Computer Networks

A computer network is number of computers (nodes) connected by some communication lines.
Two computers connected to the network can communicate with each other through nodes if they are not directly connected.
Some of the nodes in the network may not be computers at all but they are network devices (like switches routers etc) to facilitate communications.

Four characteristics for effective data communication

1. Delivery-System must deliver data to correct destination
2. Accuracy-deliver data without error and accurately
3. Timeliness-deliver data in time
4. Jitter-deviation from true periodicity of a periodic signal. It is undesired. Packet sent early reached early

Components of data communication

1. Message-Message is data or information to be communicated-text, image, audio, video etc.
2. Sender-is a device which sends message-computer, workstation, telephone handset, video camera
3. Receiver
4. Transmission medium- Physical medium by which message travels form sender to receiver-twisted cable, coaxial cable, fiber optic cable, radio waves
5. Protocol- set of rules that governs data communication

The basic networking criteria

1. Performance-can be measured in term of transmit time, response time, efficiency of the connected software and hardware
2. Reliability- It is measured by the frequency of failure, and network robustness in catastrophes. Mean time to repair-less , Mean time between failure-long
3. Security- Protecting data from unauthorized access, damage and development, and implementing policies and procedures for recovery from breaches and data losses.

Use of computer networks

1.Network for companies-Many organizations have substantial number of computers in operation often located apart-keep track of productivity, inventory and payroll. Worked in isolation. Management decided to connect them to correlate information about entire company. Resource Sharing – user happens to away 1000 km from data should not be prevented. Tyranny of geography.
2.High reliable- copies of data if unavailable due to hardware failure copies could be used.
3.Saving money- Small computers have much better price performance ratio than large one. Mainframes room size computers are roughly a factor of 10 faster than personal computers but they cost a thousand time more. This imbalance has caused many system designer to build system consisting of personal computers one per user with data kept on one or more shared file server machine. In this model user is called client whole arrangement is called client server model.
4.Scalability- the ability to increase system performance gradually as workload grows just by adding more processor.
5.Powerful communication medium among widely separated employees- they can write report together, one can change other and see the change. Increases cooperation
6.Networks for people
Access to remote information
Person to person communication
Interactive entertainment

7.Social issues-introduced new social, ethical and political problem. Trouble starts when newsgroups posts the topic people cares about like politics and religion. Views sometime become offensive to some people.

Mode of communication

Point to point-copper or fiber line

Dedicated-Simplex-mainframe to monitor only in certain direction, half duplex (Walkie Talkie) one direction at a time, full duplex-telephonic communication

Shared-Multiplexing –communication link is shared

Broadcasting – satellite

Dedicated – Channel level one way

Shared- Multiple access

Multicasting- Communicating to specific group

Classification

LAN- Privately owned, building, restricted in size, same policy. They are widely used to connect personal computers and workstations in company offices and factories to share resources such as printers and exchange information. LANS are distinguished from other kind of network by three characteristics- their size, their transmission technology and their topology. Transmission technology consisting of single cable to which all the machine are attached. Have low delay and make few errors. Bus and ring topology

MAN- Bigger version of LAN and uses similar technology. It might cover a group of nearby corporate office or a city and might be either private or public.

WAN- spans a large geographical area often a country or continent. It contains a collection of machine intended for running user application program. Contains numerous cables and telephone lines each one connecting a pair of routers. The host are connected to communication subnet.

Categories of topology

The term physical topology refers to the way in which a network is laid out physically

Topology- Mesh, Star, Bus, Ring, hybrid

Mesh- 5C2-10 links

Reference Model

OSI Reference Model- This model is based on the proposal developed by Internation Standard Organisation(ISO) as a first step towards international standardization of the protocol used in the various layers. The model is called the ISO OSI(Open System Interconnection) reference model because it deals with connecting open system- that is systems that are open for communication with other systems. The OSI model has 7 layers

1. The Application Layer-used by network application means computer applications that use internet for example Chrome, Firefox, Outlook, Skype. Web browser uses AL protocol HTTP and HTTPs for web surfing. Dozens of AL protocols like FTP, Telnet, DHCP, SMTP are basis for various network services like file transfer, email, virtual terminals etc .

2. The Presentation Layer- Receives data from application layer. Data in the form of characters and numbers. Convert it into machine understandable binary format for example ASCII to EBCDIC code. This function is called translation. Before transmission it reduces number of bits of data called data compression. This can be lossy or lossless, helps in real time video and audio streaming. To enhance integrity of data data is encrypted in this layer. Secure Socket layer protocol is used in PL for encryption and decryption.

3. The Session Layer- helps in setting up and managing connections(termination).Authentication and Authorization(You have permission of file)is done. Keep track of files that are downloaded. Helps in session management. Web browser performs all function of session, presentation and application layer.

4. The transport Layer-The basic function of the transport layer is to accept data from the session layer, split it up into smaller unit if need be, pass these to network layer and ensure that pieces arrived correctly at the other end. It controls the reliability of communication through segmentation, flow control and error control. In segmentation data received from session layer is divided into small data unit called segments. Each segment contains a source and destination port number and sequence number. Port number helps to direct each segment to correct application and sequence number reassemble segments in correct order to form correct message at the receiver. In flow control TL controls amount of data to be transmitted. Use Automatic Repeat Request in case of error. Checksum (group of bits) is added to segment to find out corrupted segment. Protocol of TL is TCP and UDP(User Datagram Protocol).Provides two types of services- connection oriented(done by TCP) and connectionless transmission(done by UDP). UDP is faster as it does not provide any feedback. Therefore lost data can be retransmitted in case of TCP. UDP is used where streaming is required – online movie songs etc. TCP-WWW, email, ftp etc.
5. The Network Layer-is concerned with controlling the operation of the subnet. The key design issue is how packets are routed from source to destination. If too many packets present in the subnet at the same time leads to congestion. The control of congestion also belongs to network layer. Some accounting function built into network layer. When packet crosses national border the accounting can become complicated. Network layer has to overcome problems related to heterogeneous network to be interconnected.
6. The Data Link Layer-Take a raw transmission facility and transform it into a line that appears free of undetected transmission errors to the network layer. It accomplishes the task by having the sender break the input data up into data frames (few hundred and few thousand bytes), transmit the frame sequentially and process the acknowledgement frames sent back by the receiver. Unlike physical layer it is DLL to create and recognize frame boundaries. This can be accomplished by attaching special bit patterns to the beginning and end of the frame. A noise burst on the line can destroy frames completely. In this case DLL software on the source machine can retransmit the frame. However multiple transmission can results in duplicate frame. A duplicate frame could be sent if acknowledge frame is lost. It is up to this layer to solve the problem caused by damaged, lost and duplicate frame. Another iissue is how to keep a fast transmitting from drowning a slow receiver in data. Therefore flow and and error control mechanism is there.
7. The Physical Layer-The physical layer is concerned with transmitting raw bits over a communication channel. It ensure when one side sends 1 bit it is received by other side as 1 bit not as 0 bit. The design issue largely deals with mechanical, electrical and procedural interfaces and physical transmission medium. (How many volts to represent 1 and 0, how many microseconds bit lasts, whether transmission may proceed simultaneously in both direction, how initial connection is establish)

Internet protocol suite

The **Internet protocol suite,** commonly known as **TCP/IP,** is the set of communications protocols used in the Internet and similar computer networks. The current foundational protocols in the suite are the Transmission Control Protocol (TCP) and the Internet Protocol (IP).

During its development, versions of it were known as the **Department of Defense** (**DoD**) **model** because the development of the networking method was funded by the United States Department of Defense through DARPA. Its implementation is a protocol stack.[1]

The Internet protocol suite provides end-to-end data communication specifying how data should be packetized, addressed, transmitted, routed, and received. This functionality is organized into four abstraction layers, which classify all related protocols according to each protocol's scope of networking.[2][3] From lowest to highest, the layers are the link layer, containing communication methods

for data that remains within a single network segment (link); the internet layer, providing internetworking between independent networks; the transport layer, handling host-to-host communication; and the application layer, providing process-to-process data exchange for applications.

The application layer is the scope within which applications, or processes, create user data and communicate this data to other applications on another or the same host. The applications make use of the services provided by the underlying lower layers, especially the transport layer which provides reliable or unreliable *pipes* to other processes. The communications partners are characterized by the application architecture, such as the client–server model and peer-to-peer networking. This is the layer in which all application protocols, such as SMTP, FTP, SSH, HTTP, operate. Processes are addressed via ports which essentially represent services.

The transport layer performs host-to-host communications on either the local network or remote networks separated by routers.[33] It provides a channel for the communication needs of applications. UDP is the basic transport layer protocol, providing an unreliable connectionless datagram service. The Transmission Control Protocol provides flow-control, connection establishment, and reliable transmission of data.

The internet layer exchanges datagrams across network boundaries. It provides a uniform networking interface that hides the actual topology (layout) of the underlying network connections. It is therefore also the layer that establishes internetworking. Indeed, it defines and establishes the Internet. This layer defines the addressing and routing structures used for the TCP/IP protocol suite. The primary protocol in this scope is the Internet Protocol, which defines IP addresses. Its function in routing is to transport datagrams to the next host, functioning as an IP router, that has the connectivity to a network closer to the final data destination.

The link layer defines the networking methods within the scope of the local network link on which hosts communicate without intervening routers. This layer includes the protocols used to describe the local network topology and the interfaces needed to affect the transmission of Internet layer datagrams to next-neighbor hosts. The link layer is used to move packets between the Internet layer interfaces of two different hosts on the same link. The processes of transmitting and receiving packets on the link can be controlled in the device driver for the network card, as well as in firmware or by specialized chipsets. These perform functions, such as framing, to prepare the Internet layer packets for transmission, and finally transmit the frames to the physical layer and over a transmission medium. The TCP/IP model includes specifications for translating the network addressing methods used in the Internet Protocol to link-layer addresses, such as media access control (MAC) addresses. All other aspects below that level, however, are implicitly assumed to exist, and are not explicitly defined in the TCP/IP model.

A **hub** is a network hardware device for connecting multiple Ethernet devices together and making them act as a single network segment. It has multiple input/output (I/O) ports, in which a signal introduced at the input of any port appears at the output of every port except the original incoming.[1] A hub works at the physical layer (layer 1) of the OSI model. Today, hubs are far less commonly deployed.

A **network switch** (also called **switching hub**, **bridging hub**, and, by the IEEE(, **MAC bridge**[1]) is networking hardware that connects devices on a computer network by using packet switching to receive and forward data to the destination device.

A network switch is a multiport network bridge that uses MAC addresses to forward data at the data link layer (layer 2) of the OSI model. Some switches can also forward data at the network layer (layer 3) by additionally incorporating routing functionality. Such switches are commonly known as layer-3 switches or multilayer switches.

A **router** is a device like a switch that routes data packets based on their IP addresses. The router is mainly a Network Layer device. Routers normally connect LANs and WANs together and have a

dynamically updating routing table based on which they make decisions on routing the data packets. Router divide broadcast domains of hosts connected through it.

A **gateway**, as the name suggests, is a passage to connect two networks together that may work upon different networking models. They basically work as the messenger agents that take data from one system, interpret it, and transfer it to another system. Gateways are also called protocol converters and can operate at any network layer. Gateways are generally more complex than switches or routers. Gateway is also called a protocol converter.

NIC or network interface card is a network adapter that is used to connect the computer to the network. It is installed in the computer to establish a LAN. It has a unique id that is written on the chip, and it has a connector to connect the cable to it. The cable acts as an interface between the computer and router or modem. NIC card is a layer 2 device which means that it works on both physical and data link layer of the network model.

A **bridge** operates at the data link layer. A bridge is a repeater, with add on the functionality of filtering content by reading the MAC addresses of source and destination. It is also used for interconnecting two LANs working on the same protocol. It has a single input and single output port, thus making it a 2 port device.

Transmission media

A physical medium in data communications is the transmission path over which a signal propagates. Many different types of transmission media are used as communications channel.

In many forms of communications, communication is in the form of electromagnetic waves. With **guided transmission media**, the waves are guided along a physical path; examples of guided media include **twisted pair cables, coaxial cables, and optical fibers**. **Unguided transmission media** are methods that allow the transmission of data without the use of physical means to define the path it takes. Examples of this include **microwave, radio or infrared**. Unguided media provide a means for transmitting electromagnetic waves but do not guide them; examples are propagation through air, vacuum and seawater.

The term direct link is used to refer to the transmission path between two devices in which signals propagate directly from transmitters to receivers with no intermediate devices, other than amplifiers or repeaters used to increase signal strength. This term can apply to both guided and unguided media.

Guided Media

Twisted pair

Twisted pair cabling is a type of wiring in which two conductors of a single circuit are twisted together for the purposes of improving electromagnetic compatibility. Compared to a single conductor or an untwisted balanced pair, a twisted pair reduces electromagnetic radiation from the pair and crosstalk between neighboring pairs and improves rejection of external electromagnetic interference. It was invented by Alexander Graham Bell.

For additional noise immunity, twisted-pair cabling may be shielded. Cable with shielding is known as shielded twisted pair (STP) and without as unshielded twisted pair (UTP). UTP is the most common cable used in computer networking. Modern Ethernet, the most common data networking standard, can use UTP cables, with increasing data rates requiring higher specification variants of the UTP cable.

Coaxial cable

Coaxial cable is a type of electrical cable that has an inner conductor surrounded by a tubular insulating layer, surrounded by a tubular conducting shield. Many coaxial cables also have an insulating outer sheath or jacket. The term coaxial comes from the inner conductor and the outer shield sharing a

geometric axis. Coaxial cable was invented by English physicist, engineer, and mathematician Oliver Heaviside, who patented the design in 1880.

Coaxial cable is a type of transmission line, used to carry high frequency electrical signals with low losses. It is used in such applications as telephone trunklines, broadband internet networking cables, high speed computer data busses, carrying cable television signals, and connecting radio transmitters and receivers to their antennas. It differs from other shielded cables because the dimensions of the cable and connectors are controlled to give a precise, constant conductor spacing, which is needed for it to function efficiently as a transmission line.

Optical fiber

Optical fiber, which has emerged as the most commonly used transmission medium for long-distance communications, is a thin strand of glass that guides light along its length. Four major factors favor optical fiber over copper: data rates, distance, installation, and costs. Optical fiber can carry huge amounts of data compared to copper. It can be run for hundreds of miles without the need for signal repeaters, in turn, reducing maintenance costs and improving the reliability of the communication system because repeaters are a common source of network failures. Glass is lighter than copper allowing for less need for specialized heavy-lifting equipment when installing long-distance optical fiber. Optical fiber for indoor applications cost approximately a dollar a foot, the same as copper.

Multimode and single mode are two types of commonly used optical fiber. Multimode fiber uses LEDs as the light source and can carry signals over shorter distances, about 2 kilometers. Single mode can carry signals over distances of tens of miles.

An optical fiber is a flexible, transparent fiber made by drawing glass (silica) or plastic to a diameter slightly thicker than that of a human hair. Optical fibers are used most often as a means to transmit light between the two ends of the fiber and find wide usage in fiber-optic communications, where they permit transmission over longer distances and at higher bandwidths (data rates) than electrical cables. Fibers are used instead of metal wires because signals travel along them with less loss; in addition, fibers are immune to electromagnetic interference, a problem from which metal wires suffer excessively. Fibers are also used for illumination and imaging, and are often wrapped in bundles so they may be used to carry light into, or images out of confined spaces, as in the case of a fiberscope. Specially designed fibers are also used for a variety of other applications, some of them being fiber optic sensors and fiber lasers.[8]

Optical fibers typically include a core surrounded by a transparent cladding material with a lower index of refraction. Light is kept in the core by the phenomenon of total internal reflection which causes the fiber to act as a waveguide. Fibers that support many propagation paths or transverse modes are called multi-mode fibers, while those that support a single mode are called single-mode fibers (SMF). Multi-mode fibers generally have a wider core diameter and are used for short-distance communication links and for applications where high power must be transmitted. Single-mode fibers are used for most communication links longer than 1,000 meters (3,300 ft).

Unguided Media

Radio Waves

Radio waves are the electromagnetic waves that are transmitted in all the directions of free space. Radio waves are omnidirectional, i.e., the signals are propagated in all the directions. The range in frequencies of radio waves is from 3Khz to 1 kHz. In the case of radio waves, the sending and receiving antenna are not aligned, i.e., the wave sent by the sending antenna can be received by any receiving antenna. An example of the radio wave is FM radio. A Radio wave is useful for multicasting when there is one sender and many receivers. An FM radio, television, cordless phones are examples of a radio wave. Radio transmission is mainly used for wide area networks and mobile cellular phones. Radio waves cover a large area, and they can penetrate the walls. Radio transmission provides a higher transmission rate.

Microwaves

Microwaves are of two types:
Terrestrial microwave

Satellite microwave communication.

Terrestrial Microwave Transmission

Terrestrial Microwave transmission is a technology that transmits the focused beam of a radio signal from one ground-based microwave transmission antenna to another.

Microwaves are the electromagnetic waves having the frequency in the range from 1GHz to 1000 GHz.

Microwaves are unidirectional as the sending and receiving antenna is to be aligned, i.e., the waves sent by the sending antenna are narrowly focussed.

In this case, antennas are mounted on the towers to send a beam to another antenna which is km away.

It works on the line of sight transmission, i.e., the antennas mounted on the towers are the direct sight of each other.

Characteristics of Microwave:

Frequency range: The frequency range of terrestrial microwave is from 4-6 GHz to 21-23 GHz.

Bandwidth: It supports the bandwidth from 1 to 10 Mbps.

Short distance: It is inexpensive for short distance.

Long distance: It is expensive as it requires a higher tower for a longer distance.

Attenuation: Attenuation means loss of signal. It is affected by environmental conditions and antenna size.

Advantages Of Microwave:

Microwave transmission is cheaper than using cables.

It is free from land acquisition as it does not require any land for the installation of cables.

Microwave transmission provides an easy communication in terrains as the installation of cable in terrain is quite a difficult task.

Communication over oceans can be achieved by using microwave transmission.

Disadvantages of Microwave transmission:

Eavesdropping: An eavesdropping creates insecure communication. Any malicious user can catch the signal in the air by using its own antenna.

Out of phase signal: A signal can be moved out of phase by using microwave transmission.

Susceptible to weather condition: A microwave transmission is susceptible to weather condition. This means that any environmental change such as rain, wind can distort the signal.

Bandwidth limited: Allocation of bandwidth is limited in the case of microwave transmission.

Satellite Microwave Communication

A satellite is a physical object that revolves around the earth at a known height.

Satellite communication is more reliable nowadays as it offers more flexibility than cable and fibre optic systems.

We can communicate with any point on the globe by using satellite communication.

How Does Satellite work?

The satellite accepts the signal that is transmitted from the earth station, and it amplifies the signal. The amplified signal is retransmitted to another earth station.

Advantages Of Satellite Microwave Communication:

The coverage area of a satellite microwave is more than the terrestrial microwave.

The transmission cost of the satellite is independent of the distance from the centre of the coverage area.

Satellite communication is used in mobile and wireless communication applications.

It is easy to install.

It is used in a wide variety of applications such as weather forecasting, radio/TV signal broadcasting, mobile communication, etc.

Disadvantages Of Satellite Microwave Communication:

Satellite designing and development requires more time and higher cost.

The Satellite needs to be monitored and controlled on regular periods so that it remains in orbit.

The life of the satellite is about 12-15 years. Due to this reason, another launch of the satellite has to be planned before it becomes non-functional.

Infrared

An infrared transmission is a wireless technology used for communication over short ranges.

The frequency of the infrared in the range from 300 GHz to 400 THz.
It is used for short-range communication such as data transfer between two cell phones, TV remote operation, data transfer between a computer and cell phone resides in the same closed area.
An infrared transmission is a wireless technology used for communication over short ranges.
The frequency of the infrared in the range from 300 GHz to 400 THz.
It is used for short-range communication such as data transfer between two cell phones, TV remote operation, data transfer between a computer and cell phone resides in the same closed area.

Transmission Impairments

Attenuation

It means loss of energy. The strength of signal decreases with increasing distance which causes loss of energy in overcoming resistance of medium. This is also known as attenuated signal. Amplifiers are used to amplify the attenuated signal which gives the original signal back and compensate for this loss.

Distortion

It means changes in the form or shape of the signal. This is generally seen in composite signals made up with different frequencies. Each frequency component has its own propagation speed travelling through a medium. And thats why it delay in arriving at the final destination Every component arrive at different time which leads to distortion. Therefore, they have different phases at receiver end from what they had at senders end.

Noise

The random or unwanted signal that mixes up with the original signal is called noise. There are several types of noise such as induced noise, crosstalk noise, thermal noise and impulse noise which may corrupt the signal.

Induced noise comes from sources such as motors and appliances. These devices act as sending antenna and transmission medium act as receiving antenna. Thermal noise is movement of electrons in wire which creates an extra signal. Crosstalk noise is when one wire affects the other wire. Impulse noise is a signal with high energy that comes from lightning or power lines

Modulation

In electronics and telecommunications, modulation is the process of varying one or more properties of a periodic waveform, called the carrier signal, with a separate signal called the modulation signal that typically contains information to be transmitted.

Modem

A modulator is a device or circuit that performs modulation. A demodulator (sometimes detector) is a circuit that performs demodulation, the inverse of modulation. A modem (from modulator–demodulator), used in bidirectional communication, can perform both operations.

Frequency modulation (FM) is the encoding of information in a carrier wave by varying the instantaneous frequency of the wave.

Amplitude modulation(AM) is a process by which the wave signal is transmitted by modulating the amplitude of the signal. It is often called AM and is commonly used in transmitting a piece of information through a radio carrier wave. Amplitude modulation is mostly used in the form of electronic communication.

Phase modulation (PM) is a modulation pattern for conditioning communication signals for transmission. It encodes a message signal as variations in the instantaneous phase of a carrier wave. Phase modulation is one of the two principal forms of **angle modulation,** together with frequency modulation.

Multiplexing

Multiplexing is the process of combining multiple signals into one signal, over a shared medium. The process is called as analog multiplexing if these signals are analog in nature.If digital signals are multiplexed, it is called as digital multiplexing.

Frequency-division multiplexing (FDM)

In telecommunications, frequency-division multiplexing (FDM) is a technique by which the total bandwidth available in a communication medium is divided into a series of non-

overlapping frequency bands, each of which is used to carry a separate signal. This allows a single transmission medium such as a cable or optical fiber to be shared by multiple independent signals. Another use is to carry separate serial bits or segments of a higher rate signal in parallel.The most common example of frequency-division multiplexing is radio and television broadcasting, in which multiple radio signals at different frequencies pass through the air at the same time. Another example is cable television, in which many television channels are carried simultaneously on a single cable. FDM is also used by telephone systems to transmit multiple telephone calls through high capacity trunklines, communications satellites to transmit multiple channels of data on uplink and downlink radio beams, and broadband DSL modems to transmit large amounts of computer data through twisted pair telephone lines, among many other uses.

Wavelength-division multiplexing (WDM)

In fiber-optic communications, wavelength-division multiplexing (WDM) is a technology which multiplexes a number of optical carrier signals onto a single optical fiber by using different wavelengths (i.e., colors) of laser light.This technique enables bidirectional communications over a single strand of fiber, also called wavelength-division duplexing, as well as multiplication of capacity.

Time-division multiplexing (TDM)

In TDM users take turns(in round robin) each can periodically taking entire bandwidth for a little burst of time. It can only used for digital data.

Circuit Switching and Packet Switching

Difference between Circuit Switching and Packet Switching	
Circuit Switching	Packet Switching
A circuit needs to be established to make sure that data transmission takes place. Dedicated	Each packet containing the information that needs to be processed goes through the dynamic route. Store and forward.
A uniform path is followed throughout the session.	There is no uniform path that is followed end to end through the session.
It is most ideal for voice communication, while also keeping the delay uniform.	It is used mainly for data transmission as the delay is not uniform.
Without a connection, it cannot exist, as the connection needs to be present on a physical layer.	A connection is not necessary, as it can exist without one too. It needs to be present on a network layer.
Data to be transmitted is processed at the source itself.	Data is processed and transmitted at the source as well as at each switching station.

Unit II

Data Link Layer: Error Detection and Error Correction: Types of errors, LRC, VRC, Checksum, CRC, and Hamming Code. Flow Control and Error Control: Stop and Wait Protocol, Sliding Window, Go-back-N-ARQ Protocol and Selective-Repeat ARQ Protocol. Channel Allocation Protocols: Random Access, Controlled and Channelization techniques such as ALOHA, CSMA, CSMA/CD, CDMA/CA, TDMA, FDMA, Token Passing, etc.

Vertical Redundancy Check (VRC)

Vertical Redundancy Check is the error detection method which is used by upper layers to detect error in data. The other name for VRC is Parity Check. A redundant bit which is also named as parity bit is added to each data unit. This method includes even parity and odd parity. When the total number of 1s in data is even that there is even parity and when the total number of 1s in data is to be odd that indicates there is odd parity in data.

Longitudinal Redundancy Check (LRC)

Longitudinal Redundancy Check (LRC) is the error detection method which is used by upper layers to detect error in data. The other name for VRC is 2-D parity check. In this method, data which the user want to send is organized into tables of rows and columns. To detect an error, a redundant bit is added to the whole block after addition this block is transmitted to receiver side. This redundant bit is used by receiver to detect error. If there is no error, receiver accepts the data and discards the redundant row of bits.

Checksum

In checksum error detection scheme, the data is divided into k segments each of m bits.
In the sender's end the segments are added using 1's complement arithmetic to get the sum. The sum is complemented to get the checksum.
The checksum segment is sent along with the data segments.
At the receiver's end, all received segments are added using 1's complement arithmetic to get the sum. The sum is complemented.
If the result is zero, the received data is accepted; otherwise discarded.

Cyclic redundancy check (CRC)

Unlike checksum scheme, which is based on addition, CRC is based on binary division.
In CRC, a sequence of redundant bits, called cyclic redundancy check bits, are appended to the end of data unit so that the resulting data unit becomes exactly divisible by a second, predetermined binary number.
At the destination, the incoming data unit is divided by the same number. If at this step there is no remainder, the data unit is assumed to be correct and is therefore accepted.
A remainder indicates that the data unit has been damaged in transit and therefore must be rejected.

Hamming Code

Hamming code is a block code that is capable of detecting up to two simultaneous bit errors and correcting single-bit errors. It was developed by R.W. Hamming for error correction.
In this coding method, the source encodes the message by inserting redundant bits within the message. These redundant bits are extra bits that are generated and inserted at specific positions

in the message itself to enable error detection and correction. When the destination receives this message, it performs recalculations to detect errors and find the bit position that has error.

Stop-and-wait ARQ

Stop-and-wait ARQ also referred to as alternating bit protocol, is a method in telecommunications to send information between two connected devices. It ensures that information is not lost due to dropped packets and that packets are received in the correct order. It is the simplest automatic repeat-request (ARQ) mechanism. A stop-and-wait ARQ sender sends one frame at a time; it is a special case of the general sliding window protocol with transmit and receive window sizes equal to one in both cases. After sending each frame, the sender doesn't send any further frames until it receives an acknowledgement (ACK) signal. After receiving a valid frame, the receiver sends an ACK. If the ACK does not reach the sender before a certain time, known as the timeout, the sender sends the same frame again. The timeout countdown is reset after each frame transmission. The above behavior is a basic example of Stop-and-Wait. However, real-life implementations vary to address certain issues of design.
Typically the transmitter adds a redundancy check number to the end of each frame. The receiver uses the redundancy check number to check for possible damage. If the receiver sees that the frame is good, it sends an ACK. If the receiver sees that the frame is damaged, the receiver discards it and does not send an ACK—pretending that the frame was completely lost, not merely damaged.
One problem is when the ACK sent by the receiver is damaged or lost. In this case, the sender doesn't receive the ACK, times out, and sends the frame again. Now the receiver has two copies of the same frame, and doesn't know if the second one is a duplicate frame or the next frame of the sequence carrying identical DATA.
Another problem is when the transmission medium has such a long latency that the sender's timeout runs out before the frame reaches the receiver. In this case the sender resends the same packet. Eventually the receiver gets two copies of the same frame, and sends an ACK for each one. The sender, waiting for a single ACK, receives two ACKs, which may cause problems if it assumes that the second ACK is for the next frame in the sequence.
To avoid these problems, the most common solution is to define a 1 bit sequence number in the header of the frame. This sequence number alternates (from 0 to 1) in subsequent frames. When the receiver sends an ACK, it includes the sequence number of the next packet it expects. This way, the receiver can detect duplicated frames by checking if the frame sequence numbers alternate. If two subsequent frames have the same sequence number, they are duplicates, and the second frame is discarded. Similarly, if two subsequent ACKs reference the same sequence number, they are acknowledging the same frame.
Stop-and-wait ARQ is inefficient compared to other ARQs, because the time between packets, if the ACK and the data are received successfully, is twice the transit time (assuming the turnaround time can be zero). The throughput on the channel is a fraction of what it could be. To solve this problem, one can send more than one packet at a time with a larger sequence number and use one ACK for a set. This is what is done in Go-Back-N ARQ and the Selective Repeat ARQ.

Sliding window protocol

Sliding window protocol is a feature of packet-based data transmission protocols. Sliding window protocols are used where reliable in-order delivery of packets is required, such as in the

data link layer (OSI layer 2) as well as in the Transmission Control Protocol (TCP). They are also used to improve efficiency when the channel may include high latency.
Packet-based systems are based on the idea of sending a batch of data, the packet, along with additional data that allows the receiver to ensure it was received correctly, perhaps a checksum. The paradigm is similar to a window sliding sideways to allow entry of fresh packets and reject the ones that have already been acknowledged. When the receiver verifies the data, it sends an acknowledgment signal, or "ACK", back to the sender to indicate it can send the next packet. In a simple automatic repeat request protocol (ARQ), the sender stops after every packet and waits for the receiver to ACK. This ensures packets arrive in the correct order, as only one may be sent at a time.
The time that it takes for the ACK signal to be received may represent a significant amount of time compared to the time needed to send the packet. In this case, the overall throughput may be much lower than theoretically possible. To address this, sliding window protocols allow a selected number of packets, the window, to be sent without having to wait for an ACK. Each packet receives a sequence number, and the ACKs send back that number. The protocol keeps track of which packets have been ACKed, and when they are received, sends more packets. In this way, the window slides along the stream of packets making up the transfer.
Sliding windows are a key part of many protocols. It is a key part of the TCP protocol, which inherently allows packets to arrive out of order, and is also found in many file transfer protocols like UUCP-g and ZMODEM as a way of improving efficiency compared to non-windowed protocols like XMODEM.

Go-Back-N ARQ
Go-Back-N ARQ is a specific instance of the automatic repeat request (ARQ) protocol, in which the sending process continues to send a number of frames specified by a window size even without receiving an acknowledgement (ACK) packet from the receiver. It is a special case of the general sliding window protocol with the transmit window size of N and receive window size of 1. It can transmit N frames to the peer before requiring an ACK.
The receiver process keeps track of the sequence number of the next frame it expects to receive. It will discard any frame that does not have the exact sequence number it expects (either a duplicate frame it already acknowledged, or an out-of-order frame it expects to receive later) and will send an ACK for the last correct in-order frame.[1] Once the sender has sent all of the frames in its window, it will detect that all of the frames since the first lost frame are outstanding, and will go back to the sequence number of the last ACK it received from the receiver process and fill its window starting with that frame and continue the process over again.
Go-Back-N ARQ is a more efficient use of a connection than Stop-and-wait ARQ, since unlike waiting for an acknowledgement for each packet, the connection is still being utilized as packets are being sent. In other words, during the time that would otherwise be spent waiting, more packets are being sent. However, this method also results in sending frames multiple times – if any frame was lost or damaged, or the ACK acknowledging them was lost or damaged, then that frame and all following frames in the send window (even if they were received without error) will be re-sent. To avoid this, Selective Repeat ARQ can be used.

Selective Repeat ARQ
Selective Repeat is part of the automatic repeat request (ARQ). With selective repeat, the sender sends a number of frames specified by a window size even without the need to wait for

individual ACK from the receiver as in Go-Back-N ARQ. The receiver may selectively reject a single frame, which may be retransmitted alone; this contrasts with other forms of ARQ, which must send every frame from that point again. The receiver accepts out-of-order frames and buffers them. The sender individually retransmits frames that have timed out.

Channel Allocation Protocol

ALOHA is a multiple access protocol for transmission of data via a shared network channel. It operates in the medium access control sublayer (MAC sublayer) of the open systems interconnection (OSI) model. Using this protocol, several data streams originating from multiple nodes are transferred through a multi-point transmission channel.
In ALOHA, each node or station transmits a frame without trying to detect whether the transmission channel is idle or busy. If the channel is idle, then the frames will be successfully transmitted. If two frames attempt to occupy the channel simultaneously, collision of frames will occur and the frames will be discarded. These stations may choose to retransmit the corrupted frames repeatedly until successful transmission occurs.
Versions of ALOHA Protocols
Pure ALOHA
In pure ALOHA, the time of transmission is continuous.Whenever a station hasan available frame, it sends the frame. If there is collision and the frame is destroyed, the sender waits for a random amount of time before retransmitting it.
Slotted ALOHA
Slotted ALOHA reduces the number of collisions and doubles the capacity of pure ALOHA. The shared channel is divided into a number of discrete time intervals called slots. A station can transmit only at the beginning of each slot. However,there can still be collisions if more than one station tries to transmit at the beginning of the same time slot.

Carrier-sense multiple access (CSMA)
Carrier-sense multiple access (CSMA) is a media access control (MAC) protocol in which a node verifies the absence of other traffic before transmitting on a shared transmission medium, such as an electrical bus or a band of the electromagnetic spectrum.
Under CSMA, a transmitter uses a carrier-sense mechanism to determine whether another transmission is in progress before initiating a transmission. That is, it tries to detect the presence of a carrier signal from another node before attempting to transmit. If a carrier is sensed, the node waits for the transmission in progress to end before initiating its own transmission. Using CSMA, multiple nodes may, in turn, send and receive on the same medium. Transmissions by one node are generally received by all other nodes connected to the medium.

Carrier-sense multiple access with collision avoidance (CSMA/CA)
Carrier-sense multiple access with collision avoidance (CSMA/CA) in computer networking, is a network multiple access method in which carrier sensing is used, but nodes attempt to avoid collisions by beginning transmission only after the channel is sensed to be "idle".When they do transmit, nodes transmit their packet data in its entirety.

It is particularly important for wireless networks, where the collision detection of the alternative CSMA/CD is not possible due to wireless transmitters desensing their receivers during packet transmission.
CSMA/CA is unreliable due to the hidden node problem.
CSMA/CA is a protocol that operates in the Data Link Layer (Layer 2) of the OSI model.

Carrier-sense multiple access with collision detection (CSMA/CD)
Carrier-sense multiple access with collision detection (CSMA/CD) is a media access control (MAC) method used most notably in early Ethernet technology for local area networking. It uses carrier-sensing to defer transmissions until no other stations are transmitting. This is used in combination with collision detection in which a transmitting station detects collisions by sensing transmissions from other stations while it is transmitting a frame. When this collision condition is detected, the station stops transmitting that frame, transmits a jam signal, and then waits for a random time interval before trying to resend the frame.
CSMA/CD is a modification of pure carrier-sense multiple access (CSMA). CSMA/CD is used to improve CSMA performance by terminating transmission as soon as a collision is detected, thus shortening the time required before a retry can be attempted.

Time-division multiple access (TDMA)
Time-division multiple access (TDMA) is a channel access method for shared-medium networks. It allows several users to share the same frequency channel by dividing the signal into different time slots.[1] The users transmit in rapid succession, one after the other, each using its own time slot. This allows multiple stations to share the same transmission medium (e.g. radio frequency channel) while using only a part of its channel capacity. Dynamic TDMA is a TDMA variant that dynamically reserves a variable number of time slots in each frame to variable bit-rate data streams, based on the traffic demand of each data stream.

Frequency-division multiple access (FDMA)
Frequency-division multiple access (FDMA) is a channel access method used in some multiple-access protocols. FDMA allows multiple users to send data through a single communication channel, such as a coaxial cable or microwave beam, by dividing the bandwidth of the channel into separate non-overlapping frequency sub-channels and allocating each sub-channel to a separate user. Users can send data through a sub channel by modulating it on a carrier wave at the subchannel's frequency. It is used in satellite communication systems and telephone trunk lines.
FDMA splits the total bandwidth into multiple channels. Each ground station on the earth is allocated a particular frequency group (or a range of frequencies). Within each group, the ground station can allocate different frequencies to individual channels, which are used by different stations connected to that ground station. Before the transmission begins, the transmitting ground station looks for an empty channel within the frequency range that is allocated to it and once it finds an empty channel, it allocates it to the particular transmitting station.

Token Passing
On a local area network, token passing is a channel access method where a packet called a token is passed between nodes to authorize that node to communicate. In contrast to polling access

methods, there is no pre-defined "master" node.[4] The most well-known examples are IBM Token Ring and ARCNET, but there were a range of others, including FDDI (Fiber Distributed Data Interface), which was popular in the early to mid 1990s.

Token passing schemes degrade deterministically under load, which is a key reason why they were popular for industrial control LANs such as MAP, (Manufacturing Automation Protocol).[5] The advantage over contention based channel access (such as the CSMA/CD of early Ethernet), is that collisions are eliminated, and that the channel bandwidth can be fully utilized without idle time when demand is heavy.The disadvantage is that even when demand is light, a station wishing to transmit must wait for the token, increasing latency.

Some types of token passing schemes do not need to explicitly send a token between systems because the process of "passing the token" is implicit. An example is the channel access method used during "Contention Free Time Slots" in the ITU-T G.hn standard for high-speed local area networking using existing home wires (power lines, phone lines and coaxial cable).

Unit III

Network Layer: Switching Techniques: Circuit Switching, Packet Switching, and Message Switching. Logical addressing: IPv4 and IPv6 Address schemes, Classes and subnetting Network Layer Protocols: ARP, RARP, BOOTP and DHCP Routing Techniques: Interdomain and Intradomain routing with examples.

Switching techniques

In large networks, there can be multiple paths from sender to receiver. The switching technique will decide the best route for data transmission.
Switching technique is used to connect the systems for making one-to-one communication.

Circuit switching

Circuit switching is a switching technique that establishes a dedicated path between sender and receiver.
In the Circuit Switching Technique, once the connection is established then the dedicated path will remain to exist until the connection is terminated.
Circuit switching in a network operates in a similar way as the telephone works.
A complete end-to-end path must exist before the communication takes place.
In case of circuit switching technique, when any user wants to send the data, voice, video, a request signal is sent to the receiver then the receiver sends back the acknowledgment to ensure the availability of the dedicated path. After receiving the acknowledgment, dedicated path transfers the data.
Circuit switching is used in public telephone network. It is used for voice transmission.
Fixed data can be transferred at a time in circuit switching technology.

Message Switching

Message Switching is a switching technique in which a message is transferred as a complete unit and routed through intermediate nodes at which it is stored and forwarded.
In Message Switching technique, there is no establishment of a dedicated path between the sender and receiver.
The destination address is appended to the message. Message Switching provides a dynamic routing as the message is routed through the intermediate nodes based on the information available in the message.
Message switches are programmed in such a way so that they can provide the most efficient routes.
Each and every node stores the entire message and then forward it to the next node. This type of network is known as store and forward network.
Message switching treats each message as an independent entity.

The packet switching

The packet switching is a switching technique in which the message is sent in one go, but it is divided into smaller pieces, and they are sent individually.
The message splits into smaller pieces known as packets and packets are given a unique number to identify their order at the receiving end.
Every packet contains some information in its headers such as source address, destination address and sequence number.

Packets will travel across the network, taking the shortest path as possible.
All the packets are reassembled at the receiving end in correct order.
If any packet is missing or corrupted, then the message will be sent to resend the message.
If the correct order of the packets is reached, then the acknowledgment message will be sent.

Logical addressing: IPv4 and IPv6 Address schemes
Go through the following website for this topic
https://www.javatpoint.com/ipv4-vs-ipv6https://www.javatpoint.com/ipv4-vs-ipv6

The Address Resolution Protocol (ARP)
The Address Resolution Protocol (ARP) is a communication protocol used for discovering the link layer address, such as a MAC address, associated with a given internet layer address, typically an IPv4 address. This mapping is a critical function in the Internet protocol suite.
Operating scope Edit
The Address Resolution Protocol is a request-response protocol whose messages are encapsulated by a link layer protocol. It is communicated within the boundaries of a single network, never routed across internetworking nodes. This property places ARP into the link layer of the Internet protocol suite.[2]
Packet structure
The Address Resolution Protocol uses a simple message format containing one address resolution request or response. The size of the ARP message depends on the link layer and network layer address sizes. The message header specifies the types of network in use at each layer as well as the size of addresses of each. The message header is completed with the operation code for request (1) and reply (2). The payload of the packet consists of four addresses, the hardware and protocol address of the sender and receiver hosts.

The Reverse Address Resolution Protocol (RARP)
The Reverse Address Resolution Protocol (RARP) is an obsolete computer communication protocol used by a client computer to request its Internet Protocol (IPv4) address from a computer network, when all it has available is its link layer or hardware address, such as a MAC address. The client broadcasts the request and does not need prior knowledge of the network topology or the identities of servers capable of fulfilling its request.
RARP requires one or more server hosts to maintain a database of mappings of Link Layer addresses to their respective protocol addresses. Media Access Control (MAC) addresses need to be individually configured on the servers by an administrator. RARP is limited to serving only IP addresses.

The Bootstrap Protocol (BOOTP)
The Bootstrap Protocol (BOOTP) is a computer networking protocol used in Internet Protocol networks to automatically assign an IP address to network devices from a configuration server. The BOOTP was originally defined in RFC 951.
When a network-connected computer boots-up, its IP-stack broadcasts BOOTP network-messages requesting an IP-address assignment. A BOOTP configuration-server replies to the request by assigning an IP address from a pool of addresses, which is preconfigured by an administrator.

BOOTP is implemented using the User Datagram Protocol (UDP) for transport protocol, port number 67 is used by the (DHCP) server for receiving client-requests and port number 68 is used by the client for receiving (DHCP) server responses. BOOTP operates only on IPv4 networks. Historically, BOOTP has also been used for Unix-like diskless workstations to obtain the network location of their boot image, in addition to the IP address assignment. Enterprises used it to roll out a pre-configured client (e.g., Windows) installation to newly installed PCs.
Initially requiring the use of a boot floppy disk to establish the initial network connection, manufacturers of network cards later embedded the protocol in the BIOS of the interface cards as well as system boards with on-board network adapters, thus allowing direct network booting. While some parts of BOOTP have been effectively superseded by the Dynamic Host Configuration Protocol (DHCP), which adds the feature of leases, parts of BOOTP are used to provide service to the DHCP protocol. DHCP servers also provide the legacy BOOTP functionality.

The Dynamic Host Configuration Protocol (DHCP)
The Dynamic Host Configuration Protocol (DHCP) is a network management protocol used on Internet Protocol (IP) networks for automatically assigning IP addresses and other communication parameters to devices connected to the network using a client–server architecture.
The technology eliminates the need for individually configuring network devices manually, and consists of two network components, a centrally installed network DHCP server and client instances of the protocol stack on each computer or device. When connected to the network, and periodically thereafter, a client requests a set of parameters from the DHCP server using the DHCP protocol.
DHCP can be implemented on networks ranging in size from residential networks to large campus networks and regional ISP networks.[2] Many routers and residential gateways have DHCP server capability. Most residential network routers receive a unique IP address within the ISP network. Within a local network, a DHCP server assigns a local IP address to each device. DHCP services exist for networks running Internet Protocol version 4 (IPv4), as well as version 6 (IPv6). The IPv6 version of the DHCP protocol is commonly called DHCPv6.

Intra-domain routing

Routing within an AS(Autonomous System).
Ignores the internet outside the autonomous system.
Protocols for intra domain routing are also called interior gateway protocols.
Popular protocols are RIP(Routing Information Protocol)ams OSPF(Open Shortest Path First).

Inter-domain routing

Routing between AS's.
Assumes that the internet consists of a collection of interconnected AS's.
Protocol for inter domain routing are also called exterior gateway protocols.
routing protocols are BGP(Border Gateway Protocol)

Unit IV

Reliable and unreliable Connection, Port and Socket Addressing Transport Layer Protocols with packet formats: User Datagram Protocol (UDP), Transmission Control Protocol (TCP), Stream Control Transmission Protocol (SCTP). Congestion Control: Techniques for handling the Congestion Control. Quality of Service (QoS): Flow Characteristics and techniques to improve QoS.

Transport Layer

In computer networking, the transport layer is a conceptual division of methods in the layered architecture of protocols in the network stack in the Internet protocol suite and the OSI model. The protocols of this layer provide host-to-host communication services for applications. It provides services such as connection-oriented communication, reliability, flow control, and multiplexing.

Transport layer services are conveyed to an application via a programming interface to the transport layer protocols. The services may include the following features:

Connection-oriented communication

Connection-oriented communication: It is normally easier for an application to interpret a connection as a data stream rather than having to deal with the underlying connection-less models, such as the datagram model of the User Datagram Protocol (UDP) and of the Internet Protocol (IP).

Same order delivery: The network layer doesn't generally guarantee that packets of data will arrive in the same order that they were sent, but often this is a desirable feature. This is usually done through the use of segment numbering, with the receiver passing them to the application in order. This can cause …

The Transmission Control Protocol (TCP) is one of the main protocols of the Internet protocol suite. It originated in the initial network implementation in which it complemented the Internet Protocol (IP). Therefore, the entire suite is commonly referred to as TCP/IP. TCP provides reliable, ordered, and error-checked delivery of a stream of octets (bytes) between applications running on hosts communicating via an IP network. Major internet applications such as the World Wide Web, email, remote administration, and file transfer rely on TCP, which is part of the Transport Layer of the TCP/IP suite. SSL/TLS often runs on top of TCP.

TCP is connection-oriented, and a connection between client and server is established before data can be sent. The server must be listening (passive open) for connection requests from clients before a connection is established. Three-way handshake (active open), retransmission, and error-detection adds to reliability but lengthens latency. Applications that do not require reliable data stream service may use the User Datagram Protocol (UDP), which provides a connectionless datagram service that prioritizes time over reliability. TCP employs network congestion avoidance. However, there are vulnerabilities to TCP including denial of service, connection hijacking, TCP veto, and reset attack.

User Datagram Protocol (UDP)

In computer networking, the User Datagram Protocol (UDP) is one of the core members of the Internet protocol suite. With UDP, computer applications can send messages, in this case referred to as datagrams, to other hosts on an Internet Protocol (IP) network. Prior communications are not required in order to set up communication channels or data paths.

UDP uses a simple connectionless communication model with a minimum of protocol mechanisms. UDP provides checksums for data integrity, and port numbers for addressing different functions at the source and destination of the datagram. It has no handshaking dialogues, and thus exposes the user's program to any unreliability of the underlying network; there is no guarantee of delivery, ordering, or duplicate protection. If error-correction facilities are needed at the network interface level, an application may use Transmission Control Protocol (TCP) or Stream Control Transmission Protocol (SCTP) which are designed for this purpose. UDP is suitable for purposes where error checking and correction are either not necessary or are performed in the application; UDP avoids the overhead of such processing in the protocol stack. Time-sensitive applications often use UDP because dropping packets is preferable to waiting for packets delayed due to retransmission, which may not be an option in a real-time system.

The Stream Control Transmission Protocol (SCTP)

The Stream Control Transmission Protocol (SCTP) is a computer networking communications protocol in the transport layer of the Internet protocol suite. Originally intended for Signaling System 7 (SS7) message transport in telecommunication, the protocol provides the message-oriented feature of the User Datagram Protocol (UDP), while ensuring reliable, in-sequence transport of messages with congestion control like the Transmission Control Protocol (TCP). Unlike UDP and TCP, the protocol supports multihoming and redundant paths to increase resilience and reliability.

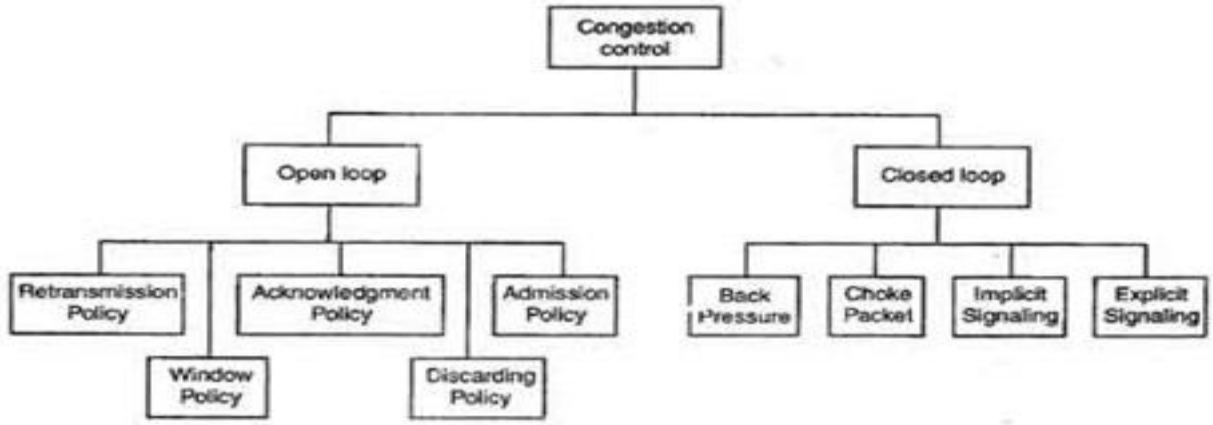
Quality of service (QoS)

Quality of service (QoS) is the description or measurement of the overall performance of a service, such as a telephony or computer network or a cloud computing service, particularly the performance seen by the users of the network. To quantitatively measure quality of service, several related aspects of the network service are often considered, such as packet loss, bit rate, throughput, transmission delay, availability, jitter, etc.

In the field of computer networking and other packet-switched telecommunication networks, quality of service refers to traffic prioritization and resource reservation control mechanisms rather than the achieved service quality. Quality of service is the ability to provide different priorities to different applications, users, or data flows, or to guarantee a certain level of performance to a data flow.

Quality of service is particularly important for the transport of traffic with special requirements. In particular, developers have introduced Voice over IP technology to allow computer networks to become as useful as telephone networks for audio conversations, as well as supporting new applications with even stricter network performance requirements.

Congestion Control: Techniques for handling the Congestion Control



Types of Congestion Control Methods

Congestion in a network may occur when the load on the network (i.e. the number of packets sent to the network) is greater than the capacity of the network (i.e. the number of packets a network can handle.)

• The various causes of congestion in a subnet are:

i. The input traffic rate exceeds the capacity of the output lines.

ii. The routers are too slow to perform bookkeeping tasks (queuing buffers, updating tables, etc.).

iii. The routers' buffer is too limited.

iv. Congestion in a subnet can occur if the processors are slow. Slow speed CPU at routers will perform the routine tasks such as queuing buffers, updating table etc slowly.

• Congestion Control refers to techniques and mechanisms that can either prevent congestion, before it happens, or remove congestion, after it has happened. Congestion control mechanisms are divided into two categories, one category prevents the congestion from happening and the other category removes congestion after it has taken place.

• These two categories are:

1. Open loop
2. Closed loop

• Open Loop Congestion Control

i. In this method, policies are used to prevent the congestion before it happens.

ii. Congestion control is handled either by the source or by the destination. The various methods used for open loop congestion control are:

1) Retransmission Policy

a. The sender retransmits a packet, if it feels that the packet it has sent is lost or corrupted.

b. However retransmission in general may increase the congestion in the network. But we need to implement good retransmission policy to prevent congestion.

c. The retransmission policy and the retransmission timers need to be designed to optimize efficiency and at the same time prevent the congestion.

2) Window Policy

a. To implement window policy, selective reject window method is used for congestion control.

b. Selective Reject method is preferred over Go-back-n window as in Go-back-n method, when timer for a packet times out, several packets are resent, although some may have arrived safely at the receiver. Thus, this duplication may make congestion worse.
c. Selective reject method sends only the specific lost or damaged packets.

3) Acknowledgement Policy

a. The acknowledgement policy imposed by the receiver may also affect congestion.
b. If the receiver does not acknowledge every packet it receives it may slow down the sender and help prevent congestion.
c. Acknowledgments also add to the traffic load on the network. Thus, by sending fewer acknowledgements we can reduce load on the network.
d. To implement it, several approaches can be used:

- A receiver may send an acknowledgement only if it has a packet to be sent.
- A receiver may send an acknowledgement when a timer expires.
- A receiver may also decide to acknowledge only N packets at a time.

4) Discarding Policy

a. A router may discard less sensitive packets when congestion is likely to happen.
b. Such a discarding policy may prevent congestion and at the same time may not harm the integrity of the transmission.

5) Admission Policy

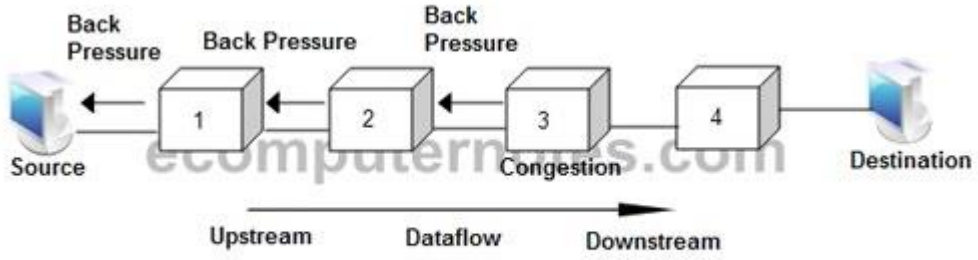
a. An admission policy, which is a quality-of-service mechanism, can also prevent congestion in virtual circuit networks.
b. Switches in a flow first check the resource requirement of a flow before admitting it to the network.
c. A router can deny establishing a virtual circuit connection if there is congestion in the "network or if there is a possibility of future congestion.

• Closed Loop Congestion Control

Closed loop congestion control mechanisms try to remove the congestion after it happens.The various methods used for closed loop congestion control are:

i. Backpressure

a. Backpressure is a node-to-node congestion control that starts with a node and propagates, in the opposite direction of data flow.



Backpressure Method

b. The backpressure technique can be applied only to virtual circuit networks. In such virtual circuit each node knows the upstream node from which a data flow is coming.
c. In this method of congestion control, the congested node stops receiving data from the immediate upstream node or nodes.
d. This may cause the upstream node on nodes to become congested, and they, in turn, reject data from their upstream node or nodes.

e. As shown in fig node 3 is congested and it stops receiving packets and informs its upstream node 2 to slow down. Node 2 in turns may be congested and informs node 1 to slow down. Now node 1 may create congestion and informs the source node to slow down. In this way the congestion is alleviated. Thus, the pressure on node 3 is moved backward to the source to remove the congestion.

ii. Choke Packet a. In this method of congestion control, congested router or node sends a special type of packet called choke packet to the source to inform it about the congestion.

b. Here, congested node does not inform its upstream node about the congestion as in backpressure method.

c. In choke packet method, congested node sends a warning directly to the source station i.e. the intermediate nodes through which the packet has traveled are not warned.

iii. Implicit Signaling

a. In implicit signaling, there is no communication between the congested node or nodes and the source.

b. The source guesses that there is congestion somewhere in the network when it does not receive any acknowledgment. Therefore the delay in receiving an acknowledgment is interpreted as congestion in the network.

c. On sensing this congestion, the source slows down.

d. This type of congestion control policy is used by TCP.

iv. Explicit Signaling

a. In this method, the congested nodes explicitly send a signal to the source or destination to inform about the congestion.

b. Explicit signaling is different from the choke packet method. In choke packed method, a separate packet is used for this purpose whereas in explicit signaling method, the signal is included in the packets that carry data .

c. Explicit signaling can occur in either the forward direction or the backward direction .

d. In backward signaling, a bit is set in a packet moving in the direction opposite to the congestion. This bit warns the source about the congestion and informs the source to slow down.

e. In forward signaling, a bit is set in a packet moving in the direction of congestion. This bit warns the destination about the congestion. The receiver in this case uses policies such as slowing down the acknowledgements to remove the congestion.

Unit V

Application Layer: Basic Concept of Application Layer: Domain Name System, World Wide Web, Hyper Text Transfer Protocol, Electronic mail, File Transfer Protocol, Remote login. Introduction to Cryptography: Definition, Goal, Applications, Attacks, Encryption, decryption, public-key and private key cryptography.

Application layer

An application layer is an abstraction layer that specifies the shared communications protocols and interface methods used by hosts in a communications network. An application layer abstraction is specified in both the Internet Protocol Suite (TCP/IP) and the OSI model. Although both models use the same term for their respective highest-level layer, the detailed definitions and purposes are different.

In the Internet protocol suite, the application layer contains the communications protocols and interface methods used in process-to-process communications across an Internet Protocol (IP) computer network. The application layer only standardizes communication and depends upon the underlying transport layer protocols to establish host-to-host data transfer channels and manage the data exchange in a client–server or peer-to-peer networking model.

Domain Name System

The Domain Name System (DNS) is the hierarchical and decentralized naming system used to identify computers, services, and other resources reachable through the internet or other internet protocol networks. The resource records contained in the DNS associate domain names with other forms of information. These are most commonly used to map human-friendly domain names to the numerical IP addresses computers need to locate services and devices using the underlying network protocols, but have been extended over time to perform many other functions as well. The Domain Name System has been an essential component of the functionality of the Internet since 1985.

An often-used analogy to explain the Domain Name System is that it serves as the phone book for the Internet by translating human-friendly computer hostnames into IP addresses. For example, the domain name www.example.com translates to the addresses 93.184.216.34 (IPv4) and 2606:2800:220:1:248:1893:25c8:1946 (IPv6). The DNS can be quickly and transparently updated, allowing a service's location on the network to change without affecting the end users, who continue to use the same hostname. Users take advantage of this when they use meaningful Uniform Resource Locators (URLs) and e-mail addresses without having to know how the computer actually locates the services.An important and ubiquitous function of the DNS is its central role in distributed Internet services such as cloud services and content delivery networks. When a user accesses a distributed Internet service using a URL, the domain name of the URL is translated to the IP address of a server that is proximal to the user. The key functionality of the DNS exploited here is that different users can simultaneously receive different translations for the same domain name, a key point of divergence from a traditional phone-book view of the DNS. This process of using the DNS to assign proximal servers to users is key to providing faster and more reliable responses on the Internet and is widely used by most major Internet services.

World Wide Web

The World Wide Web (WWW), commonly known as the Web, is an information system where documents and other web resources are identified by Uniform Resource Locators (URLs, such as https://example.com/), which may be interlinked by hyperlinks, and are accessible over the Internet. The resources of the Web are transferred via the Hypertext Transfer Protocol (HTTP), may be accessed by users by a software application called a web browser, and are published by a software application called a web server. The World Wide Web is not synonymous with the Internet, which pre-dated the Web in some form by over two decades and upon the technologies of which the Web is built.

English scientist Tim Berners-Lee co-invented the World Wide Web in 1989 along with Robert Cailliau. He wrote the first web browser in 1990 while employed at CERN near Geneva, Switzerland. The browser was released outside CERN to other research institutions starting in January 1991, and then to the general public in August 1991. The Web began to enter everyday use in 1993–1994, when websites for general use started to become available. The World Wide Web has been central to the development of the Information Age and is the primary tool billions of people use to interact on the Internet.

Web resources may be any type of downloaded media, but web pages are hypertext documents formatted in Hypertext Markup Language (HTML).[] Special HTML syntax displays embedded hyperlinks with URLs, which permits users to navigate to other web resources. In addition to text, web pages may contain references to images, video, audio, and software components, which are either displayed or internally executed in the user's web browser to render pages or streams of multimedia content.

Multiple web resources with a common theme and usually a common domain name make up a website. Websites are stored in computers that are running a web server, which is a program that responds to requests made over the Internet from web browsers running on a user's computer. Website content can be provided by a publisher or interactively from user-generated content. Websites are provided for a myriad of informative, entertainment, commercial, and governmental reasons.

Hypertext Transfer Protocol

The Hypertext Transfer Protocol (HTTP) is an application layer protocol in the Internet protocol suite model for distributed, collaborative, hypermedia information systems. HTTP is the foundation of data communication for the World Wide Web, where hypertext documents include hyperlinks to other resources that the user can easily access, for example by a mouse click or by tapping the screen in a web browser.

Development of HTTP was initiated by Tim Berners-Lee at CERN in 1989 and summarized in a simple document describing the behavior of a client and a server using the first HTTP protocol version that was named 0.9.

That first version of HTTP protocol soon evolved into a more elaborated version that was the first draft toward a far future version 1.0.

HTTP functions as a request–response protocol in the client–server model. A web browser, for example, may be the client and a process, named web server, running on a computer hosting one or more websites may be the server. The client submits an HTTP request message to the server. The server, which provides resources such as HTML files and other content or performs other functions on behalf of the client, returns a response message to the client. The response contains

completion status information about the request and may also contain requested content in its message body.
A web browser is an example of a user agent (UA). Other types of user agent include the indexing software used by search providers (web crawlers), voice browsers, mobile apps, and other software that accesses, consumes, or displays web content.

Electronic Mail
Electronic Mail (e-mail) is one of most widely used services of Internet. This service allows an Internet user to send a message in formatted manner (mail) to the other Internet user in any part of world. Message in mail not only contain text, but it also contains images, audio and videos data. The person who is sending mail is called sender and person who receives mail is called recipient. It is just like postal mail service.
Components of E-Mail System :
The basic components of an email system are : User Agent (UA), Message Transfer Agent (MTA), Mail Box, and Spool file. These are explained as following below.

1. User Agent (UA) :
   The UA is normally a program which is used to send and receive mail. Sometimes, it is called as mail reader. It accepts variety of commands for composing, receiving and replying to messages as well as for manipulation of the mailboxes.
2. Message Transfer Agent (MTA) :
   MTA is actually responsible for transfer of mail from one system to another. To send a mail, a system must have client MTA and system MTA. It transfer mail to mailboxes of recipients if they are connected in the same machine. It delivers mail to peer MTA if destination mailbox is in another machine. The delivery from one MTA to another MTA is done by Simple Mail Transfer Protocol.
3. Mailbox :
   It is a file on local hard drive to collect mails. Delivered mails are present in this file. The user can read it delete it according to his/her requirement. To use e-mail system each user must have a mailbox . Access to mailbox is only to owner of mailbox.
4. Spool file :
   This file contains mails that are to be sent. User agent appends outgoing mails in this file using SMTP. MTA extracts pending mail from spool file for their delivery. E-mail allows one name, an alias, to represent several different e-mail addresses. It is known as mailing list, Whenever user have to sent a message, system checks recipients's name against alias database. If mailing list is present for defined alias, separate messages, one for each entry in the list, must be prepared and handed to MTA. If for defined alias, there is no such mailing list is present, name itself becomes naming address and a single message is delivered to mail transfer entity.

Services provided by E-mail system:

- Composition –
  The composition refer to process that creates messages and answers. For composition any kind of text editor can be used.
- Transfer –
  Transfer means sending procedure of mail i.e. from the sender to recipient.

- Reporting –
  Reporting refers to confirmation for delivery of mail. It help user to check whether their mail is delivered, lost or rejected.
- Displaying –
  It refers to present mail in form that is understand by the user.
- Disposition –
  This step concern with recipient that what will recipient do after receiving mail i.e save mail, delete before reading or delete after reading.

File Transfer Protocol

The File Transfer Protocol (FTP) is a standard communication protocol used for the transfer of computer files from a server to a client on a computer network. FTP is built on a client–server model architecture using separate control and data connections between the client and the server. FTP users may authenticate themselves with a clear-text sign-in protocol, normally in the form of a username and password, but can connect anonymously if the server is configured to allow it. For secure transmission that protects the username and password, and encrypts the content, FTP is often secured with SSL/TLS (FTPS) or replaced with SSH File Transfer Protocol (SFTP). The first FTP client applications were command-line programs developed before operating systems had graphical user interfaces, and are still shipped with most Windows, Unix, and Linux operating systems. Many FTP clients and automation utilities have since been developed for desktops, servers, mobile devices, and hardware, and FTP has been incorporated into productivity applications, such as HTML editors.

Remote Login

Remote Login **is** a process in which user can login into remote site i.e. computer and use services that are available on the remote computer. With the help of remote login a user is able to understand result of transferring result of processing from the remote computer to the local computer.
It is implemented using Telnet.

Procedure of Remote Login

1. When the user types something on local computer, then local operating system accepts character.
2. Local computer does not interpret the characters, it will send them to TELNET client.
3. TELNET client transforms these characters to a universal character set called Network Virtual Terminal (NVT) characters and it will pass them to the local TCP/IP protocol Stack.
4. Commands or text which is in the form of NVT, travel through Internet and it will arrive at the TCP/IP stack at remote computer.
5. Characters are then delivered to operating system and which later on passed to TELNET server.
6. Then TELNET server changes that characters to characters which can be understandable by remote computer.
7. Remote operating system receives character from a pseudo-terminal driver, which is a piece of software that pretends that characters are coming from a terminal.
8. Operating system then passes character to the appropriate application program.

Cryptography

Cryptography is the practice and study of techniques for secure communication in the presence of adversarial behavior.[] More generally, cryptography is about constructing and analyzing protocols that prevent third parties or the public from reading private messages; various aspects in information security such as data confidentiality, data integrity, authentication, and non-repudiation are central to modern cryptography. Modern cryptography exists at the intersection of the disciplines of mathematics, computer science, electrical engineering, communication science, and physics. Applications of cryptography include electronic commerce, chip-based payment cards, digital currencies, computer passwords, and military communications.

Cryptography prior to the modern age was effectively synonymous with **encryption,** converting information from a readable state to unintelligible nonsense. The sender of an encrypted message shares the decoding technique only with intended recipients to preclude access from adversaries. The cryptography literature often uses the names Alice ("A") for the sender, Bob ("B") for the intended recipient, and Eve ("eavesdropper") for the adversary.[5] Since the development of rotor cipher machines in World War I and the advent of computers in World War II, cryptography methods have become increasingly complex and its applications more varied.

Cryptography referred almost exclusively to **encryption**, which is the process of converting ordinary information (called **plaintext**) into unintelligible form (called **ciphertext**). **Decryption** is the reverse, in other words, moving from the unintelligible ciphertext back to plaintext.
A *cipher* (or *cypher*) is a pair of algorithms that carry out the encryption and the reversing decryption. The detailed operation of a cipher is controlled both by the algorithm and, in each instance, by a "key". The key is a secret (ideally known only to the communicants), usually a string of characters (ideally short so it can be remembered by the user), which is needed to decrypt the ciphertext.
Historically, ciphers were often used directly for encryption or decryption without additional procedures such as authentication or integrity checks. There are, generally, two kinds of cryptosystems: **symmetric and asymmetric**. In symmetric systems, the only ones known until the 1970s, the same key (the **secret key**) is used to encrypt and decrypt a message. Data manipulation in symmetric systems is faster than asymmetric systems in part because they generally use shorter key lengths. Asymmetric systems use a "**public key**" to encrypt a message and a related "private key" to decrypt it. The use of asymmetric systems enhances the security of communication, largely because the relation between the two keys is very hard to discover. Examples of asymmetric systems include **RSA (Rivest–Shamir–Adleman), and ECC (Elliptic Curve Cryptography)**.