

# COMPUTER NETWORKS

<del>Overview of Data Communication and Networking</del>	2
<del>Physical Level</del>	20
Data Link Layer	25
Medium Access Sub Layer	39
<del>Network Layer</del>	53
Transport Layer	69
<del>Application Layer</del>	78
Modern Topics	91

## NOTE:

WBUT course structure and syllabus of 7th Semester has been changed from 2013. **COMPUTER NETWORKS** has been introduced as a new subject in present curriculum. Taking special care of this matter we are providing chapterwise complete solutions of new University Question Papers along with some model questions and answers, so that students can get an idea about university questions patterns.

# OVERVIEW OF DATA COMMUNICATION AND NETWORKING

## Multiple Choice Type Questions

1. A hub is a  
a) router                      b) bridge                      c) repeater                      d) all of these. [WBUT 2013, 2016]  
Answer: (c)

2. Repeaters function in the ..... layer  
a) data link                      b) physical                      c) network                      d) transport [WBUT 2014]  
Answer: (b)

3. Which address cannot be changed?  
a) Hardware address                      b) logical address                      c) both (a) and (b)                      d) none of this [WBUT 2014]  
Answer: (a)

4. A \_\_\_\_\_ is a device that forwards packets between networks by processing the routing information included in the packet.  
a) bridge                      b) firewall                      c) router                      d) switch [WBUT 2015]  
Answer: (c)

5. Which transmission media has the highest transmission speed in a network?  
a) coaxial cable                      b) twisted pair cable                      c) optical fiber                      d) electrical cable [WBUT 2015]  
Answer: (c)

6. Which of this is not a network edge device?  
a) PC                      b) smartphone                      c) servers                      d) switch [WBUT 2015]  
Answer: (d)

7. The total number of links required to connect  $n$  devices using Mesh topology is  
a)  $2^n$                       b)  $n(n+1)/2$                       c)  $n(n-1)/2$                       d)  $n^2$  [WBUT 2016]  
Answer: (c)

8. WDM methodology is popularly used for  
a) twisted pair cable                      b) coaxial cable                      c) optical fibre                      d) wireless transmission [WBUT 2017]  
Answer: (c)

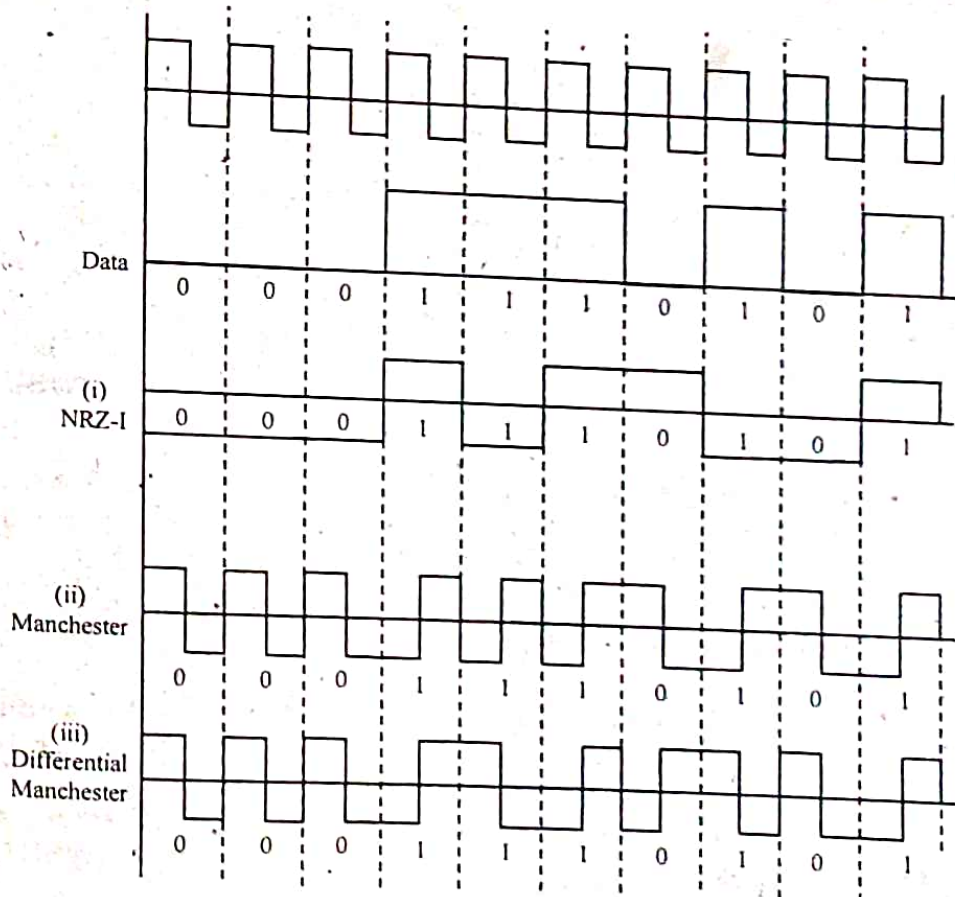
9. Method of communication in which transmission takes place in both directions, but only in one direction at a time, is called  
 a) Simplex                      b) Full duplex  
 Answer: (d)                      c) Four wire circuit                      d) Half duplex  
 [WBUT 2017]

10. The duration of time it takes to send a message from one end of a network to the other and back is called  
 a) Round trip time                      b) Full Duplex Time  
 Answer: (a)                      c) Circle trip time                      d) Data Travelling time  
 [WBUT 2017]

**Short Answer Type Questions**

1. Draw the following encoding schemes for the bit stream 0001110101:  
 i) NRZ-I                      [WBUT 2013, 2016]  
 ii) Manchester coding  
 iii) Differential Manchester coding.

Answer:



2. What is Bit Rate? What is Baud Rate?  
 An analog signal carries 4 bits in each signal unit. If 1000 signal units are sent per second, find the baud rate and bit rate.  
 [WBUT 2013, 2014]



## POPULAR PUBLICATIONS

**Answer:**

**1<sup>st</sup> Part:**

Bit rate is a measure of the number of data bits (that's 0's and 1's) transmitted in one second. A figure of 2400 bits per second means 2400 zeros or ones can be transmitted in one second, hence the abbreviation 'bps'.

Baud rate by definition means the number of times a signal in a communications channel changes state. For example, a 2400 baud rate means that the channel can change states up to 2400 times per second.

**2<sup>nd</sup> Part:**

There are 1000 signal units are sent per second.

And each signal carries 4 bits, as we know

Bit rate = No. of bits per second =  $4 \times 1000 \text{ bit/sec.} = 4000 \text{ bit/sec.} = 4 \text{ kbps.}$

Where Baud rate = No. of signal units per second =  $1000 \text{ bits/sec.} = 1 \text{ kbps.}$

**3. a) Write down the advantages of fibre-optic cable over twisted pair and coaxial cable.** [WBUT 2013, 2016]

**Answer:**

Optical fibre is a cable with numerous advantages:

Light-weight

Immune to noise

Low attenuation

Tolerates data rates on the order of 100 Mbps

Bandwidth from tens of megahertz to several gigahertz (monomode fibre)

**b) Suppose that a signal has  $2^n$  times the power as a noise signal that is added to it. Find the SNR in decibels.** [WBUT 2013]

**Answer:**

$$x = 10 \log \text{ratio} = 10 \log 2 = 3 \text{ dB}$$

$$x = 10 \log 10 = 10 \text{ dB}$$

The last two, you need a value for n or k. If you want a general answer:

$$x = 10 \log \text{ratio} = 10 \log (2^n) = 10n \log 2 = 3n \text{ dB}$$

$$x = 10 \log \text{ratio} = 10 \log (10^k) = 10k \log 10 = 10k \text{ dB}$$

**4. How does Manchester encoding differ from differential Manchester encoding?** [WBUT 2014, 2016]

OR,

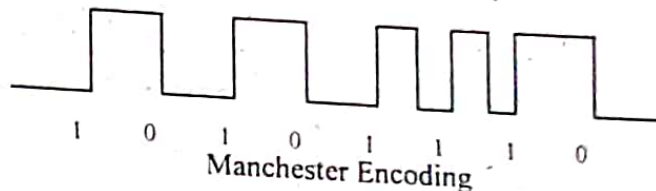
**State the differences between Manchester and Differential Manchester encoding schemes with an example.** [WBUT 2015]

**Answer:**

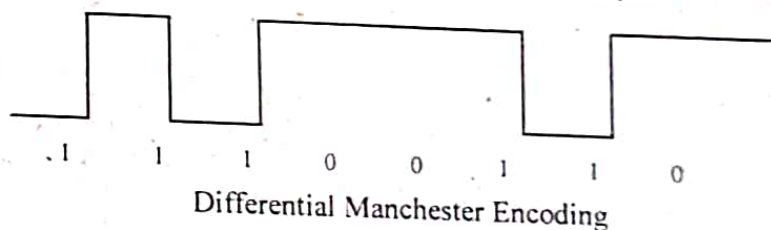
A simple example of a Physical Layer protocol is the Manchester encoding technique used on copper-cabled local area networks (LANs). This is a synchronous protocol, because it is based on the "ticks" of an electronic timer. Each binary bit is allocated a fixed slice of time. At the middle of that time slice, if the voltage changes from low to



high, this is interpreted as a binary 1. If the voltage drops from high to low at the middle of the bit time, this is a 0. The Manchester Encoding Diagram shows how a binary number is represented using this signaling technique. The device that receives this signal, such as a NIC, only pays attention to voltage changes that occur in the middle of a 1-bit time segment. Thus, to represent a series of 1s, the signal must first drop to low voltage at the beginning of a bit time, so it is ready to change from low to high again to represent another binary 1.



A variation of this method, called Differential Manchester encoding, avoids this skipping signal. It counts each voltage change at a clock tick, from high to low or low to high, as a binary 1. A binary 0 is represented by no voltage change at the clock tick. The Differential Manchester Encoding Diagram displays an example of this encoding scheme.



5. What do you mean by low-pass and band-pass channels?

[WBUT 2015]

Answer:

If a channel can carry base band processes, the channel is called a *low-pass channel*. If it can carry narrow-band processes, we call it a *band-pass channel*. The low-pass channel is a model for much channels as pair of wires or a coaxial cable. For wave guides, light guides and open space radio channels, the band-pass channel is the suitable model.

6. a) What is TDM?

[WBUT 2015]

b) A constellation diagram consists of eight equally spaced points on a circle. If the bit rate is 4800 bps, what is the baud rate?

Answer:

a) Time-division multiplexing (TDM) is a method of putting multiple data streams in a single signal by separating the signal into many segments, each having a very short duration. Each individual data stream is reassembled at the receiving end based on the timing.

b) The constellation indicates 8-PSK with the points 45 degrees apart. Since  $2^3 = 8$ , 3 bits are transmitted with each signal unit. Therefore, the baud rate is  $4800/3 = 1600$  baud.

7. Physical address operates in a local domain whereas logical address has a global domain. Explain, Define bandwidth of a media.

[WBUT 2016]

## POPULAR PUBLICATIONS

### **Answer:**

- i) A Physical address is a 48-bit flat address burned into the ROM of the NIC card which is a Layer1 device of the OSI model. This is divided into 24-bit vendor code and 24-bit serial address. This is unique for each system and cannot be changed.  
A Logical address is a 32-bit address assigned to each system in a network. This works in Layer-3 of OSI Model. This would be generally the IP address.
- ii) Physical address also called MAC address. It is present on Network interface card. It won't change.  
Logical addressing is used when a packet passes n/w boundary.

### ***Band Width:***

Bandwidth (computing) or digital bandwidth: a rate of data transfer, throughput or bit rate, measured in bits per second

Bandwidth (signal processing) or analog bandwidth: a measure of the width of a range of frequencies, measured in hertz.

## **8. Explain Client Server Model. What is the Idea of web based e-mail. [WBUT 2017]**

### **Answer:**

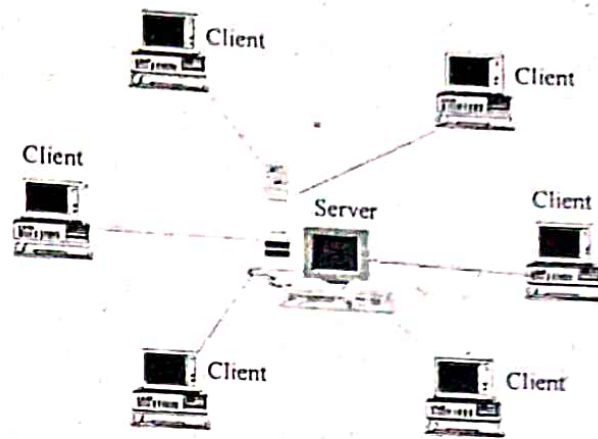
The client-server model describes how a server provides resources and services to one or more clients. Examples of servers include web servers, mail servers, and file servers. Each of these servers provides resources to client devices, such as desktop computers, laptops, tablets, and smart phones. Most servers have a one-to-many relationship with clients, meaning a single server can provide resources to multiple clients at one time.

When a client requests a connection to a server, the server can either accept or reject the connection. If the connection is accepted, the server establishes and maintains a connection with the client over a specific protocol. For example, an email client may request an SMTP connection to a mail server in order to send a message. The SMTP application on the mail server will then request authentication from the client, such as the email address and password. If these credentials match an account on the mail server, the server will send the email to the intended recipient.

Online multiplayer gaming also uses the client-server model. One example is Blizzard's Battle.net service, which hosts online games for World of Warcraft, StarCraft, Overwatch, and others. When players open a Blizzard application, the game client automatically connects to a Battle.net server. Once players log in to Battle.net, they can see who else is online, chat with other players, and play matches with or against other gamers.

While Internet servers typically provide connections to multiple clients at a time, each physical machine can only handle so much traffic. Therefore, popular online services distribute clients across multiple physical servers, using a technique called distributed computing. In most cases, it does not matter which specific machine users are connected to, since the servers all provide the same service.





Client-Server Model

**Web based e-mail:** Webmail are web-based email accounts. These are usually free email accounts that are operated from a website. Examples include Hotmail, GMail and Yahoo Mail.

Webmail allows the users to access their emails as long as they have access to an Internet connection and a web browser. This also means that the user cannot read an old email or draft a new email offline.

**9. Distinguish between Amplitude modulation and Frequency modulation. What is the difference between Single mode and Multimode fibres? [WBUT 2017]**

**Answer:**

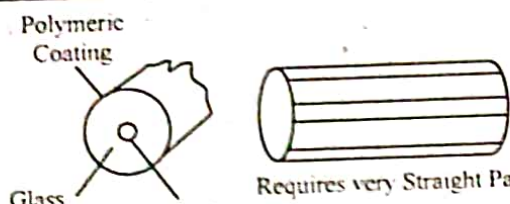
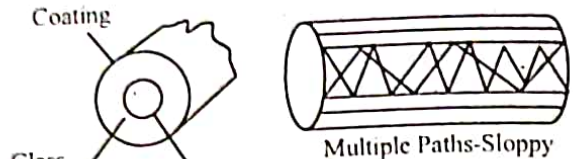
**1<sup>st</sup> part:**

Amplitude Modulation	Frequency Modulation
In AM, a radio wave known as the "carrier" or "carrier wave" is modulated in amplitude by the signal that is to be transmitted. The frequency and phase remain the same.	In FM, a radio wave known as the "carrier" or "carrier wave" is modulated in frequency by the signal that is to be transmitted. The amplitude and phase remain the same.
AM radio ranges from 535 to 1705 KHz (OR) Up to 1200 bits per second.	FM radio ranges in a higher spectrum from 88 to 108 MHz. (OR) 1200 to 2400 bits per second.
AM stands for Amplitude Modulation	FM stands for Frequency Modulation
AM has poorer sound quality compared with FM, but is cheaper and can be transmitted over long distances. It has a lower bandwidth so it can have more stations available in any frequency range.	FM is less prone to interference than AM. However, FM signals are impacted by physical barriers. FM has better sound quality due to higher bandwidth.



**POPULAR PUBLICATIONS**

2<sup>nd</sup> part:

Single mode	Multimode
 <p>Polymeric Coating</p> <p>Glass Cladding 125 Microns d/a</p> <p>Glass Core = 5.8 Microns</p> <p>Requires very Straight Paths</p>	 <p>Coating</p> <p>Glass Cladding 125 Microns d/a</p> <p>Glass Core = 60 Microns</p> <p>Multiple Paths-Sloppy</p>
<ul style="list-style-type: none"> <li>• Small Core</li> <li>• Less Dispersion</li> <li>• Suited for Long- Distance Applications (Upto ~ 3km)</li> <li>• Uses Lasers as the Light Source Often within Campus Backbones for Distances of several Thousand meters</li> </ul>	<ul style="list-style-type: none"> <li>• Larger Core than Single-Mode Cable (50 microns or greater)</li> <li>• Allows Greater Dispersion and therefore, Loss of Signal</li> <li>• Used for Long-Distance Application, but shorter than Single-Mode (Upto ~2km)</li> <li>• Uses LEDs as the Light Source Often within LANs or Distances of a Couple Hundred Meters with a Campus Network</li> </ul>

**Long Answer Type Questions**

1. a) Briefly discuss about the different guided media that are used in computer networks and make a comparison among them. [WBUT 2014, 2016]

**Answer:**

There are four basic types of Guided Media:

- Open Wire
- Twisted Pair
- Coaxial Cable
- Optical Fiber

**Open Wire**

Open Wire is traditionally used to describe the electrical wire strung along power poles. There is a single wire strung between poles. No shielding or protection from noise interference is used. This media is susceptible to a large degree of noise and interference and consequently not acceptable for data transmission except for short distances under 20 ft.

**Twisted Pair**

The wires in Twisted Pair cabling are twisted together in pairs. Each pair would consist of a wire used for the positive data signal and a wire used for the negative data signal. Any noise that appears on one wire of the pair would occur on the other wire. Because the wires are opposite polarities, they are 180 degrees out of phase and the noise

appearing on the wires cancels itself out. Twisted Pair cables are most effectively used in systems that use a balanced line method of transmission. The degree of reduction in noise interference is determined specifically by the number of turns per foot. Increasing the number of turns per foot reduces the noise interference. To further improve noise rejection, a foil or wire braid shield is woven around the twisted pairs.

**Coaxial Cable**

Coaxial Cable consists of two conductors. The inner conductor is held inside an insulator with the other conductor woven around it providing a shield. An insulating protective coating called a jacket covers the outer conductor. The outer shield protects the inner conductor from outside electrical signals. The distance between the outer conductor (shield) and inner conductor plus the type of material used for insulating the inner conductor determine the cable properties or impedance. Typical impedances for coaxial cables are 75 ohms for Cable TV, 50 ohms for Ethernet Thinnet and Thicknet. The excellent control of the impedance characteristics of the cable allows higher data rates to be transferred than Twisted Pair cable.

**Optical Fibre**

Optical Fibre consists of thin glass fibres that can carry information at frequencies in the visible light spectrum and beyond. The typical optical fibre consists of a very narrow strand of glass called the Core. Around the Core is a concentric layer of glass called the Cladding. A typical Core diameter is 62.5 microns (1 micron = 10<sup>-6</sup> meters). Typically Cladding has a diameter of 125 microns. Coating the cladding is a protective coating consisting of plastic, it is called the Jacket. Data is transmitted as light waves which undergo continuous total internal reflection.

The cost of optical fibre is a trade-off between capacity and cost. At higher transmission capacity, it is cheaper than copper. At lower transmission capacity, it is more expensive.

Topic	Twisted Pair	Co-Axial Cable	Optical Fiber
Number of Cable	One pair of cables are required	Single cable is required	Single Cable is required
Medium	Electrical medium is used	Electrical medium is used	Illumination medium is used
Noise	Noise immunity is low	Noise immunity is moderate.	Noise immunity is high
Speed	Communication speed is low, nearly 4 Mbps	Communication speed is moderate, nearly 500 Mbps	Communication speed is high, nearly 2 Gbps
Bandwidth	Low Bandwidth, 3 MHz	Comparatively high bandwidth, 350MHz	Very High bandwidth, 2 GHz
Distance	Cover small distance, 2 to 10 km	Cover small distance, 1 to 10 km	Cover large distance, 10 to 100km
Usage	Used in LAN, T1 Lines	Used in Cable TV, Ethernet Channel	Used in WAN,MAN etc.



## POPULAR PUBLICATIONS

[WBUT 2014]

b) What is OSI reference model?

**Answer:**

The Open Systems Interconnection Reference Model (OSI Model or OSI Reference Model for short) is a layered abstract description for communications and computer network protocol design, developed as part of the Open Systems Interconnection initiative. It is also called the OSI seven layer model.

The OSI model divides the functions of a protocol into a series of seven layers (listed as decreasing "distance" from the application software):

1. Physical Layer
2. Data Link Layer
3. Network Layer
4. Transport Layer
5. Session Layer
6. Presentation Layer
7. Application Layer

c) Write down the similarities and differences between OSI and TCP/IP model.

[WBUT 2014]

OR,

What are the differences of OSI reference model from TCP/IP reference model?

[WBUT 2015]

**Answer:**

Below we describe similarities and differences between the OSI and TCP/IP models.

### *Similarities*

The main similarities between the two models include the following:

- They share similar architecture – Both of the models share a similar architecture. This can be illustrated by the fact that both of them are constructed with layers.
- They share a common application layer – Both of the models share a common "application layer". However in practice this layer includes different services depending upon each model.
- Both models have comparable transport and network layers – This can be illustrated by the fact that whatever functions are performed between the presentation and network layer of the OSI model similar functions are performed at the Transport layer of the TCP/IP model.
- Knowledge of the both models is required by networking professionals – According to article obtained from the internet networking professionals "need to know both models".
- Both models assume that packets are switched – Basically this means that individual packets may take differing paths in order to reach the same destination.

### *Differences*

The main differences between the two models are as follows:

- TCP/IP Protocols are considered to be standards around which the internet has developed. The OSI model however is a "generic, protocol-independent standard".



- TCP/IP combines the presentation and session layer issues into its application layer.
- TCP/IP combines the OSI data link and physical layers into the network access layer.
- TCP/IP appears to be a more simpler model and this is mainly due to the fact that it has fewer layers.
- TCP/IP is considered to be a more credible model- This is mainly due to the fact because TCP/IP protocols are the standards around which the internet was developed therefore it mainly gains creditability due to this reason. Where as in contrast networks are not usually built around the OSI model as it is merely used as a guidance tool.
- The OSI model consists of 7 architectural layers whereas the TCP/IP only has 4 layers.

**2. Discuss in detail about OSI reference model mentioning the functions performed by each layer in it. [WBUT 2015]**

**Answer:**

The Open Systems Interconnection Reference Model (OSI Model or OSI Reference Model for short) is a layered abstract description for communications and computer network protocol design, developed as part of the Open Systems Interconnection initiative. It is also called the OSI seven layer model.

The OSI model divides the functions of a protocol into a series of seven layers (listed as decreasing "distance" from the application software):

**Physical (Layer 1)**

OSI Model, Layer 1 conveys the bit stream - electrical impulse, light or radio signal — through the network at the electrical and mechanical level. It provides the hardware means of sending and receiving data on a carrier, including defining cables, cards and physical aspects. Fast Ethernet, RS232, and ATM are protocols with physical layer components.

**Data Link (Layer 2)**

At OSI Model, Layer 2, data packets are encoded and decoded into bits. It furnishes transmission protocol knowledge and management and handles errors in the physical layer, flow control and frame synchronization. The data link layer is divided into two sub layers: The Media Access Control (MAC) layer and the Logical Link Control (LLC) layer. The MAC sub layer controls how a computer on the network gains access to the data and permission to transmit it. The LLC layer controls frame synchronization, flow control and error checking.

**Network (Layer 3)**

Layer 3 provides switching and routing technologies, creating logical paths, known as virtual circuits, for transmitting data from node to node. Routing and forwarding are functions of this layer, as well as addressing, internetworking, error handling, congestion control and packet sequencing.

Layer 3 Network examples include AppleTalk DDP, IP, IPX.

## POPULAR PUBLICATIONS

### **Transport (Layer 4)**

OSI Model, Layer 4, provides transparent transfer of data between end systems, or hosts, and is responsible for end-to-end error recovery and flow control. It ensures complete data transfer.

Layer 4 Transport examples include SPX, TCP, UDP.

### **Session (Layer 5)**

This layer establishes, manages and terminates connections between applications. The session layer sets up, coordinates, and terminates conversations, exchanges, and dialogues between the applications at each end. It deals with session and connection coordination.

Layer 5 Session examples include NFS, NetBios names, RPC, SQL.

### **Presentation (Layer 6)**

This layer provides independence from differences in data representation (e.g., encryption) by translating from application to network format, and vice versa. The presentation layer works to transform data into the form that the application layer can accept. This layer formats and encrypts data to be sent across a network, providing freedom from compatibility problems. It is sometimes called the syntax layer.

Layer 6 Presentation examples include encryption, ASCII, EBCDIC, TIFF, GIF, PICT, JPEG, MPEG, MIDI.

### **Application (Layer 7)**

OSI Model, Layer 7, supports application and end-user processes. Communication partners are identified, quality of service is identified, user authentication and privacy are considered, and any constraints on data syntax are identified. Everything at this layer is application-specific. This layer provides application services for file transfers, e-mail, and other network software services. Telnet and FTP are applications that exist entirely in the application level. Tiered application architectures are part of this layer.

3. a) What are the directions of data flow? Explain with suitable examples.
- b) How do we measure the performance of a computer network? Explain.
- c) Discuss in detail different topologies for computer networks.
- d) What is throughput?
- e) Differentiate between internet, intranet and extranet.

[WBUT 2015]

Answer:

a) Network devices use three transmission modes (methods) to exchange data, *simplex*, *half duplex*, and *full duplex*.

- **Simplex transmission** is like a one-way street where traffic moves in only one direction. Simplex mode is a one-way-only transmission, which means that data can flow only in one direction from the sending device to the receiving device. Figure 1-7 illustrates simplex transmission.
- **Half-duplex transmission** is like the center lane on some three-lane roads. It is a single lane in which traffic can move in one direction or the other, but not in both



directions at the same time. Half-duplex mode limits data transmission because each device must take turns using the line. Therefore, data can flow from A to B and from B to A, but not at the same time. Figure 1-8 illustrates half-duplex transmission.

- **Full-duplex transmission** is like a major highway with two lanes of traffic, each lane accommodating traffic going in opposite directions. Full-duplex mode accommodates two-way simultaneous transmission, which means that both sides can send and receive at the same time. In full-duplex mode, data can flow from A to B and B to A at the same time. Figure 1-9 illustrates full-duplex transmission.

b) Measures of computer network performance are commonly stated in units of bits per second (bps). This quantity can represent either an actual data rate or a theoretical limit to available network bandwidth.

Modern networks support very large numbers of bits per second. Instead of quoting 10,000 or 100,000 bps, networks normally express these quantities in terms of kilobits, megabits and gigabits.

The following equations illustrate the mathematics behind these terms:

- 1 Kbps = 1 kbps = 1 kilobit per second = 1,000 bits per second
- 1 Mbps = 1,000 Kbps
- 1 Gbps = 1,000 Mbps

Technically, network speed can also be expressed in units of bytes per second, abbreviated as "Bps" with a capital 'B'.

Use of these quantities is strongly discouraged in networking to avoid confusion with the bits per second standard:

- 1 KBps = 1 kBps = 1 kilobyte per second = 8,000 bits per second = 8 Kbps

Finally, the conventions used for measuring the capacity of computer disks and memory might appear similar at first to those for networks.

Data storage capacity is normally measured in units of kilobytes, megabytes and gigabytes. In this non-network style of usage, 'K' represents a multiplier of 1,024 and 'k' represents a multiplier of 1,000 units of capacity.

The following equations define the mathematics behind these terms:

- 1 KB = 1,024 bytes
- 1 kB = 1,000 bytes
- 1 MB = 1,024 KB
- 1 GB = 1,024 MB

c) Below five devices arranged in different network topology

i) **Mesh**



Number of cable = 10

Each node is connected through a four cable. If one connection fails, the entire system does not halt.



## POPULAR PUBLICATIONS

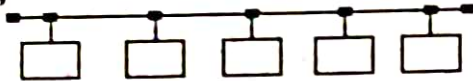
ii) *Star*



Number of cable = 4

If one connection fails all other links remains active.

iii) *Bus*



Number of cable = 1

If the connection fails, the entire network goes down.

iv) *Ring*



Number of cable = 5

If one connection fails, the ring can disable the entire network.

d) Throughput is a measure of how many units of information a system can process in a given amount of time. It is applied broadly to systems ranging from various aspects of computer and network systems to organizations. Related measures of system productivity include, the speed with which some specific workload can be completed, and response time, the amount of time between a single interactive user request and receipt of the response.

e) The Internet is a network of LAN-s that uses the IP protocol at the network layer and covers the entire world. The Intranet is similar, i.e., it is also a network of networks driven by the IP protocol. However, all the networks of the Intranet belong to the same organization.

An extranet is a private network that uses Internet technology and the public telecommunication system to securely share part of a business's information or operations with suppliers, vendors, partners, customers, or other businesses.

4. Explain TCP/IP and ADSL.

[WBUT 2017]

Answer:

1<sup>st</sup> Part:

**TCP/IP:** TCP/IP means Transmission Control Protocol and Internet Protocol. It is the network model used in the current Internet architecture as well. Protocols are set of rules which govern every possible communication over a network. These protocols describe the movement of data between the source and destination or the internet. They also offer

simple naming and addressing schemes. It contains four layers, unlike seven layers in the OSI model. The layers are:

1. Process/Application Layer
2. Host-to-Host/Transport Layer
3. Internet Layer
4. Network Access/Link Layer

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

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

**Layer 1: Network Access Layer**

1. Lowest layer of the all.
2. Protocol is used to connect to the host, so that the packets can be sent over it.
3. Varies from host to host and network to network.

**Layer 2: Internet layer**

1. Selection of a packet switching network which is based on a connectionless internetwork layer is called a internet layer.
2. It is the layer which holds the whole architecture together.
3. It helps the packet to travel independently to the destination.
4. Order in which packets are received is different from the way they are sent.
5. IP (Internet Protocol) is used in this layer.
6. The various functions performed by the Internet Layer are:
  - o Delivering IP packets
  - o Performing routing
  - o Avoiding congestion

**Layer 3: Transport Layer**

1. It decides if data transmission should be on parallel path or single path.
2. Functions such as multiplexing, segmenting or splitting on the data is done by transport layer.
3. The applications can read and write to the transport layer.
4. Transport layer adds header information to the data.
5. Transport layer breaks the message (data) into small units so that they are handled more efficiently by the network layer.
6. Transport layer also arrange the packets to be sent, in sequence.

**Layer 4: Application Layer**

The TCP/IP specifications described a lot of applications that were at the top of the protocol stack. Some of them were TELNET, FTP, SMTP, DNS etc.



## POPULAR PUBLICATIONS

1. TELNET is a two-way communication protocol which allows connecting to a remote machine and run applications on it.
2. FTP (File Transfer Protocol) is a protocol that allows File transfer amongst computer users connected over a network. It is reliable, simple and efficient.
3. SMTP (Simple Mail Transport Protocol) is a protocol, which is used to transport electronic mail between a source and destination, directed via a route.
4. DNS (Domain Name Server) resolves an IP address into a textual address for Hosts connected over a network.
5. It allows peer entities to carry conversation.
6. It defines two end-to-end protocols: TCP and UDP
  - o TCP (Transmission Control Protocol): It is a reliable connection-oriented protocol which handles byte-stream from source to destination without error and flow control.
  - o UDP (User-Datagram Protocol): It is an unreliable connection-less protocol that does not want TCPs, sequencing and flow control. E.g.: One-shot request-reply kind of service.

### **2<sup>nd</sup> Part:**

#### **ADSL:**

*Asymmetric digital subscriber line* (ADSL) is a type of DSL broadband Communications technology used for connecting to the Internet. ADSL allows more data to be sent over existing copper telephone lines (POTS), when compared to traditional modem lines. A special filter, called a microfilter, is installed on a subscriber's telephone line to allow both ADSL and regular voice (telephone) services to be used at the same time. ADSL requires a special ADSL modem and subscribers must be in close geographical locations to the provider's central office to receive ADSL service. Typically this distance is within a radius of 2 to 2.5 miles. ADSL supports data rates of from 1.5 to 9 Mbps when receiving data (known as the downstream rate) and from 16 to 640 Kbps when sending data (known as the upstream rate).

5. List the layers of TCP model. Describe the function of each of the Layers with necessary diagram. How does the layer of TCP correlate with the OSI model?  
[WBUT 2017]

**Answer:**

*Refer to Question No. 4(1<sup>st</sup> Part) of Long Answer Type Questions.*

6. Write short notes on the following:

- a) Circuit Switching
- b) QAM
- c) Twisted Pair Cables

[WBUT 2013]  
[WBUT 2015]  
[WBUT 2015]

**Answer:**

- a) **Circuit Switching:**

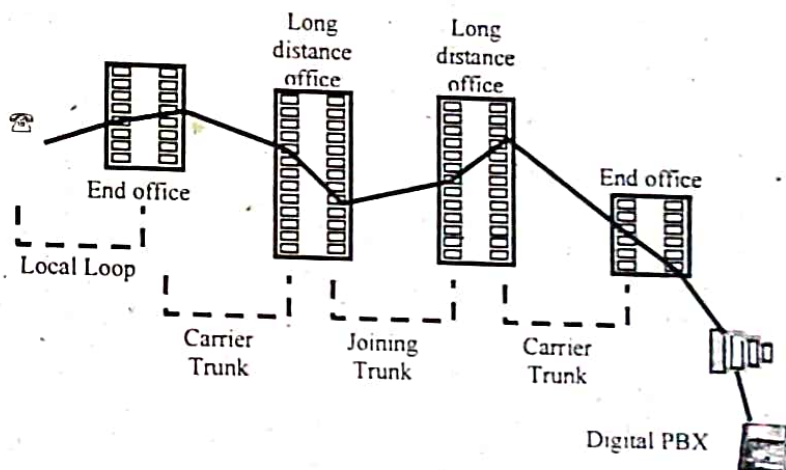
When we or our computer places a telephone call, the switching equipment within the telephone system seeks out a physical "copper" (including fibre and radio) path all the



way from our telephone to the receiver's telephone. This technique is called circuit switching and is shown schematically in Fig (a). Each of the six rectangles represents a carrier switching office (end office, toll office, etc.) In this example, each office has three incoming lines and three outgoing lines. When a call passes through a switching office, a physical connection is (conceptually) established between the line on which the call came in and one of the output lines, as shown by the dotted lines.

The model shown in the figure is highly simplified of course, because parts of the "copper" path between the two telephones may, in fact, be microwave links onto which thousands of calls are multiplexed. Nevertheless, the basic idea is valid: once a call has been set up, a dedicated path between both ends exists and will continue to exist until the call is finished.

An important property of circuit switching is the need to set up an end-to-end path before any data can be sent. The elapsed time between the end of dialing and the start of ringing interval, the telephone system is hunting for a copper path, as shown in fig. Note that before data transmission can even begin, the call request signal must propagate all the way to the destination, and be acknowledged. For many computer applications (e.g. point-of-sale credit verification), long setup times are undesirable.



Example of Connection Over a Public Circuit Switching Network

#### b) Quadrature Amplitude Modulation:

Quadrature Amplitude Modulation or QAM is a form of modulation which is widely used for modulating data signals onto a carrier used for radio communications. It is widely used because it offers advantages over other forms of data modulation such as PSK, although many forms of data modulation operate alongside each other.

Quadrature Amplitude Modulation, QAM is a signal in which two carriers shifted in phase by 90 degrees are modulated and the resultant output consists of both amplitude and phase variations. In view of the fact that both amplitude and phase variations are present it may also be considered as a mixture of amplitude and phase modulation.

A motivation for the use of quadrature amplitude modulation comes from the fact that a straight amplitude modulated signal, i.e. double sideband even with a suppressed carrier

## POPULAR PUBLICATIONS

occupies twice the bandwidth of the modulating signal. This is very wasteful of the available frequency spectrum. QAM restores the balance by placing two independent double sideband suppressed carrier signals in the same spectrum as one ordinary double sideband suppressed carrier signal.

### c) Twisted Pair Cables:

*Refer to Question No. 1(a) of Long Answer Type Questions.*

7. a) What is the purpose of Guard Bands?

[MODEL QUESTION]

b) What is the relationship between FDM and WDM?

c) In FDM, suppose there are 3 signal sources each having bandwidth 300 MHz, find the minimum bandwidth of the path if 10 MHz guard bands are used.

d) What is the drawback of synchronous TDM that leads to the concept of asynchronous TDM?

e) Explain bit stuffing and interleaving in TDM.

**Answer:**

a) Guard band is a narrow part of the radio spectrum between radio bands, for the purpose of preventing interference.

It is a narrow frequency range used to separate two wider frequency ranges to ensure that both can transmit simultaneously without interfering each other. It is used in TDM/TDMA/FDM/FDMA. It may be used in both wired and wireless communications, so that adjacent frequency bands on the same media can avoid interference.

b) fdm: total frequency bands are divided into several users

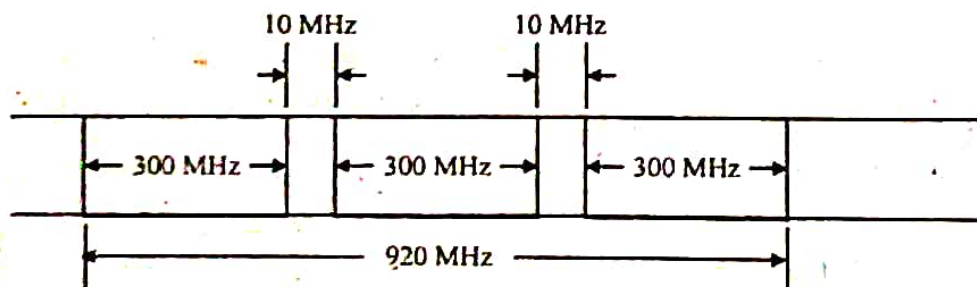
e.g.: television broad casting

wdm: total wave length is divided in to number of users

e.g.: optical networking

c) For 3 signals we require at least 2 guard bands.

$\therefore$  maximum bandwidth =  $3 \times 300 + 2 \times 10 = 920$  MHz.



### d) Disadvantages:

One drawback of the TDM approach, as discussed earlier, is that many of the time slot in the frame are wasted. It is because, if a particular terminal has no data to transmit at particular instant of time, an empty time slot will be transmitted. An efficient alternative to this synchronous TDM is statistical TDM, also known as asynchronous TDM. It dynamically allocates the time slots on demand to separate input channels, thus saving



the channel capacity. As with Synchronous TDM, statistical multiplexers also have many I/O lines with a buffer associated to each of them. During the input, the multiplexer scans the input buffers, collecting data until the frame is filled and send the frame. At the receiving end, the demultiplexer receives the frame and distributes the data to the appropriate buffers.

e) Inserting bits in data in order to break up a bit pattern that may cause the transmission to go out of synchronization. For example, in T1 lines, timing is maintained by detecting a change from 0 to 1. If too many zero bits are transmitted consecutively, the receiving end may lose synchronization because too much time has passed without sensing voltage. Therefore, in long strings of zeros, a set of bits that begins with a 1 and functions as a timing signal is "stuffed" into the stream of zeros at certain intervals.

## PHYSICAL LEVEL

### Multiple Choice Type Questions

1. PPP is a ..... Oriented protocol. [WBUT 2013]  
a) phase b) bit c) byte d) none of these  
Answer: (c)
2. What network topology implements at least two paths to and from each node? [WBUT 2014]  
a) bus b) ring c) mesh d) star  
Answer: (b)
3. In this topology there is a central controller or hub [WBUT 2015]  
a) star b) mesh c) ring d) bus  
Answer: (a)
4. The topology with highest reliability is [WBUT 2017]  
a) bus topology b) star topology c) ring topology d) mesh topology  
Answer: (d)
5. Protocols are [WBUT 2017]  
a) agreement on how communication components and DTEs are to communicate  
b) logical communication channels used for transferring data  
c) physical communication channels used for transferring data  
d) none of these  
Answer: (a)

### Short Answer Type Questions

1. What is transmission impairment? How many types of transmission impairments are three? Discuss them. [WBUT 2013]

OR,

Discuss about the different types of transmission impairments. [WBUT 2015]

Answer:

Transmission Impairments is a condition that causes information to be lost in a signal. The following are some aspects of transmission impairments: (1) Attenuation. Signals loose power in time. (2) Dispersion. Signals tend to spread as they travel, with the amount of spreading dependent on the frequency. (3) Delay distortion. Due to velocity of propagation that varies with frequency. Thus, various frequency components of a signal arrive at the receiver at different times. (4) Noise; sources from Thermal, Intermodulation, Crosstalk.



2. We have a channel with a 1MHz bandwidth. The SNR for the channel is 63. What is the bit rate and signal level? [WBUT 2015]

Answer:

First, we use the Shannon formula to find the upper limit.

$$C = B \log_2 (1 + \text{SNR}) = 10^6 \log_2 (1 + 63) = 10^6 \log_2 64 = 6 \text{ Mbps}$$

The Shannon formula gives us 6 Mbps, the upper limit. For better performance we choose something lower, 4 Mbps, for example. Then we use the Nyquist formula to find the number of signal levels.

$$4 \text{ Mbps} = 2 \times 1 \text{ MHz} \times \log_2 L \Rightarrow L = 4$$

3. Write down the advantages and disadvantages of mesh topology. [WBUT 2016]

Answer:

**Advantages of mesh:** Since every end station is connected to every other directly, the communication path between any pair is dedicated and unhampered by the traffic in the rest of the network.

**Disadvantage:** Requires much more cabling. Also, fallback strategies when a link goes down, is not very well-defined.

4. What are the drawbacks of mesh topology? [WBUT 2017]

Answer:

*Refer to Question No. 3(2<sup>nd</sup> Part) of Short Answer Type Questions.*

5. Differentiate circuit switching and packet switching. [MODEL QUESTION]

Answer:

Circuit switching	Packet switching
Circuit switching establishes fixed bandwidth circuit/channel between nodes and terminals before the users may communicate	Packet switching is a communication in which packet are routed between node over data links shared with other traffic. In each network node, packets are queued in buffered, resulting in variable delay.

6. Why circuit switching is preferred over packet switching in case of real time communication? [MODEL QUESTION]

Answer:

Circuit switching is faster than packet switching since during communication, the channel always remains established. Because of this, there is no overhead in circuit switching to either packetize data or use other means to guarantee delivery of the data. In circuit-switching, the data bits arrive at the receiver in the same order they were transmitted. The same can not be assured in packet switching. This leads to more computation in packet switching for re-arranging received packets to get back the transmitted stream.

While packet switching can not overcome the speed disadvantage, it can overcome the "guaranteed delivery" and "in-order" delivery of data using protocols. Several protocol

## POPULAR PUBLICATIONS

features like sequencing numbering and ACK mechanisms using sliding windows protocols at different layers (mostly used in transport and data-link layers) can be used to ensure guaranteed in-order deliver. For example, TCP achieves this using a complicated protocol.

### **Long Answer Type Questions**

[MODEL QUESTION]

1. a) What is composite signal?
- b) We measure decibel in logarithmic forms. What is the actual reason behind this?
- c) Suppose transmission channels become virtually error-free. Is the data link layer still needed? Explain.

**Answer:**

a) A Composite Signal is a signal which actually carries multiple other signals that are often related to each other. On the most common examples of a composite signal is the "composite video" signal that is fed to an analog television set. Composite video is usually available in standard formats such as NTSC, PAL, and SECAM. It is a composite of three source signals called Y, U and V (together referred to as YUV) with sync pulses. Y represents the brightness or luminance of the picture and includes synchronizing pulses, so that by itself it could be displayed as a monochrome picture. U and V represent hue and saturation or chrominance.

b) The decibel (dB) is a logarithmic unit of measurement that expresses the magnitude of a physical quantity (usually power or intensity) relative to a specified or implied reference level. Since it expresses a ratio of two quantities with the same unit, it is a dimensionless unit.

***The use of the decibel has a number of merits:***

The decibel's logarithmic nature means that a very large range of ratios can be represented by a convenient number, in a similar manner to scientific notation. This allows one to clearly visualize huge changes of some quantity.

The mathematical properties of logarithms mean that the overall decibel gain of a multi-component system (such as consecutive amplifiers) can be calculated simply by summing the decibel gains of the individual components, rather than needing to multiply amplification factors.

The human perception of, for example, sound or light, is, roughly speaking, such that a doubling of actual intensity causes perceived intensity to always increase by the same amount, irrespective of the original level. The decibel's logarithmic scale, in which a doubling of power or intensity always causes an increase of approximately 3 dB, corresponds to this perception.

c) Even if the transmission channels become error free, there would still be a need for the data link layer. The data link layer is responsible for breaking up the data it receives from a higher layer into frames and decide upon the most appropriate time to put such a frame on the network through the physical layer. Address management of network interfaces is



also the responsibility of the data link layer. In other words, the absence of errors in the network possibly does away with the LLC functionality but the MAC layer responsibilities remain. Without the MAC layer functionalities, the network layer cannot become independent of the physical nature of the transmission medium. For example, without a data link layer, an IP layer for Ethernet (CSMA/CD protocol) would be different from the IP layer for WLAN (CSMA/CA).

**2. Distinguish among the working principles of circuit switching, message switching and packet switching techniques.** [MODEL QUESTION]

**Answer:**

Different types of switching techniques are employed to provide communication between two computers. These are: Circuit switching, message switching and packet switching.

**Circuit Switching:** In this technique, first the complete physical connection between two computers is established and then data are transmitted from the source computer to the destination computer. That is, when a computer places a telephone call, the switching equipment within the telephone system seeks out a physical copper path all the way from sender telephone to the receiver's telephone. The important property of this switching technique is to setup an end-to-end path (connection) between computer before any data can be sent.

**Message Switching:** In this technique, the source computer sends data or the message to the switching office first, which stores the data in its buffer. It then looks for a free link to another switching office and then sends the data to this office. This process is continued until the data are delivered to the destination computers. Owing to its working principle, it is also known as store and forward. That is, store first (in switching office), forward later, one jump at a time.

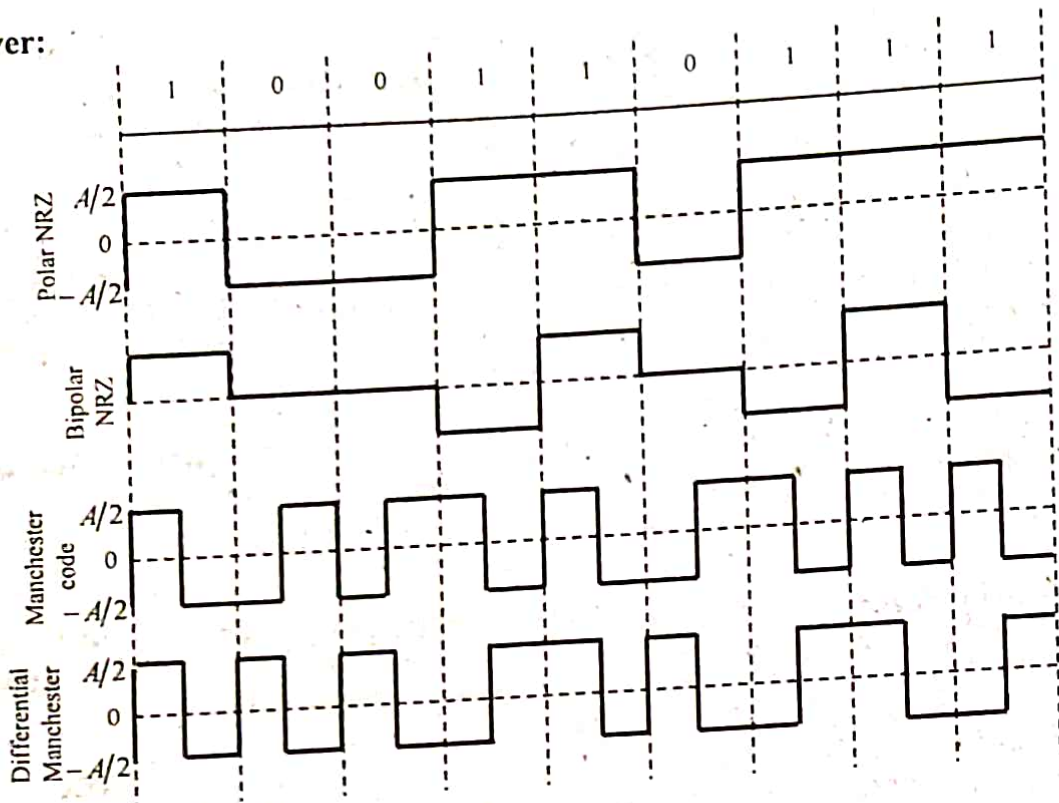
**Packet Switching:** With message switching, there is no limit on block size, in contrast, packet switching places a tight upper limit on block size. A fixed size of packet which can be transmitted across the network is specified. Another point of its difference from message switching is that data packets are stored on the disk in message switching whereas in packet switching, all the packets of fixed size are stored in main memory. This improves the performance as the access time (time taken to access a data packet) is reduced, thus, the throughput (measure of performance) of the network is improved.

**3. a) Find the NRZ-I, Manchester and Differential Manchester encoding for the binary Data 100110111.**

**b) Suppose that a signal has  $2^n$  times the power as a noise signal that is added to it. Find the SNR (Signal to Noise Ratio) in decibels.** [MODEL QUESTION]

Answer:

a)



b)  $SNR = 10 \log_{10} 2^n = 10n \log_{10} 2 = 3.01n \text{ dB}$



# DATA LINK LAYER

## Multiple Choice Type Questions

1. Flow control in OSI reference model is performed in  
 a) data link layer  
 c) session layer  
 b) network layer  
 d) application layer  
 Answer: (a) [WBUT 2013]
2. Checksum is used for  
 a) error detection  
 c) error encapsulation  
 b) error correction  
 d) both (a) and (b)  
 Answer: (a) [WBUT 2013, 2016]
3. Which channel access method is used in IEEE 802.5 network?  
 a) CSMA/CD      b) token bus  
 c) token ring  
 d) all of these  
 Answer: (b) [WBUT 2014]
4. The hamming code is used for  
 a) error detection  
 c) error encapsulation  
 b) error correction  
 d) both (a) and (b)  
 Answer: (d) [WBUT 2014]
5. Which channel access method is used in Ethernet network?  
 a) CSMA/CD      b) token bus  
 c) token ring  
 d) all of these  
 Answer: (a) [WBUT 2014, 2016]
6. Which one of the following task is not done by data link layer?  
 a) framing      b) error control  
 c) flow control      d) channel coding  
 Answer: (d) [WBUT 2015]
7. Flow control is the responsibilities of the  
 a) Data link layer  
 c) Both of these  
 b) Transport layer  
 d) none of these  
 Answer: (c) [WBUT 2016]
8. For stop-and-wait flow control, for  $n$  data packets sent, how many acknowledgements are needed?  
 a)  $n$       b)  $2n$       c)  $n-1$       d)  $n+1$   
 Answer: (a) [WBUT 2017]

## Short Answer Type Questions

1. What is the minimum window size required for selective-repeat ARQ protocol and how?  
 [WBUT 2013]

## POPULAR PUBLICATIONS

**Answer:**

The size of the sending and receiving windows must be equal and half the maximum sequence number (assuming that sequence numbers are numbered from 0 to  $n-1$ ) to avoid miscommunication in all cases of packets being dropped. To understand this, consider the case when all ACKs are destroyed.

If the receiving window is larger than half the maximum sequence number, some, possibly even all, of the packages that are resent after timeouts are duplicates that are not recognized as such. The sender moves its window for every packet that is acknowledged.

**2. What do you mean by Data transparency? What is Bit stuffing in HDLC? Why bit stuffing is needed?** [WBUT 2013, 2016, 2017]

**Answer:**

**1<sup>st</sup> Part:**

The data transfer rate (DTR) is the amount of digital data that is moved from one place to another in a given time.

**2<sup>nd</sup> & 3<sup>rd</sup> Part:**

HDLC frames can be transmitted over synchronous or asynchronous links. Those links have no mechanism to mark the beginning or end of a frame, so the beginning and end of each frame has to be identified. This is done by using a frame delimiter, or flag, which is a unique sequence of bits that is guaranteed not to be seen inside a frame. This sequence is '01111110', or, in hexadecimal notation, 7E. Each frame begins and ends with a frame delimiter. A frame delimiter at the end of a frame may also mark the start of the next frame. A sequence of 7 or more consecutive 1-bits within a frame will cause the frame to be aborted.

**3. Applying CRC algorithm, determine the check sum and the transmitted frame for the bit stream 11010111 and for the generator polynomial  $x^3 + x^2 + 1$ . [WBUT 2013]**

**Answer:**

Frame: 11010111

Generator  $G(x)$  of degree 3,  $x^3 + x^2 + 1$ : 1101

$T(x)$  is the frame with 3 attached 0-bits: 11010111000

Divide  $T(x)$  by  $G(x)$  by using XOR,

1101 | 11010111000 | 1000010

1101  
0000

01110

1101

000110 → Remainder

The remainder  $R(x) = 110$ . The Transferred frame: 11010111 110



4. A 12 bit data bit block 011101010111 is to be set using hamming code for error detection and correction. Show how the receiver corrects an error that occurs in 6<sup>th</sup> bit position from right. [WBUT 2013]

Answer:

We need 5 parity bits of positions 1, 2, 4, 8 and 16 from the left — the left most position being 1. Thus we have  $P_1P_20P_3111P_40101011P_51$ .

So,  $P_1 = 0 \oplus 1 \oplus 1 \oplus 0 \oplus 0 \oplus 0 \oplus 0 \oplus 1 \oplus 1 = 0$  (i.e., Ex-or of bits 3, 5, 7, 9, 11, 13, 15 and 17)

$P_2 = 0 \oplus 1 \oplus 1 \oplus 1 \oplus 0 \oplus 1 \oplus 1 = 1$  (i.e. Ex-or of bits 3, 6, 7, 10, 11, 14 and 15)

$P_3 = 1 \oplus 1 \oplus 1 \oplus 1 \oplus 0 \oplus 1 \oplus 1 = 0$  (Ex-or of bits 5, 6, 7, 12, 13, 14 and 15)

$P_4 = 0 \oplus 1 \oplus 0 \oplus 1 \oplus 0 \oplus 1 \oplus 1 = 0$  (Ex-or of bits 9, 10, 11, 12, 13, 14 and 15)

$P_5 = 1$  (Bit 17)

So, transmitted code is 0100111001010111

If Sixth bit from right has error, the received data is 0100111001000111

In receiver, we calculate  $P_1 - P_4$  again try calculating the parity as in the transmitter side and the ex-or with the received parity bit.

$$P_1 = 0$$

$$P_2 = 0$$

$$P_3 = 1$$

$$P_4 = 1$$

$$P_5 = 0$$

This gives  $01100_2 = 12$  -the position from left as the position of this erroneous bit. So, the received data can be corrected to 010011100101111, which is the same as the transmitted code. Stripping off the parity bits, we get the transmitted data word.

5. What is the difference between Flow Control & Error Control. [WBUT 2016]

Answer:

Flow control and Error control are the control mechanism at data link layer and transport layer. Whenever the sends the data to the receiver these two mechanisms helps in proper delivering of the reliable data to the receiver. The main difference between the flow control and error control is that the flow control observes the proper flow of the data from sender to receiver, on the other hand, the error control observes that the data delivered to the receiver is error free and reliable. Let's study the difference between Flow control and Error control with a comparison chart.

Basis for comparison	Flow control	Error control
Basis	Flow control is meant for the proper transmission of the data from sender to the receiver.	Error control is meant for delivering the error-free data to the receiver.
Approach	Feedback-based flow control and rate-based flow control are the approaches to achieve the proper flow control.	Parity checking, Cyclic Redundancy Code (CRC) and checksum are the approaches to detect the error in data. Hamming code, Binary Convolution codes, Reed-Solomon code, Low-

**POPULAR PUBLICATIONS**

Basis for comparison	Flow control	Error control
		Density Parity Check codes are the approaches to correct the error in data.
Impact	Avoid overrunning of receivers buffer the data loss.	Detects and correct the error occurred in the data.

6. Given a 10 bit sequence 1010011110 and a divisor of 1011. Find the CRC. [WBUT 2016]

**Answer:**

Since divisor is 1101, we append four 0-s to the data and divide.

$$\begin{array}{r}
 100100011 \\
 1011 \overline{) 10100111100000} \\
 \underline{1011} \phantom{0000} \\
 1100 \phantom{0000} \\
 \underline{1011} \phantom{0000} \\
 1110 \phantom{0000} \\
 \underline{1011} \phantom{0000} \\
 1010 \phantom{0000} \\
 \underline{1011} \phantom{0000} \\
 0010
 \end{array}$$

Remainder → 0010

∴ Data with CRC is 1010 0111 1000 10

7. Discuss the function of data link Layer.

[WBUT 2017]

**Answer:**

**Functions of data link layer:**

- i) Converting the frames to bits and vice versa.
- ii) Error detection by CRC check.
- iii) flow control
- iv) Sensing and collision detection the channel before transmission and is responsible for reception of frames.

**Long Answer Type Questions**

1. a) Explain CRC code with an example.

[WBUT 2014]

**Answer:**

A cyclic redundancy check (CRC) or polynomial code checksum is a hash function designed to detect accidental changes to raw computer data and is commonly used in



digital networks and storage devices such as hard disk drives. A CRC-enabled device calculates a short, fixed-length binary sequence, known as the CRC code or just CRC, for each block of data and sends or stores them both together. When a block is read or received the device repeats the calculation; if the new CRC does not match the one calculated earlier, then the block contains a data error and the device may take corrective action such as rereading or requesting the block be sent again, otherwise the data is assumed to be error free.

Applying the CRC algorithm, here we determine the transmitted frame for the data 11010111 and for the generator polynomial  $x^3 + x^2 + 1$ .

We append 000 (since highest power of generator polynomial is 3) to get 11010111000.

```

1101) 1101 01110 00(1000 10 1
      1101
      ----
        1110
        1101
        ----
          1100
          1101
          ----
            001 ← Remainder
    
```

So, transmitted string is 11010111001

When the received string is again divided by 1001, we get remainder 000 as shown below:

```

1001) 1010 00 0 1 1 1 1 (10 1 10 1 1 1
      1001
      ----
        1100
        1001
        ----
          1010
          1001
          ----
            1111
            1001
            ----
              1101
              1001
              ----
                1001
                1001
                ----
                  000 ← Remainder
    
```

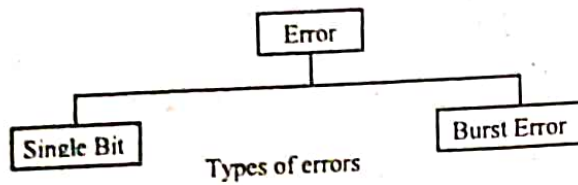
b) How does a single bit error differ from a burst error?

[WBUT 2014]

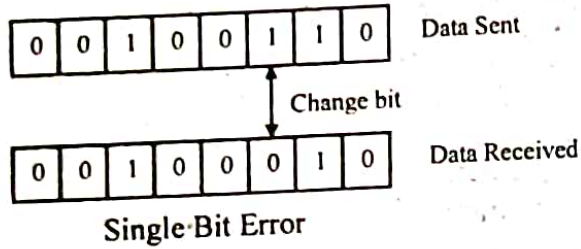
**Answer:**

There are two main types of errors in transmissions:

1. Single bit error
2. Burst error

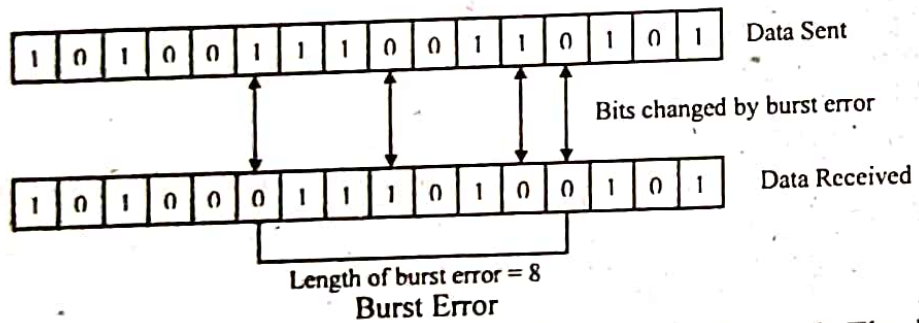


**Single bit error:** It means only one bit of data unit is changed from 1 to 0 or from 0 to 1 as shown in fig.



Single bit error can happen in parallel transmission where all the data bits are transmitted using separate wires. Single bit errors are the least likely type of error in serial transmission.

**Burst Error:** It means two or more bits in data unit are changed from 1 to 0 from 0 to 1 as shown in fig.



In burst error, it is not necessary that only consecutive bits are changed. The length of burst error is measured from first changed bit to last changed bit. As shown in Fig. length of burst error is 8, although some bits are unchanged in between. Burst error is most likely to occur in a serial transmission. The noise occurring for a longer duration affects multiple bits. The number of bits affected depends on the data rate & duration of noise. For e.g. if data rate is 1 kbps, a noise of 1/100 second can affect 10 bits.

**2. Discuss in detail about different framing techniques.**

[WBUT 2015]

**Answer:**

A point-to-point connection between two computers or devices consists of a wire in which data is transmitted as a stream of bits. However, these bits must be framed into discernible blocks of information. Framing is a function of the data link layer. It provides a way for a sender to transmit a set of bits that are meaningful to the receiver. Ethernet,



token ring, frame relay, and other data link layer technologies have their own frame structures. Frames have headers that contain information such as error-checking codes. There are three different types of framing, each of which provides a way for the sender to tell the receiver where the block of data begins and ends:

- **Byte-oriented framing:** Computer data is normally stored as alphanumeric characters that are encoded with a combination of 8 bits (1 byte). This type of framing differentiates one byte from another. It is an older style of framing that was used in the terminal/mainframe environment. Examples of byte-oriented framing include IBM's BISYNC protocol.
- **Bit-oriented framing:** This type of framing allows the sender to transmit a long string of bits at one time. IBM's SDLC (Synchronous Data Link Control) and HDLC (High-level Data Link Control) are examples of bit-oriented protocols. Most LANs use bit-oriented framing. There is usually a maximum frame size. For example, Ethernet has a maximum frame size of 1,526 bytes. The beginning and end of a frame is signaled with a special bit sequence (01111110 for HDLC). If no data is being transmitted, this same sequence is continuously transmitted so the end systems remain synchronized.
- **Clock-based framing:** In a clock-based system, a series of repetitive pulses are used to maintain a constant bit rate and keep the digital bits aligned in the data stream. SONET (Synchronous Optical Network) is a synchronous system in which all the clocks in the network are synchronized back to a master clock reference. SONET frames are then positioned within the clocked stream.

3. a) Explain in detail how an error could be detected using the Checksum method for error detection.

b) What do you mean by flow control problem?

c) What is an ARQ? Discuss about the different operations performed by Stop & Wait ARQ. [WBUT 2015]

Answer:

a) A checksum is a simple type of redundancy check that is used to detect errors in data. Errors frequently occur in data when it is written to a disk, transmitted across a network, or otherwise manipulated. The errors are typically very small, for example, a single incorrect bit, but even such small errors can greatly affect the quality of data, and even make it useless.

In its simplest form, a checksum is created by calculating the binary values in a packet or other block of data using some algorithm and storing the results with the data. When the data is retrieved from memory or received at the other end of a network, a new checksum is calculated and compared with the existing checksum. A non-match indicates an error; a match does not necessarily mean the absence of errors, but only that the simple algorithm was not able to detect any.

Among the types of errors that cannot be detected by simple checksum algorithms are reordering of the bytes, inserting or deleting zero-valued bytes and multiple errors that cancel each other out. Fortunately, however, these errors can be detected with more sophisticated methods, such as cyclic redundancy checks (CRC). Although such

## POPULAR PUBLICATIONS

techniques have the disadvantage of requiring greater system resources (in the form of processor time and bandwidth), this has become an increasingly unimportant consideration in recent years as a result of the continued increases in processor speed and bandwidth.

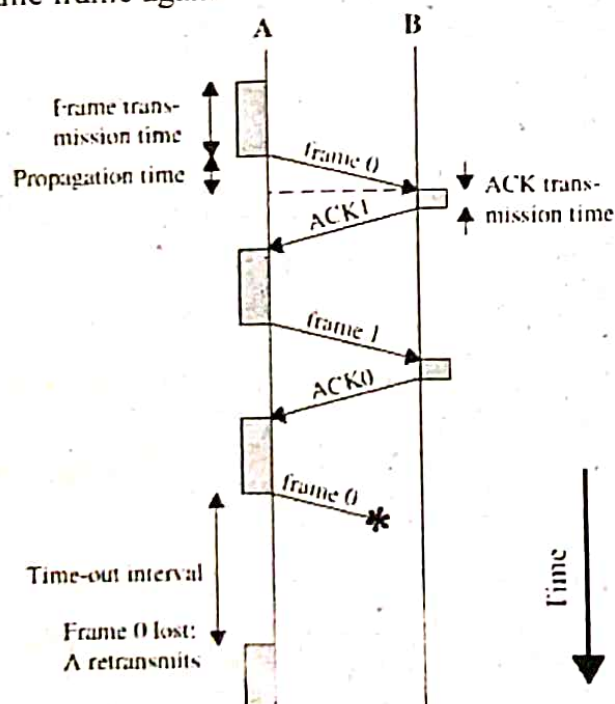
b) Flow control is the mechanism that ensures the rate at which a sender is transmitting is in proportion with the receiver's receiving capabilities. Flow control is utilized in data communications to manage the flow of data/packets among two different nodes, especially in cases where the sending device can send data much faster than the receiver can digest.

### c) 1<sup>st</sup> Part:

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 packet.

### 2<sup>nd</sup> Part:

**Stop-and-wait ARQ** is a method used to send information between two connected devices. It ensures that information is not lost due to dropped packets and that packets are received in the correct order. It is the simplest kind of automatic repeat-request (ARQ) method. A stop-and-wait ARQ sender sends one frame at a time; it is a special case of the general sliding window protocol with both transmit and receive window sizes equal to 1. After sending each frame, the sender doesn't send any further frames until it receives an acknowledgement (ACK) signal. After receiving a good frame, the receiver sends an ACK. If the ACK does not reach the sender before a certain time, known as the timeout, the sender sends the same frame again.





4. a) Discuss about the different modes of operations performed by HDLC.  
b) What do you mean by data transparency and bit stuffing in HDLC?  
c) What is bandwidth-delay product?

Answer:

[WBUT 2015]

a) The HDLC protocol is a general purpose data link control protocol capable of supporting a range of modes of operation. The two most prevalent modes are:

- **The best-effort or datagram service:** In this mode, the packets are carried in a UI frame, and a best-effort delivery is performed (i.e. there is no guarantee that the packet carried by the frame will be delivered.) The link layer does not provide error recovery of lost frames. This mode is used for point-to-point links carrying a network protocol which itself uses datagram packets (e.g. IP). The control field of HDLC follows the address field and is the second part of all HDLC frames. The best-effort service is provided through the use of U (un-numbered) frames consisting of a single byte with the value of 0x03.
- **The Asynchronous Balanced Mode (ABM):** This provides a reliable data point-to-point data link service and may be used to provide a service which supports either a datagram or reliable network protocol. In this mode, the packets are carried in numbered I-frames, which are acknowledged by the receiver using numbered supervisory frames. Error recovery (e.g. checkpoint or go-back-n error recovery) is employed to ensure a well-ordered and reliable flow of frames.

b) Refer to Question No. 2 of Short Answer Type Questions.

c) The Bandwidth Delay Product, or BDP for short determines the amount of data that can be in transit in the network. It is the product of the available bandwidth and the latency, or RTT. BDP is a very important concept in a Window based protocol such as TCP. It plays an especially important role in high-speed / high-latency networks, such as most broadband internet connections. It is one of the most important factors of tweaking TCP in order to tune systems to the type of network used.

The BDP simply states that:

$BDP \text{ (bits)} = \text{total\_available\_bandwidth (bits/sec)} \times \text{round\_trip\_time (sec)}$

or, since RWIN/BDP is usually in bytes, and latency is measured in milliseconds:

$BDP \text{ (bytes)} = \text{total\_available\_bandwidth (KBytes/sec)} \times \text{round\_trip\_time (ms)}$

5. a) What is the basic difference between CSMA and CSMA/CD? [WBUT 2016]  
c) What do you mean by back off factor in case of CSMA/CD protocol?  
d) What is the working operation of stop and wait ARQ for lost acknowledgement?  
e) Selective Repeat ARQ of the window size must be at most  $2^m/2$ . Explain it.

Answer:

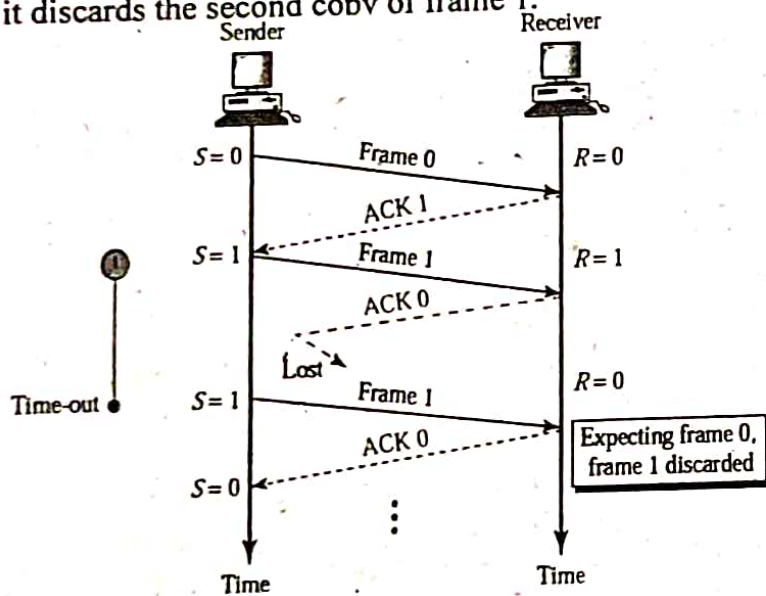
a) CSMA/CD is a protocol that can detect collision whereas CSMA is unable to detect it.

b) If a collision is detected, the transmitting station stops sending the frame data and sends a 32-bit "jam sequence". If the collision is detected very early in the frame transmission, the transmitting station will complete sending of the frame preamble before

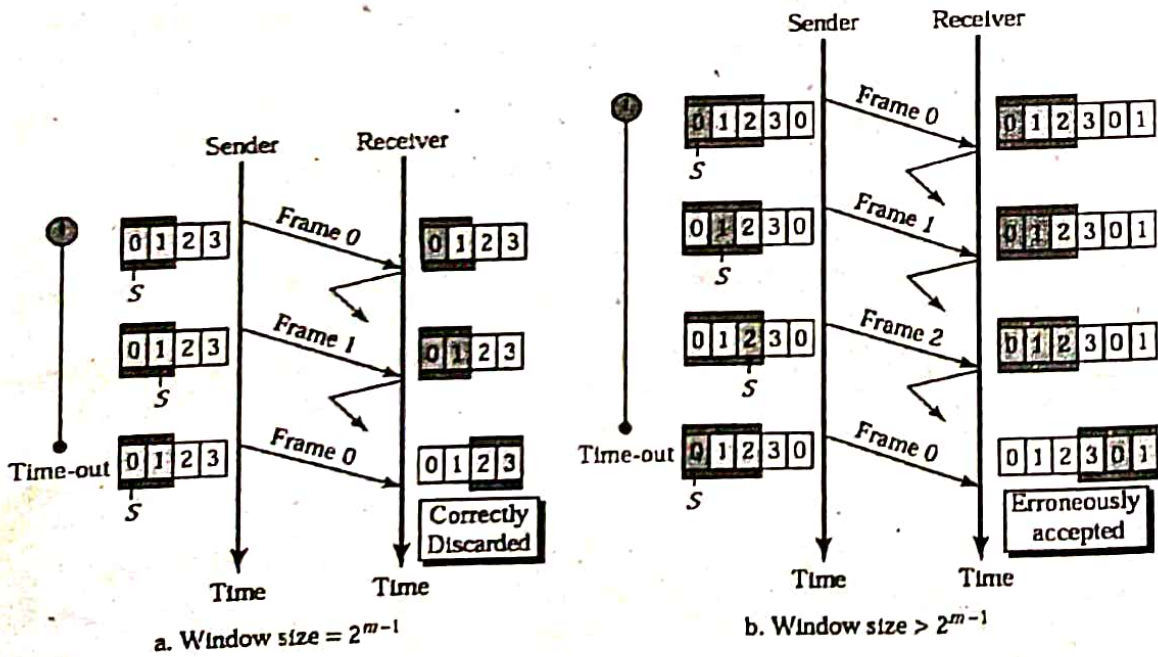
**POPULAR PUBLICATIONS**

starting transmission of the jam sequence. The sequence jam is transmitted to ensure that the length of the collision is sufficient to be noticed by the other transmitting stations. After sending the jam sequence the transmitting station waits a random period of time chosen using a random number generator before starting the transmission process over from step 1 above. This process is called "backoff". The probability of a repeated collision is reduced by having the colliding stations wait a random period of time before retransmitting.

- c)
- If the sender receives a damaged ACK, it discards it.
  - When the timer of the sender expires, the sender retransmits frame 1.
  - Receiver has already received frame 1 and expecting to receive frame 0 (R=0). Therefore it discards the second copy of frame 1.



d)





Size of the sender and receiver windows must be at most one-half of  $2^m$ . If  $m = 2$ , window size should be  $2^m / 2 = 2$ . Fig compares a window size of 2 with a window size of 3. Window size is 3 and all ACKs are lost, sender sends duplicate of frame 0, window of the receiver expect to receive frame 0 (part of the window), so accepts frame 0, as the 1st frame of the next cycle – an error.

6. Write short notes on the following:

- a) Hamming Code
- b) Go back-N ARQ

[WBUT 2015]  
[WBUT 2015]

Answer:

a) Hamming Code:

Hamming code can be applied to data units of any length and uses the relationship between the data bits and redundant bits as discussed.

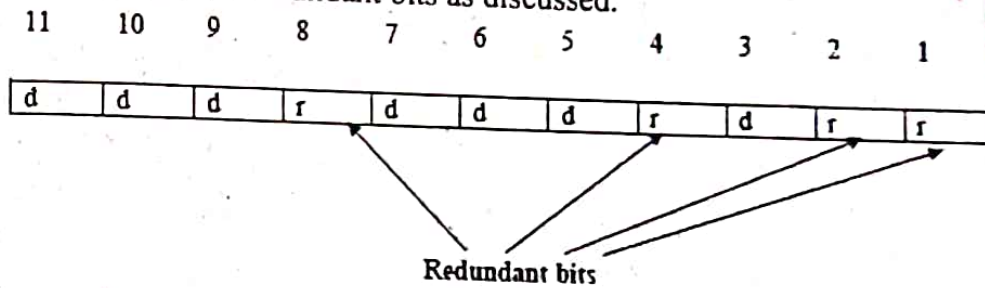


Figure Positions of redundancy bits in hamming code

Basic approach for error detection by using Hamming code is as follows:

- To each group of  $m$  information bits  $k$  parity bits are added to form  $(m+k)$  bit code as shown in above figure.
- Location of each of the  $(m+k)$  digits is assigned a decimal value.
- The  $k$  parity bits are placed in positions 1, 2, ...,  $2^k-1$  positions. –  $k$  parity checks are performed on selected digits of each codeword.
- At the receiving end the parity bits are recalculated. The decimal value of the  $k$  parity bits provides the bit-position in error, if any.

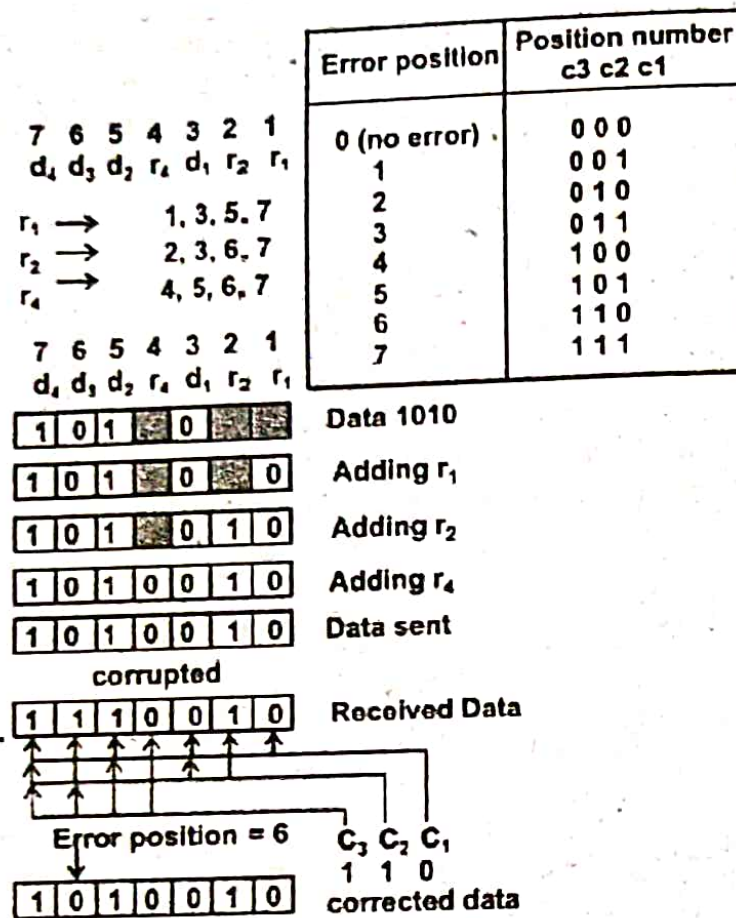


Figure Use of Hamming code for error correction for a 4-bit data

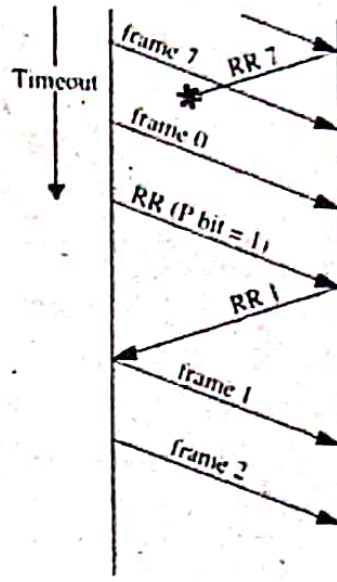
Figure above shows how hamming code is used for correction for 4-bit numbers ( $d_4d_3d_2d_1$ ) with the help of three redundant bits ( $r_3r_2r_1$ ). For the example data 1010, first  $r_1$  (0) is calculated considering the parity of the bit positions, 1, 3, 5 and 7. Then the parity bits  $r_2$  is calculated considering bit positions 2, 3, 6 and 7. Finally, the parity bits  $r_4$  is calculated considering bit positions 4, 5, 6 and 7 as shown. If any corruption occurs in any of the transmitted code 1010010, the bit position in error can be found out by calculating  $r_3r_2r_1$  at the receiving end. For example, if the received code word is 1110010, the recalculated value of  $r_3r_2r_1$  is 110, which indicates that bit position in error is 6, the decimal value of 110.

b) Go back-N ARQ:

- Receiver sends Ack for the correctly received frame
- An Acknowledgement field has a meaning of "next expected sequence number" (Example: Ack 2 means "next expected packet sequence number is 2 and all packets up to 2(0, 1) are received)
- Sender keeps on sending frames (limited to the Window size) and receiver keeps on acknowledging.
- When a frame is damaged, receiver sends a Reject control packet (Nak)



- Sender goes back to the Rejected frame and sends all the frames starting with the rejected one even if those frames are already sent to the receiver
- Sender's buffer size = Window size
- Receiver's buffer size = 1



(a) Go-back-N ARQ

7. a) Is Bit stuffing needed in the control field of HDLC data frame?  
 b) Briefly discuss the Token management using priority in IEEE 802.5.

[MODEL QUESTION]

Answer:

a) HDLC frames can be transmitted over synchronous or asynchronous links. Those links have no mechanism to mark the beginning or end of a frame, so the beginning and end of each frame has to be identified. This is done by using a frame delimiter, or flag, which is a unique sequence of bits that is guaranteed not to be seen inside a frame. This sequence is '01111110', or, in hexadecimal notation, 7E. Each frame begins and ends with a frame delimiter. A frame delimiter at the end of a frame may also mark the start of the next frame. A sequence of 7 or more consecutive 1-bits within a frame will cause the frame to be aborted.

b) Token Bus was a 4 Mbps Local Area Networking technology created by IBM to connect their terminals to IBM mainframes. Token bus utilized a copper coaxial cable to connect multiple end stations (terminals, workstations, shared printers etc.) to the mainframe. The coaxial cable served as a common communication bus and a token was created by the Token Bus protocol to manage or 'arbitrate' access to the bus. Any station that holds the token packet has permission to transmit data. The station releases the token when it is done communicating or when a higher priority device needs to transmit (such as the mainframe). This keeps two or more devices from transmitting information on the bus at the same time and accidentally destroying the transmitted data.

Token Bus suffered from two limitations. Any failure in the bus caused all the devices beyond the failure to be unable to communicate with the rest of the network. Second,

## POPULAR PUBLICATIONS

adding more stations to the bus was somewhat difficult. Any new station that was improperly attached was unlikely to be able to communicate and all devices beyond it were also affected. Thus, token bus networks were seen as somewhat unreliable and difficult to expand and upgrade.



# MEDIUM ACCESS SUB LAYER

## Multiple Choice Type Questions

1. When host knows its IP address but not its physical address, it can use .  
 a) RARP                      b) ICMP                      c) ARP                      [WBUT 2016]  
 Answer: (c)                      d) IGMP
2. A network which is used for sharing data, software and hardware among several users owning microcomputers is called  
 a) WAN                      b) LAN                      c) MAN                      [WBUT 2017]  
 Answer: (b)                      d) VAN
3. What is the minimum size of a IP packet?  
 a) 16 byte.                      b) 10 byte                      c) 20 byte                      [WBUT 2017]  
 Answer: (c)                      d) 32 byte
4. In the ..... Random-access method there is no collision.  
 a) ALOHA                      b) CSMA / CD                      c) CSMA / CA                      [MODEL QUESTION]  
 Answer: (d)                      d) Token-passing
5. The 1-persistent CSMA / CD can be considered as a special case of p-persistent approach with p equal to  
 a) 0.1                      b) 0.5                      c) 1.0                      [MODEL QUESTION]  
 Answer: (c)                      d) None of these
6. IEEE 802.5 standard is  
 a) Token Ring                      b) Token Bus                      c) LLC                      [MODEL QUESTION]  
 Answer: (a)                      d) FDDQ
7. How much channel throughput of slotted ALOHA will be in comparison to pure Aloha?  
 a) Same                      b) Double                      c) Three times                      [MODEL QUESTION]  
 Answer: (b)                      d) None of these
8. In which OSI layers does FDDI protocol operate?  
 a) Physical                      b) Data link                      c) Network                      [MODEL QUESTION]  
 Answer: (b)                      d) (a) & (b) both
9. PPP is a ..... oriented protocol.  
 a) phase                      b) bit                      c) byte                      [MODEL QUESTION]  
 Answer: (c)                      d) none of these

## POPULAR PUBLICATIONS

10. Which of the following network architectures does not use the token passing access method? [MODEL QUESTION]

a) IEEE 802.4

b) FDDI

c) CSMA/CD

d) IEEE802.5

Answer: (c)

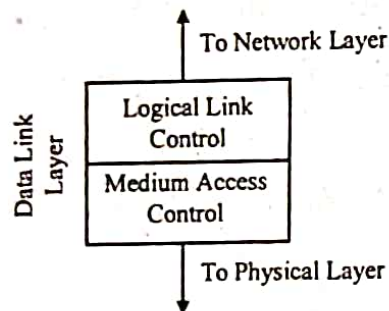
### Short Answer Type Questions

1. What do you mean by MAC and LLC? Explain.

[WBUT 2014]

Answer:

- In any broadcast network, the stations must ensure that only one station transmits at a time on the shared communication channel.
- The protocol that determines who can transmit on a broadcast channel are called Medium Access Control (MAC) protocol.
- The MAC protocols are implemented in the MAC sublayer which is the lower sublayer of the data link layer.
- The higher portion of the data link layer is often called Logical Link Control (LLC).



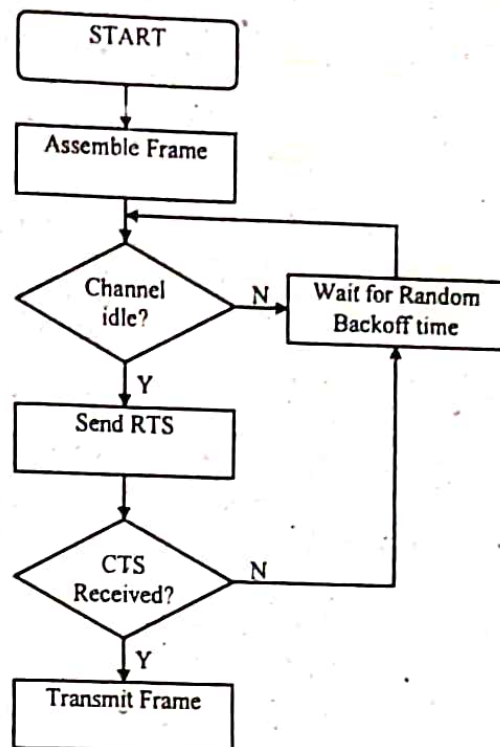
- Layer 2 uses Logical Link Control (LLC) to communicate with the upper-level layers.
- Layer 2 uses Media Access Control (MAC) to decide which computer will transmit.
- LLC serves to communicate upward to Network layer, independent of the specific LAN technology used and Upper layer.
- MAC serves to access and communicate downward to the technology-specific Physical layer.



2. Discuss CSMA/CA with the help of a flowchart.

[WBUT 2016]

Answer:



The flow chart for CSMA/CA is given above.

When station receives data to transmit, it converts it into frames of appropriate size. Then it waits to see if the channel is idle and backs off for a random time if not idle. When the channel becomes idle, the station transmits a special sequence called "Request to Send" (RTS) to the receiver and awaits for a short while for the receiver in turn to send the special "Clear to Send" (CTS) sequence. Only upon receiving a CTS does the station transmit frames. Or else, it again backs off.

3. Find the expressions for average delay and throughput for both pure ALOHA and slotted ALOHA. Compare their performances as well. [WBUT 2016]

Answer:

Suppose the stations generate frames following a Poisson distribution of mean  $S$  frames per second. Also, the probability of  $k$  transmissions attempts per time frame is a Poisson distribution with mean  $G$  per frame time, i.e.

$$P(k) = \frac{G^k e^{-G}}{k!}$$

Thus,  $P(\text{No frames generated in frame duration}) = e^{-G}$

Now, throughput =  $G * P(\text{transmission is successful})$

Hence,  $S = GP(0)$

Collision happens if another frame is generated during twice the time duration of a frame.

This is  $P(0) = e^{-2G}$

Solving for  $S$  we get

$$S = Ge^{-2G}$$

Maximum throughput occurs at  $G = 0.5$ , where  $S = 1/2e = 0.184$

## POPULAR PUBLICATIONS

In slotted ALOHA, we need to check for collision only within duration of frame because no new frame can start within that time (collision can happen at the beginning only). This gives us:

$$S = Ge^{-2G} \quad \text{where maximum } S = 1/e = 0.368$$

### Comparison:

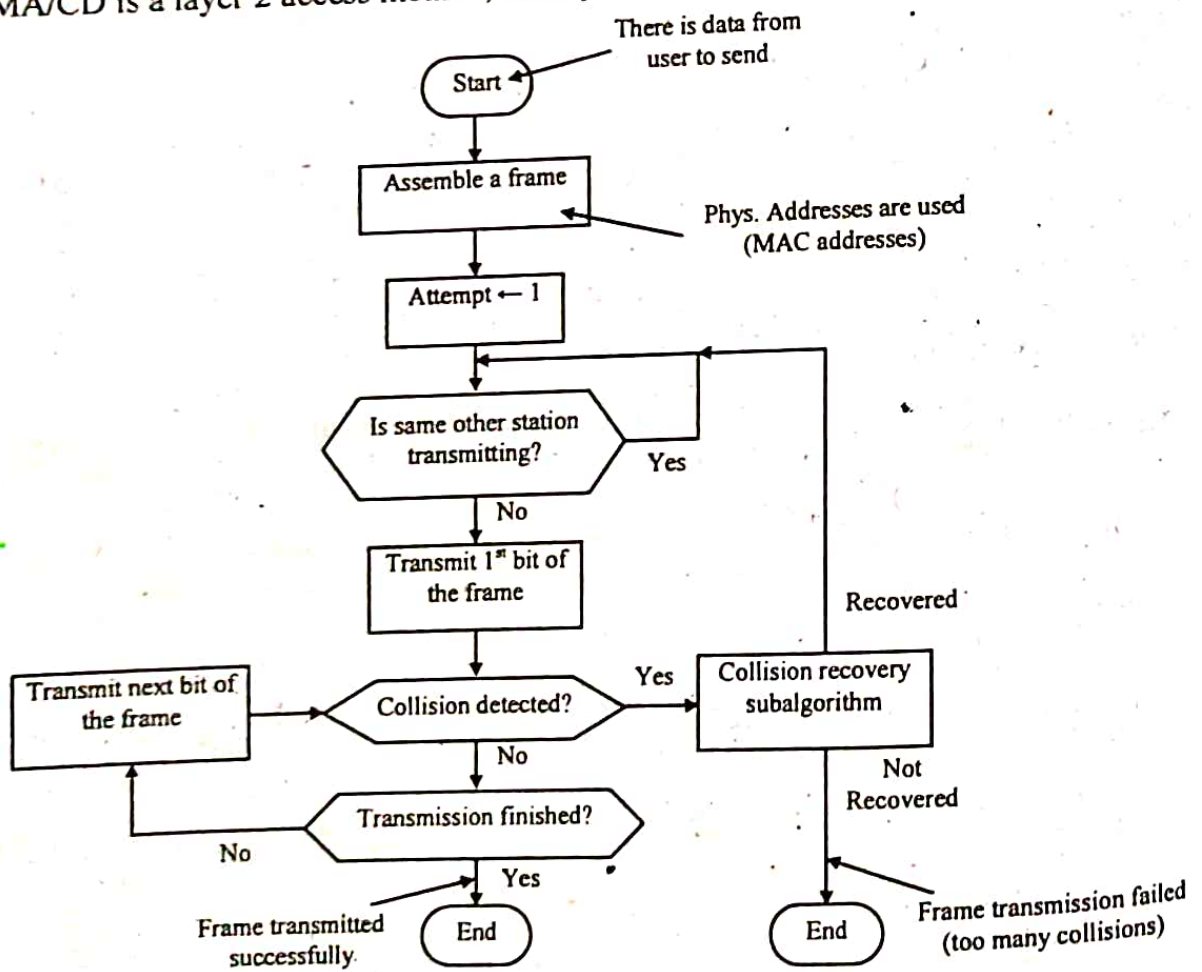
- Pure Aloha is a Continuous time system whereas Slotted ALOHA is discrete time system.
- Pure ALOHA doesn't check whether the channel is busy before transmission. Slotted ALOHA send the data at the beginning of timeslot. Pure ALOHA not divided in to time. Slotted ALOHA divided in to time

[WBUT 2017]

### 4. Explain CSMA/CD. What is its usage?

#### Answer:

CSMA/CD is a modification of pure Carrier sense multiple access (CSMA). CSMA/CD is used to improve CSMA performance by terminating transmission as soon as a collision is detected, thus reducing the probability of a second collision on retry. A jam signal is sent which will cause all transmitters to back off by random intervals, reducing the probability of a collision when the first retry is attempted. CSMA/CD is a layer 2 access method, not a protocol of the OSI model.





**5. Discuss the principles of operation of a wireless LAN.**

**[MODEL QUESTION]**

**Answer:**

A wireless LAN (or WLAN, for wireless local area network, sometimes referred to as LAWN, for local area wireless network) is one in which a mobile user can connect to a local area network (LAN) through a wireless (radio) connection. The IEEE 802.11 group of standards specify the technologies for wireless LANs. 802.11 standards use the Ethernet protocol and CSMA/CA (carrier sense multiple access with collision avoidance) for path sharing and include an encryption method, the Wired Equivalent Privacy algorithm.

High-bandwidth allocation for wireless will make possible a relatively low-cost wiring of classrooms in the United States. A similar frequency allocation has been made in Europe. Hospitals and businesses are also expected to install wireless LAN systems where existing LANs are not already in place.

Using technology from the Symbionics Networks, Ltd., a wireless LAN adapter can be made to fit on a Personal Computer Memory Card Industry Association (PCMCIA) card for a laptop or notebook computer.

**6. Explain the difference between Point to Point and Multi-Point connection?**

**[MODEL QUESTION]**

**Answer:**

A point to point connection is one in which data can flow from one point to another in a unidirectional or bi-directional manner. A telephone connection or RS 232 are examples of point to multi-point connections. In a point to multi-point connections, several hosts are simultaneously connected to each other in one or more shared data paths. Such a connection, for example a bus connection as in Ethernet, allows one host to simultaneously send data to all hosts (broadcast) or a subset of hosts (multicast).

**7. What are the basic differences between Pure ALOHA and Slotted ALOHA?**

**[MODEL QUESTION]**

**Answer:**

- 1) Pure Aloha is a Continuous time system whereas Slotted Aloha is discrete time system.
- 2) Pure ALOHA doesn't check whether the channel is busy before transmission. Slotted ALOHA send the data at the beginning of timeslot.
- 3) Pure aloha not divided in to time. Slotted aloha divided in to time

**8. a) Differentiate between FHSS and DSSS spread spectrum. [MODEL QUESTION]**

**b) Why address field is always set to all 1's in PPP frame format?**

**Answer:**

a) FHSS (Frequency-hopping spread spectrum) is typically used by wireless mobile devices such as blue tooth and wireless phones. The transmission distance of FHSS is shorter and not very reliable. DSSS is used by wireless immobile devices. The transmission speed of DSSS is faster than FHSS and is more reliable.



## POPULAR PUBLICATIONS

b) The address field of PPP header indicates which recipient receives the frame. Now PPP being a point-to-point protocol, there can be only one recipient. Hence the address must always be all 1-s.

[MODEL QUESTION]

**9. Why is CSMA/CD not implemented in WLAN?**

**Answer:**

In Wireless LAN, a transmitter never gets to know whether its data got corrupted while on way. That is, it never can detect collision. Hence, CSMA/CD, which is based on collision detection, is based on collision detection, is not used in WLAN.

[MODEL QUESTION]

**10. i) Why bit stuffing is needed in HDLC frame?  
ii) What is the purpose of the jam signal in CSMA/CD?**

**Answer:**

i) Bit stuffing is the insertion of one or more bits into a transmission unit as a way to provide signaling information to a receiver. The receiver knows how to detect and remove or disregard the stuffed bits.

For example, the timing or bit rate of T-carrier system signals is constantly synchronized between any terminal device and an adjacent repeater or between any two repeaters. The synchronization is achieved by detecting the transition in polarity for 1 bits in the data stream. (T-1 signaling uses bipolar signaling, where each successive bit with a value of 1 is represented by voltage with a reverse polarity from the previous bit. Bits with a value of 0 are represented by a no-voltage time slot). If more than 15 bits in a row are sent with a 0 value, this "lull" in 1 bits that the system depends on for synchronization may be long enough for two end points to become out of synchronization. To handle this situation (the sequence of more than 150 bits), the signal is "stuffed" with a short, unique bit pattern (which includes some 1 bits) that is recognized as a synchronization pattern. The receiving end removes the stuffed bits and restores the bit stream to its original sequence. In another example of bit stuffing, a standard HDLC packet begins and ends with 01111110. To make sure this sequence doesn't appear again before the end of the packet, a 0 is inserted after every five consecutive 1s.

Bit stuffing is defined by some to include bit padding, which is the addition of bits to a transmission to make the transmission unit conform to a standard size, but is distinct from bit robbing, a type of in-band signaling.

ii) A network in which the medium access control protocol requires carrier sense and where a station always starts transmission by sending a jam signal; if there is no collision with jam signals from other stations, it begins sending data; otherwise, it stops transmission and then tries again later.

### **Long Answer Type Questions**

1. a) Explain the operation of CDMA technology.  
b) Describe 802.3 header format. Why padding is required?

[WBUT 2014]



**Answer:**

a) In cellular service there are two main competing network technologies: Global System for Mobile Communications (GSM) and Code Division Multiple Access (CDMA). One of the basic concepts in data communication is the idea of allowing several transmitters to send information simultaneously over a single communication channel. This allows several users to share a band of frequencies (see bandwidth). This concept is called multiplexing. CDMA employs spread-spectrum technology and a special coding scheme (where each transmitter is assigned a code) to allow multiple users to be multiplexed over the same physical channel. By contrast, time division multiple access (TDMA) divides access by time, while frequency-division multiple access (FDMA) divides it by frequency. CDMA is a form of spread-spectrum signaling, since the modulated coded signal has a much higher data bandwidth than the data being communicated.

b) Ethernet traffic is transported in units of a frame, where each frame has a definite beginning and end. The form of the frame is in the figure below.

Preamble	Dest Addr	Src Addr	Type	Data	CRC
----------	-----------	----------	------	------	-----

- **The Preamble Field** (8 bytes, 64 bits) is used for synchronization. The first seven bytes contain the bit pattern 10101010 and the eighth contain the pattern 10101011.
- **Destination Address** specifies the Ethernet address of the destination station, 48-bits
- **Source Address** specifies Ethernet address of the source station, 48-bits
- **Type field** specifies the type of data encapsulated, e.g. IP, ARP, RARP, etc, 16-bits.
- **Data Field** carries 46-1500 bytes of data. If data length is lower than 46 bytes, it must be padded to 46 bytes.
- **CRC** or Cyclical Redundancy Check, used for error detection

The reason why there is an upper limit to the length of the data field, is fairly obvious --- so that each station gets a fair chance with the channel. The lower limit, and the reason for padding in case that limit is not met, is as follows:

Suppose a station at one extreme of sends a very short frame. Before this frame reaches the other extreme, another station starts transmitting since it saw that the channel was free. This of course leads to collision but the fact that collision happens must travel back to the first station for it to realize that and that must happen before it has finished with transmitting the frame. Thus the minimum frame size is of duration twice the time a signal takes to travel from one end of the network to the other, which is roughly 5 micro-seconds on a 1 Km long cable. 802.3 standard therefore specifies that the minimum data length is 46 bytes which must be padded up if not present.

**2. Explain in detail the concept of connection establishment using LCP in case of PPP.**  
[WBUT 2015]

## POPULAR PUBLICATIONS

### Answer:

PPP starts with LCP configure packets that negotiate option settings, acknowledgements and rejects. PPP negotiation is an iterative process. One endpoint proposes to a peer the list of PPP options it wants the peer to use. If the peer rejects the proposal, this endpoint must send a revised one. This continues until an agreement is reached. Figure illustrates the PPP negotiation sequence and the LCP packets involved. Link options are independent for each direction of a point-to-point connection. Each endpoint actively negotiates options for its receiving direction. Thus, both Host A and Host B begin by sending a configure-request packet. It doesn't matter who initiated the call, since PPP operates peer to peer. Although the diagram shows negotiations separately in time for each direction, in practice, these events are intertwined.

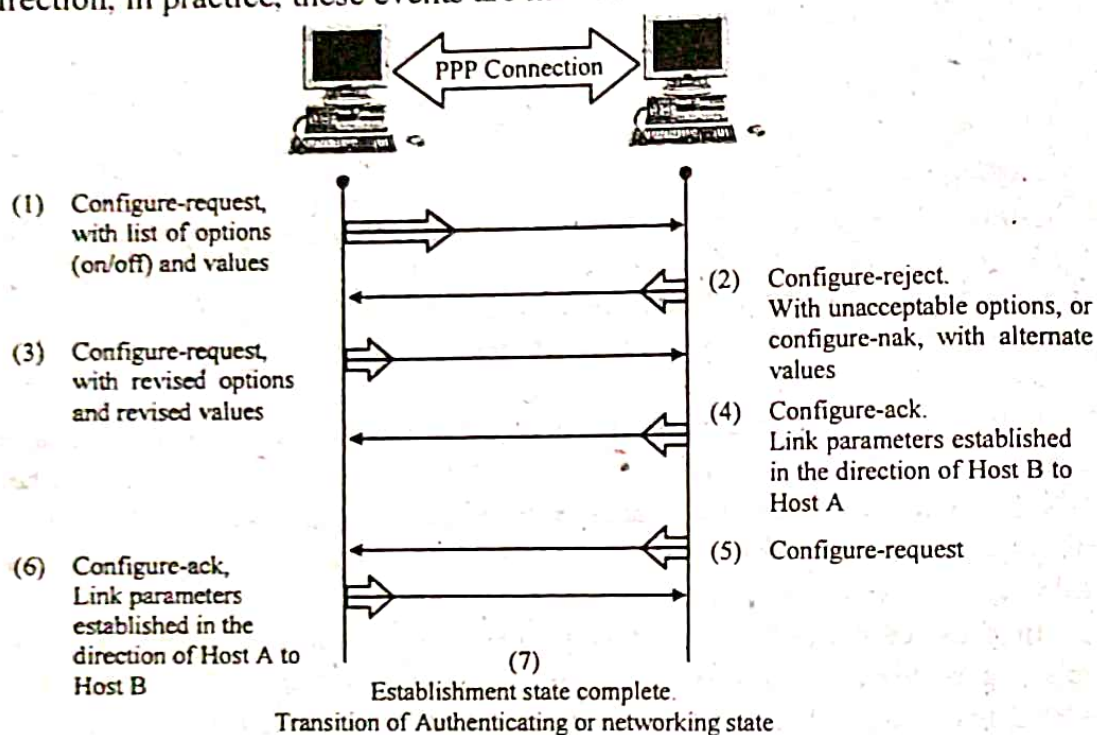


Fig: PPP Negotiation

The LCP configure packets are:

#### Configure-Request (code-1)

The PPP endpoint sending the configure-request places the list of all options (zero or more) it wishes to negotiate into the LCP data field. All configurable options must be negotiated simultaneously.

#### Configure-Ack (code-2)

If all the options listed in the configure-request are recognizable and acceptable to the peer, the peer replies with a configure-ack. The acknowledgment includes the options as requested in the original configure-request message.

#### Configure-Nak (Negative Acknowledge) (code-3)

If the peer recognizes all options, but some options have unacceptable values, the peer responds with a configure-nak. This response contains the offending option and hints regarding acceptable values. A peer can also reply with configure-nak if it requires an



option omitted in the original configure-request. The PPP endpoint originally sending the configure-request must now send a revised configure-request based on this reply.

**Configure-Reject (code-4)**

If the peer doesn't recognize some options or refuses to accept some "do this" options, the peer replies with a configure-reject. This reply includes the list of unrecognized or unacceptable options. The sender of the original configure-request must now send a revised request based on this reply.

A configure-request LCP packet embeds multiple PPP options. Only those that need to be changed from their default values are included in this packet. When PPP operates with all default settings, the configure-request sender doesn't include any options in the LCP data field. A PPP peer responding to a configuration request responds with LCP configure-reject, configure-nak, or configure-ack.

**3. Write short note on IEEE 802.11.**

[WBUT 2016]

**Answer:**

**IEEE 802.11:**

The original 802.11 standard had two variations both offering the same speeds but differing in the RF spread spectrum used. One of the 802.11 used FHSS. This 802.11 variant used the 2.4 GHz radio frequency band and operated with a 1 or 2 Mbps data rate. Since this original standard, wireless implementations have favored DSSS.

The second 802.11 variation used DSSS and specified a 2 Mbps-peak data rate with optional fallback to 1 Mbps in very noisy environments. 802.11, 802.11b and 802.11g use the DSSS spread spectrum, this means that the underlying modulation scheme is very similar between each standard, enabling all DSSS systems to coexist with 2, 11 and 54 Mbps 802.11 standards. Because of the underlying differences between 802.11a and the 802.11b/g, they are not compatible.

Distributed coordination function (DCF) is the fundamental MAC technique of the IEEE 802.11 based WLAN standard. DCF employs a CSMA/CA with Binary exponential backoff algorithm.

DCF requires a station wishing to transmit to listen for the channel status for a DIFS interval. If the channel is found busy during the DIFS interval, the station defers its transmission. In a network where a number of stations contend for the wireless medium. If multiple stations sense the channel busy and defer their access, they will also virtually simultaneously find that the channel is released and then try to seize the channel. As a result, collisions may occur. In order to avoid such collisions, DCF also specifies random backoff, which forces a station to defer its access to the channel for an extra period.

Point coordination function (PCF) is a Media Access Control (MAC) technique used in IEEE 802.11 based WLANs. It resides in a point coordinator also known as Access Point (AP), to coordinate the communication within the network. The AP waits for PIFS duration rather than DIFS duration to grasp the channel. PIFS is less than DIFS duration and hence the point coordinator always has the priority to access the channel.

The PCF is located directly above the Distributed Coordination Function (DCF), in the IEEE 802.11 MAC Architecture. Channel access in PCF mode is centralized and hence the point coordinator sends CF-Poll frame to the PCF capable station to permit it to



## POPULAR PUBLICATIONS

transmit a frame. In case the polled stations does not have any frames to send, then it must transmit null frame.

4. a) Differentiate between non-persistent and 1-persistent CSMA. How is the chance of collision reduced in CSMA/CD?
- b) How does the receiver acknowledge a frame in token ring?
- c) What is the function of wire center in token ring?
- d) How a new station is introduced in token bus?
- e) Describe the frame format in HDLC.

[MODEL QUESTION]

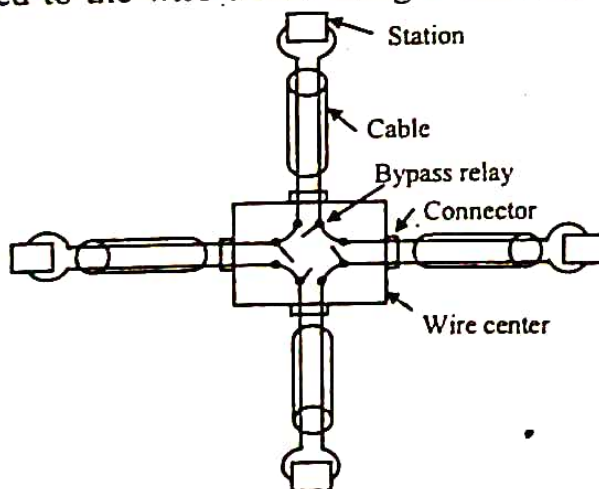
**Answer:**

a) In CSMA, a station having data to send first listens to the channel to see if anyone else is transmitting at that moment. If the channel is busy, the station waits till it finds the channel idle. If the station finds the channel free in 1-persistent CSMA, it transmits a frame (i.e., it transmits with probability 1). In non-persistent CSMA, the station does not continually sense the channel if it found the channel busy when it tried to transmit. Instead, it waits for a random period of time before trying again.

In CSMA/CD, which is a special case of 1-persistent CSMA, the transmitting station stops transmitting immediately upon sensing a collision, and backs off for a random time. This way channel bandwidth is saved because the entire frame is not transmitted in case of collision.

b) In 802.5 token ring, a special bit pattern called a "token" circulates around an idle network. A transmitting station must first seize the token to start transmitting. The frame format keeps a bit reserved for ACK, which is set to zero during transmission. The destination station ACK-s the frame by setting this bit to one but also re-adjusts the checksum.

c) One problem of any ring network is that a cable break anywhere kills the entire network. A wire center solves this problem. Through logically a ring, physically each end station is connected to the wire center using at least two twisted pairs, as shown in the figure.



Four stations connected via a wire center



Inside the wire center there are bypass relays driven by currents from the station. If the ring breaks or a station goes down, the relays do not get the drive current and are released, carrying the problematic station to be passed.

d) In 802.4 token bus is physically linear or free shaped but logically organized as a ring. Just after power on, a station is not in the ring. The 802.4 standards specify a complex methodology for such a station to join the ring. Periodically, the token holder sends a SOLICIT-SUCCESSOR frame to solicit bids from stations willing to join. If no station bids to enter within a "response window", normal business follows. If exactly one new station bids, it is included in the ring. If more than one station bids, there will be a collision. The token holder then runs an arbitration algorithm that starts with broadcasting a RESOLVE-CONTENTION frame.

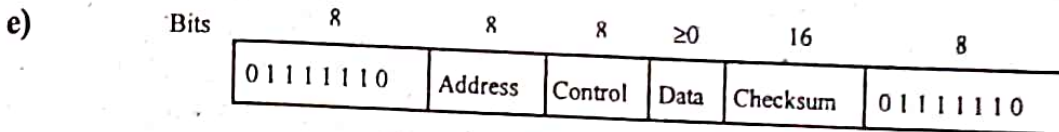


Fig: Frame format for bit-oriented protocols

The HDLC frame has a starting flag byte (7EH) followed by an 8-bit Address to identify a terminal in a multi-terminal line. The 8-bit control field is used for sequence numbers, acknowledgements etc. The data field is arbitrarily long. After the data is a 16-bit CRC field based on CRC-CCITT generator polynomial. The frame ends with a flag byte. There are three kinds of frames – Information, Supervisory and Unnumbered.

5. a) How is CSMA a clear improvement over ALOHA? How is it further improved by implementing CSMA/CD?

b) Suppose in a CSMA/CD LAN, the maximum end to end propagation delay is 25.6 μsecond. If the LAN is operating in 100Mbps, then what will be the minimum frame length (in bytes) of the LAN? [MODEL QUESTION]

Answer:

a) In both slotted and pure ALOHA, a node's decision to transmit is made independently of the activity of the other nodes attached to the broadcast channel. In particular, a node neither pays attention to whether another node happens to be transmitting when it begins to transmit, nor stops transmitting if another node begins to interfere with its transmission.

Listen before speaking: If someone else is speaking, wait until they are done. To the channel before transmitting if a frame from another node is currently being transmitted into the channel, a node then waits ("backs off") a random amount of time and then again senses the channel. If the channel is sensed to be idle, the node then begins frame transmission. Otherwise, the node waits another random amount of time and repeats this process.

In CSMA, the "listen before speaking" principle is employed. A node listens to the channel before transmitting. If a frame from another node is currently being transmitted, a node "backs off" for some (random) time before sensing if the channel has become idle and so on.



## POPULAR PUBLICATIONS

In CSMA/CD, additionally "collision-detection" is employed. A node additionally checks whether a frame put on the channel "collides" with another frame transmitted by another channel. In such a case the node again "backs off" and repeats listening before speaking.

b)  $RTT = 51.2 \mu\text{second}$

Minimum frame length =  $(100 \text{ Mbps} * 51.2 \mu\text{s}) = 5120 \text{ bits} = 640 \text{ octets}$ .

6. What is the difference between bit oriented and byte oriented protocols? [MODEL QUESTION]

**Answer:**

In bit oriented Protocol, a flag is used to frame the bits sent. Simply put, you have a flag (01111110) and the required bits are sent after the flag and you end the transmission again with a flag. Using this method you can send any number of bits of any length. Another important fact is the zero insertion method used. Say for example, you want to send the bit string 01111110. You cannot do this because it will be interpreted as a flag. However, by adding a zero after 5 consecutive 1's as a standard, this bit stream can be sent. The transmitter sends the string as 011111010 and the receiver removes the zero after 5 consecutive 1's and stores the data as 01111110.

In byte oriented protocol (character oriented protocol) the receiver considers 8 bits at a time and figures out the relevant character. This system is used when communicating with printers and keyboards which use ASCII characters exclusively. (All the ASCII characters can be covered by 8 bits (256 characters)). The main disadvantage of COP is that you cannot send 9 or 10 bits, arbitrary bits. Furthermore, in COP there are special characters – channel control characters, e.g. SYN character which is used to synchronize the receiver and the transmitter. These characters cannot be transferred as data. They will be misread as control characters.

7. a) What do you mean by channel utilization? [MODEL QUESTION]

b) Why are medium access control techniques required? List three popular medium access control techniques.

c) A 1 km 10 Mbps CSMA/ CD LAN has a propagation speed of 200 m/ $\mu$  sec. Data frames are 256 bits long including 32 bits of header, checksum and other overhead. The first bit slot after a successful transition is reserved for the receiver to capture the channel to send a 32 bit acknowledge frame. What is the effective data rate excluding overhead assuming there is no collusion.

**Answer:**

a) Channel utilization means channel throughput.

In communication networks, throughput or network throughput is the average rate of successful message delivery over a communication channel. This data may be delivered over a physical or logical link, or pass through a certain network node. The throughput is usually measured in bits per second (bit/s or bps), and sometimes in data packets per second or data packets per time slot.

b) The Media Access Control (MAC) data communication protocol sub-layer, also known as the Medium Access Control, is a sublayer of the Data Link Layer specified in



the seven-layer OSI model (layer 2). It provides addressing and channel access control mechanisms that make it possible for several terminals or network nodes to communicate within a multi-point network, typically a local area network (LAN) or metropolitan area network (MAN).

CSMA

CSMA/CD

CSMA/CA

c) Round trip propagation time =  $\frac{1000 \text{ mtr} \times 2}{200} = 10 \text{ m}/\mu\text{sec}.$

Transmission can be divided into 6 stages.

i) Sender size cable  $T_1 = \text{round trip propagation time} = 10 \mu\text{sec}.$

ii) Data frame transmission  $T_2 = \frac{256}{10} \text{ Mbps} = 25.6 \text{ Mbps}.$

iii) Delay for last bit to reach the end  $T_3 = \frac{1000 \text{ mtr}}{200 \text{ mtr}/\mu\text{sec}} = 5 \mu\text{sec}$

iv) Acknowledgement frame transmission,  $T_5 = 32 \text{ bit}/10 \text{ Mbps} = 3.2 \mu\text{sec}.$

v) Delay for last bit to reach end

$$T_6 = T_3 = 5 \mu\text{sec}.$$

$$\therefore T = T_1 + T_2 + T_3 + T_4 + T_5 + T_6 = 10 + 25.6 + 5 + 10 + 3.2 + 5 = 58.5 \mu\text{sec}.$$

$$\text{Effective data rate} = \frac{(256 - 32) \text{ bit}}{58.8 \mu\text{sec}} = 3.8 \text{ Mbps}.$$

8. Write down about IEEE 802.5 and FDDI.

Answer:

[MODEL QUESTION]

IEEE 802.5:

Token Ring is a LAN protocol defined in the IEEE 802.5 where all stations are connected in a ring and each station can directly hear transmissions only from its immediate neighbor. Permission to transmit is granted by a message (token) that circulates around the ring.

Token Ring as defined in IEEE 802.5 is originated from the IBM Token Ring LAN technologies. Both are based on the Token Passing technologies. While they differ in minor ways but generally compatible with each other.

Token-passing networks move a small frame, called a token, around the network. Possession of the token grants the right to transmit. If a node receiving the token has no information to send, it seizes the token, alters 1 bit of the token (which turns the token into a start-of-frame sequence), appends the information that it wants to transmit, and sends this information to the next station on the ring. While the information frame is circling the ring, no token is on the network, which means that other stations wanting to transmit must wait. Therefore, collisions cannot occur in Token Ring networks.



## POPULAR PUBLICATIONS

The information frame circulates the ring until it reaches the intended destination station, which copies the information for further processing. The information frame continues to circle the ring and is finally removed when it reaches the sending station. The sending station can check the returning frame to see whether the frame was seen and subsequently copied by the destination.

Unlike Ethernet CSMA/CD networks, token-passing networks are deterministic, which means that it is possible to calculate the maximum time that will pass before any end station will be capable of transmitting. This feature and several reliability features make Token Ring networks ideal for applications in which delay must be predictable and robust network operation is important.

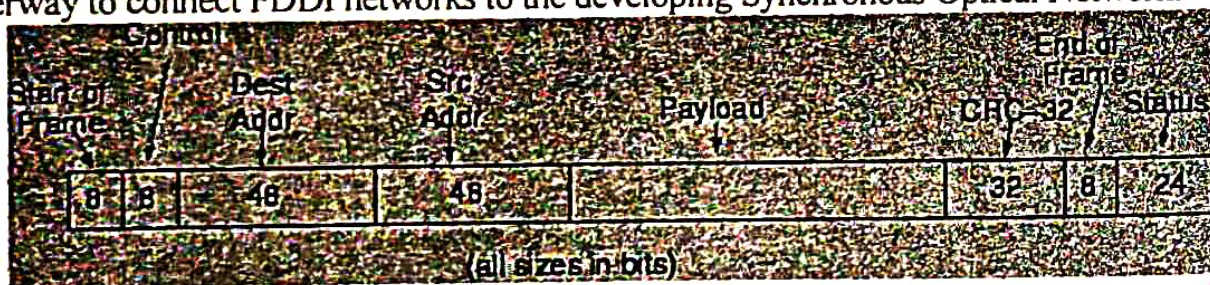
The Fiber Distributed-Data Interface (FDDI) also uses the Token Passing protocol.

### **FDDI:**

FDDI (Fiber-Distributed Data Interface) is a standard for data transmission on fiber optic lines in that can extend in range up to 200 km (124 miles). The FDDI protocol is based on the token ring protocol. In addition to being large geographically, an FDDI local area network can support thousands of users.

An FDDI network contains two token rings, one for possible backup in case the primary ring fails. The primary ring offers up to 100 Mbps capacity. If the secondary ring is not needed for backup, it can also carry data, extending capacity to 200 Mbps. The single ring can extend the maximum distance; a dual ring can extend 100 km (62 miles).

FDDI is a product of American National Standards Committee X3-T9 and conforms to the open system interconnect (OSI) model of functional layering. It can be used to interconnect LANs using other protocols. FDDI-II is a version of FDDI that adds the capability to add circuit-switched service to the network so that voice signals can also be handled. Work is underway to connect FDDI networks to the developing Synchronous Optical Network.





# NETWORK LAYER

## Multiple Choice Type Questions

1. If subnet mask is 255.255.252.0 then how many subnets is available?  
 a) 2                                      b) 18                                      c) 4                                      d) 24  
 Answer: (c) [WBUT 2013]
  
2. Which of the following is an interior routing protocol?  
 a) RIP                                      b) OSPF                                      c) BGP                                      d) both (a) & (b)  
 Answer: (d) [WBUT 2013]
  
3. When host knows its IP address but not its physical address, it can use  
 a) RARP                                      b) ICMP                                      c) ARP                                      d) IGMP  
 Answer: (c) [WBUT 2013]
  
4. Which of the following is a valid host for network 192.168.10.32/28?  
 a) 192.168.10.39      b) 192.168.10.47      c) 192.168.10.14      d) 192.168.10.54  
 Answer: (a) [WBUT 2013, 2016]
  
5. Which class of IP address is reserved for multicast communication?  
 a) Class A                                      b) Class B                                      c) Class C                                      d) Class D  
 Answer: (d) [WBUT 2013, 2014, 2016]
  
6. The network layer concerns with \_\_\_\_\_  
 a) packets      b) bits                                      c) frames                                      d) IP  
 Answer: (a) [WBUT 2015, 2016]
  
7. An endpoint of an inter-process communication flow across a computer network is called  
 a) socket                                      b) pipe                                      c) port                                      d) none of these  
 Answer: (a) [WBUT 2015]
  
8. IPv6 addresses have a size of \_\_\_\_\_  
 a) 32 bits                                      b) 64 bits                                      c) 128 bits                                      d) 265 bits  
 Answer: (c) [WBUT 2015]
  
9. ICMP resides at the same layer as which of the following protocols mentioned below?  
 a) TCP                                      b) UDP                                      c) IP                                      d) ARP  
 Answer: (c) [WBUT 2016]

## POPULAR PUBLICATIONS

10. Which one of the following routine algorithms can be used for network layer design? [WBUT 2017]

- a) Shortest path Algorithm
- c) Link State Routine

- b) Distance Vector Routine
- d) All of these

Answer: (d)

11. ICMP is primarily used for

- a) Error diagnostic
- c) Forwarding

- b) Addressing
- d) None of these

Answer: (a)

[WBUT 2017]

### **Short Answer Type Questions**

1. What is Gateways? Differentiate between hub and switch? [WBUT 2014, 2017]

Answer:

A Gateway is a network node that is equipped to interface with another network that possibly uses different protocols. Gateways are therefore protocol converters that may operate at any layer.

Hubs and switches are networking equipments that inter-connect several hosts. They differ in the way that they pass on network traffic that they receive. A hub repeats everything it receives on all other ports. A switch on the other hand makes a short analysis of the packet received and tries to repeat it only on an appropriate port. For Ethernet, a hub does not isolate collision domain. Switches on the other hand isolate collision domain and hence permit a larger number of hosts to operate smoothly with low collision levels.

2. Difference between router & bridge?

[WBUT 2014, 2017]

Answer:

- 1) Routers are more intelligent than bridges in the sense that it runs an algorithm that depends on the contents of a packet. For example, an IP router runs the routing algorithm based on the destination IP address of the packet.
- 2) Routers can operate on interfaces that lead to identical media types but bridges are meant to interconnect different kinds of media. For example we can have a router connecting Ethernet LANs. A bridge on the other hand can connect an Ethernet LAN with a Token-ring LAN (for example).
- 3) Routers allow hosts that aren't practically on the same logical network to be able to communicate with each other, while bridges can only connect networks that are logically the same.
- 4) Routers operate at the layer 3 (network layer) of the OSI model, while bridges are only at the layer 2 (Data link layer).

3. What is distance vector routing protocol? What is difference between RIP and EGP?

[WBUT 2014]



**Answer:**

**1<sup>st</sup> Part:**

Distance Vector Routing Protocol (DVRP) is one of two major routing protocols for communications methods that use data packets sent over Internet Protocol (IP). DVRP requires routing hardware to report the distances of various nodes within a network or IP topology in order to determine the best and most efficient routes for data packets.

**2<sup>nd</sup> Part:**

Routing Information Protocol (RIP) is a dynamic protocol used to find the best route or path from end-to-end (source to destination) over a network by using a routing metric/hop count algorithm. This algorithm is used to determine the shortest path from the source to destination, which allows the data to be delivered at high speed in the shortest time.

RIP plays an important role providing the shortest and best path for data to take from node to node. The hop is the step towards the next existing device, which could be a router, computer or other device. Once the length of the hop is determined, the information is stored in a routing table for future use. RIP is being used in both local and wide area networks and is generally considered to be easily configured and implemented.

Exterior Gateway Protocol (EGP) is a protocol for exchanging routing information between two neighbour gateway hosts (each with its own router) in a network of autonomous systems. EGP is commonly used between hosts on the Internet to exchange routing table information. The routing table contains a list of known routers, the addresses they can reach, and a cost metric associated with the path to each router so that the best available route is chosen. Each router polls its neighbour at intervals between 120 to 480 seconds and the neighbour responds by sending its complete routing table. EGP-2 is the latest version of EGP.

**4. a) An organization with a site address of 145.99.0.0 needs to be subnetted. The network administrator wants to create 32 subnets. What should be the value of the subnet mask? Design the subnets.**

**b) What do you mean by a supernet?**

[WBUT 2015]

**Answer:**

a) Address of the site is 145.99.0.0

To set 32 subnets we need 6 subnet bits. So the last octet in binary will be 1111 1100.

Here number of hosts per subnet is 2.

So Address: 145.99.0.0

Network:  $255.255.255.252 = 30$

Network: 145.99.0.0 / 30

Broadcast: 145.99.0.3

Host Min: 145.99.0.1

Host Max: 145.99.0.2

Hosts / Net: 2



**POPULAR PUBLICATIONS**

b) A supernet is created by combining several Internet Protocol (IP) networks or subnets into one network with a single classless interdomain routing (CIDR) prefix. The new combined network has the same routing prefix as the collection of the prefixes of the subnets. The procedure used to create a supernet is commonly called supernetting, route aggregation or route summarization. Supernetting enables organizations to modify their network size and minimize the extensive requirement of network routing devices by combining several independent routes. It also helps to conserve address space and helps the router to effectively store routing information and minimize processing overheads while matching the routes. Supernetting supports the CIDR address coding scheme, allowing routing table entries to be reduced.

**5. What do you mean by transparent bridge? How the loop problem is removed in transparent bridge? [WBUT 2016]**

**Answer:**

**1<sup>st</sup> Part:**

Transparent bridges are devices which connects more than one network segments with other bridges to make all routing decisions. A transparent bridge is essentially used to learn the MAC addresses of all nodes and their associated port, to filter incoming frames whose destination MAC addresses are located on the same incoming port, and to forward incoming frames to the destination MAC through their associated port.

**2<sup>nd</sup> Part:**

To solve the looping problem, the bridges use the spanning tree algorithm to create a loop less topology.

**Long Answer Type Questions**

1. a) State the difference between IPV4 and IPV6. [WBUT 2013, 2016]

Discuss IPV6 packet format. [WBUT 2013]

b) What is the purpose of subnetting? Find the net ID and the host ID of the following IP addresses: [WBUT 2013, 2014, 2016]

i) 19.34.21.5

ii) 220.34.8.9

c) A network has subnet mask 255.255.255.224. Determine the maximum number of Host in this network. Determine the broadcast address of the network. [WBUT 2013, 2014, 2016]

**Answer:**

**a) 1<sup>st</sup> Part:**

IPv4	IPv6
Addresses are 32 bits (4 bytes) in length. So, maximum 232 addresses possible.	Addresses are 128 bits (16 bytes) in length. So, maximum 2 <sup>128</sup> addresses are possible.
Dotted Number notation, e.g., 192.168.10.160	Hexadecimal number notation, e.g., 32FE:4201:39A6:0000:0000:0000:1234:ABCD
IPSec is optional and should be supported externally	IPSec support is not optional



IPv4	IPv6
Header does not identify packet flow for QoS handling by routers	Header contains Flow Label field, which identifies packet flow for QoS handling by router.
Both routers and the sending host fragment packets.	Routers do not support packet fragmentation. Sending host fragments packets.
Header includes a checksum.	Header does not include a checksum.
Header includes options.	Optional data is supported as extension headers.
ARP uses broadcast ARP request to resolve IP to MAC/Hardware address.	Multicast Neighbour Solicitation messages resolve IP addresses to MAC addresses.
Broadcast addresses are used to send traffic to all nodes on a subnet.	IPv6 uses a link-local scope all-nodes multicast address.
Configured either manually or through DHCP.	Does not require manual configuration or DHCP.
Must support a 576-byte packet size (possibly fragmented).	Must support a 1280-byte packet size (without fragmentation).

**2<sup>nd</sup> Part:**

The IPv6 protocol defines a set of headers, including the basic IPv6 header and the IPv6 extension headers. The following figure shows the fields that appear in the IPv6 header and the order in which the fields appear.

Version	Traffic class	Flow label	
Payload length		Next header	Hop limit
Source address			
Destination address			

The following list describes the function of each header field.

- Version – 4-bit version number of Internet Protocol = 6.
- Traffic class – 8-bit traffic class field.
- Flow label – 20-bit field.
- Payload length – 16-bit unsigned integer, which is the rest of the packet that follows the IPv6 header, in octets.
- Next header – 8-bit selector. Identifies the type of header that immediately follows the IPv6 header. Uses the same values as the IPv4 protocol field.
- Hop limit – 8-bit unsigned integer. Decremented by one by each node that forwards the packet. The packet is discarded if the hop limit is decremented to zero.
- Source address – 128 bits. The address of the initial sender of the packet.
- Destination address – 128 bits. The address of the intended recipient of the packet. The intended recipient is not necessarily the recipient if an optional routing header is present.

**POPULAR PUBLICATIONS**

**b) 1<sup>st</sup> Part:**

The main purpose of subnetting is to help relieve network congestion. Congestion used to be a bigger problem than it is today because it was more common for networks to use hubs than switches. When nodes on a network are connected through a hub, the entire network acts as a single collision domain. What this means is that if one PC sends a packet to another PC, every PC on the entire network sees the packet. Each machine looks at the packet header, but ignores the packet if it isn't the intended recipient.

**2<sup>nd</sup> Part:**

a) Network Address	Class	Host bits	Network-id	Host-id
(i) 19.34.21.5	A	34.21.5	19	34.21.5
(ii) 220.34.8.9	C	9	220.34.8	9

c) Number of Hosts = 12. Here in the Broadcast address, host = 11111. So, the broadcast address is 255.255.255.255

2. a) What is autonomous system (AS)? What is the difference between intradomain and Inter domain AS? Explain an Interdomain routing protocol. [WBUT 2013]

**Answer:**

**1<sup>st</sup> Part:**

On the Internet, an autonomous system (AS) is the unit of router policy, either a single network or a group of networks that is controlled by a common network administrator. (or group of administrators) on behalf of a single administrative entity (such as a university, a business enterprise, or a business division). An autonomous system is also sometimes referred to as a routing domain. An autonomous system is assigned a globally unique number, sometimes called an Autonomous System Number (ASN). Networks within an autonomous system communicate routing information to each other using an Interior Gateway Protocol (IGP) like RIP, OSPF, etc. An autonomous system shares routing information with other autonomous systems using the Border Gateway Protocol (BGP).

**2<sup>nd</sup> Part:**

Intra-Autonomous System	Inter-Autonomous System
An intra-AS routing protocol is used to configure and maintain the routing tables within an autonomous system (AS).  Intra-AS routing protocols are also known as interior gateway protocols  RIP: Routing Information Protocol	An inter-autonomous system routing protocol provides routing between autonomous systems (that is, administrative domains).    The Border Gateway Protocol (BGP)

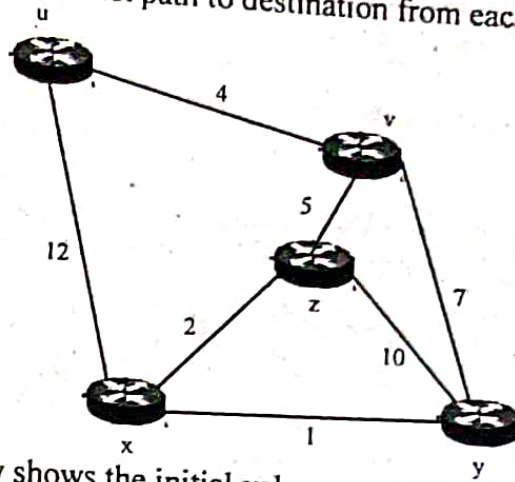
**3<sup>rd</sup> Part:**

Distance vector routing protocol is an example of inter domain routing protocol:



COMPUTER NETWORKS

- i) pass periodic copies of routing table to neighbour routers
- ii) accumulate distance vectors
- iii) routers discover the best path to destination from each neighbour.



A: The first table below shows the initial values at z. The second table shows the contents after one hop of information received from the neighbours, the third after two hops, and the last after three hops (where the least-cost path from x-to-u via z is found).

Cost to

	u	v	x	y	z
From v	$\infty$	$\infty$	$\infty$	$\infty$	$\infty$
From x	$\infty$	$\infty$	$\infty$	$\infty$	$\infty$
From y	$\infty$	$\infty$	$\infty$	$\infty$	$\infty$
From z	$\infty$	5	2	10	0

Cost to

	u	v	x	y	z
From v	4	0	$\infty$	7	5
From x	12	$\infty$	0	1	2
From y	$\infty$	7	1	0	10
From z	9	5	2	3	0

Cost to

	u	v	x	y	z
From v	4	0	7	7	5
From x	12	7	0	1	2
From y	11	7	1	0	3
From z	9	5	2	3	0

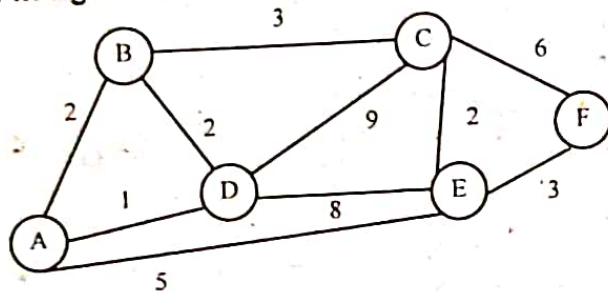
Cost to

	u	v	x	y	z
From v	4	0	7	7	5
From x	11	7	0	1	2
From y	11	7	1	0	3
From z	9	5	2	3	0

b) What is the difference between RIP and OSPF?

**Answer:**  
 RIP is based on Bellman Ford algorithm. OSPF is based on Link state routing. RIP uses hop count for calculating shortest route. OSPF uses topological graph for calculating shortest path.  
 RIP uses classfull (RIP v1) and classless/subnetting (RIP v2) networking in different versions. OSPF uses both in same version.

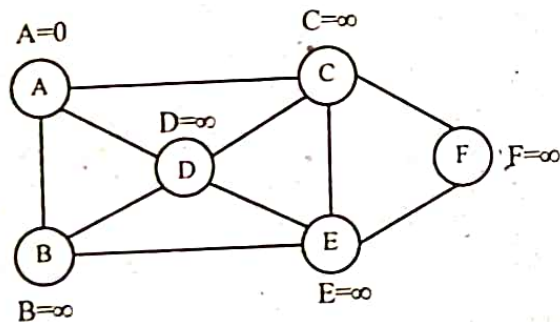
c) Apply Dijkstra algorithm to find the shortest path from node A to node F of the network graph shown in figure below. Do the same for Bellman-Ford algorithm. [WBUT 2013]



**Answer:**

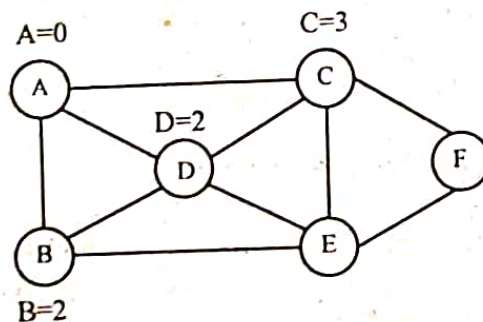
In the above, A is the root node initiated to = 0 and other are set to  $\infty$ .

**Step 1:**



**Step 2:**

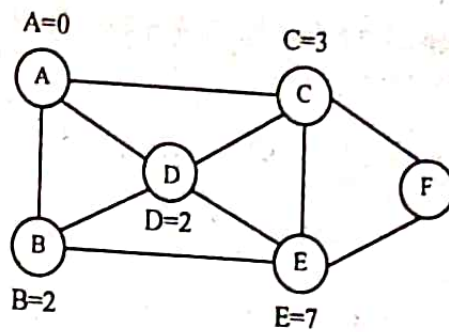
As, **Node A** is connected to B, D & c, so, it visits the adjacent nodes.



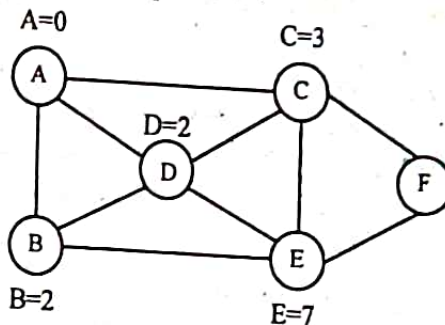
**Step 3:**

Taking **Node B**, are precede such that if  $d[u] + w(u,v) < d[v]$  Then,  
 $d[v] = d[u] + w(u,v)$

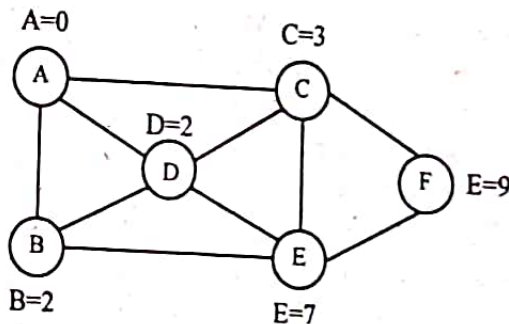




**Step 4:**  
Taking **Node D**, from D not transition possible.



**Step 5:**  
Taking **Node C**,



**Step 6:**  
Taking node E, F will be 10 which is  $>9$   
So, the shortest path is ACF.

*Dijkstra's algorithm* requires global information of network where *Bellman-Ford algorithm* uses only local knowledge of neighboring nodes. The result of the above problem will be same as the Dijkstra's solution.

3. a) State the advantage of IPV6 over IPV4.

[WBUT 2014]

Answer:

1. **Larger Address Space:** Address filed in IPv6 is 128 bits long while the address filed of IPv4 is only 32 bits in length. IPv6 offers very large, i.e. 296 address space as compared to IPv4.
2. **Better header format:** The header of IPv6 has been designed in a way to speed-up the routing process. In header of IPv6 options are separated from the base header. Options are inserted into base header only when required by the upper-layer data.

## POPULAR PUBLICATIONS

3. **Provision for extension:** IPv6 has been designed in a way that a protocol can be extended easily to meet the requirements of emerging technologies or new applications.
4. **Resource Allocation support in IPv6:** IPv6 provides a mechanism called Flow Label for resource allocation. Flow label enables source to send request for the special handling of a packet. This mechanism is really helpful in real-time audio and video transmission.
5. **Security Features:** To ensure confidentiality and packet's integrity encryption and authentication options are included in IPv6.

[WBUT 2014, 2016]

b) Differentiate between ARP and RARP.

**Answer:**

**ARP: (Address Resolution Protocol)**

When an Ethernet frame is sent from one host on a LAN to another, it is the 48-bit Ethernet address that determines for which interface the frame is destined. The device driver software never looks at the destination IP address in the IP datagram. Address resolution provides a mapping between the two different forms of addresses: 32-bit IP addresses and whatever type of address the data link uses. ARP provides a dynamic mapping from an IP address to the corresponding hardware address. We use the term dynamic since it happens automatically and is normally not a concern of either the application user or the system administrator.

**RARP: (Reverse Address Resolution Protocol)**

Each system on a network has a unique hardware address, assigned by the manufacturer of the network interface. The principle of RARP is for the diskless system to read its unique hardware address from the interface card and send an RARP request (a broadcast frame on the network) asking for someone to reply with the diskless system's IP address (in an RARP reply).

4. a) What is CIDR notation? What is its significance in case of classless addressing?

b) What do you mean by a private address? What is NAT?

[WBUT 2015]

**Answer:**

a) 1<sup>st</sup> Part:

Classless Inter Domain Routing (CIDR) is a method for assigning IP addresses without using the standard IP address classes like Class A, Class B or Class C.

In CIDR notation, an IP address is represented as A.B.C.D /n, where "/n" is called the IP prefix or network prefix. The IP prefix identifies the number of significant bits used to identify a network. For example, 192.9.205.22 /18 means, the first 18 bits are used to represent the network and the remaining 14 bits are used to identify hosts. Common prefixes are 8, 16, 24, and 32.



**2<sup>nd</sup> Part:**

In order to extend the life of IP version 4 until the newer IP version 6 could be completed, it was necessary to take a new approach to addressing IPv4 devices. This new system calls for eliminating the notion of address classes entirely, creating a new classless addressing scheme sometimes called Classless Inter-Domain Routing (CIDR).

b) A private IP address is a non-Internet facing IP address on an internal network. Private IP addresses are provided by network devices, such as routers, using network address translation (NAT).

Originally it was thought that IPv4's 32-bit IP addressing system -- yielding 4,294,967,296 theoretical IP addresses -- would be adequate for all purposes. However, as the Internet grew it became apparent that something had to fill the gap between IPv4 and a future system (which would turn out to be IPv6) that would take time to develop and implement. Private IP addressing and NAT fill that gap with the private IP range. Private IP addressing uses addresses from the class C range reserved for NAT (192.168.0.0 - 192.168.255.255). Private addresses can be assigned by the router using DHCP or be manually set, after which those addresses can communicate with one another through the router.

Private IP addresses can only be guaranteed unique to an internal network, excepting conflicts. If a directly connected computer does not have a static IP address assigned, even assigning a private IP address manually will not enable communication.

Private IP addresses cannot be directly contacted over the Internet as a computer with a public IP address can. This situation affords an extra layer of security: A network NAT device communicates with the Internet using its public IP address from an ISP and checks to see if any incoming data was requested by one of the private IP-assigned computers. If so, it is directed to that computer; if not it is typically discarded.

Another benefit of using NAT, for those who do tend to have incoming requests -- like websites, file and game servers -- is the ability to quickly switch servers in the event of a crash, as the incoming traffic can all be forwarded to a back-up server very easily.

5. a) State the difference between static and dynamic routing.

[WBUT 2016]

Answer:

static routing	dynamic routing
Static routing is when you statically configure a router to send traffic for particular destinations in preconfigured directions	Dynamic routing is when you use a routing protocol such as OSPF, ISIS, EIGRP, and/or BGP to figure out what paths traffic should take.

b) Describe any shortest path algorithm.

[WBUT 2016]

Answer:

Let the node at which we are starting be called the initial node. Let the distance of node Y be the distance from the initial node to Y. Dijkstra's shortest path algorithm will assign some initial distance values and will try to improve them step by step.



## POPULAR PUBLICATIONS

1. Assign to every node a tentative distance value: set it to zero for our initial node and to infinity for all other nodes.
2. Mark all nodes unvisited. Set the initial node as current. Create a set of the unvisited nodes called the unvisited set consisting of all the nodes except the initial node.
3. For the current node, consider all of its unvisited neighbours and calculate their tentative distances. For example, if the current node A is marked with a distance of 6 and the edge connecting it with a neighbour B has length 2, then the distance to B (through A) will be  $6+2=8$ . If this distance is less than the previously recorded tentative distance of B, then overwrite that distance. Even though a neighbour has been examined, it is not marked as "visited" at this time and it remains in the unvisited set.
4. When we are done considering all of the neighbours of the current node, mark the current node as visited and remove it from the unvisited set. A visited node will never be checked again.
5. If the destination node has been marked visited (when planning a route between two specific nodes) or if the smallest tentative distance among the nodes in the unvisited set is infinity (when planning a complete traversal), then stop. The algorithm has finished.
6. Select the unvisited node that is marked with the smallest tentative distance and set it as the new "current node" then go back to step 3.

6. With respect to Ethernet protocol answer the following:

[WBUT 2017]

- a) How is collision usually detected?
- b) What will the transmission station do upon collision?
- c) Why is there a minimum limit to the size of the frame?

**Answer:**

a) In Ethernet world, the result of two nodes transmitting in the same time. The frames from each machine impact and collide when they meet on the physical media. This contention-based methods allow any device to try to access the medium whenever it has data to send. To prevent complete "choking" on the media, these methods use a Carrier Sense Multiple Access (CSMA) process to first detect if the media is transmitting any signal in that moment. If there is a signal on the media from another computer, it means that another device is talking. When the device attempting to transmit sees that the media is in use, it will wait and try again after a short period of time. If no carrier signal is detected, the device transmits its data. Ethernet and wireless networks use contention-based media access control.

It is possible that the CSMA process will fail and two devices will transmit at the same time. This is called a data collision. If this occurs, the data sent by both devices will be corrupted and will need to be resent. As the number of nodes increases on a shared media, the probability of successful media access without a collision decreases. Additionally, the recovery mechanisms required to correct errors due to these collisions further diminishes the overall throughput.



**b) CSMA/CD Protocol:**

It is used when more than two computers are sharing the same medium typically something that is happening in LAN networks when computers are connected through hub. CSMA/CD is a practice used for multiple access control protocols. Transmission will be taken place by a particular station at a time but when more than one station will transmit at the same time as a result collision can be occurred.

**CSMA/CA Protocol:**

CSMA/CA (Carrier Sense Multiple Access/Collision Avoidance) that has been introduced to get better the CSMA performance. According to that a station will sense the transmission medium before sending the frame. CSMA/CA protocol is used in wireless (802.11) LANs. Moreover, when a station sense collision in case of CSMA/CA, it first waits for some time after that but before packets transmission, it will listen to the channel for its idleness, if so packets transmission will start otherwise it will wait for the medium to become unoccupied.

Note that above mentioned both CSMA/CD and CSMA/CA protocols are the best example of Physical Protocols.

c) The minimum frame size on Ethernet is so that by the time the beginning of a frame gets all the way across a maximum-width network, if a collision is detected there on the far side of the network, there's still enough time for the jam signal (collision detection notification) to make it all the way back across the network while the transmitter is still transmitting, so that the transmitter will receive the jam signal and know it got collided with so it will have to retransmit.

Anything below 64 bytes is just considered a runt (a buggy transmission) and ignored. Runts are not collisions and do not trigger retransmissions.

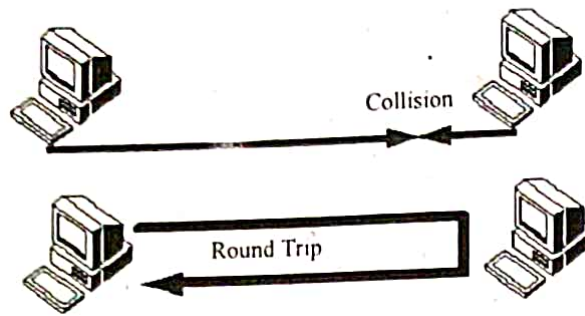
But this is all pretty much moot as nobody runs hubs anymore, since Gigabit Ethernet requires switches. So today's networks are always full duplex and CSMA/CD is a thing of the past

- A sender sends the packet (frame) and determine whether it got received by receiver on the other side of channel or not. It may not be reached there mostly due to collisions with other packets in transit.

So there must be a mechanism by which sender get to know whether a packet is reached at the receiver or not. To check this, you want the head of the packet to transit from one end of the wire and back again before the tail of the packet finished transmission. If there's a transmission anywhere on the wire overlapping, you'll hear it collide at your receiver.

Frames must be at least 64 bytes long, not including the preamble, so, if the data field is shorter than 46 bytes, it must be compensated by the Pad field.

## POPULAR PUBLICATIONS



- Secondly setting a minimum frame size allows you to spend multiple receive cycles verifying your frames' check sums.

7. Write short notes on the following:

- a) Socket
- b) BGP
- c) RIP
- d) ARP & RARP

[WBUT 2013]  
[WBUT 2014]  
[WBUT 2014]  
[WBUT 2017]

**Answer:**

**a) Socket:**

A network socket is an endpoint of an inter-process communication flow across a computer network. Today, most communication between computers is based on the Internet Protocol; therefore most network sockets are Internet sockets.

A socket API is an application programming interface (API), usually provided by the operating system, that allows application programs to control and use network sockets. Internet socket APIs are usually based on the Berkeley sockets standard.

A socket address is the combination of an IP address and a port number, much like one end of a telephone connection is the combination of a phone number and a particular extension. Based on this address, internet sockets deliver incoming data packets to the appropriate application process or thread.

**b) BGP:**

BGP is a complex, advanced distance Exterior Gateway Protocol (EGP), BGP exchange routing information between Autonomous Systems (ASs).

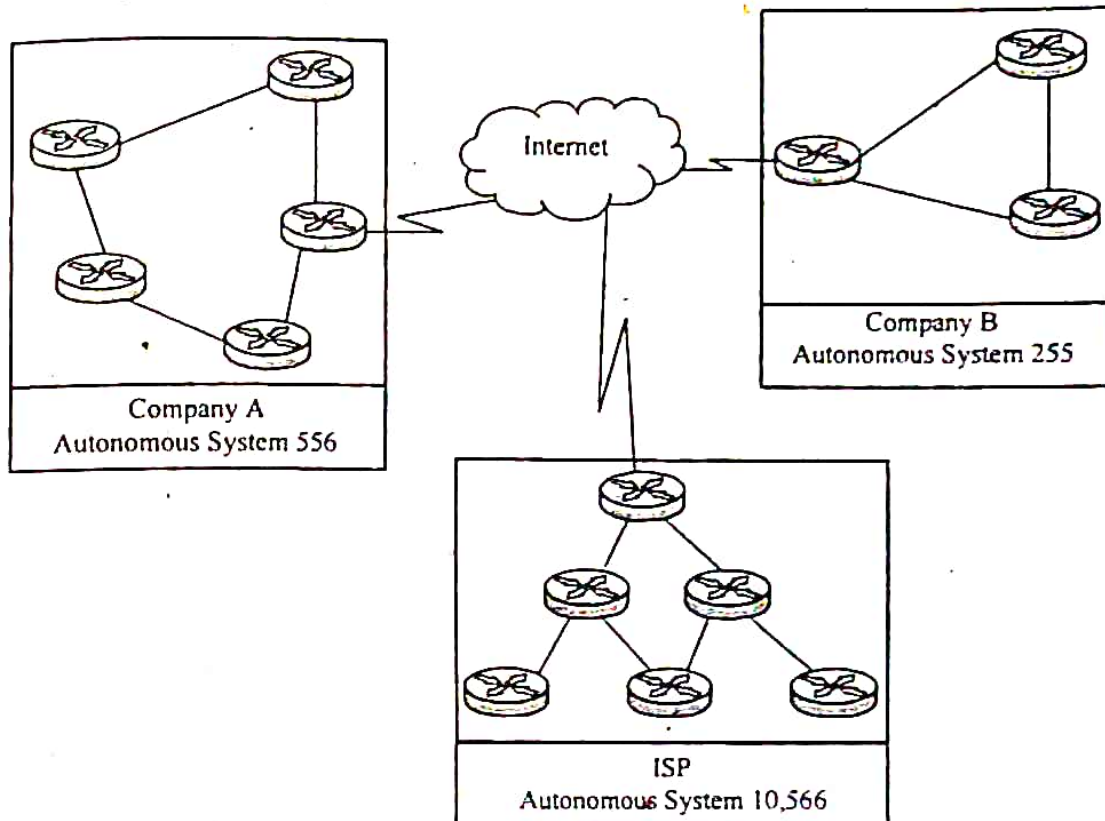
Unlike Interior routing protocols such as RIP, EIGRP, and OSPF that run inside a company's network, BGP uses a different basic algorithm for building a loop-free topology than any of the above mentioned protocols.

BGP is especially used for exchanging routing information between all of the major Internet Service Providers (ISPs), as well between larger client sites and their respective ISPs. And, in some large enterprise networks, BGP is used to interconnect different geographical or administrative regions.

BGP is Primarily used to support the complexity of the public Internet; Cisco has added several clever and useful features to its BGP implementation (BGP 4). Some of the primary attributes of BGP is the use of pieces of information about a known route, where it came from, and how to reach it, A BGP router will also generate an error message if it



receives a route that is missing these are mandatory attributes. Clients/ Corporate Networks being connected by BGP.



### e) RIP:

**The Routing Information Protocol (RIP)** is one of the most commonly used Interior Gateway Protocol (IGP) routing protocols on internal networks (and to a lesser extent, networks connected to the Internet), which helps routers dynamically adapt to changes of network connections by communicating information about which networks each router can reach and how far away those networks are.

Although RIP is still actively used, it has largely been made obsolete by routing protocols such as OSPF and IS-IS.

The routing algorithm used in RIP, the **Bellman-Ford algorithm**, was first deployed in a computer network in 1969, as the initial routing algorithm of the ARPANET.

A version of RIP which supported the Internet Protocol (IP) was later included in the Berkeley Software Distribution (BSD) of the Unix operating system as the routed daemon, and various other vendors would implement their own implementations of the routing protocol. Eventually RFC 1058 was issued to unify the various implementations under a single standard.

**RIP is a distance-vector routing protocol**, which employs the hop count as a routing metric. The maximum number of hops allowed with RIP is 15. Each RIP router transmits full updates every 30 seconds by default, generating large amounts of network traffic in lower bandwidth networks. It runs above the network layer of the Internet protocol suite, using UDP port 520 to carry its data. A mechanism called split horizon with limited poison reverse is used to avoid routing loops. Routers of some brands also use a holddown mechanism known as heuristics, whose usefulness is arguable and is not a part of the standard protocol.

## POPULAR PUBLICATIONS

There are three versions of RIP, RIPv1, RIPv2, and RIPng.

**RIPv1** uses classful routing. The routing updates do not carry subnet information, lacking support for variable length subnet masks. This limitation makes it impossible to have different-sized subnets inside of the same network class.

Due to the deficiencies of RIPv1, **RIPv2** was developed in 1994 and included the ability to carry subnet information, thus supporting Classless Inter-Domain Routing. However to maintain backwards compatibility the 15 hop count limit remained. Rudimentary plain text authentication was added to secure routing updates. Later, MD5 authentication was defined in RFC 2082.

**d) ARP & RARP:** *Refer to Question No. 3(b) of Long Answer Type Questions.*



# TRANSPORT LAYER

## Multiple Choice Type Questions

1. Process-to-process delivery is the function of ..... layer. [WBUT 2014]  
 a) transport      b) network      c) physical      d) none of these

Answer: (a)

2. Port number is: [WBUT 2014]  
 a) process number      b) computer physical address  
 c) both (a) and (b)      d) none of these

Answer: (a)

3. UDP is: [WBUT 2014]  
 a) Connectionless      b) connection-oriented  
 c) both (a) and (b)      d) none of these

Answer: (a)

4. Which one of the following is a transport layer protocol used in internet? [WBUT 2015]  
 a) TCP      b) TCP and UDP      c) UDP      d) none

Answer: (b)

5. Which of the following is *not* Network support Layer? [WBUT 2017]  
 a) Transport Layer      b) Network Layer  
 c) Data Link Layer      d) Physical Layer

Answer: (a)

6. The amount of data that can be carried from one point to another in a given period of time is [WBUT 2017]  
 a) Scope      b) Bandwidth      c) Limitation      d) Capacity

Answer: (b)

## Short Answer Type Questions

1. "TCP and UDP" – which one is better? Justify your answer. [WBUT 2013]

Answer:

TCP ensures a reliable and ordered delivery of a stream of bytes from user to server or vice versa. UDP is not dedicated to end to end connections and communication does not check readiness of receiver.

**Reliability:**

TCP is more reliable since it manages message acknowledgment and retransmissions in case of lost parts. Thus there is absolutely no missing data. UDP does not ensure that

## POPULAR PUBLICATIONS

communication has reached receiver since concepts of acknowledgment, time out and retransmission are not present.

### **Ordering:**

TCP transmissions are sent in a sequence and they are received in the same sequence. In the event of data segments arriving in wrong order, TCP reorders and delivers application. In the case of UDP, sent message sequence may not be maintained when it reaches receiving application. There is absolutely no way of predicting the order in which message will be received.

### **Connection:**

TCP is a heavy weight connection requiring three packets for a socket connection and handles congestion control and reliability. UDP is a lightweight transport layer designed atop an IP. There are no tracking connections or ordering of messages.

### **Method of transfer:**

TCP reads data as a byte stream and message is transmitted to segment boundaries. UDP messages are packets which are sent individually and on arrival are checked for their integrity. Packets have defined boundaries while data stream has none.

[WBUT 2014]

## **2. Indicate QoS in transport layer.**

### **Answer:**

In packet-switched computer networking, Quality of Service (QoS) refers to the probability of the telecommunication network meeting a given traffic contract. Sometimes, QoS is used informally to refer to the probability of a packet succeeding in passing between two points in the network. For example, telephony QoS refers to lack of noise and tones on the circuit, appropriate loudness levels etc.

The Internet was not conceived with a need for QoS application and the entire Internet ran on a "best effort" system. However, several things that can happen to packets as they travel from origin to destination:

- **Dropped packets:** The routers might fail to deliver (drop) some packets if they arrive when their buffers are already full. Some, none, or all of the packets might be dropped, depending on the state of the network, and it is impossible to determine what happened in advance. The receiving application must ask for this information to be retransmitted, possibly causing severe delays in the overall transmission.
- **Delay:** It might take a long time for a packet to reach its destination, because it gets held up in long queues, or takes a less direct route to avoid congestion. Alternatively, it might follow a fast, direct route. Thus delay is very unpredictable.
- **Jitter:** Packets from source will reach the destination with different delays. This variation in delay is known as jitter and can seriously affect the quality of streaming audio and/or video.
- **Out-of-order delivery:** When a collection of related packets are routed through the Internet, different packets may take different routes, each resulting in a different delay. The result is that the packets arrive in a different order to the one



with which they were sent. This problem necessitates special additional protocols responsible for rearranging out-of-order packets once they reach their destination.

- **Error:** Sometimes packets are misdirected, or combined together, or corrupted, while en route. The receiver has to detect this and, just as if the packet was dropped, ask the sender to repeat itself.
- Throughput
- Security

Applications which require QoS are of the following types:

- **Streaming multimedia**, which may require guaranteed throughput.
- **IP telephony** or *Voice over IP* (VOIP), which may require strict limits on jitter and delay.
- **Video Teleconferencing** (VTC), which requires low jitter.
- **Dedicated link emulation**, which requires both guaranteed throughput and imposes limits on maximum delay and jitter.
- **A safety-critical application**, such as remote surgery, may require a guaranteed level of availability (this is also called hard QoS).

These types of service are called inelastic, meaning that they require a certain level of bandwidth to function - any more than required is unused, and any less will render the service non-functioning. By contrast, elastic applications can take advantage of however much or little bandwidth is available.

**3. State the basic differences between TCP and UDP.**

[WBUT 2016]

Answer:

TCP (Transmission Control Protocol)	UDP (User Datagram Protocol)
TCP is a connection-oriented protocol, a connection can be made from client to server, and from then on any data can be sent along that connection.	A simpler message-based connectionless protocol. With UDP you send messages (packets) across the network in chunks.
<b>Reliable</b> - when you send a message along a TCP socket, you know it will get there unless the connection fails completely. If it gets lost along the way, the server will re-request the lost part. This means complete integrity, things don't get corrupted.	<b>Unreliable</b> - When you send a message, you don't know if it'll get there, it could get lost on the way.
<b>Ordered</b> - if you send two messages along a connection, one after the other, you know the first message will get there first. You don't have to worry about data arriving in the wrong order.	<b>Not ordered</b> - If you send two messages out, you don't know what order they'll arrive in.
<b>Heavyweight</b> - when the low level parts of the TCP "stream" arrive in the wrong order, resend requests have to be sent, and all the out of sequence parts have to be put back together, so requires a bit of work to piece together.	<b>Lightweight</b> - No ordering of messages, no tracking connections, etc. It's just fire and forget! This means it's a lot quicker, and the network card / OS have to do very little work to translate the data back from the packets.



4. Discuss the function of Transport Layer.

**Answer:**

***Functions of Transport Layer:***

The purpose of the Transport Layer is to provide transparent "peer to peer" communication, with the remote (peer) transport entity, thus relieving the upper layers from any concern with providing reliable and cost-effective data transfer. The transport layer usually turns the unreliable and very basic service provided by the Network Layer into a more powerful one. It provides end-to-end control and information transfer with the quality of service needed by the application program.

5. Besides bandwidth and latency, which other parameters are needed to give a good characterization of QoS offered by a network used for digitized voice traffic? [MODEL QUESTION]

**Answer:**

QoS (Quality of Service) refers to a broad collection of networking technologies and techniques. The goal of QoS is to provide guarantees on the ability of a network to deliver predictable results. Elements of network performance within the scope of QoS often include availability (uptime), bandwidth (throughput), latency (delay), and error rate.

QoS involves prioritization of network traffic. QoS can be targeted at a network interface, toward a given server or router's performance, or in terms of specific applications. A network monitoring system must typically be deployed as part of QoS, to insure that networks are performing at the desired level.

QoS is especially important for the new generation of Internet applications such as VoIP, video-on-demand and other consumer services. Some core networking technologies like Ethernet were not designed to support prioritized traffic or guaranteed performance levels, making it much more difficult to implement QoS solutions across the Internet.

6. What is choke packet? [MODEL QUESTION]

**Answer:**

A specialized packet that is used for flow control along a network. A router detects congestion by measuring the percentage of buffer in use, line utilization and average queue lengths. When it detects congestion, it sends a choke packet across the network to the entire data source associated the congestion.

7. What is connection oriented protocol? Briefly explain the services of that protocol. [MODEL QUESTION]

**Answer:**

In telecommunications, connection-oriented describes a means of transmitting data in which the devices at the end points use a preliminary protocol to establish an end-to-end connection before any data is sent. Connection-oriented protocol service is sometimes called a "reliable" network service, because it guarantees that data will arrive in the proper sequence. Transmission Control Protocol (TCP) is a connection-oriented protocol.



For connection-oriented communications, each end point must be able to transmit so that it can communicate. The alternative to connection-oriented transmission is the connectionless approach, in which data is sent from one end point to another without prior arrangement. Connectionless protocols are usually described as stateless because the end points have no protocol-defined way to remember where they are in a "conversation" of message exchanges. Because they can keep track of a conversation, connection-oriented protocols are sometimes described as stateful.

**Long Answer Type Questions**

1. What do you mean by traffic shaping? Explain in detail leaky bucket algorithm?

[WBUT 2015]

**Answer:**

**1<sup>st</sup> Part:**

Traffic shaping, also known as "packet shaping," is the practice of regulating network data transfer to assure a certain level of performance, quality of service (QoS) or return on investment (ROI). The practice involves delaying the flow of packets that have been designated as less important or less desired than those of prioritized traffic streams. Regulating the flow of packets into a network is known as "bandwidth throttling." Regulation of the flow of packets out of a network is known as "rate limiting."

**2<sup>nd</sup> Part:**

The leaky bucket is an algorithm used in packet switched computer networks and telecommunications networks to check that data transmissions conform to defined limits on bandwidth and burstiness (a measure of the unevenness or variations in the traffic flow). The leaky bucket algorithm is also used in leaky bucket counters, e.g. to detect when the average or peak rate of random or stochastic events or stochastic processes exceed defined limits.

The Leaky Bucket Algorithm is based on an analogy of a bucket that has a hole in the bottom through which any water it contains will leak away at a constant rate, until or unless it is empty. Water can be added intermittently, i.e. in bursts, but if too much is added at once, or it is added at too high an average rate, the water will exceed the capacity of the bucket, which will overflow.

There are actually two different methods of applying this analogy described in the literature. These give what appear to be two different algorithms, both of which are referred to as the leaky bucket algorithm. This has resulted in confusion about what the leaky bucket algorithm is and what its properties are.

In one version, the analogue of the bucket is a counter or variable, separate from the flow of traffic, and is used only to check that traffic conforms to the limits, i.e. the analogue of the water is brought to the bucket by the traffic and added to it so that the level of water in the bucket indicates conformance to the rate and burstiness limits. This version is referred to here as the leaky bucket as a meter. In the second version, the traffic passes through a queue that is the analogue of the bucket, i.e. the traffic is the analogue of the water passing through the bucket. This version is referred to here as the leaky bucket as a

## POPULAR PUBLICATIONS

queue. The leaky bucket as a meter is equivalent to (a mirror image of) the token bucket algorithm, and given the same parameters will see the same traffic as conforming or nonconforming. The leaky bucket as a queue can be seen as a special case of the leaky bucket as a meter.

2. Write short notes on the following:

a) Token Bucket Algorithm

[WBUT 2016]

b) QoS in transport layer

[WBUT 2016]

Answer:

a) **Token Bucket Algorithm:**

The token bucket is similar in some respects to the leaky bucket, but the primary difference is that the token bucket allows bursty traffic to continue transmitting while there are tokens in the bucket, up to a user-configurable threshold. It thereby accommodates traffic flows with bursty characteristics. The token bucket mechanism dictates that traffic can be transmitted based on the presence of tokens in the bucket. Tokens each represent a given number of bytes and when tokens are present a flow is allowed to transmit traffic up to its peak burst rate if there are adequate tokens in the bucket and if the burst threshold is configured appropriately.

The algorithm is as follows (assume each token = 1 byte):

- a token is added to the bucket every  $1/r$  seconds
- the bucket can hold at the most  $b$  tokens
- if a token arrives when the bucket is full, it is discarded
- when a packet of  $n$  bytes arrives,  $n$  tokens are removed from the bucket and the packet is sent to the network
- if fewer than  $n$  tokens are available, no tokens are removed from the bucket and the packet is considered to be nonconformant.

The algorithm allows bursts of up to  $b$  bytes, but over the long run the output of conformant packets is limited to the constant rate,  $r$ . Nonconformant packets can be treated in various ways:

- dropped
- queued for subsequent transmission when sufficient tokens are in the bucket
- transmitted but marked as non-conformant and possibly to be dropped subsequently if the network is overloaded.

b) QoS in transport layer: *Refer Question No. 2 of Short Answer Type Questions.*

3. a) What is the difference between the flow control and the congestion control? Justify for the long haul communication, the window flow control is ineffective.

b) Compare reservation based congestion control with permit based congestion control.

[MODEL QUESTION]



**Answer:**

**a) Flow control vs. congestion control:**

Flow control means preventing the source from sending data that the sink will end up dropping because it runs out of buffer space. This is fairly easy with a sliding window protocol--just make sure the source's window is no larger than the free space in the sink's buffer. TCP does this by letting the sink advertise its free buffer space in the window field of the acks. Congestion control means preventing (or trying to prevent) the source from sending data that will end up getting dropped by a router because its queue is full. This is more complicated, because packets from different sources travelling different paths can converge on the same queue.

In long haul communication networks, bandwidth is usually so limited that calls for memory buffers or processor cycles be satisfied in much less time than it takes to send/receive a message. Credits given to senders can be honoured without necessarily tying up more than a small amount of buffers, typically one for each message being reassembled. That is, receivers can "lie" in promising buffers which may not be available at the time credits are sent. Nevertheless, by the time buffers are needed, the receiver can manage to find some. A common strategy is to share a buffer pool among many receivers, or alternatively, to page out inactive buffers.

**b) Reservation-Based** --the hosts attempt to reserve network capacity when the flow is established.

--The routers allocate resources to satisfy reservations or the flow is rejected.

--The reservation can be receiver-based (e.g., RSVP) or sender-based.

- **Permit-Based** --The sender's rate is controlled by the receiver indicating the bits per second it can absorb.

**4. What is congestion? Why does congestion occur? Explain Leaky bucket algorithm for congestion control. [MODEL QUESTION]**

**Answer:**

The leaky bucket is an algorithm used in packet switched computer networks and telecommunication networks to check that data transmissions conform to defined limits on bandwidth and burstiness (a measure of the unevenness or variations in the traffic flow). The leaky bucket algorithm is also used in leaky bucket counters, e.g. to detect when the average or peak rate of random or stochastic events or stochastic processes exceed defined limits.

The Leaky Bucket Algorithm is based on an analogy of a bucket that has a hole in the bottom through which any water it contains will leak away at a constant rate, until or unless it is empty. Water can be added intermittently, i.e. in bursts, but if too much is added at once, or it is added at too high an average rate, the water will exceed the capacity of the bucket, which will overflow.

There are actually two different methods of applying this analogy described in the literature. These give what appear to be two different algorithms, both of which are referred to as the leaky bucket algorithm. This has resulted in confusion about what the leaky bucket algorithm is and what its properties are.



## POPULAR PUBLICATIONS

In one version, the analogue of the bucket is a counter or variable, separate from the flow of traffic, and is used only to check that traffic conforms to the limits, i.e. the analogue of the water is brought to the bucket by the traffic and added to it so that the level of water in the bucket indicates conformance to the rate and burstiness limits. This version is referred to here as the leaky bucket as a meter. In the second version, the traffic passes through a queue that is the analogue of the bucket, i.e. the traffic is the analogue of the water passing through the bucket. This version is referred to here as the leaky bucket as a queue. The leaky bucket as a meter is equivalent to (a mirror image of) the token bucket algorithm, and given the same parameters will see the same traffic as conforming or nonconforming. The leaky bucket as a queue can be seen as a special case of the leaky bucket as a meter.

5. a) What is the difference between congestion control and flow control?  
b) Explain the working of leaky bucket algorithm. Give argument why the leaky bucket should allow just one packet per tick independent of how large the packet is.

[MODEL QUESTION]

Answer:

a)

Congestion control	Flow Control
When there is a bursty situation over the network path and which packet should be chosen and how are the subject of this mechanism	The over all packet and data transmission over a network path is controlled by this mechanism.
Mainly Transport Layer responsibility.	Mainly Datalink layer responsibility though every layer governs the data flow in their own manner.
Token bucket, Leaky Bucket etc algorithms are used.	Stop and Wait, Selective Repeat ARQ, Routing algorithms are used.

b) The leaky bucket is an algorithm used in packet switched computer networks and telecommunications networks to check that data transmissions conform to defined limits on bandwidth and burstiness (a measure of the unevenness or variations in the traffic flow). The leaky bucket algorithm is also used in leaky bucket counters, e.g. to detect when the average or peak rate of random or stochastic events or stochastic processes exceed defined limits.

The Leaky Bucket Algorithm is based on an analogy of a bucket that has a hole in the bottom through which any water it contains will leak away at a constant rate, until or unless it is empty. Water can be added intermittently, i.e. in bursts, but if too much is added at once, or it is added at too high an average rate, the water will exceed the capacity of the bucket, which will overflow.

There are actually two different methods of applying this analogy described in the literature. These give what appear to be two different algorithms, both of which are referred to as the leaky bucket algorithm. This has resulted in confusion about what the leaky bucket algorithm is and what its properties are.

In one version, the analogue of the bucket is a counter or variable, separate from the flow of traffic, and is used only to check that traffic conforms to the limits, i.e. the analogue of



the water is brought to the bucket by the traffic and added to it so that the level of water in the bucket indicates conformance to the rate and burstiness limits. This version is referred to here as the leaky bucket as a meter. In the second version, the traffic passes through a queue that is the analogue of the bucket, i.e. the traffic is the analogue of the water passing through the bucket. This version is referred to here as the leaky bucket as a queue. The leaky bucket as a meter is equivalent to (a mirror image of) the token bucket algorithm, and given the same parameters will see the same traffic as conforming or nonconforming. The leaky bucket as a queue can be seen as a special case of the leaky bucket as a meter

# APPLICATION LAYER

## Multiple Choice Type Questions

1. Which of the following is an application layer service? [WBUT 2013, 2016]  
 a) remote login                      b) file transfer and access  
 c) mail service                         d) all of these  
 Answer: (d)
2. When displaying a web page, the application layer uses the [WBUT 2015]  
 a) FTP protocol    b) SMTP protocol    c) HTTP protocol    d) all of these  
 Answer: (c)
3. The packet of information at the application layer is called [WBUT 2015]  
 a) packet                b) message                c) segment                d) frame  
 Answer: (b)
4. E-mail cannot be sent [MODEL QUESTION]  
 a) if the sending site does not use TCP/IP  
 b) if the receiving site does not use TCP/IP  
 c) through private networks  
 d) none of these  
 Answer: (d)
5. All objects managed by SNMP are given an object identifier. The object [MODEL QUESTION]  
 identifier always starts with  
 a) 0                                b) 1.3.2.6.1.1                c) 1.3.6.1.2.1                d) none of these  
 Answer: (c)
6. If user A wants to send a message to user B confidentially, the plain text is [MODEL QUESTION]  
 encrypted with the public key of  
 a) A                                b) B                                c) the network                d) Either A or B  
 Answer: (b)
7. A ..... can forward or block messages based on the information in [MODEL QUESTION]  
 the message itself.  
 a) proxy firewall                b) packet filter firewall  
 c) message digest                d) private key  
 Answer: (b)

## Short Answer Type Questions

1. What do you understand by data privacy? How can authentication, integrity and non-repudiation be implemented by the digital signature technique? [WBUT 2014]



**Answer:**

**1<sup>st</sup> Part:**

Data privacy refers to the evolving relationship between technology and the legal right to, or public expectation of privacy in the collection and sharing of data.

Privacy problems exist wherever uniquely identifiable data relating to a person or persons are collected and stored, in digital form or otherwise. Improper or non-existent disclosure control can be the root cause for privacy issues.

**2<sup>nd</sup> Part: Refer to Question No. 1(b) Long Answer Type Questions.**

**2. a) Discuss about the four basic principles of network security.**

**[WBUT 2015]**

**b) What is firewall?**

**Answer:**

a) Four basic principles of network security are as follows:

- **Confidentiality** - The message the recipient gets can be proven not to have been read by anyone else since it was encoded.
- **Integrity** - The message the recipient gets can be proven not to have been changed since it was encoded.
- **Authenticity** - The message the recipient gets can be proven to have been encoded by (edit) a positively-identified sender.
- **Non-repudiation** - The sender, given a message received by a recipient, cannot validly deny that the message was sent by him or that it was not the original content sent by him.

b) A system designed to prevent unauthorized access to or from a private network. Firewalls can be implemented in both hardware and software, or a combination of both. Firewalls are frequently used to prevent unauthorized Internet users from accessing private networks connected to the Internet, especially intranets. All messages entering or leaving the intranet pass through the firewall, which examines each message and blocks those that do not meet the specified security criteria.

There are several types of firewall techniques:

- **Packet filter:** Looks at each packet entering or leaving the network and accepts or rejects it based on user-defined rules. Packet filtering is fairly effective and transparent to users, but it is difficult to configure. In addition, it is susceptible to IP spoofing.
- **Application gateway:** Applies security mechanisms to specific applications, such as FTP and Telnet servers. This is very effective, but can impose a performance degradation.
- **Circuit-level gateway:** Applies security mechanisms when a TCP or UDP connection is established. Once the connection has been made, packets can flow between the hosts without further checking.
- **Proxy server:** Intercepts all messages entering and leaving the network. The proxy server effectively hides the true network addresses.

## POPULAR PUBLICATIONS

3. What is cryptography? Explain Public & private Key cryptography with example. [WBUT 2016]

**Answer:**

**1<sup>st</sup> Part:**

Cryptography involves creating written or generated codes that allows information to be kept secret. Cryptography converts data into a format that is unreadable for an unauthorized user, allowing it to be transmitted without anyone decoding it back into a readable format, thus compromising the data.

Information security uses cryptography on several levels. The information cannot be read without a key to decrypt it. The information maintains its integrity during transit and while being stored. Cryptography also aids in non-repudiation. This means that neither the creator nor the receiver of the information may claim they did not create or receive it.

**2<sup>nd</sup> Part:**

Public key encryption is considered very secure because it does not require a secret shared key between the sender and receiver. Other encryption technologies that use a single shared key to both encrypt and decrypt data rely on both parties deciding on a key ahead of time without other parties finding out what that key is. However, the fact that it must be shared between both parties opens the door to third parties intercepting the key. This type of encryption technology is called symmetric encryption, while public key encryption is known as asymmetric encryption.

Symmetric encryption (also called private-key encryption or secret-key encryption) involves using the same key for encryption and decryption.

Encryption involves applying an operation (an algorithm) to the data to be encrypted using the private key to make them unintelligible. The slightest algorithm (such as an exclusive OR) can make the system nearly tamper proof (there being so such thing as absolute security).

The main disadvantage of a secret-key cryptosystem is related to the exchange of keys. Symmetric encryption is based on the exchange of a secret (keys). The problem of key distribution therefore arises:

Moreover, a user wanting to communicate with several people while ensuring separate confidentiality levels has to use as many private keys as there are people. For a group of  $N$  people using a secret-key cryptosystem, it is necessary to distribute a number of keys equal to  $N * (N-1) / 2$ .

4. Describe the purpose of DNS protocol in the internet. [WBUT 2017]

**Answer:**

Websites are identified in computer systems by a series of numbers called IP (Internet Protocol) addresses. So that humans do not have to remember multiple numbers for all the websites they want to visit, these numbers are matched by names in a database table housed on special types of computers called Domain Name Servers. The DNS server translates the website names into the correct IP address.



- **Benefits:** Without domain name servers, navigating the Internet would become an extremely cumbersome task. Given the millions of websites in existence, keeping track of these by IP number would be impossible.
- **Function:** When you type a name such as `www.ehow.com` into a browser, the request first goes to a DNS server. If that server can translate the name to an IP address, it does so. Otherwise, the request is forwarded to a higher level server.
- **Size:** According to Dan Kaminsky, a security researcher, the Internet has about 9 million DNS servers. About 10 percent are vulnerable to malicious attacks (see Additional Resources).
- **Expert Insight:** You can learn what DNS servers are being used in your own setup by using a Windows command. In Start/Run type "`cmd`". When a black box appears, type "`ipconfig/all`". This will display the DNS servers running.
- **Warning:** When DNS servers develop problems or are maliciously hacked, you may find yourself on what you thought was the web page wanted but actually redirected to fraudulent sites.

**5. What is peer process?**

[WBUT 2017]

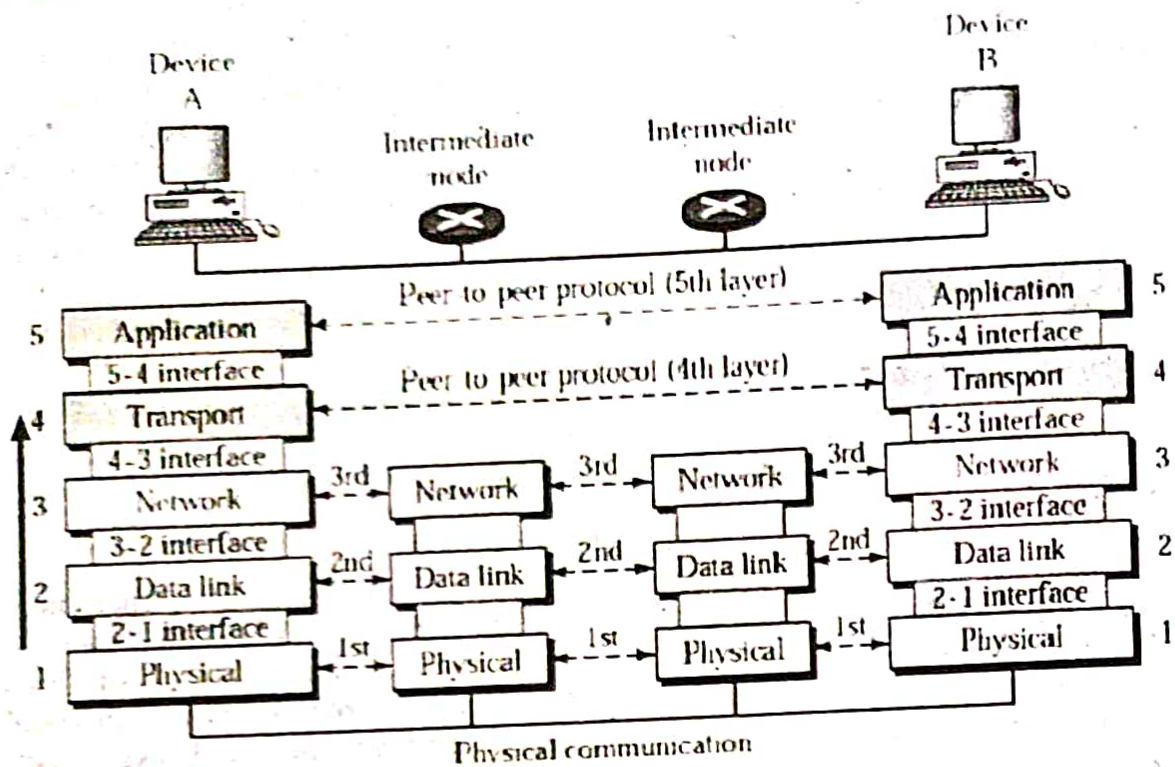
**Answer:**

**Peer-to-Peer Process:**

Within a single machine, each layer calls upon the services of the layer just below it. Layer 3, for example, uses the services provided by layer 2 and provides services for layer 4. Between machines, layer x on one machine communicates with layer x on another machine. This communication is governed by an agreed-upon series of rules and conventions called protocols. The processes on each machine that communicate at a given layer are called peer-to-peer processes. Communication between machines is therefore a peer-to-peer process using the protocols appropriate to a given layer.

At the physical layer, communication is direct as shown in the following Figure. Device A sends a stream of bits to device B (through intermediate nodes). At the higher layers, however, communication must move down through the layers on device A, over to device B, and then back up through the layers. Each layer in the sending device adds its own information to the message it receives from the layer just above it and passes the whole package to the layer just below it.

At layer 1 the entire package is converted to a form that can be transmitted to the receiving device. At the receiving machine, the message is unwrapped layer by layer, with each process receiving and removing the data meant for it. For example, layer 2 removes the data meant for it, and then passes the rest to layer 3. Layer 3 then removes the data meant for it and passes the rest to layer 4, and so on.



**Long Answer Type Questions**

1. a) What do you understand by message security? Explain the following terms:

- i) User Authentication
- ii) Key management
- iii) Security protocols.

[WBUT 2013]

Answer:

1<sup>st</sup> Part:

Cryptography is the science of message security. The word is derived from the Greek *kryptos*, meaning hidden.

There are two kinds of cryptosystems: symmetric and asymmetric. Symmetric cryptosystems use the same key (the secret key) to encrypt and decrypt a message, and asymmetric cryptosystems use one key (the public key) to encrypt a message and a different key (the private key) to decrypt it. Asymmetric cryptosystems are also called public key cryptosystems.

2<sup>nd</sup> Part:

- **User Authentication:** Authentication is the process of verifying an identity claimed by or for a system entity. Authentication process consists of two steps --- Identification step, where an identifier is presented to the security system and a Verification step, where authentication information that corroborates the binding between the entity and the presented identifier, is generated. One common method of authentication is the through the familiar username-password verification. However, more complex schemes are also employed in situations that demand high security.



- **Key Management:** In general, the strength of encryption is related to the difficulty of discovering the key, which in turn depends on both the cipher used and the length of the key. For example, the difficulty of discovering the key for the RSA cipher most commonly used for public-key encryption depends on the difficulty of factoring large numbers, a well-known mathematical problem. Encryption strength is often described in terms of the size of the keys used to perform the encryption: in general, longer keys provide stronger encryption.
- **Security protocols:** Network security protocols are a type network protocol that ensures the security and integrity of data in transit over a network connection. Network security protocols define the processes and methodology to secure network data from any illegitimate attempt to review or extract the contents of data. Network security protocols are primarily designed to prevent any unauthorized user, application, service or device from accessing network data. This applies to virtually all data types regardless of the network medium used. Network security protocols generally implement cryptography and encryption techniques to secure the data so that it can only be decrypted with a special algorithm, logical key, mathematical formula and/or a combination of all of them. Some of the popular network security protocols include Secure File Transfer Protocol (SFTP), Secure Hypertext Transfer Protocol (HTTPS) and Secure Socket Layer (SSL).

**b) How can Authentication, Integrity and Non-Repudiation be implemented by digital signature?** [WBUT 2013]

**Answer:**

Authenticity, integrity, non-repudiation can be explained by digital signature and digital certificate.

A digital signature is basically a way to ensure that an electronic document (e-mail, spreadsheet, text file, etc.) is authentic. Authentic means that you know who created the document and you know that it has not been altered in any way since that person created it.

Digital certificates - To implement public key encryption on a large scale, such as a secure Web server might need, requires a different approach. This is where digital certificates come in. A digital certificate is essentially a bit of information that says the Web server is trusted by an independent source known as a Certificate Authority. The Certificate Authority acts as the middleman that both computers trust. It confirms that each computer is in fact who they say they are and then provides the public keys of each computer to the other.

**c) Explain RSA algorithm with an example.**

[WBUT 2013]

**Answer:**

In cryptography, RSA is an algorithm for public-key encryption. The algorithm was described in 1977 by Ron Rivest, Adi Shamir and Len Adleman at MIT; the letters RSA are the initials of their surnames. RSA involves two keys: public key and private key. The public key is known to everyone and is used to encrypt messages.

## POPULAR PUBLICATIONS

The following are steps to generate a public key and a private key:  
Choose two large prime numbers  $p$  and  $q$  such that  $p \neq q$ , randomly and independently of each other.

Compute  $n = pq$ .

Compute  $\phi(n) = (p-1)(q-1)$ .

Choose an integer  $e$  such that  $1 < e < \phi(n)$  which is coprime to  $\phi(n)$

Compute  $d$  such that  $de \equiv 1 \pmod{\phi(n)}$ .

### **Encrypting messages**

Suppose Bob wishes to send a message  $M$  to Alice. He turns  $M$  into a number  $m < n$ , using some previously agreed-upon reversible protocol. Bob now has  $m$ , and knows  $n$  and  $e$ , which Alice has announced. He then computes the ciphertext  $c$  corresponding to  $m$ :

$$c = m^e \pmod{n}$$

This can be done quickly using the method of exponentiation by squaring. Bob then transmits  $c$  to Alice.

### **Decrypting messages**

Alice receives  $c$  from Bob, and knows her private key  $d$ . She can recover  $m$  from  $c$  by the following procedure:  $m = c^d \pmod{n}$

Given  $m$ , she can recover the original message  $M$ . The decryption procedure works because  $c^d \equiv (m^e)^d \equiv m^{ed} \pmod{n}$ .

Now, since  $ed \equiv 1 \pmod{p-1}$  and  $ed \equiv 1 \pmod{q-1}$ , Fermat's little theorem yields  $m^{ed} \equiv m \pmod{p}$  and  $m^{ed} \equiv m \pmod{q}$

Since  $p$  and  $q$  are distinct prime numbers, applying the Chinese remainder theorem to these two congruences yields

$$m^{ed} \equiv m \pmod{pq}$$

Thus,  $c^d \equiv m \pmod{n}$ .

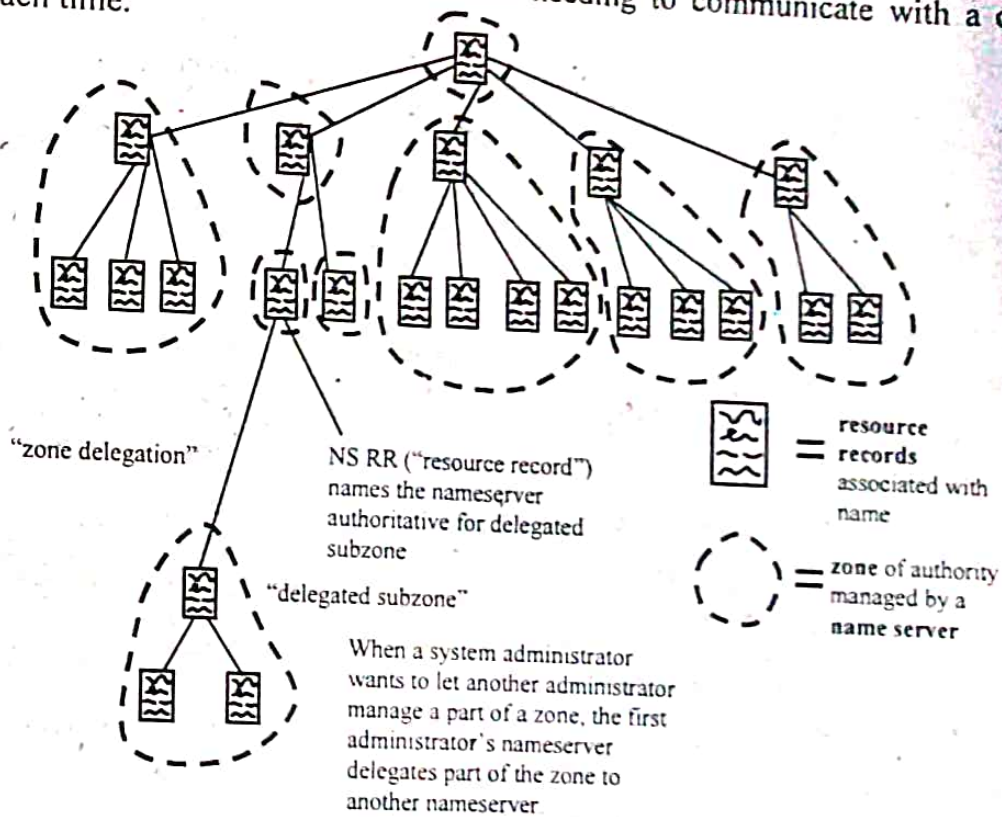
### **Example:**

- Choose  $p = 3$  and  $q = 11$
- Compute  $n = p * q = 3 * 11 = 33$
- Compute  $\phi(n) = (p-1) * (q-1) = 2 * 10 = 20$
- Choose  $e$  such that  $1 < e < \phi(n)$  and  $e$  and  $n$  are coprime. Let  $e = 7$
- Compute a value for  $d$  such that  $(d * e) \% \phi(n) = 1$ . One solution is  $d = 3$  [(3 \* 7) % 20 = 1]
- Public key is  $(e, n) \Rightarrow (7, 33)$
- Private key is  $(d, n) \Rightarrow (3, 33)$
- The encryption of  $m = 2$  is  $c = 2^7 \% 33 = 29$
- The decryption of  $c = 29$  is  $m = 29^3 \% 33 = 2$



2. What do you understand by Domain Name Server (DNS)? Explain the function of browser in World Wide Web?  
 Answer:  
 1<sup>st</sup> Part:  
 [WBUT 2017]

The Domain Name System or Domain Name Server (DNS) is a system that stores information associated with domain names in a distributed database on networks, such as the Internet. DNS associates many types of information with domain names, but most importantly, it provides the IP address associated with the domain name. DNS is an essential component of contemporary Internet use. Most well known, the DNS makes it possible to attach DNS is useful for several reasons. Humans take advantage of this when they recite URLs hard-to-remember IP addresses (such as 207.142.131.206) to easy-to-remember domain names (such as "microsoft.com") and e-mail addresses. Less recognized, the domain name system makes it possible for people to assign authoritative names, without needing to communicate with a central registrar each time.



Domain names are arranged in a tree, and cut into zones, which are served by **nameservers**.

The domain name space is a tree of domain names. Each node or leaf in the tree is associated with **resource records**, which hold the information associated with the domain name. The tree is divided into **zones**. A zone is a collection of connected nodes that are authoritatively served by an **authoritative DNS nameserver**. A single nameserver can host several zones.

The information associated with nodes is looked up by a **resolver**. A resolver knows how to communicate with name servers by sending DNS requests, and heeding DNS

## POPULAR PUBLICATIONS

responses. Resolving usually entails **recursing** through several name servers to find the needed information.

Some resolvers are simple, and can only communicate with a single name server. These simple resolvers rely on a **recursing name server** to perform the work of finding information for it.

A domain name usually consists of two or more parts (technically *labels*), separated by dots. For example *microsoft.com*.

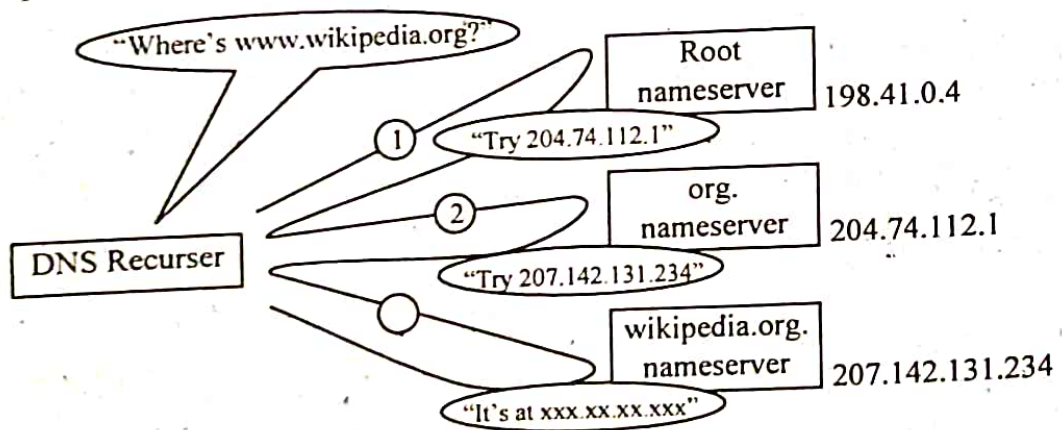
The rightmost label conveys the **top-level domain** (for example, the address *mail.yahoo.com* has the top-level domain *.org*).

Each label to the left specifies a subdivision or **subdomain** of the domain above it. Note that "subdomain" expresses relative dependence, not absolute dependence. For example, *yahoo.com* comprises a subdomain of the domain, *com* and *mail.yahoo.com* is a subdomain of the domain *yahoo.com*. In theory, this subdivision can go down to 127 levels deep, and each label can contain up to 63 characters, as long as the whole domain name does not exceed a total length of 255 characters. But in practice some domain registries have shorter limits than that.

A domain name that has one or more associated IP addresses is called a **hostname**. For example, the *yahoo.com* and *mail.yahoo.com* domains are both hostnames, but the *com* domain is not.

The DNS consists of a hierarchical set of **DNS servers**. Each domain or subdomain has one or more **authoritative DNS servers** that publish information about that domain and the name servers of any domains "beneath" it. The hierarchy of authoritative DNS servers matches the hierarchy of domains. At the top of the hierarchy stand the **root servers**: the servers to query when looking up (**resolving**) a top-level domain name.

### **An example of theoretical DNS recursion**



Here, the DNS recursor consults three nameservers to resolve *www.wikipedia.org*.

### **2<sup>nd</sup> Part:**

A web browser is a software program that allows a user to locate, access, and display web pages. In common usage, a web browser is usually shortened to "browser." Browsers are used primarily for displaying and accessing websites on the internet, as well as other



content created using languages such as Hypertext Markup Language (HTML) and Extensible Markup Language (XML). Browsers translate web pages and websites delivered using Hypertext Transfer Protocol (HTTP) into human-readable content. They also have the ability to display other protocols and prefixes, such as secure HTTP (HTTPS), File Transfer Protocol (FTP), email handling (mailto:), and files (file:). In addition, most browsers also support external plug-ins required to display active content, such as in-page video, audio and game content.

**3. Write short notes on the following:**

- a) Firewall
- b) DNS
- c) HTTP
- d) SMTP
- e) Cryptography
- f) FTP
- g) SNMP

[WBUT 2013]  
[WBUT 2013, 2014, 2016]  
[WBUT 2014, 2017]  
[WBUT 2014]  
[WBUT 2015]  
[WBUT 2016, 2017]  
[WBUT 2017]

Answer:

a) Firewall: *Refer to Question No. 2(b) of Short Answer Type Questions.*

b) DNS: *Refer to Question No. 2(1<sup>st</sup> Part) of Long Answer Type Questions.*

**c) HTTP:**

Short for HyperText Transfer Protocol, HTTP is the underlying protocol used by the World Wide Web. HTTP defines how messages are formatted and transmitted, and what actions Web servers and browsers should take in response to various commands. For example, when we enter a URL in your browser, this actually sends an HTTP command to the Web server directing it to fetch and transmit the requested Web page.

The other main standard that controls how the World Wide Web works is HTML, which covers how Web pages are formatted and displayed.

HTTP is called a stateless protocol because each command is executed independently, without any knowledge of the commands that came before it. This is the main reason that it is difficult to implement Web sites that react intelligently to user input. This shortcoming of HTTP is being addressed in a number of new technologies, including ActiveX, Java, JavaScript and cookies.

Errors on the Internet can be quite frustrating — especially if we do not know the difference between a 404 error and a 502 error. These error messages, also called HTTP status codes are response codes given by Web servers and help identify the cause of the problem.

For example, "404 File Not Found" is a common HTTP status code. It means the Web server cannot find the file you requested. The file -- the webpage or other document we try to load in our Web browser -- has either been moved or deleted, or you entered the wrong URL or document name.



**d) SMTP:**

SMTP is a relatively simple, text-based protocol, where one or more recipients of a message are specified (and in most cases verified to exist) and then the message text is transferred. SMTP uses TCP port 25. SMTP started becoming widely used in the early 1980s and gradually replaced UUCP which was better suited to handle e-mail transfers between Unix machines that were intermittently connected. SMTP works best when both the sending and receiving machines are connected to the network all the time. *Sendmail* was one of the first (if not the first) mail transfer agents to implement SMTP. Today, there are several programs that implement SMTP as a client or a server, for example, *exim*, *Postfix*, *qmail*, and *Microsoft Exchange Server*. This protocol started out as purely ASCII and did not deal well with binary files. Later, standards such as MIME were developed to encode binary files for transfer through SMTP.

SMTP is a "push" protocol that does not allow one to "pull" messages from a remote server on demand. To do this a mail client must use POP3 or IMAP.

**e) Cryptography: Refer to Question No. 4 of Short Answer Type Questions.**

**f) FTP:**

**FTP or File Transfer Protocol** is a commonly used protocol for exchanging files over any network that supports the TCP/IP protocol. There are two computers involved in an FTP transfer --- a server and a client. The **FTP server**, running FTP server software, listens on the network for connection requests from other computers. The client computer, running FTP client software, initiates a connection to the server. Once connected, the client can do a number of file manipulation operations such as uploading files to the server, download files from the server, rename or delete files on the server and so on. Any computer connected to a TCP/IP based network can manipulate files on another computer on that network regardless of which operating systems are involved (if the computers permit FTP access). There are many existing FTP client and server programs, and many of these are free.

FTP is commonly run on two ports, 20 and 21, and runs exclusively over TCP. The FTP server listens on port 21 for incoming connection from FTP clients. A connection on this port forms the control stream, on which commands are passed to the FTP server. For the actual file transfer to take place, a different connection is required. Depending on the transfer mode, the client (active mode) or the server (passive mode) can listen for the incoming data connection. Before file transfer begins, the client and server also negotiate the port of the data connection. In case of active connections (where the server connects to the client to transfer data), the server binds on port 20 before connecting to the client. For passive connections, there is no such restriction.

While data is being transferred via the data stream, the control stream sits idle. This can cause problems with large data transfers through firewalls which time out sessions after lengthy periods of idleness. While the file may well be successfully transferred, the control session can be disconnected by the firewall, causing an error to be generated.



Many sites that run FTP servers enable so-called "anonymous ftp". Under this arrangement, users do not need an account on the server. The user name for anonymous access is typically 'anonymous' or 'ftp'. This account does not need a password. Although users are commonly asked to send their email addresses as their passwords for authentication, usually there is trivial or no verification.

While transferring data over the network, two modes can be used

- ASCII mode
- Binary mode

The two types differ in the way they send the data. When a file is sent using an ASCII-type transfer, the individual letters, numbers and characters are sent using their ASCII character codes. The receiving machine saves these in a text file in the appropriate format (for example, a Unix machine saves it in a Unix format, a Macintosh saves it in a Mac format). Hence if an ASCII transfer is used it can be assumed plain text is sent, which is stored by the receiving computer in its own format.

Sending a file in binary mode is different. The sending machine sends each file bit for bit and as such the recipient stores the bitstream as it receives it.

By default, most FTP clients use ASCII mode. Some clients try to determine the required transfer-mode by inspecting the file's name or contents.

#### **g) SNMP:**

In typical SNMP uses, one or more administrative computers, called managers, have the task of monitoring or managing a group of hosts or devices on a computer network. Each managed system executes, at all times, a software component called an *agent* which reports information via SNMP to the manager.

SNMP agents expose management data on the managed systems as variables. The protocol also permits active management tasks, such as modifying and applying a new configuration through remote modification of these variables. The variables accessible via SNMP are organized in hierarchies. An SNMP-managed network consists of three key components:

- Managed device
- Agent — software which runs on managed devices
- Network management station (NMS) — software which runs on the manager

A *managed device* is a network node that implements an SNMP interface that allows unidirectional (read-only) or bidirectional (read and write) access to node-specific information. Managed devices exchange node-specific information with the NMSs. Sometimes called network elements, the managed devices can be any type of device, including, but not limited to, routers, access servers, switches, bridges, hubs, IP telephones, IP video cameras, computer hosts, and printers.

An *agent* is a network-management software module that resides on a managed device. An agent has local knowledge of management information and translates that information to or from an SNMP-specific form.

A *network management station* (NMS) executes applications that monitor and control managed devices. NMSs provide the bulk of the processing and memory resources

## POPULAR PUBLICATIONS

required for network management. One or more NMSs may exist on any managed network.

4. a) State the threats that can arise in a data network. Also, explain the security requirements to be met due to the stated threats.
- b) Explain 'public key encryption' system as a means of secure transfer of information over a network. [MODEL QUESTION]

### Answer:

- a) Unauthorized entry into any compartmented computer system.  
Unauthorized searching/browsing through classified computer libraries.  
Unauthorized modification, destruction, manipulation, or denial of access to information residing on a computer system.  
Storing or processing classified information on any system not explicitly approved for classified processing.  
Attempting to circumvent or defeat security or auditing systems, without prior authorization from the system administrator, other than as part of a legitimate system testing or security research.  
Any other willful violation of rules for the secure operation of your computer network.

- b) A cryptographic system that uses two keys -- a public key known to everyone and a private or secret key known only to the recipient of the message. When John wants to send a secure message to Jane, he uses Jane's public key to encrypt the message. Jane then uses her private key to decrypt it.

An important element to the public key system is that the public and private keys are related in such a way that only the public key can be used to encrypt messages and only the corresponding private key can be used to decrypt them. Moreover, it is virtually impossible to deduce the private key if you know the public key.

Public key cryptography was invented in 1976 by Whitfield Diffie and Martin Hellman. For this reason, it is sometime called Diffie-Hellman encryption. It is also called asymmetric encryption because it uses two keys instead of one key (symmetric encryption).



## **MODERN TOPICS**

### **Multiple Choice Type Questions**

1. Blue-tooth uses ..... To communicate between two devices. [MODEL QUESTION]
- a) Radiowave
  - b) Microwave
  - c) Infrared
  - d) none of these, a separate technology exists

Answer: (a)

### **Short Answer Type Questions**

1. What are the functions of B-ISDN? [MODEL QUESTION]

Answer:

BISDN is both a concept and a set of services and developing standards for integrating digital transmission services in a broadband network of fiber optic and radio media. BISDN will encompass frame relay service for high-speed data that can be sent in large bursts, the Fiber Distributed-Data Interface (Fiber Distributed-Data Interface), and the Synchronous Optical Network (Synchronous Optical Network). BISDN will support transmission from 2 Mbps up to much higher, but as yet unspecified, rates.

BISDN is the broadband counterpart to Integrated Services Digital Network, which provides digital transmission over ordinary telephone company copper wires on the narrowband local loop.

2. What is hand off in cellular telephony? [MODEL QUESTION]

Answer:

As a mobile user moves from one service area to the next, a hand-off occurs from one service area to the next. The hand-off would disrupt the call for 100 to 200 ms. This is just enough to disrupt the carrier detect (CD) cycle; hence, the modem assumes that one of the callers has disconnected, and it hangs up. This problem can be overcome similar to fax modems over cellular links. The modem will delay 400 ms before hanging up, giving the hand-off enough time to take place. Some data might be affected, but error detection, and error correction procedures (CRCs) will detect and correct the data bits that have been corrupted. But, all these techniques lower the effective throughput of our communication system and the effective throughputs achieved with cellular modems hover around 19200 bits/s

3. What do you mean by geosynchronous satellite? [MODEL QUESTION]

Answer:

A **geosynchronous satellite** is a satellite whose orbital track on the Earth repeats regularly over points on the Earth over time. If such a satellite's orbit lies over the equator and the orbit is circular, it is called a **geostationary satellite**.

**Long Answer Type Questions**

[MODEL QUESTION]

1. Write short notes on the following:

- a) ISDN
- b) Cable Modem
- c) Bluetooth
- d) Wi-Max technology
- e) Distributed system
- f) Satellite transmission

Answer:

**a) ISDN:**  
**Integrated Services Digital Network (ISDN)** is a type of circuit switched telephone network system, designed to allow digital transmission of voice and data over ordinary telephone copper wires, resulting in better quality and higher speeds than available with analog systems. More broadly, **ISDN** is a set of protocols for establishing and breaking circuit switched connections, and for advanced call features for the user. In a videoconference, **ISDN** provides simultaneous voice, video, and text transmission between individual desktop videoconferencing systems and group (room) videoconferencing systems.

**Configurations**

In **ISDN**, there are two types of channels, *B* (for "Bearer") and *D* (for "Delta"). *B channels* are used for data (which may include voice), and *D channels* are intended for signalling and control (but can also be used for data). There are two kinds of access to **ISDN**. **Basic rate interface (BRI)** — also **Basic rate access (BRA)** — consists of two *B* channels, each with bandwidth of 64 kbit/s, and one *D* channel with a bandwidth of 16 kbit/s. Together these three channels can be designated as **2B+D**. **Primary rate interface (PRI)** — also **Primary rate access (PRA)** — contains a greater number of *B* channels and a *D* channel with a bandwidth of 64 kbit/s.

**b) Cable Modem:**

A **cable modem** is a special type of modem that is designed to modulate a data signal over cable television infrastructure. Cable modems are primarily used to deliver broadband Internet access, taking advantage of unused bandwidth on a cable television network. In practice, cable modems and DSL differ little and are both superior alternatives to dial-up access. Both offer snappy 40-70ms response, or the round-trip time of a data packet sent to a server. Dial-up is a more sluggish 150-400ms.



There is greater differentiation in bandwidth, or the rate at which one can send and receive data, between cable and the various types of DSL. A dial-up modem can download and upload at some 40 kbs, or 0.04 Mbs. Cable modems across most services consistently attain 3-6 Mbs down / 0.3-0.4 MBs up. There are few attempts to offer different service tiers beyond the traditional 'home' and 'business' designations.



In comparison, DSL tends to offer less speed and more variance between service packages and prices. Service quality is also far more dependent on your location in relation to the local ISP.

There are three traditional disadvantages to cable internet:

- Users in a neighborhood share the available bandwidth provided by a single coaxial cable line. Therefore, connection speed can vary depending on how many people are using the service at the same time.
- Cable networks using a shared line risk a loss of privacy, especially in light of the availability of hacking tools for cable modems. This issue is addressed by encryption and other privacy features specified in the DOCSIS (Data Over Cable Service Interface Specification) standard used by most cable modems.
- Many cable Internet providers are reluctant to offer cable modem access without tying it to a cable television subscription. This has ramifications similar to those of the lack of naked DSL.

### c) Bluetooth

**Bluetooth** is an industrial specification for wireless personal area networks (PANs). Bluetooth provides a way to connect and exchange information between devices like personal digital assistants (PDAs), mobile phones, laptops, PCs, printers and digital cameras via a secure, low-cost, globally available short range radio frequency.



A typical Bluetooth mobile phone headset



A Bluetooth mouse

Bluetooth is a radio standard primarily designed for low power consumption, with a short range (power class dependent: 10 centimeters, 10 meters, 100 meters) and with a low-cost transceiver microchip in each device.

Bluetooth lets these devices talk to each other when they come in range, even if they are not in the same room, as long as they are within up to 100 meters of each other, dependent on the power class of the product. Products are available in one of three power classes:

Class	Power (mW)	Power (dBm)	Range (approximate)
Class 1	100 mW	20 dBm	~100 meters
Class 2	2.5 mW	4 dBm	~10 meters
Class 3	1 mW	0 dBm	~10 cm (1 meter max)

### *Bluetooth Application*

- Wireless networking between desktops and laptops, or desktops in a confined space and where little bandwidth is required
- Bluetooth peripherals such as printers, mice and keyboards



## POPULAR PUBLICATIONS

- Bluetooth cell phones have been sold in large numbers, and are able to connect to computers, personal digital assistants (PDAs), certain automobile handsfree systems and various other devices. The standard also includes support for more powerful, longer-range devices suitable for constructing wireless LANs.
- Certain mp3 players and digital cameras to transfer files to and from computers
- Bluetooth headsets for mobile phones and smartphones
- Some testing equipment is Bluetooth enabled
- Some medical applications are under development

### **d) Wi-Max technology :**

WiMAX (Worldwide Interoperability for Microwave Access) is a telecommunications protocol that provides fixed and fully mobile Internet access. The current WiMAX revision provides up to 40 Mbit/s. with the IEEE 802.16m update expected to offer up to 1 Gbit/s fixed speeds. The name "WiMAX" was created by the WiMAX Forum, which was formed in June 2001 to promote conformity and interoperability of the standard. The forum describes WiMAX as "a standards-based technology enabling the delivery of last mile wireless broadband access as an alternative to cable and DSL".

WiMAX refers to interoperable implementations of the IEEE 802.16 wireless-networks standard (ratified by the WiMAX Forum), in similarity with Wi-Fi, which refers to interoperable implementations of the IEEE 802.11 Wireless LAN standard (ratified by the Wi-Fi Alliance). The WiMAX Forum certification allows vendors to sell their equipment as WiMAX (Fixed or Mobile) certified, thus ensuring a level of interoperability with other certified products, as long as they fit the same profile.

The IEEE 802.16 standard forms the basis of 'WiMAX' and is sometimes referred to colloquially as "WiMAX", "Fixed WiMAX", "Mobile WiMAX", "802.16d" and "802.16e". Clarification of the formal names are as follow:  
802.16-2004 is also known as 802.16d, which refers to the working party that has developed that standard. It is sometimes referred to as "Fixed WiMAX", since it has no support for mobility.

802.16e-2005, often abbreviated to 802.16e, is an amendment to 802.16-2004. It introduced support for mobility, among other things and is therefore also known as "Mobile WiMAX".

Mobile WiMAX is the WiMAX incarnation that has the most commercial interest to date and is being actively deployed in many countries. Mobile WiMAX is also the basis of future revisions of WiMAX. As such, references to and comparisons with "WiMAX" in this Wikipedia article mean "Mobile WiMAX".

The bandwidth and range of WiMAX make it suitable for the following potential applications:

Providing portable mobile broadband connectivity across cities and countries through a variety of devices. Providing a wireless alternative to cable and DSL for "last mile" broadband access.

Providing data, telecommunications (VoIP) and IPTV services (triple play).

Providing a source of Internet connectivity as part of a business continuity plan.



**e) Distributed System:**

Distributed computing is a field of computer science that studies distributed systems. A distributed system consists of multiple autonomous computers that communicate through a computer network. The computers interact with each other in order to achieve a common goal. A computer program that runs in a distributed system is called a distributed program, and distributed programming is the process of writing such programs.

Distributed computing also refers to the use of distributed systems to solve computational problems. In distributed computing, a problem is divided into many tasks, each of which is solved by one computer.

There are two main reasons for using distributed systems and distributed computing. First, the very nature of the application may require the use of a communication network that connects several computers. For example, data is produced in one physical location and it is needed in another location.

Second, there are many cases in which the use of a single computer would be possible in principle, but the use of a distributed system is beneficial for practical reasons. For example, it may be more cost-efficient to obtain the desired level of performance by using a cluster of several low-end computers, in comparison with a single high-end computer. A distributed system can be more reliable than a non-distributed system, as there is no single point of failure. Moreover, a distributed system may be easier to expand and manage than a monolithic uniprocessor system.

Examples of distributed systems and applications of distributed computing include the following:

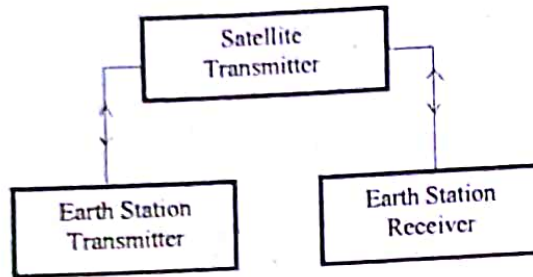
- Telecommunication networks.
- Telephone networks and cellular networks.
- Computer networks such as the Internet.
- Wireless sensor networks.
- Routing algorithms.
- Network applications.
- World Wide Web and peer-to-peer networks.
- Massively multiplayer online games and virtual reality communities.
- Distributed databases and distributed database management systems.
- Network file systems.
- Distributed information processing systems such as banking systems and airline reservation systems.

**f) Satellite transmission:**

In Satellite transmission, signal transferring between the sender and receiver is done with the help of satellite. In this process, the signal which is basically a beam of modulated microwaves is sent towards the satellite. Then the satellite amplifies the signal and sent it back to the receiver's antenna present on the earth's surface. So, all the signal transferring is happening in space. Thus this type of communication is known as space communication.

## POPULAR PUBLICATIONS

Two satellites which are commonly used in satellite communication are Active and passive satellites.





# QUESTION 2013

## Group – A

### (Multiple Choice Type Questions)

1. Choose the correct alternatives for the following:

i) A hub is a

a) router

b) bridge

c) repeater

d) all of these

ii) If subnet mask is 255.255.252.0 then how many subnets is available?

a) 2

b) 18

c) 4

d) 24

iii) Flow control in OSI reference model is performed in

a) data link layer

b) network layer

c) session layer

d) application layer

iv) Which of the following is an application layer service?

a) remote login

b) file transfer and access

c) mail service

d) all of these

v) PPP is a ..... Oriented protocol.

a) phase

b) bit

c) byte

d) none of these

vi) Which of the following is an interior routing protocol?

a) RIP

b) OSPF

c) BGP

d) both (a) & (b)

vii) Checksum is used for

a) error detection

b) error correction

c) error encapsulation

d) both (a) and (b)

viii) When host knows its IP address but not its physical address, it can use

a) RARP

b) ICMP

c) ARP

d) IGMP

ix) Which of the following is a valid host for network 192.168.10.32/28?

a) 192.168.10.39

b) 192.168.10.47

c) 192.168.10.14

d) 192.168.10.54

x) Which class of IP address is reserved for multicast communication?

a) Class A

b) Class B

c) Class C

d) Class D

## POPULAR PUBLICATIONS

### Group – B

(Short Answer Type Questions)

2. What is the minimum window size required for selective repeat ARQ protocol and how?

See Topic: DATA LINK LAYER, Short Answer Type Question No. 1.

3. What do you mean by Data transparency? What is Bit stuffing in HDLC? Why bit stuffing is needed?

See Topic: DATA LINK LAYER, Short Answer Type Question No. 2.

4. Draw the following encoding schemes for the bit stream 0001110101:

i) NRZ-I

ii) Manchester coding

iii) Differential Manchester coding.

See Topic: OVERVIEW OF DATA COMMUNICATION AND NETWORKING, Short Answer Type Question No. 1.

5. Applying CRC algorithm, determine the check sum and the transmitted frame for the bit stream 11010111 and for the generator polynomial  $x^3 + x^2 + 1$ .

See Topic: DATA LINK LAYER, Short Answer Type Question No. 3.

6. What is Bit Rate? What is Baud Rate?

An analog signal carries 4 bits in each signal unit. If 1000 signal units are sent per second, find the baud rate and bit rate.

See Topic: OVERVIEW OF DATA COMMUNICATION AND NETWORKING, Short Answer Type Question No. 2.

### Group – C

(Long Answer Type Questions)

7. a) State the difference between IPV4 and IPV6. Discuss IPV6 packet format.

b) "TCP and UDP" – which one is better? Justify your answer.

c) What is the purpose of subnetting? Find the net ID and the host ID of the following IP addresses:

i) 19.34.21.5

ii) 220.34.8.9

d) A network has subnet mask 255.255.255.224. Determine the maximum number of Host in this network. Determine the broadcast address of the network.

a), c) & d) See Topic: NETWORK LAYER, Long Answer Type Question No. 1.

b) See Topic: TRANSPORT LAYER, Short Answer Type Question No. 1.



8. a) What do you understand by message security? Explain the following terms.

- i) User Authentication
- ii) Key management
- iii) Security protocols.

b) How can Authentication, Integrity and Non-Repudiation be implemented by digital signature?

c) Explain RSA algorithm with an example.

See Topic: **APPLICATION LAYER**, Long Answer Type Question No. 1.

9. a) Write down the advantages of Fibre-optic cable over twisted pair and coaxial cables.

b) Suppose that a signal has  $2^n$  times the power as a noise signal that is added to it. Find the SNR in decibels.

c) A 12 bit data bit block 011101010111 is to be set using hamming code for error detection and correction. Show how the receiver corrects an error that occurs in 6<sup>th</sup> bit position from right.

d) What is transmission impairment? How many types of transmission impairments are there? Discuss them.

a) & b) See Topic: **OVERVIEW OF DATA COMMUNICATION AND NETWORKING**. Short Answer Type Question No. 3.

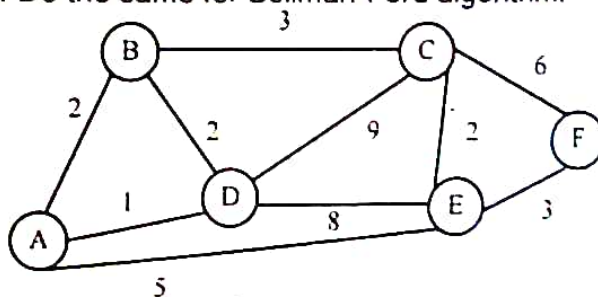
c) See Topic: **DATA LINK LAYER**, Short Answer Type Question No. 4.

d) See Topic: **PHYSICAL LEVEL**, Short Answer Type Question No. 1.

10. a) What is autonomous system (AS)? What is the difference between intradomain and Inter domain AS? Explain an Interdomain routing protocol.

b) What is the difference between RIP and OSPF?

c) Apply Dijkstra algorithm to find the shortest path from node A to node F of the network graph shown in figure below. Do the same for Bellman-Ford algorithm.



See Topic: **NETWORK LAYER**, Long Answer Type Question No. 2.

11. Write short notes of any *three* of the following:

- a) Firewall
- b) Circuit switching
- c) DNS
- d) QoS in transport layer
- e) Socket

## POPULAR PUBLICATIONS

- a) See Topic: APPLICATION LAYER, Long Answer Type Question No. 3(a).
- b) See Topic: OVERVIEW OF DATA COMMUNICATION AND NETWORKING, Long Answer Type Question No. 6(a).
- c) See Topic: APPLICATION LAYER, Long Answer Type Question No. 3(b).
- d) See Topic: TRANSPORT LAYER, Long Answer Type Question No. 1.
- e) See Topic: NETWORK LAYER, Long Answer Type Question No. 7(a).

## QUESTION 2014

### GROUP - A

(Multiple Choice Type Question)

1. Answer all questions:

- (i) Process to process delivery is the function of ..... layer.  
✓a) transport      b) network      c) physical      d) none of these
- (ii) Which channel access method is used in IEEE 802.5 network?  
a) CSMA/CD      ✓b) token bus      c) token ring      d) all of these
- (iii) Which class of IP address is reserved for multicast communication?  
a) class A      b) class B      c) class C      ✓d) class D
- (iv) Repeaters function in the ..... layer  
a) data link      ✓b) physical      c) network      d) transport
- (v) Port number is:  
✓a) process number      b) computer physical address  
c) both (a) and (b)      d) none of these
- (vi) What network topology implements at least two paths to and from each node?  
a) bus      ✓b) ring      c) mesh      d) star
- (vii) The hamming code is used for:  
a) error detection      b) error correction  
c) error encapsulation      ✓d) both (a) and (b)
- (viii) Which channel access method is used in Ethernet network?  
✓a) CSMA/CD      b) token bus      c) token ring      d) all of these



(ix) UDP is:

- ✓ a) Connectionless
- c) both (a) and (b)

- b) connection-oriented
- d) none of these

(x) Which address cannot be changed?

- ✓ a) Hardware address
- c) both (a) and (b)

- b) logical address
- d) none of this

**GROUP – B**

**(Short Answer Type Question)**

2. a) What is the purpose of subnetting? Find the net-ID and the Host-ID of the following IP addresses.

- i) 19.34.21.5
- ii) 220.34.8.9

b) A network has subnet mask 255.255.255.224. Determine the maximum number of Host in this network. Also determine the broadcast address of this network.

See Topic: **NETWORK LAYER**, Long Answer Type Question No. 1(b) & (c).

3. a) What is bit rate? What is baud rate?

b) An analog signal carries 4 bits in each signal unit. If 1000 signal units are sent per second, find the baud rate and bit rate.

See Topic: **OVERVIEW OF DATA COMMUNICATION AND NETWORKING**, Short Answer Type Question No. 2.

4. How does Manchester encoding differ from differential Manchester encoding?

See Topic: **OVERVIEW OF DATA COMMUNICATION AND NETWORKING**, Short Answer Type Question No. 4.

5. What is Gateways? Differentiate between Hub and Switch.

See Topic: **NETWORK LAYER**, Short Answer Type Question No. 1.

6. What do you mean by MAC and LLC? Explain.

See Topic: **MEDIUM ACCESS SUB LAYER**, Short Answer Type Question No. 1.

**GROUP – C**

**(Long Answer Type Question)**

7. a) Explain the operation of CDMA technology.

b) Difference between router & bridge?

## POPULAR PUBLICATIONS

c) Briefly discuss about the different guided media that are used in computer networks and make a comparison among them.

d) What is OSI reference model?

a) See Topic: **MEDIUM ACCESS SUB LAYER**, Long Answer Type Question No. 1(a).

b) See Topic: **NETWORK LAYER**, Short Answer Type Question No. 2.

c) & d) See Topic: **OVERVIEW OF DATA COMMUNICATION AND NETWORKING**, Long Answer Type Question No. 1(a) & (b).

8. a) Explain CRC code with example.

b) Describe 802.3 header formats. Why is padding required?

c) Indicate QoS in transport layer.

a) See Topic: **DATA LINK LAYER**, Long Answer Type Question No. 1(a).

b) See Topic: **MEDIUM ACCESS SUB LAYER**, Long Answer Type Question No. 1(b).

c) See Topic: **TRANSPORT LAYER**, Short Answer Type Question No. 2.

9.(a) How does a single bit error differ from a burst error?

b) State the advantage of IPV6 over IPV4.

c) Differentiate between ARP and RARP.

a) See Topic: **DATA LINK LAYER**, Long Answer Type Question No. 1(b).

b) & c) See Topic: **NETWORK LAYER**, Long Answer Type Question No. 3(a) & (b).

10. a) What is distance vector routing protocol ? What is difference between RIP and EGP?

b) What do you understand by data privacy? How can the authentication integrity and non-repudiation be implemented by digital signature?

c) Write down the similarities and differences between OSI and TCP/IP model.

a) See Topic: **NETWORK LAYER**, Short Answer Type Question No. 3.

b) See Topic: **APPLICATION LAYER**, Short Answer Type Question No. 1.

c) See Topic: **OVERVIEW OF DATA COMMUNICATION AND NETWORKING**, Long Answer Type Question No. 1(c).

11. Write short notes on any three of the following:

a) HTTP

b) BGP

c) RIP

d) SMTP

e) DNS

a) See Topic: **APPLICATION LAYER**, Long Answer Type Question No. 3(c).

b) See Topic: **NETWORK LAYER**, Long Answer Type Question No. 7(b).

c) See Topic: **NETWORK LAYER**, Long Answer Type Question No. 7(c).

d) See Topic: **APPLICATION LAYER**, Long Answer Type Question No. 3(d).

e) See Topic: **APPLICATION LAYER**, Long Answer Type Question No. 3(b).



**QUESTION 2015****GROUP - A****(Multiple Choice Type Questions)**

1. Choose the correct alternatives for the following:
- i) A \_\_\_\_\_ is a device that forwards packets between networks by processing the routing information included in the packet.  
 a) bridge                      b) firewall                      c) router                      d) switch
- ii) Which transmission media has the highest transmission speed in a network?  
 a) coaxial cable                      b) twisted pair cable  
 c) optical fiber                      d) electrical cable
- iii) Which one of the following task is not done by data link layer?  
 a) framing                      b) error control                      c) flow control                       d) channel coding
- iv) The network layer concerns with \_\_\_\_\_  
 a) packets                      b) bits                      c) frames                      d) IP
- v) Which one of the following is a transport layer protocol used in internet?  
 a) TCP                       b) TCP and UDP                      c) UDP                      d) none
- vi) An endpoint of an inter-process communication flow across a computer network is called  
 a) socket                      b) pipe                      c) port                      d) none of these
- vii) When displaying a web page, the application layer uses the  
 a) FTP protocol                      b) SMTP protocol                       c) HTTP protocol                      d) all of these
- viii) The packet of information at the application layer is called  
 a) packet                       b) message                      c) segment                      d) frame
- ix) In this topology there is a central controller or hub  
 a) star                      b) mesh                      c) ring                      d) bus
- x) IPv6 addresses have a size of \_\_\_\_\_  
 a) 32 bits                      b) 64 bits                       c) 128 bits                      d) 265 bits
- xi) Which of this is not a network edge device?  
 a) PC                      b) smartphone                      c) servers                       d) switch

## POPULAR PUBLICATIONS

### GROUP – B

(Short Answer Type Question)

2. a) We have a channel with a 1MHz bandwidth. The SNR for the channel is 63. What is the bit rate and signal level? b) Discuss about the different types of transmission impairments.

a) See Topic: PHYSICAL LEVEL, Short Answer Type Question No. 2.

b) See Topic: PHYSICAL LEVEL, Short Answer Type Question No. 1.

3. a) What do you mean by low-pass and band-pass channels?

b) State the differences between Manchester and Differential Manchester encoding schemes with an example.

a) See Topic: OVERVIEW OF DATA COMMUNICATION AND NETWORKING, Short Answer Type Question No. 5.

b) See Topic: OVERVIEW OF DATA COMMUNICATION AND NETWORKING, Short Answer Type Question No. 4.

4. a) What is TDM?

b) A constellation diagram consists of eight equally spaced points on a circle. If the bit rate is 4800 bps, what is the baud rate?

See Topic: OVERVIEW OF DATA COMMUNICATION AND NETWORKING, Short Answer Type Question No. 6.

5. a) An organization with a site address of 145.99.0.0 needs to be subnetted. The network administrator wants to create 32 subnets. What should be the value of the subnet mask? Design the subnets.

b) What do you mean by a supernet?

See Topic: NETWORK LAYER, Short Answer Type Question No. 4.

6. a) Discuss about the four basic principles of network security.

b) What is firewall?

See Topic: APPLICATION LAYER, Short Answer Type Question No. 2.

### GROUP – C

(Long Answer Type Question)

7. a) Discuss in detail about OSI reference model mentioning the functions performed by each layer in it. What are the differences of OSI reference model from TCP/IP reference model?

b) Discuss in detail about different framing techniques.

a) 1<sup>st</sup> part: See Topic: OVERVIEW OF DATA COMMUNICATION AND NETWORKING, Long Answer Type Question No. 2.



2<sup>nd</sup> part: See Topic: OVERVIEW OF DATA COMMUNICATION AND NETWORKING, Long Answer Type Question No. 1(c).

b) See Topic: DATA LINK LAYER, Long Answer Type Question No. 2.

8. a) Explain in detail how an error could be detected using the Checksum method for error detection.

b) What do you mean by flow control problem?

c) What is an ARQ? Discuss about the different operations performed by Stop & Wait ARQ.

See Topic: DATA LINK LAYER, Long Answer Type Question No. 3.

9. a) Discuss about the different modes of operations performed by HDLC.

b) What do you mean by data transparency and bit stuffing in HDLC?

c) Explain in detail the concept of connection establishment using LCP in case of PPP.

d) What is bandwidth-delay product?

a), b) & d) See Topic: DATA LINK LAYER, Long Answer Type Question No. 4(a), (b) & (c).

c) See Topic: MEDIUM ACCESS SUB LAYER, Long Answer Type Question No. 2.

10. a) What is CIDR notation? What is its significance in case of classless addressing?

b) What do you mean by a private address? What is NAT?

c) What do you mean by traffic shaping? Explain in detail leaky bucket algorithm?

a) & b) See Topic: NETWORK LAYER, Long Answer Type Question No. 4(a) & (b).

c) See Topic: TRANSPORT LAYER, Long Answer Type Question No. 1.

11. a) What are the directions of data flow? Explain with suitable examples.

b) How do we measure the performance of a computer network? Explain.

c) Discuss in detail different topologies for computer networks.

d) What is throughput?

e) Differentiate between internet, intranet and extranet.

See Topic: OVERVIEW OF DATA COMMUNICATION AND NETWORKING, Long Answer Type Question No. 3.

12. Write short notes on any three of the following:

a) QAM

b) Twisted Pair Cables

c) Hamming Code

d) Go back-N ARQ

e) Cryptography.

## POPULAR PUBLICATIONS

- a) See Topic: OVERVIEW OF DATA COMMUNICATION AND NETWORKING, Long Answer Type Question No. 6(b).
- b) See Topic: OVERVIEW OF DATA COMMUNICATION AND NETWORKING, Long Answer Type Question No. 6(c).
- c) See Topic: DATA LINK LAYER, Long Answer Type Question No. 6(a).
- d) See Topic: DATA LINK LAYER, Long Answer Type Question No. 6(b).
- e) See Topic: APPLICATION LAYER, Long Answer Type Question No. 3(c).

## QUESTION 2016

### Group – A

#### (Multiple Choice Type Questions)

1. Choose the correct alternatives for the following:

i) The total number of links required to connect  $n$  devices using Mesh topology is

- a)  $2^n$                       b)  $n(n+1)/2$                       ✓ c)  $n(n-1)/2$                       d)  $n^2$

ii) Flow control is the responsibilities of the

- a) Data link layer              b) Transport layer              ✓ c) Both of these              d) none of these

iii) A hub is a

- a) Router                      b) Bridge                      ✓ c) Repeater                      d) All of these

iv) ICMP resides at the same layer as which of the following protocols mentioned below?

- a) TCP                      b) UDP                      ✓ c) IP                      d) ARP

v) Which of the following is a valid host for network 192.168.10.32/28?

- ✓ a) 192.168.10.39              b) 192.168.10.47              c) 192.168.10.14              d) 192.168.10.54

vi) Which class of IP address is reserved for multicast?

- a) Class A                      b) Class B                      c) Class C                      ✓ d) Class D

vii) Which channel access method is used in Ethernet network?

- ✓ a) CSMA/CD                      b) Token bus                      c) Token ring                      d) All of these

viii) When host knows its IP address but not its physical address, it can use

- a) RARP                      b) ICMP                      ✓ c) ARP                      d) IGMP





## POPULAR PUBLICATIONS

5. a) What are the differences between TCP & UDP?

b) Physical address operates in local domain whereas logical/IP address operates in global domain. Explain.

a) See Topic: **TRANSPORT LAYER**, Short Answer Type Question No. 3.

b) See Topic: **OVERVIEW OF DATA COMMUNICATION AND NETWORKING**, Short Answer Type Question No. 7.

6. Briefly discuss about the different guided media that are used in computer networks and make a comparison among them.

See Topic: **OVERVIEW OF DATA COMMUNICATION AND NETWORKING**, Long Answer Type Question No. 1(a).

### **Group – C**

#### **(Long Answer Type Questions)**

7. a) State the differences between IPV4 and IPV6.

b) State the difference between static and dynamic routing.

c) Describe any shortest path algorithm.

d) Differentiate between ARP and RARP.

a) See Topic: **NETWORK LAYER**, Long Answer Type Question No. 1(a) (1<sup>st</sup> Part).

b) & c) See Topic: **NETWORK LAYER**, Long Answer Type Question No. 5(a) & (b).

d) See Topic: **NETWORK LAYER**, Long Answer Type Question No. 3(b).

8. a) What is the basic difference between CSMA and CSMA/CD?

b) Briefly describe CSMA/CA procedure.

c) What do you mean by back off factor in case of CSMA/CD protocol?

d) What is the working operation of stop and wait ARQ for lost acknowledgement?

e) Selective Repeat ARQ of the window size must be at most  $2^m/2$ . Explain it.

a), c), d) & e) See Topic: **DATA LINK LAYER**, Long Answer Type Question No. 5(a), (b), (c) & (d).

b) See Topic: **MEDIUM ACCESS SUB LAYER**, Short Answer Type Question No. 2.

9. a) Find the expressions for average delay and throughput for both pure ALOHA and slotted ALOHA. Compare their performances as well.

b) What is cryptography? Explain Public & private Key cryptography with example.

c) What is the difference between Flow Control & Error Control.

a) See Topic: **MEDIUM ACCESS SUB LAYER**, Short Answer Type Question No. 3.

b) See Topic: **APPLICATION LAYER**, Short Answer Type Question No. 3.

c) See Topic: **DATA LINK LAYER**, Short Answer Type Question No. 5.



10. a) Given a 10-bit sequence 1010011110 and a divisor of 1011. Find the CRC.  
b) Write down Advantage and disadvantage of Mesh Topology.  
c) Write down the advantages of fibre-optic cable over twisted pair and coaxial cable.  
d) What is transparent bridge? How the loop problem is removed in transparent bridge?
- a) See Topic: DATA LINK LAYER, Short Answer Type Question No.6.  
b) See Topic: PHYSICAL LEVEL, Short Answer Type Question No. 3.  
c) See Topic: OVERVIEW OF DATA COMMUNICATION AND NETWORKING, Short Answer Type Question No. 3(a).  
d) See Topic: NETWORK LAYER, Short Answer Type Question No. 5.
11. Write the short notes any *three* of the following:
- a) FTP  
b) IEEE 802.11  
c) Token Bucket Algorithm  
d) DNS  
e) QoS in Transport Layer
- a) See Topic: APPLICATION LAYER, Long Answer Type Question No. 3(f).  
b) See Topic: MEDIUM ACCESS SUB LAYER, Long Answer Type Question No. 3.  
c) See Topic: TRANSPORT LAYER, Long Answer Type Question No. 2(a).  
d) See Topic: APPLICATION LAYER, Long Answer Type Question No. 3(b).  
e) See Topic: TRANSPORT LAYER, Long Answer Type Question No. 2(b).

## QUESTION 2017

### Group – A

#### (Multiple Choice Type Questions)

1. Choose the correct alternatives for any *ten* of the following:
- i) WDM methodology is popularly used for
- |                       |                          |
|-----------------------|--------------------------|
| a) twisted pair cable | b) coaxial cable         |
| ✓ c) optical fibre    | d) wireless transmission |
- ii) A network which is used for sharing data, software and hardware among several users owning microcomputers is called
- |        |          |        |        |
|--------|----------|--------|--------|
| a) WAN | ✓ b) LAN | c) MAN | d) VAN |
|--------|----------|--------|--------|
- iii) Method of communication in which transmission takes place in both directions, but only in one direction at a time, is called
- |            |                |                      |                  |
|------------|----------------|----------------------|------------------|
| a) Simplex | b) Full duplex | c) Four wire circuit | ✓ d) Half duplex |
|------------|----------------|----------------------|------------------|

## POPULAR PUBLICATIONS

- iv) The topology with highest reliability is
- a) bus topology      b) star topology      c) ring topology       d) mesh topology
- v) Protocols are
- a) agreement on how communication components and DTEs are to communicate  
b) logical communication channels used for transferring data  
c) physical communication channels used for transferring data  
d) none of these
- vi) For stop-and-wait flow control, for  $n$  data packets sent, how many acknowledgements are needed?
- a)  $n$       b)  $2n$       c)  $n - 1$       d)  $n + 1$
- vii) Which of the following is *not* Network support Layer?
- a) Transport Layer      b) Network Layer  
c) Data Link Layer      d) Physical Layer
- viii) The amount of data that can be carried from one point to another in a given period of time is
- a) Scope       b) Bandwidth      c) Limitation      d) Capacity
- ix) Which one of the following routine algorithms can be used for network layer design?
- a) Shortest path Algorithm      b) Distance Vector Routine  
c) Link State Routine       d) All of these
- x) ICMP is primarily used for (Network Layer)
- a) Error diagnostic      b) Addressing  
c) Forwarding      d) None of these
- xi) The duration of time it takes to send a message from one end of a network to the other and back is called
- a) Round trip time      b) Full Duplex Time  
c) Circle trip time      d) Data Travelling time
- xii) What is the minimum size of a IP packet?
- a) 16 byte      b) 10 byte       c) 20 byte      d) 32 byte



**Group – B**

**(Short Answer Type Questions)**

2. Discuss the function of data link and Transport Layer. What are the drawbacks of mesh topology?

1<sup>st</sup> Part: See Topic: **DATA LINK LAYER**, Short Answer Type Question No. 7.

2<sup>nd</sup> Part: See Topic: **TRANSPORT LAYER**, Short Answer Type Question No. 4.

2<sup>nd</sup> Part: See Topic: **PHYSICAL LEVEL**, Short Answer Type Question No. 4.

3. Describe the purpose of DNS protocol in the internet.

See Topic: **APPLICATION LAYER**, Short Answer Type Question No. 4.

4. Explain Client Server Model. What is the Idea of web based e-mail.

See Topic: **OVERVIEW OF DATA COMMUNICATION AND NETWORKING**, Short Answer Type Question No. 8.

5. What are Gateways? Differentiate between Hub and Switch.

See Topic: **NETWORK LAYER**, Short Answer Type Question No. 1.

6. Explain GSM/CD. What is its usage?

See Topic: **MEDIUM ACCESS SUB LAYER**, Short Answer Type Question No. 4.

**Group – C**

**(Long Answer Type Questions)**

7. What do you understand by Domain Name Server (DNS)? Explain TCP/IP and ADSL. Explain the function of browser in World Wide Web?

1<sup>st</sup> & 3<sup>rd</sup> Part: See Topic: **APPLICATION LAYER**, Long Answer Type Question No. 2.

2<sup>nd</sup> part: See Topic: **OVERVIEW OF DATA COMMUNICATION AND NETWORKING**, Long Answer Type Question No. 4.

8. Write short notes on: a) HTTP and FTP, b) SNMP, c) ARP & RARP.

a) See Topic: **APPLICATION LAYER**, Long Answer Type Question No. 3(c) & (f).

b) See Topic: **APPLICATION LAYER**, Long Answer Type Question No. 3(g).

c) See Topic: **NETWORK LAYER**, Long Answer Type Question No. 7(d).

9. With respect to Ethernet protocol answer the following:

a) How is collision usually detected?

b) What will the transmission station do upon collision?

c) Why is there a minimum limit to the size of the frame? What is the difference between a bridge and a router?

## POPULAR PUBLICATIONS

- a), b) & c) See Topic: NETWORK LAYER, Long Answer Type Question No. 6.  
c) 2<sup>nd</sup> Part: See Topic: NETWORK LAYER, Short Answer Type Question No. 2.

10. List the layers of TCP model. Describe the function of each of the Layers with necessary diagram. What is peer process? How does the layer of TCP correlate with the OSI model?

1<sup>st</sup>, 2<sup>nd</sup> & 4<sup>th</sup> Part: See Topic: OVERVIEW OF DATA COMMUNICATION AND NETWORKING, Long Answer Type Question No. 5.

3<sup>rd</sup> Part: See Topic: MEDIUM ACCESS SUB LAYER, Short Answer Type Question No. 5.

11. Distinguish between Amplitude modulation and Frequency modulation. What is the difference between Single mode and Multimode fibres? What do you mean by Data Transparency? What is Bit stuffing in HDLC? Why is bit stuffing needed?

1<sup>st</sup> & 2<sup>nd</sup> Part: See Topic: OVERVIEW OF DATA COMMUNICATION AND NETWORK, Short Answer Type Question No. 9.

3<sup>rd</sup>, 4<sup>th</sup> & 5<sup>th</sup> Part: See Topic: DATA LINK LAYER, Short Answer Type Question No. 2.