two layers. Communication at the application layer is between two processes. To communicate, a process sends a request to the other process and receives a response. Process-to-process communication is the duty of the application layer. The application layer in the Internet includes many predefined protocols, but a user can also create a pair of processes to be run at the two hosts.

The Hypertext Transfer Protocol (HTTP) is a vehicle for accessing the World Wide Web (WWW). The Simple Mail Transfer Protocol (SMTP) is the main protocol used in electronic mail (e-mail) service. The File Transfer Protocol (FTP) is used for transferring files from one host to another. The Terminal Network (TELNET) and Secure Shell (SSH) are used for accessing a site remotely. The Simple Network Management Protocol (SNMP) is used by an administrator to manage the Internet at global and local levels. The Domain Name System (DNS) is used by other protocols to find the network-layer address of a computer. The Internet Group Management Protocol (IGMP) is used to collect membership in a group.

2. Transport layer:



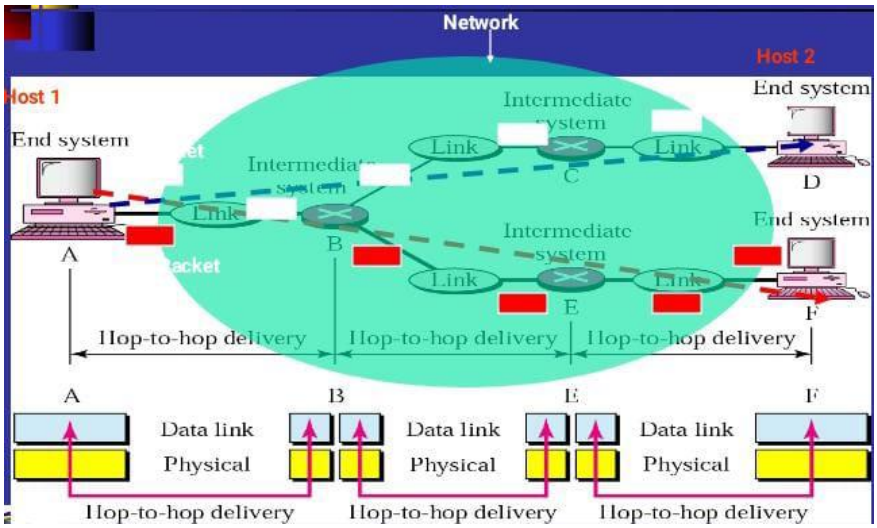
The logical connection at the transport layer is also end-to-end. The transport layer at the source host gets the message from the application layer, encapsulates it in a transport- layer packet (called a segment or a user datagram in different protocols) and sends it, through the logical (imaginary) connection, to the transport layer at the destination host. In other words, the transport layer is responsible for giving services to the application layer to get a message from an application program running on the source host and deliver it to the corresponding application program on the destination host. We may ask why we need an end-to-end transport layer when we already have an end-to-end application layer. Because, separation of tasks and duties, which we discussed earlier. The transport layer should be independent of the application layer. In addition, we will see that we have more than one protocol in the transport layer, which means that each application program can use the protocol that best matches its requirement.



Adds transport layer headers and divides long message from application to smaller segments. Then every process identified by PORT number. That is done by addressing each application/process like email to email, terminal to host, browser client to browser server. Deals with logical connection between the sender process and receiver process like connection oriented transport and connectionless transport. Transport layer defines the Quality of Service(QOS) and makes sure that requested quality of service is achieved through the layer below.

As we said, there are a few transport-layer protocols in the Internet, each designed for some specific task. The main protocol, Transmission Control Protocol (TCP), is a connection-oriented protocol that first establishes a logical connection between trans port layers at two hosts before transferring data. It creates a logical pipe between two TCPs for transferring a stream of bytes. TCP provides flow control (matching the sending data rate of the source host with the receiving data rate of the destination host to prevent overwhelming the destination), error control (to guarantee that the segments arrive at the destination without error and resending the corrupted ones), and congestion control to reduce the loss of segments due to congestion in the network. The other common protocol, User Datagram Protocol (UDP), is a connectionless protocol that transmits user data grams without first creating a logical connection. In UDP, each user datagram is an independent entity without being related to the previous or the next one (the meaning of the term connectionless). UDP is a simple protocol that does not provide flow, error, or congestion control. Its simplicity, which means small overhead, is attractive to an application program that needs to send short messages and cannot afford the retransmission of the packets involved in TCP, when a packet is corrupted or lost. A new protocol, Stream Control Transmission Protocol (SCTP) is designed to respond to new applications that are emerging in the multimedia.

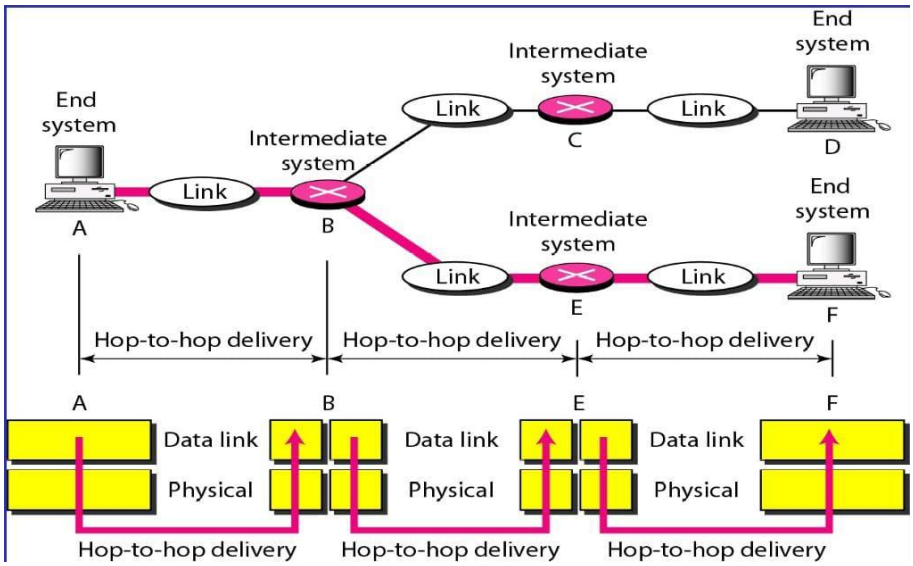
3. Network layer:



The network layer is responsible for creating a connection between the source computer and the destination computer. The communication at the network layer is host-to-host. However, since there can be several routers from the source to the destination, the routers in the path are responsible for choosing the best route for each packet. We can say that the network layer is responsible for host-to-host communication and routing the packet through possible routes. Again, we could have added the routing duty to the transport layer and dropped this layer. One reason, as we said before, is the separation of different tasks between different layers. The second reason is that the routers do not need the application and transport layers. Separating the tasks allows us to use fewer protocols on the routers.

The network layer also has some auxiliary protocols that help IP in its delivery and routing tasks. The Internet Control Message Protocol (ICMP) helps IP to report some problems when routing a packet. The Internet Group Management Protocol (IGMP) is another protocol that helps IP in multitasking. The Dynamic Host Configuration Protocol (DHCP) helps IP to get the network-layer address for a host. The Address Resolution Protocol (ARP) is a protocol that helps IP to find the link-layer address of a host or a router when its network-layer address is given.

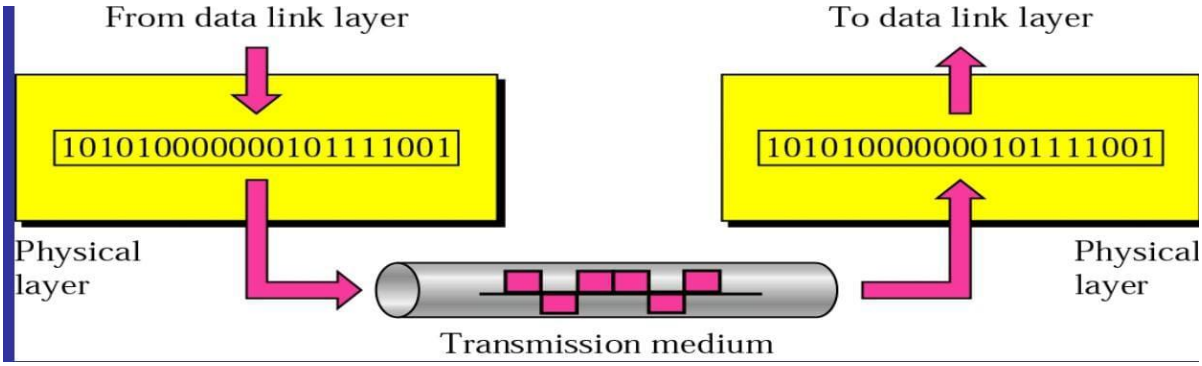
4. Data link layer:



Basically, It's a node connection. We know that an internet is made up of several links (LANs and WANs) connected by routers. There may be several overlapping sets of links that a datagram can travel from the host to the

destination. The routers are responsible for choosing the best links. However, when the next link to travel is determined by the router, the data-link layer is responsible for taking the datagram and moving it across the link. The link can be a wired LAN with a link-layer switch, a wireless LAN, a wired WAN, or a wireless WAN.
TCP/IP does not define any specific protocol for the data-link layer. It supports all the standard and proprietary protocols. Any protocol that can take the datagram and carry it through the link suffices for the network layer. The data-link layer takes a datagram and encapsulates it in a packet called a frame. Each link-layer protocol may provide a different service. Some link-layer protocols provide complete error detection and correction, some provide only error correction.

5. Physical layer:



We can say that the physical layer is responsible for carrying individual bits in a frame across the link. Although the physical layer is the lowest level, the communication between two devices at the physical layer is still a logical communication because there is another, hidden layer, the transmission media, under the physical layer. Two devices are connected by a transmission medium (cable or air). We need to know that the transmission medium does not carry bits; it carries electrical or optical signals. So the bits received in a frame from the data-link layer are transformed and sent through the transmission media, but we can think that the logical unit between two physical layers in two devices is a bit.

Module 2:

NETWORK LAYER:

Logical addressing:

Every host/gadget connected to interent, must have an unique IP address. Internet is network of networks. Global internet is divided into hundreds of sub-networks. Each Network or Sub-network is uniquely identified by an address (Network ID or Subnet ID). Every host connected to internet is part of a sub network. So, the address of a host has 2 part like subnet ID and host ID.
For example, If the IP address of a host connected to a sub network is 192.168.1.1/24, its sub net ID is 192.168.1.0 . So, the IP address, depends on the network to which it is connected. The IP address, when a client is connected at home is different from when it is connected at college campus.
An IPv4 address is a 32-bit address that uniquely and universally defines the connection of a device (for example, a computer or a router) to the Internet. The address space supported by IPv4 is: 232 or 4,294,967,296.

Mechanism used to manage IP address:
1. DHCP (Temporary solution)
2. NAT (Temporary solution)
3. IPv6 (Permanent solution)

Internet Protocol version 4(IPv4):
It provides: 1. Addressing
2. Fragmentation

3. Preliminary QoS

Types of IP Address:

1. Static: Every machine permanently gets a unique IP address that cannot be assigned to any other machine.
For example, All servers get a static IP address that is permanently assigned to them like Google's IP address.
2. Dynamic: Allows reuse of IP address.
For example, DHCP protocol allows a server to assign new IP addresses to its client.

Rules of IP Address:

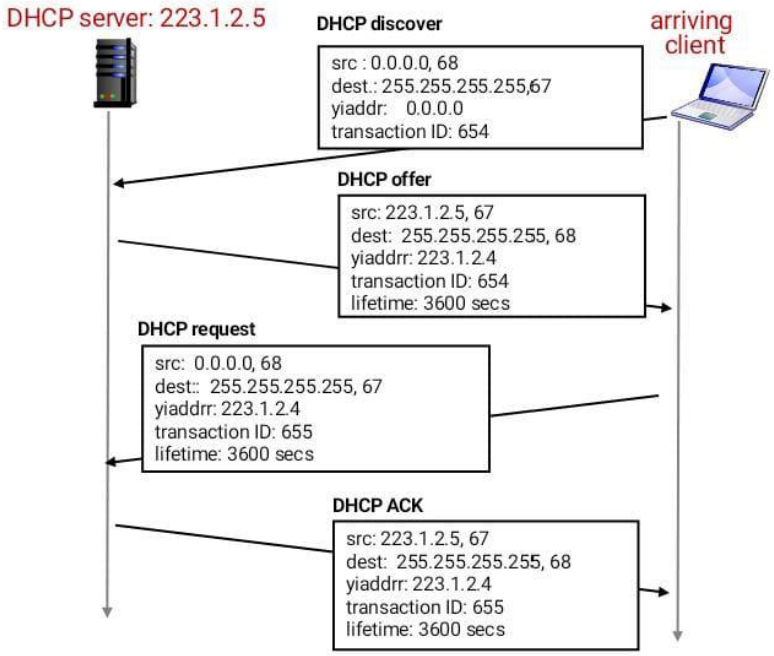
The first address in a block /subnet is normally not assigned to any device in the subnet; it is used as the subnet ID that represents the complete subnet to the rest of the world. The Last address in a block is normally not assigned to any device; it is used as a special address to broadcast a packet to all the hosts in that subnet. So, total number of usable addresses in a subnet is always total number of addresses available – 2.
For example in a classfull addressing, in class C, only 254 addresses can be used to configure hosts.

Each address in the block can be considered as a two-level hierarchical structure: the leftmost n bits (prefix) define the network; the rightmost 32 − n bits define the host.

Dynamic Host Control Protocol(DHCP):

A DHCP server takes a subnet IP address (slash notation) and distributes IP addresses from that subnet to all the other clients in that subnet. DHCP server also takes a IP address from that subnet. As more clients or exit the subnet, DHCP assigns and unassigns IP addresses to those clients. Initially, DHCP clients broadcasts a message searching for a DHCP server, in order to request an IP address. This is called discovery message. Once a DHCP server receives that broadcast message, it responds with another broadcast message with a IP address from its pool of IP addresses. This is called offer message. Notice that its an offer, client can accept it or reject it. DHCP also has conflict detection and resolution algorithms in case two clients get assigned with same IP address in a subnet. Usually when two clients request of an IP address "simultaneously" usually there is some microsecond delay between each request and server can distinguish between these clients. But in a rare case where two clients request at the exact same time, DHCP server wont assign same IPs to them since it also keeps a database of IPs assigned to each client. These days, DHCP service is integrated into routers.

DHCP client-server scenario:



The joining host creates a DHCPDISCOVER message in which only the transactionID field is set to a random number. No other field can be set because the host has no knowledge with which to do so. This message is encapsulated

in a UDP user datagram with the source port set to 68 and the destination port set to 67. The user datagram is encapsulated in an IP datagram with the source address set to 0.0.0.0 ("this host") and the destination address set to 255.255.255.255 (broadcast address). The reason is that the joining host knows neither its own address nor the server address.

The DHCP server or servers (if more than one) responds with a DHCPOFFER message in which the your address field defines the offered IP address for the joining host and the server address field includes the IP address of the server. The message also includes the lease time for which the host can keep the IP address. This message is encapsulated in a user datagram with the same port numbers, but in the reverse order. The user datagram in turn is encapsulated in a datagram with the server address as the source IP address, but the destination address is a broadcast address, in which the server allows other DHCP servers to receive the offer and give a better offer if they can. The joining host receives one or more offers and selects the best of them.

The joining host then sends a DHCPREQUEST message to the server that has given the best offer. The fields with known value are set. The message is encapsulated in a user datagram with port numbers as the first message. The user datagram is encapsulated in an IP datagram with the source address set to the new client address, but the destination address still is set to the broadcast address to let the other servers know that their offer was not accepted.

Finally, the selected server responds with a DHCPACK message to the client if the offered IP address is valid. If the server cannot keep its offer (for example, if the address is offered to another host in between), the server sends a DHCPNACK message and the client needs to repeat the process. This message is also broadcast to let other servers know that the

For example, In classroom we have to convey our message to one person, but we don't know there name. So, randomly we stand in front of all call one name, then we give message to who will response us.

Network Address Resolution:

It's a way to map multiple private addresses inside a local network to a public IP address before transferring the information onto the internet. Organizations that want multiple devices to employ a single IP address use NAT, as do most home routers.

To assign each company a single IP address (or at most, a small number of them) for internet traffic. Within company every computer gets an unique IP address. When a packet exits the company and goes to the ISP, an address translation takes place

If there is a laptop connected to a home network using NAT. That network eventually connects to a router that addresses the internet. Suppose that someone uses that laptop to search for directions to their favourite restaurant. The laptop is using NAT. So, it sends this request in an IP packet to the router, which passes that request along to the internet and the search service you're using. But before your request leaves your home network, the router first changes the internal IP address from a private local IP address to a public IP address. Your router effectively translates the private address you're using to one that can be used on the internet and then back again. Now you know that your humble little cable modem or DSL router has a little, automated translator working inside of it.

Address Resolution Protocol(ARP):

ARP stands for Address Resolution Protocol, which is used to find the MAC address of the device from its known IP address. This means, the source device already knows the IP address but not the MAC address of the destination device. The MAC address of the device is required because you cannot communicate with a device in a local area network (Ethernet) without knowing its MAC address. So, the Address Resolution Protocol helps to obtain the MAC address of the destination device.

For example, Suppose two devices (device A and device B) want to communicate with each other. The device A already knows the IP address of the Device B. But in order to communicate with the device B, device A still needs the MAC address of the device B. The IP address is used to locate a device on a local area network and the MAC address is used to identify the actual device. The device A first look at its internal list known as ARP cache (table) to check if the IP address of the device B already consists of its MAC address or not. If the ARP table consists of the MAC address of the device B, then device A simply use that MAC address and start communication.

If the table does not consist of the MAC address of device B, then device A sends an ARP broadcast message on the network to know which device has that specific IP address and ask for the MAC address of that particular device. Then the device that has matching IP address to the source address sends an ARP response message that consists of the MAC address of the device B. When device A obtains the MAC address of the device B, it will store the information in the ARP

cache (table). The ARP cache is used to make the network more efficient. It stores the IP address of the device along with its MAC address. The stored information is used when device A wants to communicate with device B on a network, and it does not need to broadcast a message on the network again. It will simply check the ARP cache for the entries and then use it for communication.

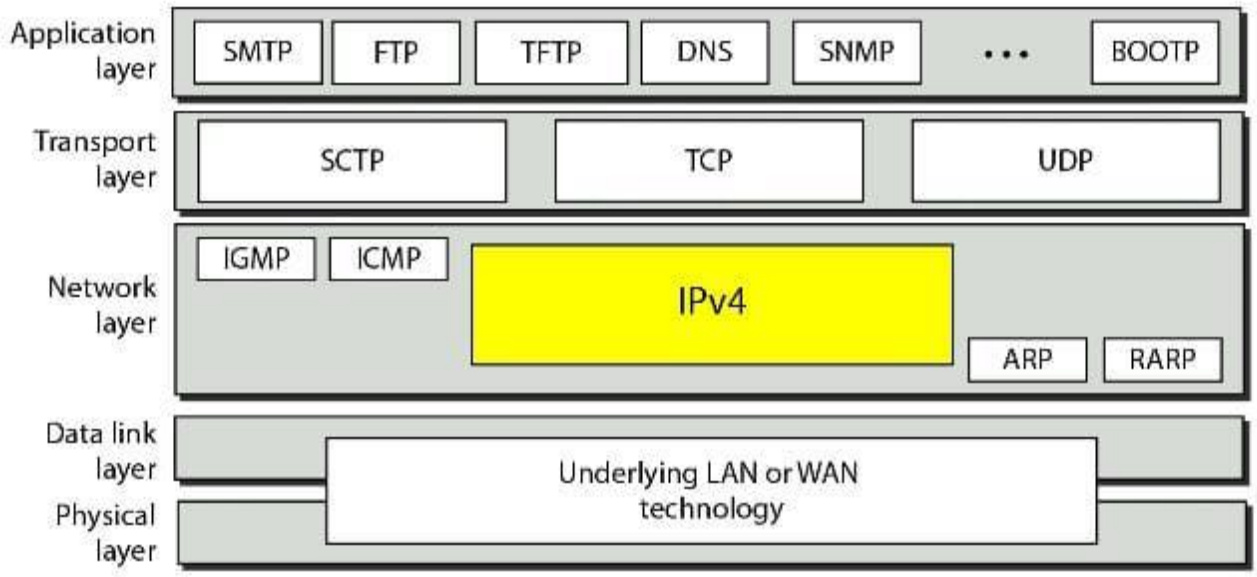
Key functions of router:

1. Forwarding packet
2. Routing calculation

Forwarding Packet: If routing is applying strategies and running some routing protocols to create the decision-making tables for each router, forwarding can be defined as the action applied by each router when a packet arrives at one of its interfaces. The decision-making table a router normally uses for applying this action is sometimes called the forwarding table and sometimes the routing table. When a router receives a packet from one of its attached networks, it needs to forward the packet to another attached network (in unicast routing) or to some attached networks (in multicast routing). To make this decision, the router uses a piece of information in the packet header, which can be the destination address or a label, to find the corresponding output interface number in the forwarding table.

Routing calculation: The network layer is responsible for routing the packet from its source to the destination. A physical network is a combination of networks (LANs and WANs) and routers that connect them. This means that there is more than one route from the source to the destination. The network layer is responsible for finding the best one among these possible routes. The network layer needs to have some specific strategies for defining the best route. In the Internet today, this is done by running some routing protocols to help the routers coordinate their knowledge about the neighbour hood and to come up with consistent tables to be used when a packet arrives.

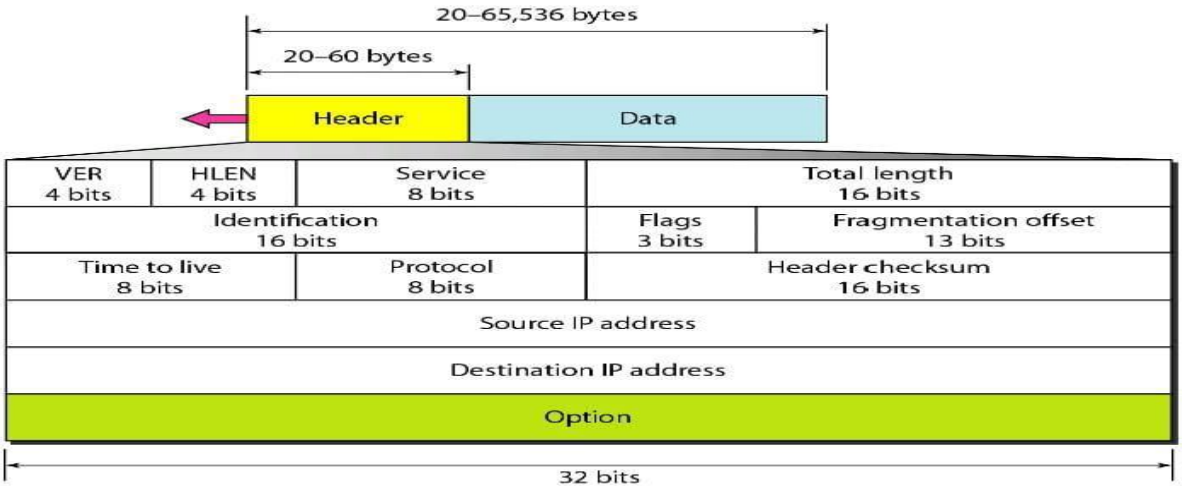
Position of IPv4 in TCP/IP protocol suite:



IPv4 is an unreliable datagram protocol a best-effort delivery service. The term best-effort means that IPv4 packets can be corrupted, be lost, arrive out of order, or be delayed, and may create congestion for the network. If reliability is important, IPv4 must be paired with a reliable transport-layer protocol such as TCP. An example of a more commonly understood best-effort delivery service is the post office. The post office does its best to deliver the regular mail but does not always succeed. If an unregistered letter is lost or damaged, it is up to the sender or would-be recipient to discover this. The post office itself does not keep track of every letter and cannot notify a sender of loss or damage of one. IPv4 is also a connectionless protocol that uses the datagram approach. This means that each datagram is handled independently, and

each datagram can follow a different route to the destination. This implies that data grams sent by the same source to the same destination could arrive out of order. Again, IPv4 relies on a higher-level protocol to take care of all these problems.

IPv4 datagram format:



Version Number: The 4-bit version number (VER) field defines the version of the IPv4 protocol, which, obviously, has the value of 4.

Header Length: The 4-bit header length (HLEN) field defines the total length of the datagram header in 4-byte words. The IPv4 datagram has a variable-length header. When a device receives a datagram, it needs to know when the header stops and the data, which is encapsulated in the packet, starts. However, to make the value of the header length (number of bytes) fit in a 4-bit header length, the total length of the header is calculated as 4-byte words. The total length is divided by 4 and the value is inserted in the field. The receiver needs to multiply the value of this field by 4 to find the total length.

Service Type: In the original design of the IP header, this field was referred to as type of service (TOS), which defined how the datagram should be handled. The use of 4-byte words for the length header is also logical because the IP header always needs to be aligned in 4-byte boundaries.

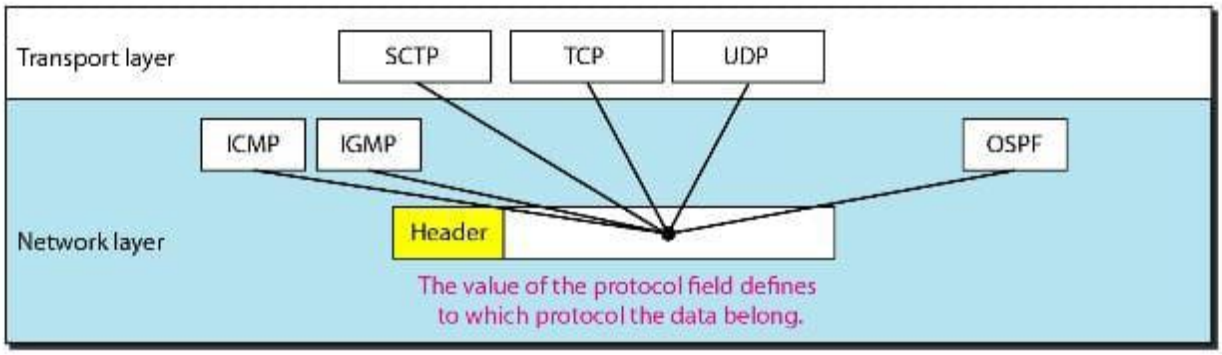
Total Length: This 16-bit field defines the total length (header plus data) of the IP datagram in bytes. A 16-bit number can define a total length of up to 65,535 (when all bits are 1s). However, the size of the datagram is normally much less than this. This field helps the receiving device to know when the packet has completely arrived. To find the length of the data coming from the upper layer, subtract the header length from the total length. The header length can be found by multiplying the value in the HLEN field by 4.

Identification, Flags, and Fragmentation Offset: These three fields are related to the fragmentation of the IP datagram when the size of the datagram is larger than the underlying network can carry.

Time-to-live: Due to some malfunctioning of routing protocols (discussed later) a datagram may be circulating in the Internet, visiting some networks over and over without reaching the destination. This may create extra traffic in the Internet. The time-to-live (TTL) field is used to control the maximum number of hops (routers) visited by the datagram. When a source host sends the datagram, it stores a number in this field. This value is approximately two times the maximum number of routers between any two hosts. Each router that processes the datagram decrements this number by one. If this value, after being decremented, is zero, the router discards the datagram.

Protocol: In TCP/IP, the data section of a packet, called the payload, carries the whole packet from another protocol. A datagram, for example, can carry a packet belonging to any transport-layer protocol such as UDP or TCP. A datagram can also carry a packet from other protocols that directly use the service of the IP, such as some routing protocols or some auxiliary protocols. The Internet authority has given any protocol that uses the service of IP a unique 8-bit number which

is inserted in the protocol field. When the payload is encapsulated in a datagram at the source IP, the corresponding protocol number is inserted in this field; when the datagram arrives at the destination, the value of this field helps to define to which protocol the payload should be delivered. In other words, this field provides multiplexing at the source and demultiplexing at the destination. Note that the protocol fields at the network layer play the same role as the port numbers at the transport layer. However, we need two port numbers in a transport-layer packet because the port numbers at the source and destination are different, but we need only one protocol field because this value is the same for each protocol no matter whether it is located at the source or the destination.



Header checksum: IP is not a reliable protocol; it does not check whether the payload carried by a datagram is corrupted during the transmission. IP puts the burden of error checking of the payload on the protocol that owns the payload, such as UDP or TCP. The datagram header, however, is added by IP, and its error-checking is the responsibility of IP. Errors in the IP header can be a disaster. For example, if the destination IP address is corrupted, the packet can be delivered to the wrong host. If the protocol field is corrupted, the payload may be delivered to the wrong protocol. If the fields related to the fragmentation are corrupted, the datagram cannot be reassembled correctly at the destination, and so on. For these reasons, IP adds a header checksum field to check the header, but not the payload. We need to remember that, since the value of some fields, such as TTL, which are related to fragmentation and options, may change from router to router, the checksum needs to be recalculated at each router. Checksum in the Internet normally uses a 16-bit field, which is the complement of the sum of other fields calculated using 1s complement arithmetic.

Source and Destination Addresses: These 32-bit source and destination address fields define the IP address of the source and destination respectively. The source host should know its IP address. The destination IP address is either known by the protocol that uses the service of IP or is provided by the DNS. Note that the value of these fields must remain unchanged during the time the IP datagram travels from the source host to the destination host.

Options: A datagram header can have up to 40 bytes of options. Options can be used for network testing and debugging. Although options are not a required part of the IP header, option processing is required of the IP software. This means that all implementations must be able to handle options if they are present in the header. The existence of options in a header creates some burden on the datagram handling; some options can be changed by routers, which forces each router to recalculate the header checksum.

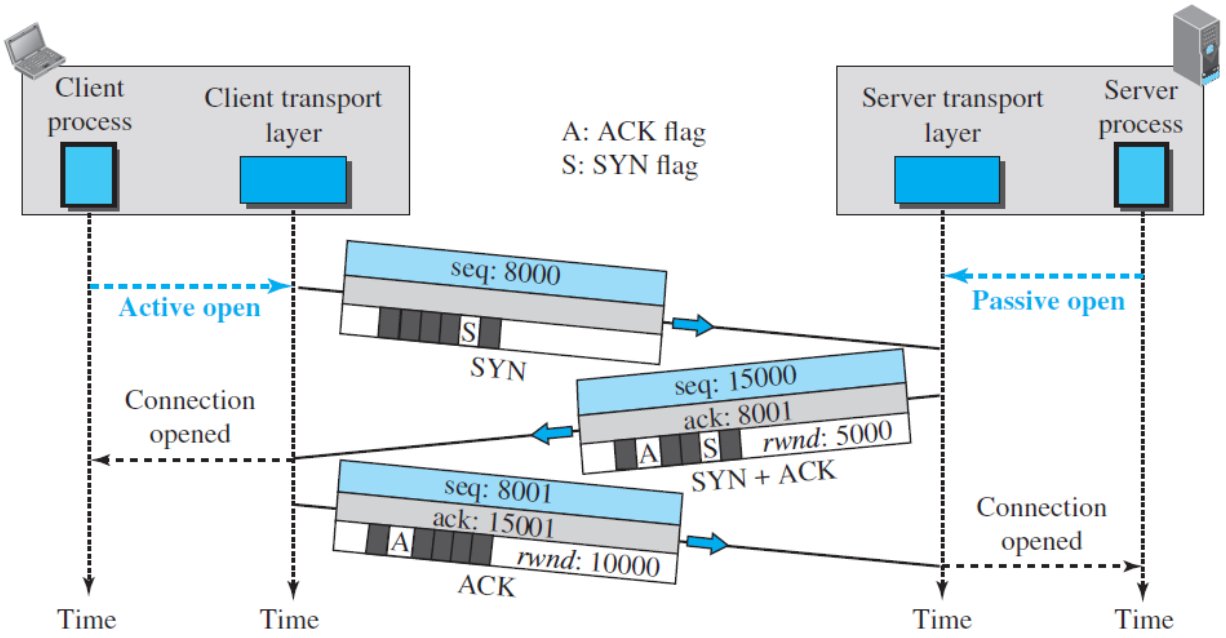
Payload: Payload, or data, is the main reason for creating a datagram. Payload is the packet coming from other protocols that use the service of IP. Comparing a datagram to a postal package, payload is the content of the package; the header is only the information written on the package.

Hyperlinks: These are links to different pages, which can be hosted on the same computer or some other computer.

Hyper Text Transfer Protocol: This is an application layer protocol. It follows on client-server request-response structure. Client sends a HTTP request to server and server responds with a HTTP response.

World Wide Web: WWW is nothing but a collection and connection of various files hosted across various computers across the world.

Three-way handshaking:



In this situation, the client TCP, after receiving a close command from the client process, sends the first segment, a FIN segment in which the FIN flag is set. Note that a FIN segment can include the last chunk of data sent by the client or it can be just a control segment as shown in the figure. If it is only a control segment, it consumes only one sequence number because it needs to be acknowledged.

The server TCP, after receiving the FIN segment, informs its process of the situation and sends the second segment, a FIN + ACK segment, to confirm the receipt of the FIN segment from the client and at the same time to announce the closing of the connection in the other direction. This segment can also contain the last chunk of data from the server. If it does not carry data, it consumes only one sequence number because it needs to be acknowledged.

The client TCP sends the last segment, an ACK segment, to confirm the receipt of the FIN segment from the TCP server. This segment contains the acknowledgment number, which is one plus the sequence number received in the FIN segment from the server. This segment cannot carry data and consumes no sequence numbers.

Routing Algorithms:

- In order to calculate which route is the best path towards the destination, a router needs to calculate a routing algorithm.
- Here's an analogy of roads to routing algorithms:
- Lets say you want to go from point A to point B.
- There is a road which is the shortest path, but contains lot of potholes and debris.
- There is a longer path which is well maintained and smooth.
- There may be paths which have toll booths with very high toll fee.
- These are some of the considerations you need to have when you plan a road trip.
- Same thing with routing as well.

  Router1 to Router2 to Router3

  1Mbps 64Kbps
- Important considerations for Routing algorithms:
- Number of HOPS.
- Bandwidth.
- Reliability of path.

Types of Routing Algorithms:

- Distance Vector Routing
- Link State Routing
- Path Vector Routing
- Routing Information Protocol (RIP)
- Open Shortest Path First (OSPF)
- Border Gateway Protocol (BGP)

Distance Vector Routing:

- Based on the Bellman–Ford algorithm and the Ford–Fulkerson algorithm, distance-vector routing protocols started to be implemented from 1969 onwards in data networks such as the ARPANET and CYCLADES.
- The term distance vector refers to the fact that the protocol manipulates vectors (arrays) of distances to other nodes in the network.
- The distance vector algorithm was the original ARPANET routing algorithm and was implemented more widely in local area networks with the Routing Information Protocol (RIP).
- This routing protocol is in convienent since it creates a lot of network traffic.
- Difficult to scale when number of routers is very high.
- Maintaining and updating distance vectors become tedious in huge networks.

Routing Information Protocol:

- Same as distance vector routing, but instead of distance it uses number of hops as routing metric.
- RIP prevents routing loops by implementing a limit on the number of hops allowed in a path from source to destination.
- The largest number of hops allowed for RIP is 15, which limits the size of networks that RIP can support.
- RIP implements the split horizon, route poisoning, and hold down mechanisms to prevent incorrect routing information from being propagated.
- In most networking environments, RIP is not the preferred choice of routing protocol, as its time to converge and scalability are poor compared to EIGRP, OSPF, or IS-IS.
- However, it is easy to configure, because RIP does not require any parameters, unlike other protocols.
- RIP uses the User Datagram Protocol (UDP) as its transport protocol, and is assigned the reserved port number 520.