

Don't believe blindly on these most questions.
It is just prediction based!

(USE MY NOTES FOR ANSWER) INTRODUCTORY CONCEPT

PREVIOUS YEARS QUESTIONS

PART-A

Q.1 What is physical address? [R.T.U. 2019]

Ans. Physical Address : In computing, physical address refers to a memory address or the location of a memory cell in the main memory. It is used by both hardware and software for accessing data. Software, however, does not use physical addresses directly; instead, it accesses memory using a virtual address. A hardware component known as the memory management unit (MMU) is responsible for translating a virtual address to a physical address.

In networking, physical address refers to a computer's MAC address, which is a unique identifier associated with a network adapter that is used for identifying a computer in a network.

In computing, a physical address (also real address or binary address) is a memory address that is represented in the form of a binary number on the address bus circuitry in order to enable the data bus to access a particular storage cell of main memory or a register of memory mapped I/O device.

Q.2 Write any two differences between UDP and TCP.

[R.T.U. 2019]

Ans. Transmission Control Protocol (TCP) : TCP is a reliable connection-oriented protocol that allows a byte stream originating on one machine to be delivered without

errors on any other machine in the internet. It fragments the incoming byte stream into discrete message and passes each one to the internet layer. At the destination, the receiving TCP process reassembles the received messages into the output stream. TCP also handles flow control to make sure a fast sender cannot swap a slow receiver with more messages than it can handle.

User Datagram Protocol (UDP) : UDP is an unreliable, connectionless protocol for application that do not want TCP's sequencing or flow control and wish to provide their own. It is also widely used for one-shot client-server type, request-reply queries and applications in which prompt delivery is more important than accurate delivery, such as transmitting speech or video. The relation of IP, TCP and UDP is shown in fig.

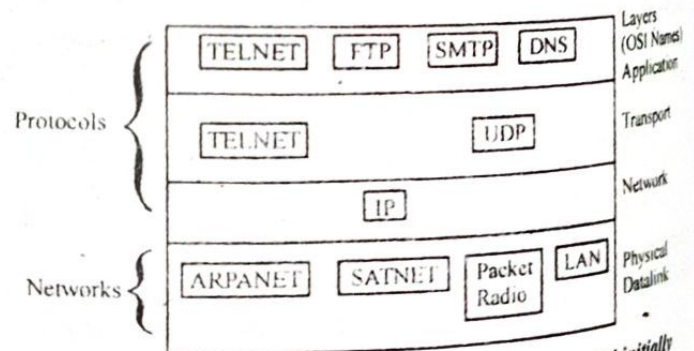


Fig. : Protocols and networks in the TCP/IP model initially

Q.3 Define framing and the reason for its need. [R.T.U. 2019]

Ans. Framing : The data link layer divides the stream of bits received from the network layer into manageable data units called frames.

DDCN, 4

(2) Polar NRZ and RZ

For polar RZ format

If symbol '1' is transmitted then

$$x(t) = \begin{cases} +A/2 & \text{for } 0 \leq t < T_b/2 \\ 0 & \text{for } T_b/2 \leq t < T_b \end{cases}$$

and

If symbol '0' is transmitted, then

$$x(t) = \begin{cases} -A/2 & \text{for } 0 \leq t < T_b/2 \\ 0 & \text{for } T_b/2 \leq t < T_b \end{cases}$$

For Polar NRZ

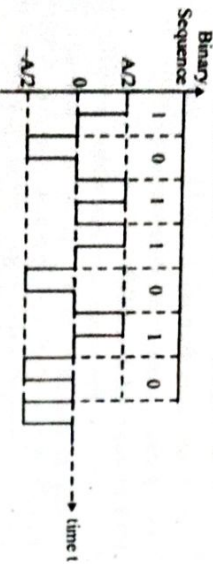
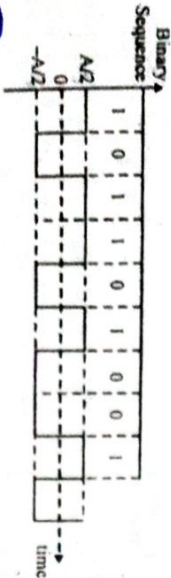


Fig. : Polar RZ Format

If symbol '1' is transmitted, then

$$x(t) = \begin{cases} -A/2 & \text{for } 0 \leq t < T_b \end{cases}$$



Q.12 Explain TCP/IP model with suitable diagram.

[R.T.U. 2019]

Ans. TCP/IP Model : TCP/IP protocol suit, used in the internet, was developed prior to OSI model. Therefore, the layers in the Transmission Control Protocol/Internet-working Protocol (TCP/IP) do not match exactly with those of OSI model.

TCP/IP is a hierarchical protocol made up of interactive modules, each of which provides a specific functionality, but they are not necessarily interdependent.

Application
Transport
Network
Data Link
Physical

B.Tech. (IV Sem.) C.S. Solved Papers

1. Internet Layer : Its job is to permit hosts to inject packets into any network and have them travel independently to the destination (potentially on a different network). They may arrive in a different order than they were sent, in which case it is the job of higher layers to rearrange them, if in order delivery is desired.

The internet layer defines an official packets format and protocol called IP (Internet Protocol). The job of the internet is to deliver IP packets where they are supposed to go. TCP/IP Internet layer is similar in functionality to the OSI network layer.

2. Transport Layer : The layer above the internet layer is transport layer. It is designed to allow peer entities on the source and destination hosts to carry on a conversation, just as in transport layer of OSI.

Two end to end transport protocols are defined here

- **Transmission Control Protocol (TCP) :** Refer to Q.2.

- **User Datagram Protocol (UDP) :** Refer to Q.2.

3. Application Layer : On the top of transport layer is the application layer. It contains higher level protocols:

TELNET : Telnet is an abbreviation for Terminating Network. TELNET enables the establishment of a connection to remote system in such a way that the local terminal appears to be a terminal at the remote system. TELNET is a general purpose client-server application program.

FTP : File Transfer Protocol is the standard mechanism provided by TCP/IP for copying files from one host to another.

SMTP : Simple Mail Transfer Protocol. It is a system for sending messages to other computer users based on e-mail addresses. SMTP provides for message exchange between users on the same or different computer.

DNS : Domain Name System is used for mapping host names.

4. Network Interface Layer : As its name suggests, this layer represents the place where the actual TCP/IP protocols running at higher layers interface to the local network. This layer is somewhat "controversial" in that some people don't even consider it a "legitimate" part of TCP/IP. This is usually because none of the core protocols run at this layer. Despite this, the network interface layer is part of the architecture. It is equivalent to the data link layer (layer two) of the OSI Reference Model.

Data Communication and Computer Networks

On many TCP/IP networks, there is no TCP/IP protocol running at all on this because it is simply not needed. For example, if we run TCP/IP over an Ethernet, then Ethernet handles layer two (and layer one) functions. However, the TCP/IP standards do define protocols for TCP/IP networks that do not have their own layer two implementation. These protocols, the Serial Line Internet Protocol (SLIP) and the Point-to-Point Protocol (PPP), serve to fill the gap between the network layer and the physical layer. They are commonly used to facilitate TCP/IP over direct serial line connections (such as dial-up telephone networking) and other technologies that operate directly at the physical layer.

Data Link Layer Services

- Unacknowledged connectionless service :
- No acks, no connection
- Error recovery up to higher layers
- For lower-rate links or vice traffic
- Acknowledge connectionless service :
- Acks improve reliability
- For unreliable channels. E.g.: Wireless Systems
- Acknowledge connection-oriented service :
- Equivalent of reliable bit-stream
- Connection establishment
- Packets delivered In-Order
- Connection Release
- In-L-R-Router Traffic

Transport Layer services : Refer to Q.10.

Q.13 Differentiate between Analog and Digital transmission.

[R.T.U. 2017]

Ans. Difference between Analog and Digital Transmission : Analog transmission is a method of conveying voice, data, image, signal, or video information.

It uses a continuous signal varying in amplitude, phase, or another property that is in proportion to a specific characteristic of a variable. Analog transmission could mean that the transmission is a transfer of an analog source signal which uses an analog modulation method (or a variance of one or more properties of high frequency and AM are examples of such a modulation). FM transmission could also use no modulation at all. It is most notably an information signal that is constantly varying. Data transmission (also known as digital transmission or digital communications) is a literal transmission of media, or storage is often represented as a microwave) discretely. These of pulses via a line also be represented always vary. E.g. digital modulated Analog transmission has a no fewer than cable, through a water. There are transmission. T (or AM). This is and works by signal in relative second is known type of communication wave, just : communicatio signal.

Q.14 (a) The

Data that be digital me (a computer c t unsmitted da call or a video into a bit stre or even mor coding of the

(b) A

(c) E

Ans.(a) The

power is a l expression:

The

network. The router is usually located within the layers of a network that determine the path for the transfer of data with the router acting as a processing unit for information packets. The router duplicates information packets for use during transmission from one network to another. The router uses a specific protocol or set of rules to determine which information packets are to be routed to certain interfaces within the network. Different types of routers perform different functions depending upon the requirements of the network system.

Network Interface Card : Network interface cards are used to connect each computer to the network so they can communicate with the network router to receive information packets. The interface cards determine the infrastructure of a local area network (LAN) and allow all of the computers to connect to the network. There are many different types of network interface cards that perform different functions within the network which include Ethernet cards and wireless network interface cards.

Network Switches : Network switches work similar to routers because they both copy information from one area of the network to the other. However, network switches contain multiple ports for copying frames of information from one port to the other. Like routers, switches operate within the layers of a network and evaluate every frame before determining the port in which the frame should be copied. Network switches are more sophisticated than their predecessor the network hub, which copied all frames to all ports instead of determining individual destinations. This required more bandwidth than what is required with network switches.

Network Bridge : A network bridge divides traffic on a local area network by separating the LAN into several different segments. It is also responsible for filtering data by determining the data destination or discarding unnecessary data. Network bridges operate within the layers of the network and also control the data that crosses the boundaries from one local area network to the other.

PART-C

Q.16 Explain any two functions of each layer in the OSI model. [R.T.U. 2019]

Ans. OSI/ISO Model : Refer to Q.4.

1. Physical Layer : The physical layer coordinates the functions required to transmit a bit stream over a physical medium.

- **Line Configuration :** The physical layer is concerned with the connection of device to the medium. In a multipoint configuration a link is shared between several devices. In a point to point configuration, two devices are connected together through a dedicated link.
- **Interface and Media :** Physical layer defines the type of transmission medium. It defines the characteristics of the interface between the devices and transmission media.
- **Bit Representation :** Physical layer data consists of a stream of bits without any interpretation. Before encoding bits must be encoded into signals, optical or electrical. The physical layer defines the encoding.
- **Transmission Rate :** Physical layer defines the duration of bit, which is how long it lasts and the number of bits sent each second is also defined by the physical layer.
- **Transmission Mode :** Physical layer defines the direction and mode of transmission between two devices : full duplex, half duplex or simplex.
- **Network Topology :** Physical layer also defines devices which are connected to each other to make network. Possible topologies are star, bus, ring, tree and mesh.

2. Data Link Layer : The data link layer transforms the physical layer, a raw transmission facility to a reliable link and is responsible for node to node delivery.

Basic features of data link layer are the following :

- **Framing :** Refer to Q.3.
- **Physical Addressing :** If frames are to be distributed to different systems on the network, the data link layer adds a header to the frame to define the physical address of the sender and/or receiver of the frame.
- **Flow Control :** If the rate at which the data are absorbed by the receiver is less than the rate of data produced in the sender, the data link layer imposes a flow control mechanism to prevent overwhelming the receiver.
- **Error Control :** Data link layer adds reliability to the physical layer by adding mechanisms to detect and retransmit damaged or lost frames. It also uses a mechanism to prevent duplication of frames. Error control is normally achieved through a trailer added to the end of frame.

Q.18 What are lossless and lossy channels? Also explain transmission impairments in detail.

DCCN. 9

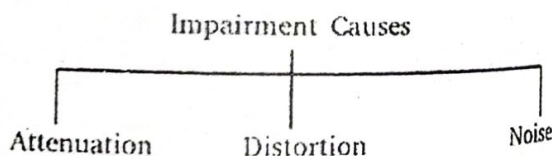
(R.T.U. 2017)

Ans. Lossless and Lossy Channels : The Lossless channel is capable of reconstituting the original form of the data. The quality of the data is not compromised. This type of channel allows a signal to restore its original form. This type of channel is used for transmitting texts.

The Lossy channel eliminates some amount of data that is not noticeable. This technique does not allow a signal to restore in its original form but significantly reduces the size. The lossy channel is beneficial if the quality of the signal is not your priority. It slightly degrades the quality of the data but is convenient when one wants to send or store the data. This type of channel is used for organic data like audio signals and images.

Transmission Impairments : In communication system, analog signals travel through transmission media, which tends to deteriorate the quality of analog signal. This imperfection causes signal impairment. This means that received signal is not same as the signal that was send.

Causes of impairment



(a) 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.

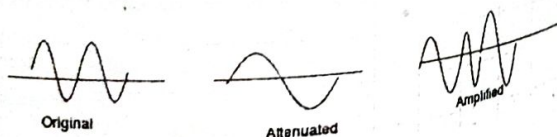


Fig.

Attenuation is measured in decibels (dB). It measures the relative strengths of two signals or one signal at two different point.

DCCN. 10

Attenuation (dB) = $10 \log_{10} (P_2/P_1)$
where, P_1 is power at sending end and P_2 is power at receiving end.

(b) Distortion : It means change in the shape of signal. This is generally seen in composite signals with different frequencies. Each frequency component has its own propagation speed travelling through a medium. Every component arrive at different time which leads to delay distortion. Therefore, they have different phases at receiver end from what they had at senders end.

(c) 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.

(i) Thermal Noise: The thermal noise is due to thermal agitation of electrons in a conductor. It is distributed across the entire spectrum and that is why it is also known as white noise (as the frequency encompass over a broad range of frequencies).

(ii) Intermodulation Noise: When more than one signal share a single transmission medium, intermodulation noise is generated. For example, two signals f_1 and f_2 will generate signals of frequencies $(f_1 + f_2)$ and $(f_1 - f_2)$, which may interfere with the signals of the same frequencies sent by the transmitter. Intermodulation noise is introduced due to nonlinearity present in any part of the communication system.

(iii) Cross Talk: Cross talk is a result of bunching several conductors together in a single cable. Signal carrying wires generate electromagnetic radiation, which is induced on other conductors because of close proximity of the conductors. While using telephone, it is a common experience to hear conversation of other people in the background. This is known as cross talk.

(iv) Impulse Noise: Impulse noise is irregular pulses or noise spikes of short duration generated by phenomena like lightning, spark due to loose contact in electric circuits, etc. Impulse noise is a primary source of bit-errors in digital data communication. This kind of noise introduces burst errors.

Q.19 (a) Explain Modulation and Demodulation.

(b) Calculate the following: (i) Signal-to-Noise Ratio (SNR) (ii) Noise Power Spectral Density (NPSD)

Ans. (a) Layer 1 to Q.4 and Q.5 Significance of Modulation and Demodulation

- It prevents the signal from being lost to other layers.
- It describes the modulation technique used in the communication system.
- Dividing the signal into components and transmitting them separately.
- Standardizing the modulation technique.
- It allows the use of software for modulation and demodulation.
- Dividing the signal into components and transmitting them separately.

Significance of Modulation and Demodulation

There are several languages and less ambiguous languages are easier to understand. It is a close analogy to the level of language implementation. It is an easier task to implement an ASCII string machine to process data from the above mentioned the alternative.

$$\log_2 \left\{ \left(1 + \frac{S}{N} \right)^{1/2} \right\}$$

rem we can say that, for a highest practical sampling an make independent gnal will be

re can therefore conclude ansmmission rate, C, will be

$$\left\{ \left(1 + \frac{S}{N} \right)^{1/2} \right\}$$

$$\left\{ 1 + \frac{S}{N} \right\}$$

nts the maximum possible n through a given channel e can transmit information ginal level, and the noise he channel's information

is
1 + SNR)

$$\log_2 (1 + 10^{2.4}) \text{ bps}$$

< 8 bps
ps
it or signaling level

$$C^b = \sqrt{(1 + \text{SNR})}$$

$$5.852^b = 4.104$$

Q.24 What are the various transmission media?
Explain guided media in detail. [R.T.U. 2013]

Ans. Transmission Media: Transmission media is the physical path between transmitter and receiver in a data transmission system. Transmission media can be classified as guided or unguided. In both cases communication is in the form of electromagnetic waves. With guided media, the waves are guided along a solid medium, such as copper twisted pair, copper coaxial cable and optical fiber. The atmosphere and other space are examples of unguided media that provide a means of transmitting electromagnetic signals but do not guide them this form of transmission is usually referred to as wireless transmission.

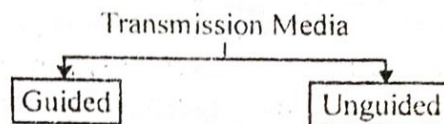


Fig.

Guided Media: A signal travelling along guided media is directed and contained by the physical limits of the medium. The transmission capacity in terms of bandwidth on data rate depends on material of media used and whether medium is point to point or multipoint.

Different categories of guided media are

- Twisted pair cable
- Coaxial cable
- Fiber optic cable

Table : Point to point transmission characteristics of guided media

Transmission medium rate	Total data Spacing	Bandwidth	Repeater
Twisted Pair	4 Mbps	3 MHz	2 to 10 Km
Coaxial Cable	500 Mbps	350 MHz	1 to 10 Km
Optical Fiber	2 Gbps	2 GHz	10 to 100 Km

Twisted Pair Cable: Twisted pair cable comes in two forms: unshielded and shielded

1. Unshielded Twisted Pair (UTP) Cables: UTP cable is the most common type of telecommunication medium used today. Its frequency range is suitable for transmitting both data and voice. A twisted pairs consists of two conductors (usually copper), each with its own coloured plastic insulation. The plastic insulation is colour banded for identification as shown in fig. Colours are used both to identify the specific conductors in a cable and to indicate which wires belong in pairs and how they relate to other pairs in a larger bundle.



Fig : Twisted pair cable

Two parallel flat wires were used for communication. However electromagnetic interference from devices such as a motor can create noise over those wires. If the two wires are parallel, the wire nearest to the source of the noise gets more interference and ends up with a higher voltage level than the wire further away, which results in an uneven load and a damaged signal as shown in fig.

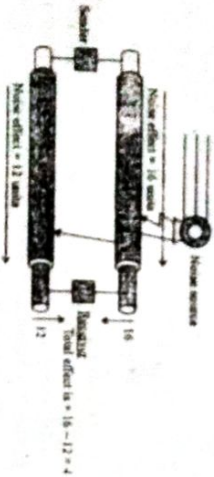


Fig : Effect of noise on two parallel flat wires

2. Shielded Twisted Pair (STP) Cable: STP cable has a metal foil or braided mesh covering that encases each pair of insulated conductors as shown in fig. The metal casing prevents the penetration of electromagnetic noise. It also can eliminate crosstalk.

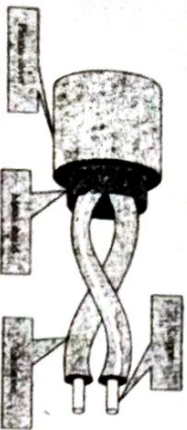


Fig : Shielded twisted pair

STP has the same quality considerations and uses the same connections as UTP, but the shield must be connected in a ground. Materials and manufacturing requirements make STP more expensive than UTP but less susceptible to noise.

Coaxial Cable: High frequency electrical current flows in the outer skin of a conductor, making twisted pair and multicore cables inefficient. This skin effect in metal conductors increases attenuation with the square root of frequency. A coaxial cable surrounds the inner conductor

with a dielectric, such as poly ethylene and a coaxial tube of solid or braided metal surrounds the dielectric. Coaxial cable like twisted pair, consists of two conductors, but is constructed differently to permit it to operate over a wider range of frequencies. It consists of a hollow outer cylindrical conductor that surrounds a single inner wire conductor as shown in fig.

The inner conductor is held in place by either regularly spaced insulating rings or a solid dielectric material. The outer conductor is covered with a jacket or shield. A single coaxial cable has a diameter of from 0.4 to about 1 inch because of its shielded, concentric construction, coaxial cable is much less susceptible to interference and crosstalk than twisted pair. Coaxial cable be used over longer distances and supports more stations on a shared line than twisted pair.

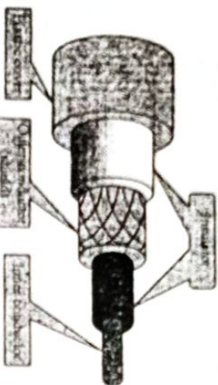


Fig : Coaxial cable

Applications: Coaxial cable is the most versatile transmission medium and is enjoying widespread use in a wide variety of applications. The most important of these are :

- Television distribution.
- Long distance telephone transmission.
- Short run computer system links.
- Local area networks.

Coaxial cable is spreading rapidly as means of distributing TV signals to individual home cable TV. From its modest beginnings as Community Antenna Television (CATV), designed to provide service to remote area, cable TV will eventually reach almost as many homes and offices as the telephone. A cable TV system can carry dozens or even hundreds of TV channels at ranges up to a few tens of miles.

Coaxial cable is also used short range connections between devices. Using digital signaling, coaxial cable can be used to provide high speed I/O channels on computer systems. Another application area for coaxial cable is local area network. Coaxial cable can support a large number of devices with a variety of data and traffic types, over distances that include a single building or group of buildings.

Optical Fiber : It is made of glass or plastic and transmits signals in the form of light. Transmission of total signal in optical fiber is based on the phenomenon of total internal reflection. An optical fiber cable has a cylindrical shape and consists of three concentric sections : the core, the cladding and the jacket.



Fig : Propagation of light in optical fiber

The core is the innermost section and consists of one or more very thin strands or fibers made of glass or plastic. Each fiber is surrounded by its own cladding, a glass or plastic coating that has optical properties different from those of the core. The outermost layer, surrounding one or a bundle of cladded fibers, is the jacket. The jacket is composed of plastic and other material layered to protect against moisture, abrasion, crushing, and other environmental dangers.

Propagation Modes: There are two mode of propagation of light in optical fibers: *multimode* and *single mode*. Each mode requires fiber with different characteristics. Multimode can be implemented in two forms : *step index* or *graded index*.

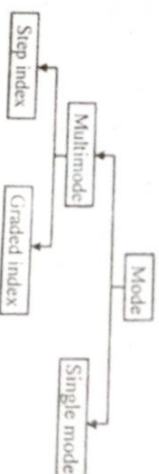


Fig.

Multimode: Multimode is so named because multiple beams from a light source move through the core in different paths. How these beams move within the cable depends on the structure of the core.

Multimode Step Index: In multimode step index fiber, the density of the core remains constant from the center to the edges. A beam of light moves through this constant density in a straight line until it reaches the interface of the core and the cladding. At the interface, there is an abrupt change to a lower density that alters the angle of the beam's motion. The term step index refers to the suddenness of this change.

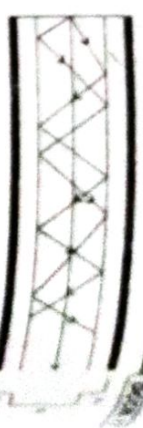


Fig : Propagation in multimode step-index fiber

The light ray travelling the straight path from the center and reaches the receiving end before the rays, which follow a zigzag path. This difference in length means that different beams arrive at the destination at different times. As these different beams recombined at the receiver, they result in a signal no longer an exact replica of the signal that was transmitted. This is known as *modal dispersion*.

Q.25 What is periodic analog signal? Explain detail.

Ans. Periodic Analog Signals : Periodic analog signal can be classified as simple or composite. A simple analog signal, a sine wave, cannot be decomposed into simpler signals. A composite periodic analog signal composed of multiple sine waves.



Fig : A sine wave

A sine wave can be represented by three parameters fully describe a sine wave: the peak amplitude, the frequency, and the phase.

Amplitude : The peak amplitude of a signal is the value of its highest intensity, proportional to the power it carries. For electric signals, peak amplitude is measured in volts.

Period and Frequency : Period refers to the time, in seconds, a signal needs to complete one cycle. Frequency refers to the number of periods a signal completes in one second.

Phase : The term phase describes the position of a waveform relative to time 0. Phase is measured in degrees or radians.

PREVIOUS YEARS QUESTIONS

PART-A

Q.1 Differentiate between single-bit error and burst error. [R.T.U. 2019]

Ans. Single-Bit error : As name suggest single-bit errors occur when a single bit gets changed during transmission of data due to interference in network communication.

"The term Single-Bit error means that only 1 bit of a given data unit (such as a byte, character or packet) is changed from 1 to 0 or from 0 to 1" by Forouzan.

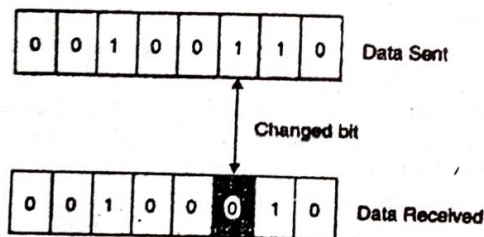


Fig. : Single Bit Error

Single-bit errors are least likely type of error because their duration or noise is normally longer than duration of 1 bit.

Burst Errors : When more than a single bit of data unit gets corrupted it is known as Burst error.

In comparison of single-bit errors, burst errors are more likely to occur. Because as we know that the duration of noise is generally longer than the duration of transferring

1bit, that means with longer duration noise can corrupt more than 1 bit easily. Number of bit affected depends on the data rate and duration of noise.

Q.2 Assume that, in a stop and wait ARQ system, the bandwidth of the line is 1 Mbps, and 1 bit takes 20ms to make a round trip. What is the bandwidth delay product? If the system data frames are 1000 bits in length, what is the utilization percentage of the link? [R.T.U. 2015]

Ans. The bandwidth-delay product is

$$1 \times 10^6 \times 20 \times 10^{-3} = 20,000 \text{ bits}$$

The system can send 20,000 bits during the time it takes for the data to go from the sender to the receiver and then back again. However, the system sends only 1000 bits. We can say that the link utilization is only $1000/20,000$, or 5%. For this reason, for a link with high bandwidth or long delay, use of Stop-and-Wait ARQ wastes the capacity of the link.

Q.3 Can the value of a checksum be all 0's (in binary)? Defend your answer. Can the value be all 1's (in binary)? Defend your answer.

[R.T.U. 2015]

Ans. The value of a checksum can be all 0's (in binary). This happens when the value of the sum (after wrapping) becomes all 1's (in binary).

It is almost impossible for the value of a checksum to be all 1's. For this to happen, the value of the sum (after wrapping) must be all 0's which means all data units must be 0's.

wait flow
4800 bits,
een device
over the
Dec. 2013/

$$\frac{1}{2} = \frac{t_p}{t_f}$$

$$0.5 t_f = t_p$$

$$t_f = \frac{L}{R}$$

$$t_f = \frac{20 \times 10^{-3}}{0.5} = 0.04$$

$$0.04 = \frac{L}{4800}$$

$$L = 192 \text{ bits}$$

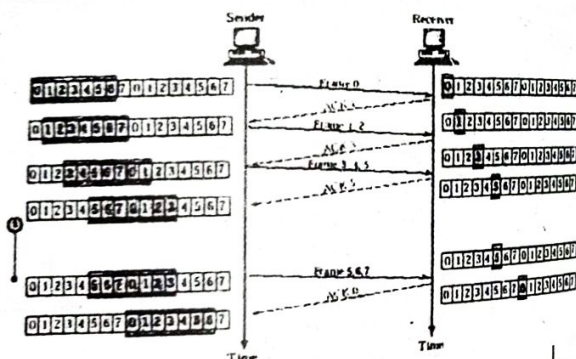
DCCN. 25

Q.6 Draw the sender and receiver window for a system using GO-Back-N-AKQ given the following:

- Frame 0 is sent; frame 0 is acknowledged
- Frame 1 and 2 are sent; frames 1 and 2 are acknowledged
- Frames 3, 4 and 5 are sent; frame 4 is acknowledged; timer for frame 5 expires.

[R.T.U. Dec. 2013]

Ans.



PART-B

Q.7 Explain block coding with suitable diagrams. [R.T.U. 2019]

Ans. Block Coding : To ensure accuracy of the received data frame, redundant bits are used. For example, in even parity, one parity bit is added to make the count of 1s in the frame even. In this way the original number of bits is increased. It is called block coding.

DCCN. 26
Block coding is represented by slash notation, mB/nB means, m-bit block is substituted with n-bit block where $n > m$. Block coding involves three steps:

- Division
- Substitution
- Combination.

Block Coding Concept

Block coding changes a block of m bits into a block of n bits, where n is larger than m. Block coding is referred to as an mB/nB encoding technique.

As block coding normally involves three steps: division, substitution and combination. In the division step, a sequence of bits is divided into groups of m bits.

For example, in 4B/5B encoding, the original bit sequence is divided into 4-bit groups. The heart of block coding is the substitution step. In this step, we substitute an m-bit group for an n-bit group.

For example, in 4B/5B encoding we substitute a 4-bit code for a 5-bit group. Finally, the n-bit groups are combined together to form a stream. The new stream has more bits than the original bits. The following figure shows the procedure.

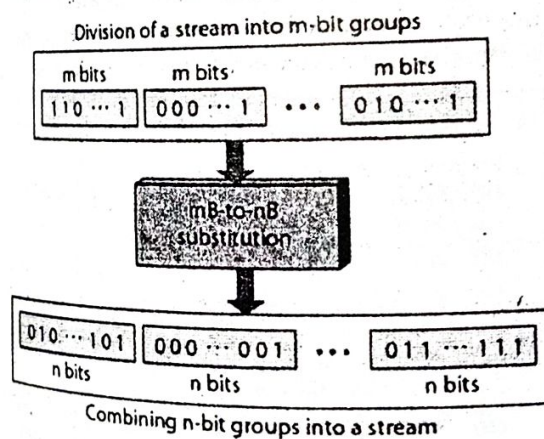


Fig.

Q.8 Explain Go-back-N ARQ protocol. [R.T.U. 2019]

Ans. Go-Back-N ARQ : Go-Back-N Automatic Repeat reQuest (Go-Back-N ARQ), is a data link layer protocol that uses a sliding window method for reliable and sequential delivery of data frames. It is a case of sliding

window protocol
receiving window

Working

Go - Back

pipelining, i.e. the acknowledgment sequentially number. The maximum size of the window is upon the size of the acknowledgment. The agreed amount of data in that frame are

The size of the sequence number is the number of the sequence number. Consequently, in order to accommodate an n-bit sequence

The sequence number. For example, the sequence number on. The number generate the b

The size

Sender

begin

frame

frame

S_win

window size

SeqFin

window

SeqN

window

while

do

Wait

if (

//c

if

window protocol having sending window size of N and receiving window size of 1.

Working Principle

Go - Back - N ARQ uses the concept of protocol pipelining, i.e. sending multiple frames before receiving the acknowledgment for the first frame. The frames are sequentially numbered upto a finite number of frames. The maximum number of frames that can be sent depends upon the size of the sending window. If the acknowledgment of a frame is not received within an agreed amount of time period, all frames starting from that frame are retransmitted.

The size of the sending window determines the sequence number of the outbound frames. If the sequence number of the frames is an n-bit field, then the range of sequence numbers that can be assigned is 0 to $2^n - 1$. Consequently, the size of the sending window is 2^{n-1} . Thus, in order to accommodate a sending window size of 2^{n-1} , an n-bit sequence number is chosen.

The sequence numbers are numbered as modulo-n. For example, if the size of sending window is 4, then the sequence numbers will be 0, 1, 2, 3, 0, 1, 2, 3, 0, 1, and so on. The number of bits in the sequence number is 2, to generate the binary sequence 00, 01, 10, 11.

The size of the receiving window is 1.

Sender Site Algorithm of Go-Back-N Protocol

```
begin
    frame s; //s denotes frame to be sent
    frame t; //t is temporary frame
    S_window = power(2,m) - 1; //Assign maximum
window size
    SeqFirst = 0; // Sequence number of first frame in
window
    SeqN = 0; // Sequence number of Nth frame
window
    while (true) //check repeatedly
    do
        Wait_For_Event(); //wait for availability of packet
        if ( Event(Request_For_Transfer)) then
            //check if window is full
            if (SeqN-SeqFirst >= S_window) then
```

```
        doNothing();
    end if;
    Get_Data_From_Network_Layer();
    s = Make_Frame();
    s.seq = SeqN;
    Store_Copy_Frame(s);
    Send_Frame(s);
    Start_Timer(s);
    SeqN = SeqN + 1;
end if;
if ( Event(Frame_Arrival)) then
    r = Receive_Acknowledgement();
    if ( AckNo > SeqFirst && AckNo < SeqN ) then
        while ( SeqFirst <= AckNo )
            Remove_copy_frame(s.seq(SeqFirst));
            SeqFirst = SeqFirst + 1;
        end while
        Stop_Timer(s);
    end if
end if
// Resend all frames if acknowledgement havn't
been received
if ( Event(Time_Out)) then
    TempSeq = SeqFirst;
    while ( TempSeq < SeqN )
        t = Retrieve_Copy_Frame(s.seq(SeqFirst));
        Send_Frame(t);
        Start_Timer(t);
        TempSeq = TempSeq + 1;
    end while
end if
end
Receiver Site Algorithm of Go-Back-N Protocol
Begin
    frame f;
    RSeqNo = 0; // Initialise sequence number of
expected frame
```

```
while (true) //
do
    Wait_For_E
    if ( Event(F
        Receive
    if ( Corru
        doNotH
    else if (
        Extra
        Deliv
        RSeq
        Send
    end if
    end if
    end while
end
```

Q.9 Explain sl

Ans. Sliding Window control protocol is a full duplex link. connected static. Thus, A is allow for any acknow. For keepi by sending an sequence num sequence num the outgoing d gets a free ri technique of t ments, so that data frame is The ack B is prepare with the num frames 2, 3, 4 has arrived sequence nu one time.

PART-C

Q.18 Explain pure ALOHA protocol with suitable diagrams. [R.T.U. 2019]

Ans. ALOHA : It is the simplest possible broadcast protocol and it sets a basis with which other broadcast protocols can be compared. It is also known as **Pure ALOHA**. The basic idea of ALOHA is simple since users transmit immediately whenever they have data to send. To determine whether a transmission was successful, a sender waits for an acknowledgement from the receiver for a time period equal to one propagation time (the time it takes to travel a packet from the sender to the receiver and back again). If no acknowledgement is received, the packet will be sent again.

There will obviously be collisions between packets sent within a packet transmission time t_p from different users as indicated in fig. 1. We first assume that all packets have the same length and each requires one time unit t_p (called a slot) for transmission. Consider an attempt by a user to send packet A starting at time t_0 . If another user generates packet B between t_0 and $t_0 + t_p$ the end of packet B will collide with the beginning of packet A. This can

occur because, owing to long propagation delays, the sender of packet A did not know that packet B was already under way when the transmission of packet A was started. Similarly, if another user attempts to transmit packet C between $t_0 + t_p$ and $t_0 + 2t_p$, the beginning of packet C will collide with the end of packet A. Thus if two packets overlap by even the slightest amount in the vulnerable period, collision will occur and both packets will be corrupted.

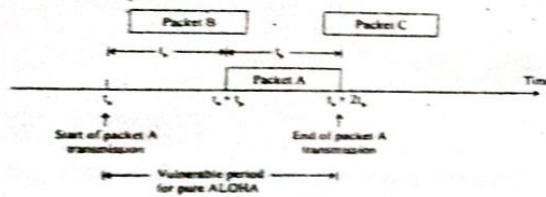


Fig. 1 : Packet transmission in ALOHA

Now let S be the channel throughput (the average number of successful transmission per time period t_p) and let G be the total traffic entering the channel from an infinite population of users (that is, G denotes the number of packet transmission that are attempted in time period t_p). To find the throughput, we first assume that the probability P_k of K transmission attempts per packet time follows a Poisson distribution with a mean G per packet time. This is given by

$$P_k = \frac{G^k e^{-G}}{k!} \quad \dots(1)$$

The throughput S is then just the offered load G times the probability of a transmission being successful. Thus

$$S = GP_0 \quad \dots(2)$$

Where P_0 is the probability that a packet does not suffer a collision. (P_0 is the probability of no other traffic being generated 'during a vulnerable period, which is, two packet, time long). From equation (1) the probability of zero packets being generated is equal to

$$P_0 = e^{-G} \quad \dots(3)$$

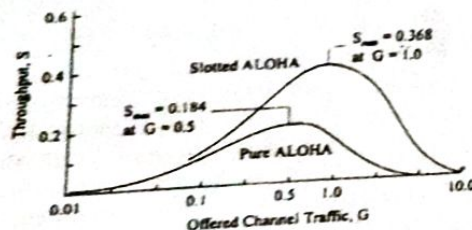


Fig. 2 : Relation between throughput and offered channel traffic
In an interval two frame times long, the mean number of frames generated is $2G$. The probability of no other

traffic being initiated during the entire vulnerable period is given by $P_0 = e^{-2G}$ by equation (2) we have

$$S = Ge^{-2G} \quad \dots(4)$$

The throughput given by equation (4) is plotted in fig. (2). The maximum value of S occurs at $G = 0.5$ where $S = 1/2e$ which is about 0.184. This means that the best channel utilization that can be achieved is around 18 percent for the pure ALOHA method.

Q.19 Compare and discuss the throughput of pure and slotted ALOHA. [R.T.U. 2017]

OR

Explain Pure ALOHA and Slotted ALOHA. Give relationship in terms of their throughput. [R.T.U. 2014]

OR

Show that slotted ALOHA has a maximum throughput of twice the pure ALOHA maximum throughput. [R.T.U. 2016]

OR

Show that the slotted ALOHA has a maximum throughput of twice the maximum throughput. [R.T.U. Dec. 2013, 2013, 2012, 2007]

Ans. Pure ALOHA : Refer to Q.18.

Slotted ALOHA

To increase the efficiency of the ALOHA method, the slotted ALOHA scheme was introduced. In this type of ALOHA the channel is divided into time slots which are exactly equal to a packet transmission time.

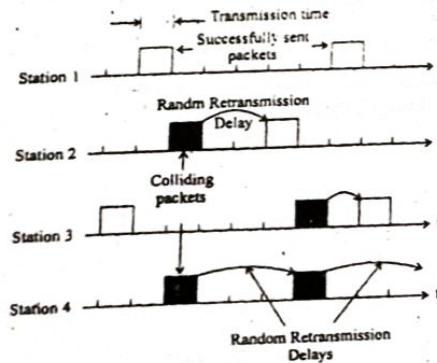


Fig. : Packet transmission in slotted ALOHA

All users are then synchronized to these time slots, so that whenever a user generates a packet it must

synchronize exactly with the next possible channel slot. Consequently, the vulnerable period in which this packet can collide with other data is reduced to one packet time period (PTP) versus two PTP for pure ALOHA. Examples of transmission attempts and random retransmission delays for colliding packets are shown in fig. for four network users.

Since the vulnerable period is now reduced by half, the probability of no other traffic occurring during the same time period as the packet, we wish to send is $P_0 = e^{-G}$. This in turn leads to a throughput

$$S = Ge^{-G}$$

As is shown in fig. (see fig. 2 in Q.18) the maximum efficiency of the slotted ALOHA system occurs at $G = 1$ where $S = 1/e$ or about 0.368, which is twice that of pure ALOHA.

Vulnerability period i.e. the period in which a transmitted frame will suffer collision $\propto \frac{1}{\text{efficiency}}$

If pure ALOHA is suffering $2T$ vulnerability period and slotted ALOHA is suffering T vulnerability period, it means efficiency of slotted ALOHA is twice that of pure ALOHA.

So, we proved efficiency of slotted ALOHA = 2 (Efficiency of pure ALOHA).

Q.20 What is two dimensional parity check? [R.T.U. 2017]

Ans. Parity Check: This error detecting technique is least expensive. Parity checking can be simple or two dimensional.

Simple Parity Check: In this technique a redundant bit called a parity bit is added to every data unit so that the total number of 1's in the unit (including parity bit) becomes even (or odd).

But in many cases even parity checking are applicable where the number of 1's should be even.

From figure suppose we want to transmit the binary data 1100001; gives us 3, an odd number. Before transmitting, we pass the data unit through a parity generator. The parity generator counts the 1's and appends the parity bit (1 in this case) to the end. The total no. of 1's is now 4, an even number. The system now transmits entire expanded unit reaches its destination, the receiver parts all 8 bits through an even parity checking function. If the receiver sees 11000011 it counts four 1's, an even number and the data unit passes.

Q20N.34
If we then attach the 8 bits to the original data and send them to the receiver.

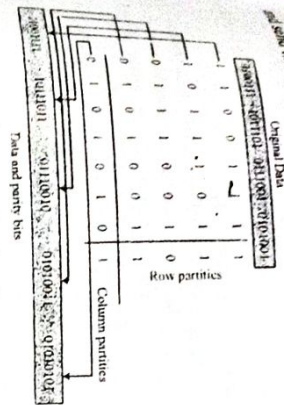


Fig. : Two dimensional parity

Performance: Two dimensional parity check method is very popular in today's life. In this method a redundancy of 7 bits can easily detect a burst error of n bits.

A burst error of more than n bits is also detected by this method with a very high probability. There is, however, one pattern of errors that remains elusive. If 2 bits in one data unit are damaged and 2 bits in exactly the same positions in another data unit are also damaged, the checker will not detect an error.

Consider, for example, two data units: 111110000 and 11000011. If the first and last bits in each of them are changed, making the data units read 01111001 and 01000010, the error be detected by this method.

Q21 Explain the types of errors and classification of codes.
(R.T.U. 2017, 2012, 2010)

Ans. Types of errors

The errors introduced in the transmitted data during their transmission may be categorized as under

- Content errors
- Flow integrity errors

Content errors:

The content errors are nothing but errors in the contents of a message i.e., a 0 may be received as 1 or vice-versa.

Flow integrity errors:

Flow integrity errors meaning missing blocks of data. It is possible that a data block may be lost in the between as it has been delivered to a wrong destination.

Types of Errors



The errors in a digital communication system are caused by noise in the communication channel (Gaussian noise introduced in analog part of common channel).

Random errors due to white Gaussian noise are introduced. Gaussian noise had been our chief concern in designing and evaluating modulators and demodulators. Sources of Gaussian are:

(a) **Thermal Noise:** Due to vibration of individual molecules about their position of equilibrium in a crystal lattice, the conduction electron of metals wander randomly throughout the volume of metal, similarly molecule of an enclosed gas are in constant motion colliding with one another and colliding also with the walls of container. These agitations of molecules are called thermal agitations because they increase with temperature.

(b) **Shot Noise:** Result from a phenomenon associated with flow of current across semiconductor junctions. The charge carriers, electrons or holes enter the junction region from one side, drift or are accumulated at the junction and are collected on other side. The average junction current determines the average interval that elapses between time when two successive carriers enter the junction. The exact interval that elapses is subject to random fluctuations. This randomness give rise to shot noise. As we know that power spectral density of Gaussian noise at receiver input is white Gaussian noise. The transmission errors introduced during a particular interval by white Gaussian noise does not affect the performance of system during subsequent signalling interval.

(c) **Burst Errors:** Which is due to impulse noise by long quite intervals followed by high amplitude noise burst. This type of noise occurs from many natural and man-made causes such as lightning and switching transients. When such noise occurs, it affects more than one symbol or bit and there is usually a dependence of errors in successive transmitted symbols.

Error control schemes for dealing with random errors are random error correcting codes and coding scheme designed to correct burst errors are burst over correcting codes.

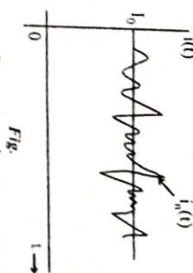
Shot Noise: Shot noise appears in active devices due to the random behaviour of charge carriers (electrons and holes). In electron tubes, shot noise is generated due to the random emission of electrons from cathodes; in semiconductor devices, it is caused due to the random diffusion of minority carriers or random generation and recombination of electron-hole pairs.

Current in electron devices (tubes or solid state) flows in the form of discrete pulses, every time a charge carrier moves from one point to the other (e.g., cathode to plate). Therefore, although current appears to be continuous, it is

B.Tech. (IV Sem.) C.S. Solved Papers

Data Communication and Computer Networks

still a discrete phenomena. The nature of current variation with time is shown in fig.



The current fluctuates about a mean value I_0 . This current $i(t)$ which wiggles around the mean value is known as shot noise. The wiggling nature of the current is not visualized by normal instruments and normally we think that the current is a constant equal to I_0 . The wiggling nature of the current can be observed in a fast sweep oscilloscope.

The total current $i(t)$ may be expressed as

$$i(t) = I_0 + i_s(t) \quad \dots (1)$$

where I_0 is the constant (mean) and $i_s(t)$ is the fluctuating (noise) current.

Power Density Spectrum of Shot Noise in Diodes: The time varying component $i_s(t)$ of the current $i(t)$ specified by eq (1) is random in nature and it cannot be expressed as a function of time, i.e. it is an indeterministic function. However, this indeterministic stationary random $i_s(t)$ can be specified by its power density spectrum.

The number of electrons contributing to the random stationary current $i_s(t)$ are large. Assuming that the electrons do not interact with each other during their movement or emission (e.g., temperature limited diode current), the process may be considered statistically independent. According to central limit theorem, such a process has a Gaussian distribution. Hence, shot-noise is Gaussian-distribution with a zero mean.

The total diode current may be taken as the sum of the current pulses, each pulse being formed by the transit of an electron from cathode to anode. It can be seen that for all practical purposes the power density spectrum of the statistically independent non-interacting random noise current $i_s(t)$ is given by:

$$S_{i_s}(\omega) = q I_0 \quad \dots (2)$$

where q is the electronic charge ($q = 1.59 \times 10^{-19}$ coulombs) and I_0 is the mean value of the current in amperes. The power density spectrum in eq (2) is frequency independent. This type of frequency independence is only up to a frequency range decided by the transit time of an electron to reach from anode to cathode. Beyond this frequency range, the power density varies with frequency as shown in fig. (a). The transit time of an electron, in a diode depends on anode voltage V and is given as

$$\tau = 3.36 \times \frac{d}{\sqrt{V}} \mu \text{ sec}$$

where d is spacing between anode and cathode. For instance, in a diode with $d = 2 \text{ mm}$ and $V = 40$ volts, we have $\tau \approx 10^{-7} \mu \text{ sec}$. In fig. (a), the power density curve may be considered flat close to the origin, i.e. $|\omega| \leq 0.5$. Therefore $S_{i_s}(\omega)$ can be considered constant up to $|\omega| = 0.5$. For $\tau = 10^{-7} \mu \text{ sec}$. The maximum frequency up to which power density $S_{i_s}(\omega)$ remains constant is given by

$$\omega = 0.5 \times 10^7 = 5 \times 10^6 \text{ rad/sec}$$

This is equivalent to a linear frequency $f = \frac{\omega}{2\pi} = 80 \text{ MHz}$. Therefore for all practical purposes, the $S_{i_s}(\omega)$ may be considered to be frequency-independent below 100 MHz.

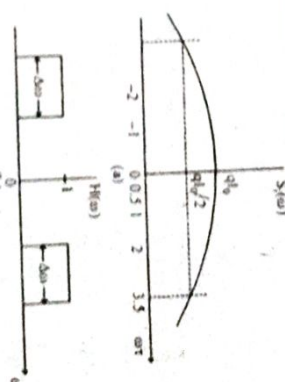


Fig. : Shot Noise : (a) Power Density Spectrum

(b) Bandwidth of Measuring System

Resistor Noise: The noise arising due to random motion of free charged particles (usually electrons) in a conducting media, such as a resistor, is called resistor noise. This noise is also known as Johnson noise, after J.B. Johnson who, investigated this type of noise in conductors. The random agitation is a universal phenomenon at atomic levels and is caused by the energy supplied through flow of heat. The intensity of random motion is proportional to thermal (heat) energy supplied (\propto temperature) and is zero at a temperature of absolute zero. This noise is also known as thermal noise. The path of the electron motion is random because of their collisions with lattice structure. The net motion of all the electrons gives rise to an electric current to flow through the resistor, causing the noise.

Power Density Spectrum of Resistor Noise:

The free electrons contributing to resistor noise are large in number. If their random motion is assumed to be statistically independent, then the central limit theorem predicts the resistor noise to be, Gaussian, distributed with a zero mean. It can be shown that the power density

Q20N.35

spectrum of the current contributing the thermal noise is given by :

$$S_i(\omega) = \frac{2kTG}{1 + \left(\frac{\omega}{\alpha}\right)^2} \quad \dots (1)$$

where T is ambient temperature in degree Kelvin, G is the conductance of the resistor in mhos, k is the Boltzmann constant and α is the average number of collisions per second per electron.

The variation of power density spectrum with frequency is shown in Fig.

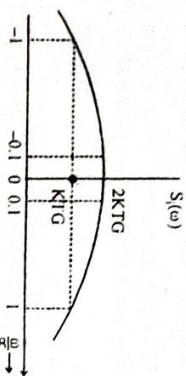


Fig. : Power Density Spectrum of the Resistor Noise Current
It is obvious from the figure that the spectrum may

be considered to be flat for $\frac{\omega}{\alpha} \leq 0.1$. The power density spectrum $S_i(\omega)$ for this range of frequency is nearly constant and is given by

$$S_i(\omega) = 2kTG \quad \dots (2)$$

The value of α is of the order of 10^{14} and hence the frequency corresponding to $\frac{\omega}{\alpha} < 0.1$ is of order of 10^{13} Hz.

Therefore, the frequency independent expression of $S_i(\omega)$ given by eq. (2) holds up to a frequency range of 10^{13} Hz. This range covers almost all the practical applications in communication systems. Hence, for all practical purposes, the power density spectrum $S_i(\omega)$ is considered to be independent of frequency.

Classification of codes :

The codes are basically classified as under:

(i) **Errors detecting codes:** The error detecting codes are capable of may detecting the errors. They cannot correct errors.

(ii) Error correcting codes

(1) Block codes (2) Convolution codes

The error correcting codes are capable of detecting as well as correcting the errors. These codes can be classified into block codes and convolution codes or linear and non-linear codes.

For error-free transmission, following codes are used :

- Block Codes
- Burst and Random Error Correcting Codes
- Interleaving

(A) Block Codes

(i) For Error Correction

1. We compare the performance of system using block codes for error correction with systems (n,k) using no error control coding.

2. Two measures of performance are :

(a) Problem of incorrectly decoding a message bit.

(b) Problem of incorrectly decoding a block of message digits.

3. We will do the comparison on the condition that rate of information transmission is same for coded and uncoded systems and both systems are operating with average signal power and noise power spectral density.

4. Coded or uncoded a block of say k message bits must be transmitted in duration of time.

$$T_w = \frac{k}{r_b}$$

where r_b = message bit rate

$$5. \therefore r_w = \frac{1}{T_w} = \frac{r_b}{k}$$

if system uses an (n, k) block code, then bit rate going into channel

$$r_c = r_b \left(\frac{n}{k} \right) \text{ or } r_c > r_b$$

6. Now

r_b = Message bit rate.

r_c = Channel bit rate.

q_c = Channel bit error probability for coded system.

q_u = Channel bit error probability for uncoded system.

P_{be}^u = Probability of incorrectly decoding a message bit in uncoded system.

P_{be}^c = Probability of incorrectly decoding a message bit in coded system.

P_{we}^u = Probability of incorrectly decoding a word of message bits in uncoded system.

P_{we}^c = Probability of incorrectly decoding a word of message bits in coded system.

7. Now in uncoded case

$P_{be}^u = q_u$ and probability that word of k message bit incorrectly received.

$P_{we}^u = 1 - P(\text{all } k \text{ message bits are correctly received})$

$$= 1 - (1 - q_u)^k \text{ when } kq_u \ll 1$$

$$= P_{we}^u = kq_u$$

Data Communication and Computer Networks
since transmission errors are assumed to be independent.

8. In coded system, a word of k message digits will be incorrectly decoded when more than t errors occur in a n-bit codeword since block code is assumed to be able to correct upto t errors.

Thus

$$P_{we}^c = P(t+1 \text{ or more errors in a codeword})$$

$$P_{we}^c = \sum_{i=t+1}^n \binom{n}{i} q_c^i (1 - q_c)^{n-i} = \sum_{i=t+1}^n P(n, i)$$

$$\text{where } P(n, i) = \binom{n}{i} q_c^i (1 - q_c)^{n-i}$$

$$\binom{n}{i} = \frac{n!}{i!(n-i)!}; r_{bw} = \frac{r_b}{k}$$

$$r_b P_{be}^c = r_{bw} (1 + 1) \frac{k}{n} P_{we}^c$$

$$\text{If } nq_c \leq 1, P(n, i+1) \leq P(n, i)$$

$$P_{we}^c = \binom{n}{t+1} (q_c)^{t+1} (1 - q_c)^{n-t-1}$$

P_{be}^c = message bit error probability.

P_{be}^c implies that majority of decoding errors are due to (t+1) bit errors in an n-bit codeword.

Out of (t+1) error, the fraction k/n represent the erroneous message bits. Hence average message bit error rate.

$$r_b P_{be}^c = r_{bw} (1 + 1) \frac{k}{n} P_{we}^c$$

$$\therefore P_{be}^c = \frac{(1 + 1)}{n} P_{we}^c$$

(ii) For Error Detection

1. We compare the performance of data transmission system using block codes for error detection with systems using direct transmission without error control coding.

2. We do the comparison under the assumed same assumption that S_{bw} , r_b remain same for both coded and uncoded systems.

3. We use probability of incorrectly decoding a block of k message bits as our measure of comparative performance.

4. Here we assume that (n, k) block code is capable of detecting upto 2t errors per block.

5. Decoder checks the received codewords for errors and when error is detected, the decoder may either discard or retransmit the message.

6. We know that data rate r_c over channel is $r_b \left(\frac{n}{k} \right)$ when an (n, k) error correcting block code

is used. The data rate r_c than $r_b \left(\frac{n}{k} \right)$ for (n, k) error because of retransmission.

Stop and Wait Transmission

1. The transmitter begins to t_0 and completes the transmission at time $t_0 + t_w$.

2. Decoder starts receiving + Δ where Δ is propagation delay.

3. At time $t_0 + \Delta + t_w$ the decoder block that was received acknowledgement (A) depending upon whether in received block.

4. If ACK is positive, then transmitted if not previously either case transmit $t_0 + t_w$ to $t_0 + t_w + 2\Delta$ for receiver.

5. To average channel all consider the transmission channel at rate r_c bits per second.

6. Total time needed to know r_c - bits per second

$$T = \frac{1}{r_c}$$

Total n bits

$$\therefore T = \frac{n}{r_c}$$

$$\text{Delay} = 2\Delta$$

$$T = \left(\frac{n}{r_c} + 2\Delta \right)$$

\therefore for N block time = N

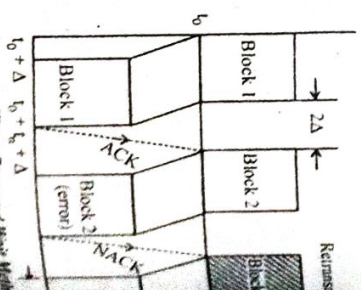


Fig. : Stop and Wait Method

PREVIOUS YEARS QUESTIONS

PART-A

Q.1 Differentiate between IPv4 address and IPv6 address. [R.T.U. 2019]

Ans. Differences between IPv4 and IPv6

IPv4	IPv6
IPv4 addresses are 32 bit length.	IPv6 addresses are 128 bit length.
IPv4 addresses are represented in decimal format	IPv6 addresses are represented in hexadecimal format.
IPSec support is optional.	Inbuilt IPSec support.
Checksum field is available in IPv4 header.	No Checksum field in IPv6 header.
Fragmentation is done by hosts and routers.	Fragmentation is done by sender hosts only.
Packet size is 576 bytes	Packet size is 1280 bytes
Router discovery is optional in IPv4.	Router discovery is required in IPv6.
IPv4 uses broadcast.	IPv6 do not use broadcast

Q.2 What is address mapping.

Ans. The delivery of a packet to a host or a router requires two levels of addressing: logical and physical. We need to be able to map a logical address to its corresponding physical address and vice versa. This can be done by using either static or dynamic mapping.

Q.3 Explain ARQ in data transmission.

Ans. Automatic repeat request (ARQ) is a protocol for error control in data transmission. When the receiver detects an error in a packet it automatically requests the transmitter to resend the packets. This process is repeated until the packet is error free or the error continues beyond a predetermined number of transmission.

PART-B

Q.4 Explain the services provided by network security. [R.T.U. 2019]

Ans. Network Security Services

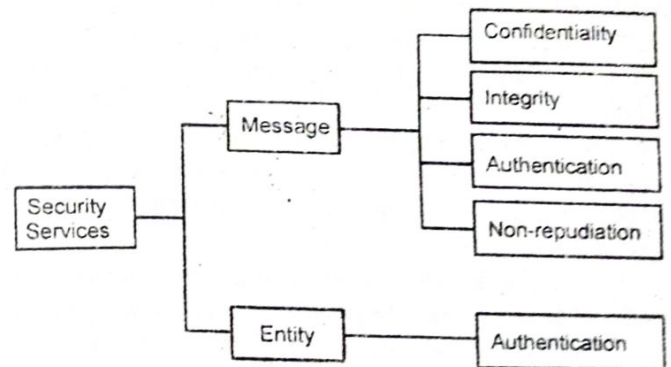


Fig.

1. Message confidentiality

- It means that the content of a message when transmitted across a network must remain confidential, i.e. only the intended receiver and no one else should be able to read the message.

- The users, therefore, want to encrypt the message they send so that an eavesdropper on the network will not be able to read the contents of the message.

2. Message Integrity

- It means the data must reach the destination without any adulteration i.e. exactly as it was sent.
- There must be no changes during transmission, neither accidentally nor maliciously.
- Integrity of a message is ensured by attaching a checksum to the message.
- The algorithm for generating the checksum ensures that an intruder cannot alter the checksum or the message.

3. Message Authentication

- In message authentication the receiver needs to be sure of the sender's identity i.e. the receiver has to make sure that the actual sender is the same as claimed to be.
- There are different methods to check the genuineness of the sender :
 - The two parties share a common secret code word. A party is required to show the secret code word to the other for authentication.
 - Authentication can be done by sending digital signature.
 - A trusted third party verifies the authenticity. One such way is to use digital certificates issued by a recognized certification authority.

4. Message non-repudiation

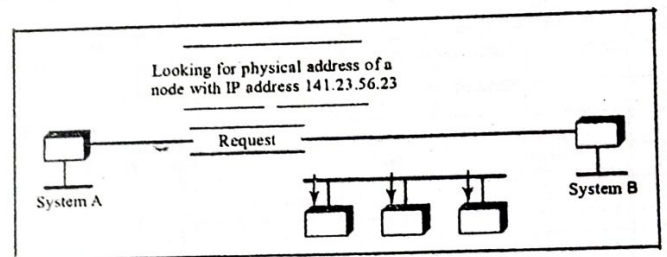
- Non-repudiation means that a sender must not be able to deny sending a message that it actually sent.
- The burden of proof falls on the receiver.
- Non-repudiation is not only in respect of the ownership of the message; the receiver must prove that the contents of the message are also the same as the sender sent.
- Non-repudiation is achieved by authentication and integrity mechanisms.

5. Entity Authentication

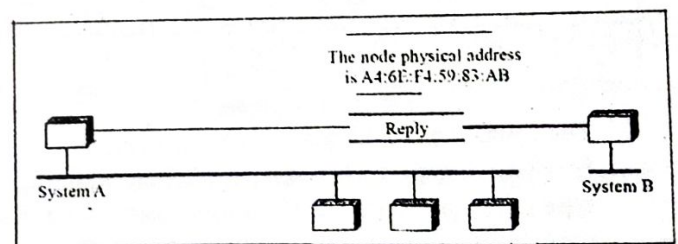
- In entity authentication (or user identification) the entity or user is verified prior to access to the system resources.

Ans. ARP : Anytime a host or a router has an IP datagram to send to another host or router, it has the logical (IP) address of the receiver. The logical (IP) address is obtained from the DNS if the sender is the host or it is found in a routing table if the sender is a router. But the IP datagram must be encapsulated in a frame to be able to pass through the physical network. This means that the sender needs the physical address of the receiver. The host or the router sends an ARP query packet. The packet includes the physical and IP addresses of the sender and the IP address of the receiver. Because the sender does not know the physical address of the receiver, the query is broadcast over the network (see Figure 1).

Every host or router on the network receives and processes the ARP query packet, but only the intended recipient recognizes its IP address and sends back an ARP response packet. The response packet contains the recipient's IP and physical addresses. The packet is unicast directly to the inquirer by using the physical address received in the query packet.



(a) ARP request is broadcast



(b) ARP reply is unicast

Fig. 1 : ARP operation

In Figure 1(a), the system on the left (A) has a packet that needs to be delivered to another system (B) with IP address 141.23.56.23. System A needs to pass the packet to its data link layer for the actual delivery, but it does not know the physical address of the recipient. It uses the services of ARP by asking the ARP protocol to send a broadcast ARP request packet to ask for the physical address of a system with an IP address of 141.23.56.23.

Q.5 Explain ARP and RARP address mapping protocols.

[R.T.U. 2019]

DCCN.54

53

ring
the
ess
an
world
his
ers
ile
is
ts

binding between the physical and IP addresses is static and fixed in a table until changed by the administrator. BOOTP is a static configuration protocol.
Ans. (ii) POP3 Vs IMAP : Both POP3 and IMAP are email accessing protocols but they differ in following manner :

POP3 (Post Office Protocol Version 3)	IMAP (Internet Message Accessing Protocol)
Message stores at user's (client) machine.	Message stores at server machine.
Message stores at client machine so it provides offline reading facility.	Online message reading facility due to message stores at server.
Because message stores at client machine so user takes backup.	Backup facility provided by email service provider.
Memory needed at clients machine to store the message.	Memory not needed at client side due to message stores at server.
User can access email through his/her own computer only.	User can access email through any machine in the world i.e. it provides portability.

Q.9 How are IP addresses assigned? Describe this with suitable example for internet. [R.T.U. 2015]

OR

How are IP addresses assigned? Describe this with suitable example for internet currently in use. [Raj. Univ. 2004]

Ans. Every host and router on the internet has an IP address, which encodes its network number and host number. The combination is unique, in principle, no two machines on the internet have the same IP address. All IP addresses are 32 bits long and are used in the source address and destination address fields of IP packets. An IP address does not actually refer to a host. It really refers to a network interface, so if a host is on two networks, it must have two IP addresses. However, in practice, most hosts are on one network and thus have one IP address. IP addresses were divided into the five categories listed in the fig. This allocation has come to be called classful addressing. The class A, B, C and D formats allow for upto 128 networks with 16 million host each, 16384 networks with up to 64K hosts and 2 million networks (e.g. LANs) with up to 256 hosts each (although a few of these are special). Also supported is multicast in which a datagram is directed to multiple hosts. Addresses beginning with 1111 are reserved for future use. Over 500,000 networks are now connected to the internet.

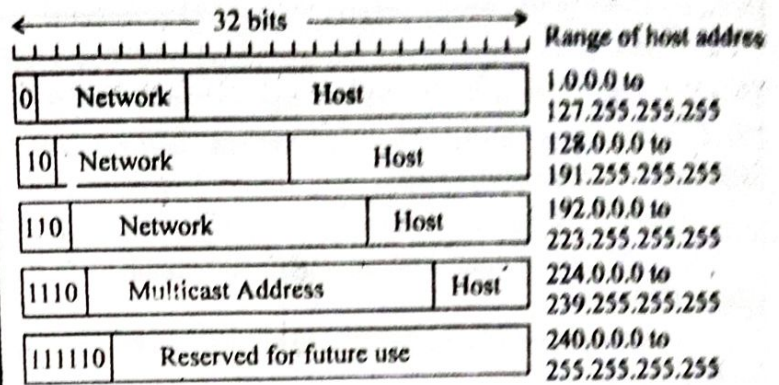


Fig. 1 : IP address format

Network addresses, which are 32 bit numbers, are usually written in dotted decimal notation. In this format, each of the 4 bytes are written in decimal, from 0 to 255. E.g. the 32 bit hexadecimal address C0290614 is written as 192.41.6.20. The lowest IP address is 0.0.0.0 and the highest 255.255.255.255.

The value 0 and 1 (all 1's) have special meanings, as shown in fig. 2. The value 0 means this network or this host. The value 1 is used as a broadcast address to mean all hosts on the indicated network.

The IP address 0.0.0.0 is used by hosts when they are being booted IP addresses with 0 as network number refer to the current network. These addresses allow machines to refer to their own network without knowing its number (but they have to know its class to know how many 0's to include). The address consisting of all 1's allows broadcasting on the local network typically a LAN. The addresses with a proper network number and all 1's in the host field allow machines to send broadcast packets to distant LANs anywhere in the internet (although many network administrators disable this feature). Finally, all addresses of the form 127.xx.yy.zz are reserved for loopback testing. Packets sent to that address are not put out onto the wire, they are processed locally and treated as incoming packets. This allows packets to be sent to the local network without sender knowing its number.

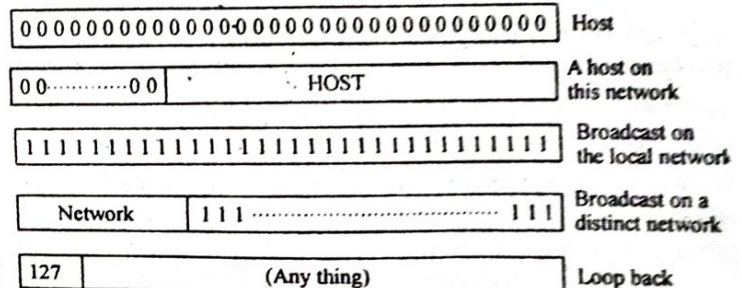


Fig. 2 : Special IP addresses

Q.9 IP, TCP and UDP all discard a packet that arrives with a checksum error and do not attempt to notify the source. Why?

[R.T.U. 2009]

TRANSPORT LAYER 4

PREVIOUS YEARS QUESTIONS

PART-A

Q.1 Differentiate between connectionless and connection-oriented service. [R.T.U. 2019]

Ans. Difference between Connection oriented and Connectionless service

1. In connection oriented service authentication is needed, while connectionless service does not need any authentication.
2. Connection oriented protocol makes a connection and checks whether message is received or not and sends again if an error occurs, while connectionless service protocol does not guarantees a message delivery.
3. Connection oriented service is more reliable than connectionless service.
4. Connection oriented service interface is stream based and connectionless is message based.

Q.2 What do you mean by connectionless transport in transport layer.

Ans. Connectionless Transport (UDP) : UDP is a connectionless, unreliable protocol that has no flow and error control. It performs very limited error checking. It uses port numbers to multiplex data from the application layer.

Q.3 What is segment structure of UDP.

Ans. Segment Structure : UDP packets, called user datagram, have a fixed-size header of 8 bytes.

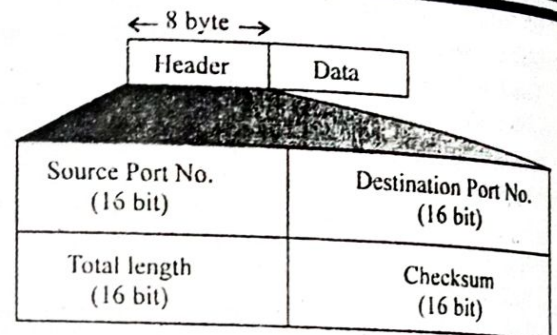


Fig.

- **Source Port Number** : This is the port number used by the process running on the source host.
- **Destination Port Number** : This is the port number used by the process running on the destination host.
- **Length** : This is a 16 bit field that defines the total length of the user datagram (Header + Data)
- **Checksum** : This field is used to detect errors over the entire user datagram (Header + Data).

Q.4 Write two difference between Token Bucket & Leaky Bucket.

Ans. Difference between Token Bucket and Leaky Bucket Algorithms

S. No.	Token Bucket Algorithm	Leaky Bucket Algorithm
1.	Token bucket throws away tokens when the bucket is full but never discards packet.	Leaky bucket discards packets when the bucket is full.
2.	Token bucket allows saving upto a maximum size of bucket n. This means that bursts of upto n packets can be sent at once, giving faster response to sudden bursts of input.	Leaky bucket also gives response to sudden bursts of input.

from the incoming segment into the *destination port* field of the outgoing segment, the process sending the reply can specify which process on the sending machine is to get it.

The *UDP length* field includes the 8-byte header and the data. The *UDP checksum* is optional and stored as 0 if not computed (a true computed 0 is stored as all 1s). Turning it off is foolish unless the quality of the data does not matter (e.g., digitized speech).

It is probably worth mentioning explicitly some of the things that UDP does not do. It does not do flow control, error control, or retransmission upon receipt of a bad segment. All of that is upto the user processes. What it does do is provide an interface to the IP protocol with the added feature of demultiplexing multiple processes using the ports. That is all it does. For applications that need to have precise control over the packet flow, error control, or timing.

One area where UDP is especially useful is in client-server situations. Often, the client sends a short request to the server and expects a short reply back. If either the request or reply is lost, the client can just time out and try again. Not only is the code simple, but fewer messages are required (one in each direction) than with a protocol requiring an initial setup.

An application that uses UDP this way is DNS (the Domain Name System), a program that needs to look up the IP address of some host name to a DNS server. The server replies with a UDP packet containing the host's IP address. No setup is needed in advance and no release is needed afterward. Just two messages go over the network.

Q.7 Explain Quality of service for transport layer.

[R.T.U. 2015, 13]

Ans. Quality of Service (QoS) : In the field of computer networking and other packet-switched telecommunication networks, the traffic engineering term quality of service (QoS) refers to resource reservation control mechanisms rather than the achieved service quality. Quality of service is the ability to provide different priority to different applications, users, or data flows, or to guarantee a certain level of performance to a data flow. For example, a required bit rate, delay, jitter, packet dropping probability and/or bit error rate may be guaranteed. Quality of service guarantees are important if the network capacity is insufficient, especially for real-time streaming multimedia applications such as voice over IP, online games and IPTV, since these often require fixed bit rate and are delay sensitive, and in networks where the capacity is a limited resource, for example in cellular data communication.

QoS is sometimes used as a quality measure, with many alternative definitions, rather than referring to the ability to

reserve resources. Quality of service sometimes refers to the level of quality of service, i.e. the guaranteed service quality. High QoS is often confused with a high level of performance or achieved service quality, for example high bit rate, low latency and low bit error probability.

Quality of service (QoS) is an internetworking issue that has been discussed more than defined. We can informally define quality of service as something a flow seeks to attain. **Flow Characteristics :** Traditionally, four types of characteristics are attributed to a flow : reliability, delay, jitter, and bandwidth, as shown in fig. 1.

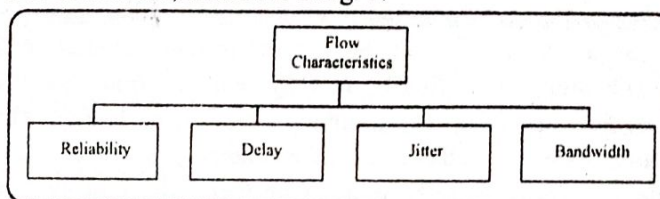


Fig. 1 : Flow Characteristics

Reliability : Reliability is a characteristic that a flow needs. Lack of reliability means losing a packet or acknowledgment, which entails retransmission. However, the sensitivity of application programs to reliability is not the same. For example, it is more important that electronic mail, file transfer, and Internet access have reliable transmissions than telephony or audio conferencing.

Delay : Source-to-destination delay is another flow characteristic. Again applications can tolerate delay in different degrees. In this case, telephony, audio conferencing, video conferencing and remote log-in need minimum delay, while delay in file transfer or e-mail is less important.

Jitter : Jitter is the variation in delay for packets belonging to the same flow. For example, if four packets depart at times 0, 1, 2, 3 and arrive at 20, 21, 22, 23, all have the same delay, 20 units of time. On the other hand, if the above four packets arrive at 21, 23, 21, and 28, they will have different delays : 21, 22, 19, and 24.

For applications such as audio and video, the first case is completely acceptable; the second case is not. For these applications, it does not matter if the packets arrive with a short or long delay as long as the delay is the same for all packets. For this application, the second case is not acceptable.

Jitter is defined as the variation in the packet delay. High jitter means the difference between delays is large; low jitter means the variation is small. If the jitter is high, some action is needed in order to use the received data.

Bandwidth : Different applications need different bandwidths. In video conferencing we need to send millions of bits per second to refresh a color screen while the total number of bits in an e-mail may not reach even a million.

The same idea can be applied to packets, as shown in Fig. (b). Conceptually, each host is connected to the network by an interface containing a leaky bucket, that is, a finite internal queue. If a packet arrives at the queue when it is full, the packet is discarded. In other words, if one or more processes within the host try to send a packet when the maximum number are already queued, the new packet is unceremoniously discarded. This arrangement can be built into the hardware interface or simulated by the host operating system. It was first proposed by Turner (1986) and is called the **leaky bucket algorithm**. In fact, it is nothing other than a single-server queuing system with constant service time.

The host is allowed to put one packet per clock tick onto the network. Again, this can be enforced by the interface card or by the operating system. This mechanism turns an uneven flow of packets from the user processes inside the host into an even flow of packets onto the network, smoothing out bursts and greatly reducing the chances of congestion.

When the packets are all the same size (e.g., ATM cells), this algorithm can be used as described. However, when variable-sized packets are being used, it is often better to allow a fixed number of bytes per tick, rather than just one packet. Thus if the rule is 1024 bytes per tick, a single 1024-byte packet can be admitted on a tick, two 512-byte packets, four 256-byte packets, and so on. If the residual byte count is too low, the next packet must wait until the next tick. Implementing the original leaky bucket algorithm is easy. The leaky bucket consists of a finite queue. When a packet arrives, if there is room on the queue it is appended to the queue; otherwise, it is discarded. At every clock tick, one packet is transmitted (unless the queue is empty).

The byte-counting leaky bucket is implemented almost the same way. At each tick, a counter is initialized to n . If the first packet on the queue has fewer bytes than the current value of the counter, it is transmitted, and the counter is decremented by that number of bytes. Additional packets may also be sent, as long as the counter is high enough. When the counter drops below the length of the next packet on the queue, transmission stops until the next tick, at which time the residual byte count is overwritten and lost.

Q.10 Discuss the reason of congestion in a network. Also discuss Leaky bucket and Token bucket algorithms in detail.

[R.T.U. 2016]

Ans. Congestion Control Algorithms : Congestion in a network may occur if the load on the network (the number of packets sent to the network) is greater than the capacity of the network (the number of packets a network can handle). Congestion in a network occurs because routers and switches have queue buffers that hold the packets before and after processing.

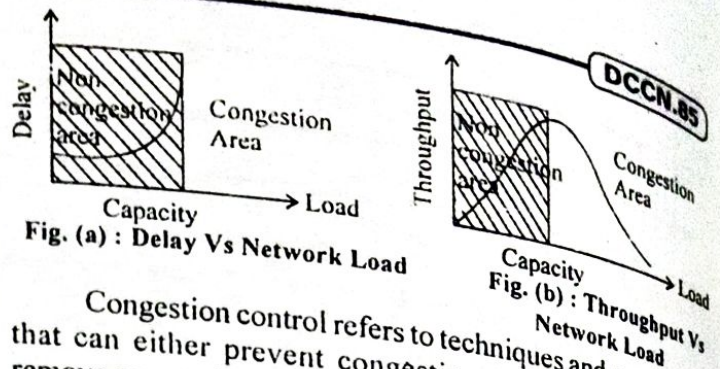


Fig. (a) : Delay Vs Network Load

Fig. (b) : Throughput Vs Network Load

Congestion control refers to techniques and mechanisms that can either prevent congestion, before it happens, or remove congestion, after it has happened. Congestion control can be divided into open loop congestion control (prevention) and closed loop control.

Token Bucket Algorithm

Tools for doing open loop control include deciding when to accept new traffic, deciding when to discard packets and which ones, and making scheduling decisions at various points in the network. All of these have in common the fact that they make decisions without regard to the current state of the network. The closed loop control is based on the concept of a feedback loop.

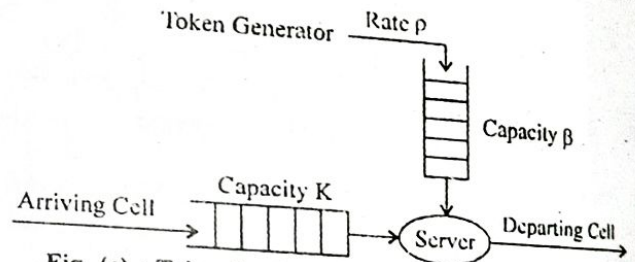


Fig. (c) : Token bucket algorithm for traffic shaping

This approach has three parts when applied to congestion control:

- (1) Monitor the system to detect when and where congestion occurs.
- (2) Pass this information to place where action can be taken.
- (3) Adjust system operation to correct the problem.

Congestion control involves two factors that measure the performance of a network: throughput and delay

The figure illustrates the basic principle of the token bucket. A token generator produces tokens at a rate of p tokens per second and places these in the token bucket, which has a maximum capacity of β tokens. Cell arriving from the source are placed in a buffer with a maximum capacity of K cells. To transmit a cell through the server, one token must be removed from the bucket. If the token bucket is empty, the cell is queued waiting for the next token.

The result of this scheme is that if there is a back log of cells and an empty bucket, then cells are emitted at a smooth flow of p cells per second with no cell delay variation until the back log is cleared. Thus, the token bucket smooths out bursts of cells.

Leaky Bucket Algorithm : Refer to Q.9.

VS.

[R.T.U. 2019]

authoritative name server is that have been configured, the domain administrator contrast to answers that S query to another name server only returns answer that have been specifically authoritative name server a slave server. A master (master) copies of es an automatic updating communication with it y of the master records.

DNS.

[R.T.U. 2019]

ers do not contain copie ve a cache file that i os it has performed in th oritative response. Whe authoritative server an passes that answer alon e answer. Thus, non thoritatively for a give uthoritative servers ar do not contain specifi oritative server answer kup cache. Any answe rver is deemed non e from an authoritativ

Q.5 Explain different services of application layer.

Ans. Application layer provides the following services :

- (i) Less time consumption i.e. fast delivery
- (ii) Reliable data transfer
- (iii) Less amount of congestion throughout the network
- (iv) Safety of data in context of threads due to intruders etc.

Q.6 Explain use of cookies in WWW and HTTP.

Ans. Use of Cookies in WWW : When a client sends a request to a server, the browser looks in the cookie directory to see if it can find a cookie sent by that server. If found, the cookie is included in the request. When the server receives the request, it knows that this is an old client, not a new one. Note that the contents of the cookie are never read by the browser or disclosed to the user. It is a cookie made by the server and read by the server.

Use of Cookies in HTTP : An HTTP server is stateless. This simplifies server design and has permitted engineers to develop high-performance web servers that can handle thousands of simultaneous TCP connections. It is often desirable for a website to identify users, either because the server wishes to restrict user access or because it wants to serve content as function of user identity. For these purposes, HTTP uses cookies. Cookies allows sites to keep track of users.

Q.7 Write the components of cookie technology.

Ans. Cookie Technology has four components :

- (i) A cookie header line in HTTP response message
- (ii) A cookie header line in HTTP request message
- (iii) A cookie file kept on user's and system and managed by the user's browser.
- (iv) A back-end data base at the website.

PART-B

- Q.8** (a) What is Proxy server and how it is related to HTTP.
 (b) What is URL and what are its components? Explain.
 (c) In electronic mail, what is MIME? [R.T.U. 2017]

Ans. (a) Proxy Server: A proxy server is a server (a computer system or an application) that acts as an intermediary for requests from client seeking resources from other servers. A client connects to the proxy server, requesting some service, such as a file, connection, web page, or other

resource available from a different server and the proxy server evaluates the request as a way to simplify and control its complexity. Proxies were invented to add structure and encapsulation to distributed systems. Today, most proxies are web proxies, facilitating access to content on the World Wide Web, providing anonymity and may be used to bypass IP address blocking.

Related to HTTP : HTTPS is Hypertext Transfer Protocol over Security Socket Layer (HTTP over SSL). It's a more safety protocol than HTTP. In view of security requirements, more and more sites transfer from HTTP to HTTPS, especially bank sites and online paying sites. As a default setting, HTTPS works upon port 443.

Proxy server handles HTTPS requests from clients is always called HTTPS proxy server. It's similar with HTTP proxy server, the only difference is the protocols they focus on. No matter HTTP or HTTPS proxy server, they both can carry out caching of information downloaded from the Internet. This is a very useful function which can speed up surfing and reduce network traffic.

Most proxy servers act both as an HTTP proxy server and as an HTTPS proxy server. Proxy settings on clients for both HTTP and HTTPS are similar, the only thing you need to care is HTTPS is mostly identified by "Secure" or "Security".

Ans. (b) Uniform Resource Locator (URL) : A client that wants to access a Web page needs the address. To facilitate the access of documents distributed throughout the world, HTTP uses locators. The uniform resource locator (URL) is a standard for specifying any kind of information on the Internet. The URL defines four things: protocol, host computer, port and path as shown as shown in fig.

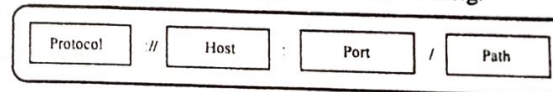


Fig. : URL

The protocol is the client/server program used to retrieve the document. Many different protocols can retrieve a document; among them is FTP or HTTP. The most common today is HTTP. The host is the computer on which the information is located, although the name of the computer can be an alias. Web pages are usually stored in computers, and computers are given alias names that usually begin with the characters "www". This is not mandatory, however, as the host can be any name given to the computer that hosts the Web page. The URL can optionally contain the port number of the server. If the port is included, it is inserted between the host and the path, and it is separated from the host by a colon. Path is the pathname of the file where the information is located. The path contains slashes.

Data Communication and Computer Networks

Cookies : A cookie, also known as a web cookie, browser cookie, and HTTP cookie, is a piece of text stored on a user's computer by their web browser. A cookie can be used for authentication, storing site preferences, shopping cart contents, the identifier for a server-based session, or anything else that can be accomplished through storing text data.

A cookie consists of one or more name-value pairs containing bits of information, which may be encrypted for information privacy and data security purposes. The cookie is sent as a field in the header of the HTTP response by a web server to a web browser and then sent back unchanged by the browser each time it accesses that server.

Cookies may be set by the server with or without an expiration date. Cookies without an expiration date exist until the browser terminates, while cookies with an expiration date may be stored by the browser until the expiration date passes. Users may also manually delete cookies in order to save space or to avoid privacy issues.

Creation and Storage of Cookies

1. When a server receives a request from a client; it stores information about the client in a file or a string. The information may include the domain name of the client, the contents of the cookie (information the server has gathered about the client such as name, registration number, and so on), a timestamp, and other information depending on the implementation.
2. The server includes the cookie in the response that it sends to the client.
3. When the client receives the response, the browser stores the cookie in the cookie directory, which is sorted by the domain server name.

Using Cookies : Refer to Q.6.

Ans. (b) Performance enhancement in WWW : WWW stands for "World Wide Web." and it is not a synonym for the Internet. The World Wide Web, or just "the Web," as ordinary people call it, is a subset of the Internet. The Web consists of pages that can be accessed using a Web browser. The Internet is the actual network of networks where all the information resides. Things like Telnet, FTP, Internet gaming, Internet Relay Chat (IRC), and e-mail are all part of the Internet, but are not part of the World Wide Web. The Hyper-Text Transfer Protocol (HTTP) is the method used to transfer Web pages to your computer. With hypertext, a word or phrase can contain a link to another Web site. All Web pages are written in the hyper-text markup language (HTML), which works in conjunction with HTTP.

Q.1 What E-mail privacy? Why do we need POP3 or IMAP4 for electronic mail.

[R.T.U. 2013]

Ans. The protection of email from unauthorized access and inspection is known as electronic privacy. In countries with a constitutional guarantee of the secrecy of correspondence, email is equated with letters and thus legally protected from all forms of eavesdropping.

The requirement refers generally to both the user's expectation that something is private and also to society's expectation that the thing should be private.

There are three situations in which privacy of e-mail could be a concern.

1. Interception during transmission, for example, by a wiretap on the telephone line at the sender's building.
2. Reading during storage on the destination computer. For example, if one sends e-mail to lstudent@fplc.edu, this e-mail is stored on a hard drive of a computer at fplc until the recipient deletes it. If the recipient does not read the message within a reasonable time, typically a few months of sending the message, the system operator may delete the message to recover space on the hard drive for other users. Good operating practice of a computer system involves making routine backup copies (typically on magnetic tape) of all files on the hard drive, since hard drives can fail. An e-mail may be retrieved from a backup tape even after that e-mail was deleted from the hard drive by the recipient.
3. Disclosure of contents by the recipient.

The actual mail transfer is done through Message Transfer Agents (MTA). To send mail, a system must have the client MTA, and to receive mail, a system must have a server MTA. The actual formal protocol that defines the MTA client and server in the Internet is called the Simple Mail Protocol (SMTP).

SMTP is used two times, between the sender and the sender's mail server and between the two mail servers. SMTP simply defines how commands and responses must be sent back and forth (forward).

SMTP uses commands and responses to transfer messages between an MTA client and an MTA server as shown in figure 1.

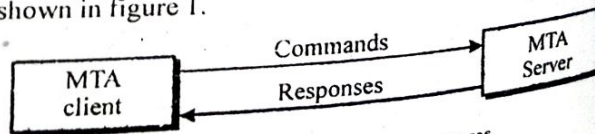


Fig. 1 : Commands and responses

SMTP expects the destination host, the mail server receiving the mail, to be on-line all the time, otherwise, a TCP connection cannot be established. For this reason, it is not practical to establish an SMTP session with a desktop computer because desktop computers are usually powered down at the end of the day.

In many organizations, mail is received by an SMTP server that is always on-line. This SMTP server provides a mail-drop service. The server receives the mail on behalf of every host in the organization. Workstations interact with the SMTP host to retrieve messages by using a client-server protocol such as Post Office Protocol (POP), version 3 (POP3).

Although POP3 is used to download messages from the server, the SMTP client is still needed on the desktop to forward messages from the workstation user to its SMTP mail server.

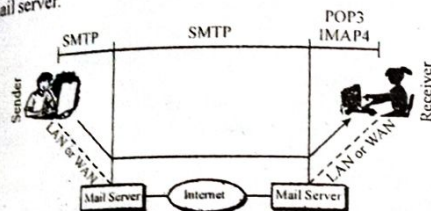


Fig. 2 : POP3 and IMAP4

Another mail access protocol is Internet Mail Access Protocol version 4 (IMAP4). IMAP4 is similar to POP3, but it has more features, IMAP4 is more powerful and more complex.

POP3 is deficient in several ways. It does not allow the user to organize her mail on the server, the user cannot have different folders on the server. In addition, POP3 does not allow the user to partially check the contents of the mail before downloading.

IMAP4 provides the following extra functions :

- A user can check the e-mail header prior to downloading.
- A user can search the contents of the e-mail for a specific string of characters prior to downloading.
- A user can partially download e-mail. This is especially useful if bandwidth is limited and the e-mail contains multimedia with high bandwidth requirements.
- A user can create, delete or rename mailboxes on the mail server.
- A user can create a hierarchy of mailboxes in a folder for e-mail storage.

Q.12 Explain the differences in persistent and non-persistent HTTP.

[R.T.U. 2012]

Ans. Persistent and Non-persistent HTTP are differentiated below, with the help of their advantages and disadvantages :

Advantages of Persistent HTTP Connections

Faster Content Delivery. Less round-trip time, everything is served via the same TCP stream which obviously saves lots of time. When adding HTTP pipelining support to this, things are even faster.

This is also extremely beneficial when it comes to secure delivery using the SSL protocol, which require extra round-trips.

1. Less CPU Usage: We are involving a less amount of low level OS routine calls.

2. Reduced Network Congestion: Less packets on the line, and more control for TCP to handle the congestion in a single (from RFC 2616 notes on persistent connections) **Disadvantages**

1. Possible Scalability Issues: In case of a traffic burst, all the "slots" on the web server (the connection pool) are kept busy by few users, while everybody else wait for a server response. This also happens with non-persistent connections as well, however the time to serve a different HTTP request is lower than with persistent connection because there is no time-out period.

2. No Simplicity Friendliness: A server serving simple one time files (such as AJAX request, basic HTML files with no embedded objects, XML files, updates statuses has no reason to server HTTP content via persistent connection, because the one-time required content can be served using one HTTP request and the client will be gone

3. Non-CDN Friendly: If serving content from a CDN which delivers content from multiple web servers for the purpose of increasing the delivery speed, the CDN solution is nilled by not being able to deliver multiple HTTP responses via the same TCP connection.

Advantages of Non-Persistent HTTP connections

1. Possibly More Scalable : Depending on the design of the application and the usage patterns (the disadvantage for persistent HTTP connections), more clients can be served if they require content from the server sporadically.

2. Simple Server Architecture : The server may be a bit faster if it does not require the implementation of the persistent HTTP connections and the pipelining support.

Disadvantages

1. Possibly Less Scalable: Depending on the type of traffic the server gets, serving individual HTTP requests on their own TCP stream may quickly starve the server's resources.

2. More CPU Usage: There are low level operating system routines involved in opening a new TCP stream for each request. This puts the web server under more work.

Q.13 What is DNS poisoning? Explain the bad effect of DNS poisoning.

[R.T.U. 2012]

Ans. DNS Poisoning :

DNS Poisoning or DNS Cache Poisoning

DNS poisoning is also called DNS cache poisoning and refers to the corruption of DNS tables and caches so

that a domain name points to a malicious IP address. Once the user is redirected to the malicious IP address his/her computer can be infected with worms, viruses, spy ware etc.

Cache poisoning is mostly done through spam emails, or through web-links and banners that attracts users to click on them. A simple click causes the user to be re-directed to a DNS poisoned server.

Cache poisoning is a security of data integrity compromise in the Domain Name System (DNS). The compromise occurs when data is introduced into a DNS name server's cache database that did not originate from authoritative DNS sources. It may be a deliberate attempt of a maliciously crafted attack on a name server. It may also be an unintended result of a misconfiguration of a DNS cache or from improper software data and caches it for performance optimization, it is considered poisoned, supplying the non-authentic data to the clients of the server.

A domain name server translates a domain name (such as example.com) into an IP address that Internet hosts use to contact Internet resources. If a DNS server is poisoned, it may return an incorrect IP address, diverting traffic to another computer.

Effect of DNS Poisoning

Poisoning attacks on a single DNS server can affect the users serviced directly by the compromised server or indirectly by its downstream server(s) if applicable.

To perform a cache poisoning attack, the attacker exploits a flaw in the DNS software. If the server does not correctly validate DNS responses to ensure that they are from an authoritative source (for example by using DNSSEC) the server will end up caching the incorrect entries locally and serve them to other users that make the same request. This technique can be used to direct users of a website to another site of the attacker's choosing.

- For example, an attacker spoofs the IP address DNS entries for a target website on a given DNS server, replacing them with the IP address of a server he controls. Then he creates files on the server he controls with names matching those on the target server.
- These files could contain malicious content, such as a computer worm or a computer virus. A user whose computer has referenced the poisoned DNS server would be tricked into accepting content coming from a non-authentic server and unknowingly download malicious content.

PART-C

Q.14 Explain the HTTP protocol with the help of suitable diagrams. [R.T.U. 2019]

OR

Describe the steps involved when a web browser requests for and obtains a web page from a web server. Why HTTP is known as stateless protocol? [R.T.U. 2010]

OR

Explain HTTP and its message formats.

[R.T.U. 2015, 13, Raj. Univ. 2008]

OR

Write short notes on HTTP.

[Raj. Univ. 2006]

Ans. HTTP is an Application layer protocol, implemented in two programs : a **client program** and a **server program**. The client program and server program, executing on different end systems, talk to each other by exchanging HTTP messages.

A **Web page** consists of **objects**. An object is simply a file—HTML file, a JPEG image, a GIF image, a Java applet, an audio clip etc., that is **addressable by a single URL**.

A **browser** is a **user agent** for the web, it displays the requested **Web page** and provides numerous navigational and configuration features.

HTTP defines how web clients request web pages from the web and how servers transfer web pages to client. Both HTTP/1.0 and HTTP/1.1 use **TCP** as their underlying transport protocol.

The HTTP client first initiates a TCP connection with the server. Once the connection is established, the browser and the server processes access TCP through their **Socket I/Fs**. On the client side the socket I/F is the "door" between, the **client process and the TCP connection**, on the server side it is the "door" between the **server process and the TCP connection**.

Once the client sends a message into its socket I/F, the message is "out of the client's hands" and is "in the hands of TCP". TCP is used because it provides the **reliable service**.

HTTP can use both **non-persistent connections** and **persistent connections**.

HTTP Message Format :

1. HTTP Request Message :

GET/Somedir/page.html HTTP/1.1 → (Request line)

Host : www.nkjaipur.com

Connection : close → (header lines)

User-agent : Mozilla/4.0 → (Netscape browser)

Accept-language

Request line has three fields : (1) The method field, (2) The URL field, (3) The HTTP version field.

The header line **Host** specifies the host on which the object resides.

In header line **Connection**, the browser is telling the server that it doesn't want to use persistent connection, it wants the server to close the connection after sending the request object.

The header line **User-agent**, specifies the type of browser used to make request to the server.

The header line **Accept-language**, indicates that the user prefers to receive a **French Version** of the object.

2. HTTP Response Message :

HTTP/1.1 200 OK 3 → Status line

Connection : Close

Date : TUE, 08 Feb. 2005 11:30:15 Ist → When the HTTP response was created and sent by the server.

Server : Apache/1.3.0 (Unix)

Host-modified : SUN, 06 Feb 2005 16:15:20 Ist

→ When the object was created or last modified.

Content-length : 7557

Content-type : Image /JPEG

Data data → Entity body

The status line has three fields : The protocol version field, a status code, and corresponding status message.

Ex. (1) 200 OK : Request succeeded and the information is returned in the response.

(2) 301 Named permanently : Requested object has been permanently named.

(3) 400 Bad Request : The request could not be understood by the server.

(4) 404 Not found : The requested document does not exist on 12 server.

(5) 505 HTTP Version Not Supported : The request HTTP protocol version is not supported by the server.

Most Web pages consist of a base HTML file and several referenced objects. For example, if a Web page contains HTML text and five JPEG images, the Web page has six objects: the base HTML file plus the five images. The base HTML file references the other objects in the page with the objects' URLs. Each URL has two components: the host name of the server that houses the object and object's path name.

For example, the URL <http://www.someSchool.edu/someDepartment/picture.gif> has www.someSchool.edu for a host name and </someDepartment/picture.gif> for a path name. A browser is a user agent for the Web, it displays the requested Web page to the user and provides numerous navigational and configuration features.

HTTP defines how Web clients (for example, browsers) request Web pages from Web servers and how servers

transfer Web pages to clients, but the general idea is illustrated in Figure. When a user requests a Web page (for example click on a hyperlink), the browser sends HTTP request messages for the objects in the page to the server. The server receives the requests and responds with HTTP response message that contain the objects.

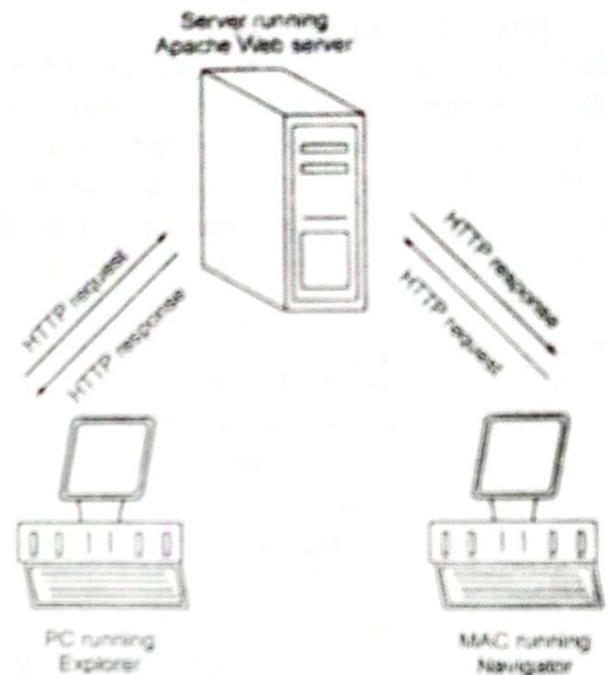


Fig. : HTTP request-response behaviour

A Web server running 1.1 can "talk" with a browser running 1.0, and a browser running 1.1 can "talk" with a server running 1.0. Because HTTP/1.1 is now dominant, henceforth when we refer to HTTP we are referring to HTTP/1.1.

HTTP uses TCP as its underlying transport protocol (rather than running on top of UDP). The HTTP client first initiates a TCP connection with the server. Once the connection is established, the browser and the server processes access TCP through their socket interfaces. On the client side the socket interface is the door between the client process and the TCP connection, on the server side it is the door between the server process and the TCP connection. The client sends HTTP request messages into its socket interface and receives HTTP response messages from its socket interface. Similarly, the HTTP server receives request messages from its socket interface and sends response messages into its socket interface. Once the client sends a message into its socket interface, the message is out of the client's hands and is "in the hands" of TCP. TCP provides a reliable data transfer service to HTTP. This implies that each HTTP request message emitted by the client process eventually arrives intact at the server, similarly each HTTP response message emitted by the server process eventually arrives at the client. HTTP need not worry about loss of data or the details of how TCP recovers from loss or reordering of data within the network. That is the job of TCP and the protocols in the lower layers of the protocol stack.

cache the information. After that time, the mapping is invalid and any query must be sent again to the authoritative server. Second, DNS requires that each server keep a TTL counter for each mapping it caches. The cache memory must be searched periodically, and those mappings with an expired TTL must be purged.

Q.17 Write short note on :

- (a) World Wide Web (WWW)
(b) File Transfer Protocol (FTP) [R.T.U. 2016]

Ans. (a) World Wide Web (WWW) : The WWW today is a distributed client/server service, in which a client using a browser can access a service using a server. However, the service provided is distributed over many locations called sites, as shown in fig. 1.

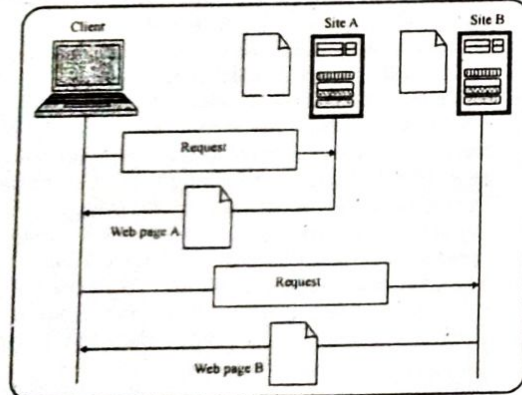


Fig.1 : WWW Architecture

Each site holds one or more documents, referred to as **Web pages**. Each Web page can contain a link to other pages in the same site or at other sites. The pages can be retrieved and viewed by using browsers. Let us go through the scenario shown in fig. 1. The client needs to see some information that it knows belongs to site A. It sends a request through its browser, a program that is designed to fetch Web documents. The request, among other information, includes the address of the site and the Web page, called the URL (Uniform Resource Locator). The server at site A finds the document and sends it to the client. When the user views the document she finds some references to other documents, including Web page at site B. The reference has the URL for the new site. The user is also interested in seeing this document. The client sends another request to the new site, and the new page is retrieved.

Client (Browser) : A variety of companies offer many commercial browsers that interpret and display a Web document, and all use nearly the same architecture.

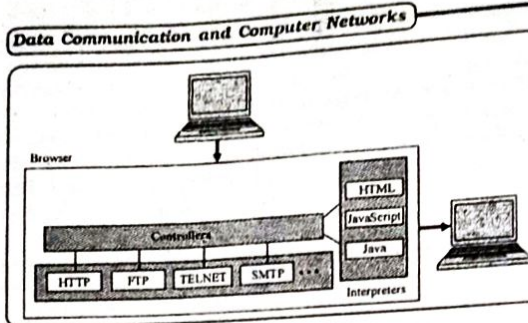


Fig.2 : Browser

Each browser usually consists of three parts: a controller, client protocol, and interpreters. The controller receives input from the keyboard or the mouse and uses the client programs to access the document. After the document has been accessed, the controller uses one of the interpreters to display the document on the screen. The client protocol can be one of the protocols such as File Transfer Protocol (FTP) or Hyper Text Transfer Protocol (HTTP). The interpreter can be HTML, Java, or JavaScript, depending on the type of document.

Server : The Web page is stored at the server. Each time a client request arrives, the corresponding document is sent to the client. To improve efficiency, servers normally store requested files in a cache in memory; memory is faster to access than disk. A server can also become more efficient through multithreading or multiprocessing. In this case, a server can answer more than one request at a time.

Uniform Resource Locator (URL) : Refer to Q.8(b).

Cookies : Refer to Q.9(a).

Using Cookies : Refer to Q.6.

Ans.(b) File Transfer Protocol (FTP) : The File Transfer Protocol (FTP) is used to copy files between two computer systems over the TCP connection. The FTP overcomes the problem of different file systems used in the network.

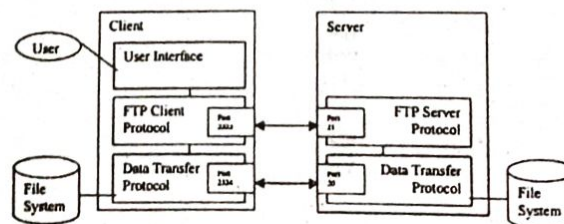


Fig. : FTP protocol model

In the FTP, the user communicates with a user interface in the local FTP client process. The local FTP client process makes a control connection to the remote server's FTP server protocol. FTP server protocol is located in the TCP port 21. The local FTP client acts as a protocol interpreter who interprets the user commands to the acronyms used between

the client and the server protocol. The control connection is basically a simple TELNET's NVT session. The control connection is used in a very simple way.

The client sends commands across the control connection to the server. The server replies to the messages according to the server protocol. If the user request a data transfer, a special data connection is opened between the server and the client and the files are sent through this connection. Separate data transfer process created for the server and the client. The data connection exists until the command that it was created for is executed. File transfer protocol contains set of command words and their parameters and numeric codes as responses. The command words can be classified to the access control, file management, data format setting, file transfer, site, error recovery and restart commands.

Earlier FTP protocols used for the Internet standard were drafted by the Internet Engineering Task Force committee as a series of RFC (Request for Comments) formal documents. In 1971 the FTP protocol RFC 114 was published. Over the years the document was revised with newer versions making changes to improve the FTP protocol.

FTP connects using two TCP ports for all communications between the server and user-

COMMAND Port: This is the main TCP port which is created when a session is connected. It is used for passing commands and replies. Port 21 (unsecured) or 990 (secured) are the default command ports used.

DATA Port: Each time when files or directories are transferred between server and client, a random TCP data connection is established and data transfer commences over the connection. Once data transfer is complete, the connection is closed. Subsequent data connections are established and terminated as required. Data connections are never left open.

Q.18 Explain e-mail architecture along with its components. [R.T.U. 2010]

Ans. E-mail Architecture : To explain the architecture of e-mail, we have four scenarios. We begin with the simplest situation and add complexity as we proceed. The fourth scenario is the most common in the exchange of email. These scenarios provide a general overview of e-mail system.

First Scenario : In the first scenario, the sender and the receiver of the e-mail are users (or application programs) on the same system, they are directly connected to a shared system. The administrator has created one mailbox for each user where the received messages are stored. A mailbox is part of a local hard drive, a special file with permission

Q.20 Explain the working of SMTP.

[R.T.U. 2009, Raj. Univ. 2006]

Ans. Simple Mail Transfer Protocol (SMTP) : One of the most popular network services is electronic mail (e-mail). The TCP/IP protocol that supports electronic mail on the Internet is called Simple Mail Transfer Protocol (SMTP). It is a system for sending messages to other computer users based on e-mail addresses. SMTP provides for mail exchange between users on the same or different computers and supports:

- Sending a single message to one or more recipients.
- Sending messages that include text, voice, video, or graphics.
- Sending messages to users on networks outside the Internet.

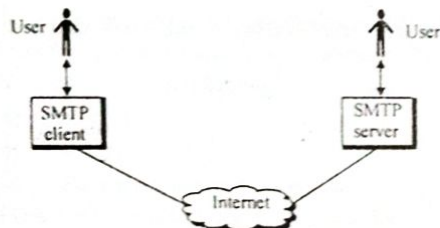


Fig.1: SMTP Concept

A simple SMTP system is shown in Fig.1. The SMTP client and server can be broken down into two components: **user agent (UA)** and **mail transfer agent (MTA)**.

The UA prepares the message, creates the envelope, and puts the message in the envelope. The MTA transfers the mail across the Internet. Figure 2 shows the previous figure with the addition of these two components.

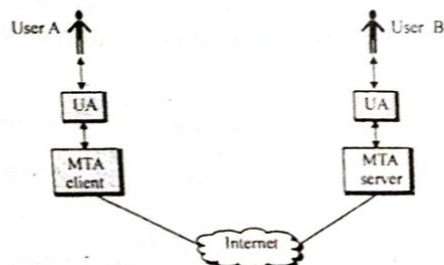


Fig.2: UAs and MTAs

SMTP protocol allows a more complex system than the one shown. Relaying could be involved. Instead of just one MTA at the sender site and one at the receiving site, other MTAs, acting either as client or server, can relay the mail.

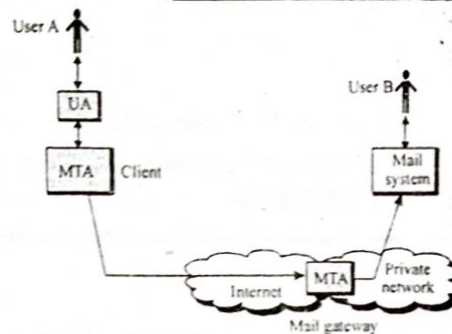


Fig.3: Mail Gateway

The relaying system allows sites that do not use the TCP/IP protocol suite to send e-mail to users on other sites that may or may not use the TCP/IP protocol suite. This is accomplished through the use of a **mail gateway**, which is a relay MTA that receives mail prepared by a protocol other than SMTP and transform it to SMTP format before sending it. It can also receive mail in SMTP format and change it to another format before sending it (Figure 3).

User Agent (UA) : A user agent is defined in SMTP. The UA is normally a program used to send and receive mail. Popular user agent programs are MH, Berkeley Mail, Elm, Zmail, and Mush.

Some user agents have an extra user interface that allows window-type interactions with the systems.

Addresses : To deliver mail, a mail handling system must use a unique addressing system. The addressing system used by SMTP consists of two parts: a **local part** and a **domain name**, separated by an @ sign.

Local Part : The local part defines the name of a special file, called the user mailbox, where all of the mail received for a user is stored for retrieval by the user agent.

Domain Name : The second part of the address is the domain name. An organization usually selects one or more hosts to receive and send e-mail, they are sometimes called mail exchangers. The domain name assigned to each mail exchanger either comes from the DNS database or is a logical name (for example, the name of the organization).

Mail Transfer Agent (MTA) : The actual mail transfer is done through mail transfer agents (MTAs). To send mail, system must have a client MTA, and to receive mail, a system must have a server MTA. Although SMTP does not define specific MTA, sendmail is a commonly used UNIX system MTA.

SMTP simply defines how commands and response must be sent back and forth. Each network is free to choose a software package for implementation. Figure 4 illustrates the process of sending and receiving e-mail described above. For a computer to be able to send and receive mail using

SMTP, it must have most of the entities (the user interface is not necessary) defined in the figure. The user interface is component that creates a user-friendly environment.

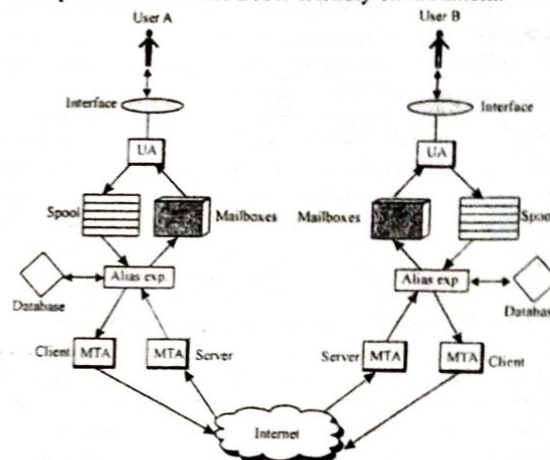


Fig.4: The Entire E-mail System

Q.21 Each internet host has at least one local name server and one authoritative name server. Describe role of each of these services in DNS.

[Raj. Univ. 2007]

Ans. In order to deal with the issue of scale, the DNS uses a large number of name servers, organized in a hierarchical fashion and distributed around the world. No single name server has all of the mappings for all of the hosts in the Internet. Instead, the mappings are distributed across the name servers. To a first approximation, there are three types of name servers: local name servers, root name servers, and authoritative name servers. These name servers, again to a first approximation, interact with each other and with the querying host as follows.

Local name servers : Each ISP—such as a university, an academic department, an employee's company, or a residential ISP—has a local name server (also called a default name server). When a host issues a DNS query message, the message is first sent to the host's local name server. The IP address of the local name server is typically configured by hand in a host. (On a Windows machine, we can find the IP address of the local name server used by our PC by opening the Control Panel, and then selecting "Network," then selecting an installed TCP/IP component, and then selecting the DNS configuration folder tab.) The local name server is typically "close to" the client. In the case of an institutional ISP, it may be on the same LAN as the client host, for a residential ISP, the name server is typically separated from the client host by no more than a few routers. If a host requests a translation for another host that is part of the same local ISP, then the local name server will immediately be able to provide the requested IP address. For example, when the