

PART-A SHORT QUESTIONS WITH SOLUTIONS

Q1. Define computer network. How is a computer network different from other types of networks?

Answer :

Dec.-19(R18), Q1(b)

Computer Network

A computer network refers to a network in which several computers placed at different locations are interconnected with each other. This interconnection is possible either by communication medium or communication device through which the data can be shared or transmitted among multiple computer systems. The system that transmits the data to the other systems within a network is referred to as a server, whereas, the systems that receive or accept the shared data are referred to as nodes.

Computer Network Different from Other Types of Network (Distributed System)

In distributed system, the users will not have any idea of the basic organization and existence of various autonomous computers. It will only run the applications or commands, the whole responsibility of choosing the right process or and transferring data to it lies with the operating system. On the other hand, in computer networks, the users will be aware of the autonomous nodes present in the networks. The user has to manually log on to the remote machine and transfer files and data, nothing is done automatically by the operating system. But at present even computer in the network are being connected using wireless networks.

Q2. Write any four reasons for using layered protocols.

Answer :

Nov./Dec.-18(R15), Q1(b)

The five reasons for using layered protocols are as follows,

1. Design

In a layered model each layer is defined separately. Thus, the design problem is broken up into smaller and manageable pieces. Another advantage is it makes protocol designers to specialize in one area (or layer).

2. Change

When changes are made to one layer, it reduces the impact on the other layers.

3. Learning

The layered approach divided a big more complex task into several smaller tasks where each small task is performed by one layer. This makes it much easier to learn and understand the concept of each layer and the model.

4. Communication

The layered approach is useful for proper organizing and handling of communication. It also provides a standard programming interface between two layers.

5. Standards

It is the most important reason for using a layered model. A layered model provides a guideline and framework not a rigid standard to be used by the various vendors when creating their products.

Q3. Write short notes on service and protocol.

Answer :

Nov./Dec.-18(R15), Q1(a)

Service

Service refers to the collection of operations that defines the layer semantics and are provided to the higher level by the lower level. It is characterized as an interface between layers. It defines only the operations to be performed by the layers. It is visible to the user. Services cannot be changed by the entities.

Protocol

Protocol refers to the collection of rules that handles the format and meaning of packets/messages that are to be exchanged between the peer entities. It is characterized as an exchange of packets between the peer entities on different machines.



Publishers and Distributors Pvt. Ltd.

Q4. Write the problems encountered in OSI reference model.**Answer :**

The problems encountered in OSI reference model are as follows,

1. The OSI reference model was designed much before the development of protocols. Thus in real time applications it is a difficult task to fix the protocol in this model.
2. It is a complex model which in turn provides poor performance while implementation of the layers present in it.
3. It is not incorporated by all telecommunication application present on the computer system. This is due to the conflicts with the methodologies and protocols used between the system and software while communication.
4. It makes use of system interruptions to report events but this is not accepted in high level programming languages.
5. It offers data integrity which is usually rejected by many applications due to presence of powerful high speed LANs with low error rates.

May/June-19(R15), Q1(a)

Q5. Discuss the merits of OSI reference model.**Answer :**

Model Paper-II, Q1(a)

The merits of OSI reference model are as follows,

1. OSI reference model divides the network process in the form of smaller components, thereby making the design, development and troubleshooting of these components simpler and easier.
2. Multiple-vendor development is possible with the help of standardization of network components.
3. Communication is possible among different types of network hardware and software.
4. Industry standardization of protocols is supported by specifying the respective functions of each OSI layer.
5. Using this model, the changes made in one layer are restricted from affecting the other layers. Due to this, the development of hardware and software is not delayed.

Q6. Write short notes on interfaces.**Answer :**

Nov./Dec.-16(R13), Q1(a)

An interface is a means of exchanging information between the neighboring layers. It defines what operations and services, a lower layer must provide to a layer above it. After deciding the number of layers to be used along with their functionalities, specific interfaces must be defined between the adjacent layers. Defining clean interfaces reduce the amount of information exchanged between the layers. Clear interfaces also make the process of replacing the implementation of one layer with an entirely different implementation in an easy manner. Hence, interfaces that are defined in an appropriate manner provides modularity to the network.

Q7. Write the advantages of layered architecture of network.**Answer :**

Nov./Dec.-17(R13), Q1(b)

The advantages of layered architecture are as follows,

1. Layered architecture enhances flexibility, maintainability and scalability factor.
2. It is possible for multiple applications to reuse the components.
3. It is possible to develop systems such that they are loosely coupled.
4. It is possible to deploy, maintain and update different components of application independently.
5. It is possible to test the components independently of each other.

Q8. What is Internet?**Answer :**

(Model Paper-I, Q1(a) | April/May-18(R13), Q1(a))

The internet is defined as the combination of more than hundreds of thousands of interconnected networks. The internet is most widely used across many countries, by millions of people for personal use, organizational use including schools, research facilities, offices, government agencies, libraries and many more. The internet is made up of many WANs and LANs interconnected by connecting devices and switching stations. The accurate representation of the internet is difficult as there are continuous changes being evolved day-by-day.

Q9. What is difference between internet and intranet?

Answer :

(Model Paper-II, Q1(b) | Dec.-19(R16), Q1(b))

Internet	Intranet
1. It is world wide network of networks, that allow users to send data, voice, browse, web pages etc.	1. It is private network that is separated from outside world i.e., non-public network link.
2. The structure of Internet is very complex. It connects different networks including intranet and extranet.	2. The structure of such a network is relatively simple.
3. It connects millions of computers i.e., public.	3. It connects internal staffs of an organization.
4. It forms network with world wide web.	4. It forms network with Local Area Network (LAN).
5. It allows flow of information to and from public.	5. It allows flow of information, internally, limited to the particular group. Example: Employees of an organization, students of a college etc.

Q10. What are the advantages and disadvantages of optical fiber?

Answer :

April/May-18(R13), Q1(b)

Advantages of Fiber Optics

- (i) It is immune to noise interference
- (ii) It has larger capacity because of bandwidth
- (iii) It covers longer distances than any other guided media.

Disadvantages of Fiber Optics

- (i) It is very expensive
- (ii) It is difficult to install and maintain..

Q11. Explain the characteristics of twisted pair cable.

Answer :

(Model Paper-I, Q1(b) | Nov./Dec.-16(R13), Q1(b))

The characteristics of twisted pair cable are as follows,

- (i) It is less expensive.
- (ii) It has very low data transfer rate i.e., 4 Mbps.
- (iii) It supports all the radio frequencies.
- (iv) It has high attenuation.
- (v) It gets affected by Electro Magnetic Interference (EMI).
- (vi) It uses electrical signal for transmitting data.
- (vii) It is usually used in telephone lines.

Q12. What are the applications of Infrared waves?

Answer :

The applications of Infrared waves are as follows,

- 1. Infrared waves are used for short range communication.
- 2. They are used by devices such as mouse, keyboards and printer inorder to communicate with PC's.
- 3. These lamps are used by doctors to relieve muscle soreness pain and the treat diseases of skin.
- 4. They are used by photographers for capturing pictures in the absence of visible light.

March-17(R13), Q1(b)

PART-A SHORT QUESTIONS WITH SOLUTIONS

Q1. Define Data link layer.
Answer :

Model Paper-II, Q1(c)

Data-link layer is the second layer which is above the physical layer whose function is to break the input data into (data) frames and take care of acknowledgments. It regulates the flow of traffic in case of fast sender transmitting to a slow receiver. It provides an error-free transmission for the network layer and solves the problems that results from frames (i.e., damage, lost and duplication). It consist of a sublayer called MAC sublayer that provides controlled access to the shared channel.

Q2. Write the functions of LLC.
Answer :

Nov./Dec.-17(R13), Q1(g)

Logical Link Control (LLC) sub layer forms the upper half of the data link layer. Its function is to conceal the difference between various types of 802 networks by providing a single frame format and interface to the network layer. The three services provided by LLC sublayer are unreliable datagram services, acknowledged datagram service and reliable connection-oriented service.

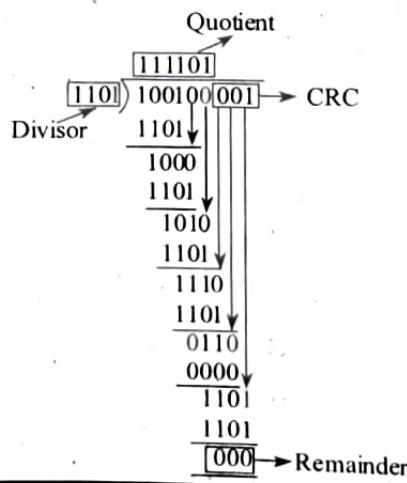
Q3. What is CRC Checker?
Answer :

Nov./Dec.-17(R13), Q1(a)

CRC stands for cyclic redundancy check. This method of error detection is based on binary division. In this method, a sequence of redundant bits known as cyclic redundancy check bits are added to the end of data unit, in order to make it exactly divisible by a predetermined binary number. At the receiver end, the incoming data unit is divided by the same binary number. If the division of operation produces no remainder, then the data unit is accepted else it gets rejected.

The CRC checker functions are almost similar to CRC generator.

After accepting (Data + CRC) it does the same modulo 2 division. If the remainder of all the bits are zero, then the data unit is accepted and hence assured error free otherwise discarded.


Q4. What is the purpose of Hamming code?
Answer :

(Model Paper-I, Q1(c) | May/June-19(R15), Q1(b))

Hamming code is a technique used for detecting and correcting errors. This technique not only detects the errors but also finds the exact bit that contains an error.

When digital information is transmitted from one system to another system an error may occur due to the presence of noise. As a result, the digital information may change from 0 to 1 or vice-versa.

In Hamming code, in order to detect an error, a parity bit is added to the information that has to be transmitted. This addition of parity bit makes the number of 1s in the information either even or odd. At receiver, the parity bit present in received information is verified by comparing it with the transmitted information. If it does not relate with the transmitted one, an error takes place, and erroneous bit is corrected by replacing 1 by 0 or vice-versa depending on the error.

Q5. Explain why there is no need for CSMA/CD on a full duplex Ethernet LAN.

Answer :

April/May-18(R13), Q1(d)

Every station in full duplex switched ethernet is connected to a switch, with the help of two separate connections. And every individual station or switch is able to transmit and receive data independently without any collision. Every connection consists of a point-to-point dedicated path between station and the switch, which considerably eliminates the requirement of carrier sensing and collision detection.

Due to this, the MAC layer can perform its functionality easily by deactivating the functionalities of CS/CD in MAC sublayer.

Q6. Briefly define the features of protocol.

Answer :

Nov./Dec.-18(R15), Q1(d)

Following are the features of a protocol.

1. Unidirectional

A protocol offers unidirectional communication between sender and receiver.

2. Noisy

A protocol offers noisy channel which helps in controlling errors.

3. Limited Buffer

A protocol can limit the amount of buffer used by devices/network.

4. Limited Speed

A protocol can limit the speed of specific application, device or network.

Q7. Write short notes on HDLC?

Answer :

Model Paper-II, Q1(d)

High Level Data Link Control (HDLC) is an ISO data link layer protocol based on the IBM SDLC. It is used to ensure that data passed to the next layer has been received exactly as transmitted. Another important function of HDLC is flow control which ensures that data is transmitted only as fast as the receiver can receive it. HDLC is a group of protocols or rules for transmitting data between the network points. In HDLC, data is organized into a unit called a frame. It also provides transparent transmission on service at the data link layer of OSI reference model. Many protocols use HDLC link layer including X.25, IP point-to-point protocol. HDLC can be used over both single point link and multipoint link communication.

Q8. What is piggy backing? How does it useful?

Answer :

Nov./Dec.-17(R13), Q1(d)

The concept and technique of delaying acknowledgment temporarily which can be fixated on next outgoing data frame is known as piggybacking.

The major and important merit of using piggybacking over having distinct acknowledgment frames is a better use of the available channel bandwidth. A separate frame needs a header, acknowledgment and a checksum whereas the ack field in the frame header needs only few bits. Furthermore, very few frames sent means that very few frames have arrived and fewer interrupts resulting in fewer buffers in the receiver. In the sliding window protocol, we analyze that the piggyback field has only one bit in the frame header whereas it rarely has more than a few bits.

Q9. How selective repeat protocol resolves issues of stop and wait protocol?

Answer :

March-17(R13), Q1(a)

Some of the issues of stop and wait protocol which are resolved by selective repeat protocol are as follows,

1. It increases the number of frames transmitted (i.e., instead of one frame, it can transmit 'N' number of frames).
2. It enhances the window size of sender and receiver (i.e., from 1 to 'N').

Q10. List the carrier sense protocols.

Answer :

Dec.-19(R16), Q1(d)

The different carrier sense protocols are as follows,

(i) 1-persistent CSMA

- ❖ If a station wants to send the data, it first listens to a transmission medium to know whether the medium is free or not.
- ❖ If the channel is busy, it waits for the channel. If the channel is free, then the station sends the frame.
- ❖ When collision occurs, the station waits for some time and starts sending the frame again.
- ❖ By observing above rules, it can be seen that the protocol is 1-persistent CSMA because the station transmits with a probability of 1 whenever it knows the medium (channel) is idle.

(ii) Non-persistent CSMA

This protocol is used to avoid long delays and it provides a better way to utilize the channel. In this algorithm, a station senses the medium before sending any frame. If the medium is idle, this means no other stations are utilizing the same medium (channel) then it will send the frame. If the medium is busy, it does not sense for a long time instead, it waits for a random time and then it repeats the algorithm. This protocol provides a better channel utilization than 1-persistent CSMA.

(iii) P-persistent CSMA

These protocols are applied to slotted channels with 1-persistent CSMA. What happens if two stations want to send data when a third station is busy in sending the data? Both wait for the third station to finish, then simultaneously launch a packet, guaranteeing a collision.

Q11. What is meant by collision free protocols?**Answer :**

Nov./Dec.-16(R13), Q1(d)

Collision-Free Protocols

Collision-free protocols refer to the protocols which make the transmission collision-free.

Using CSMA/CD, collisions are mostly avoided but not completely. One of the problems with CSMA/CD is that its frame size should be large enough that a collision is detected before the packet transmission completes.

The three major protocols used for performing collision free transmission are,

(i) Bit-map Protocol

Bit-map protocol is a collision-free protocol that avoids the collision occurring during the contention period. In this protocol, each contention period is divided into exactly N slots.

(ii) Binary Countdown Protocol

This protocol is used to overcome the problem of Bit-map protocol by using a binary bit string. With this protocol, if a station wants to use the channel, it broadcasts its address as a binary bit string, starting with the high-order bit.

(iii) Token Passing

In token passing method, the organization of stations in the network are in the form of a logical ring. Each station has a well defined predecessor and successor. The station which is logically before the station in the ring is called as predecessor and the station that is logically after the station in the ring is called as successor. The station that is currently accessing the channel is called current station.

Q12. What is a spanning tree bridge?**Answer :**

Nov./Dec.-18(R15), Q1(c)

Spanning tree bridge is a type of bridge which creates a spanning tree to traverse every LAN present in a network.

The spanning tree can be constructed in the following step-wise manner.

1. Selecting a bridge as a root of the tree depending on the unique serial number (which is embedded by the manufacturer). Basically the bridge having the lowest serial number is treated as the root of the tree.
2. Construct a tree which has the shortest path from root to every bridge and LAN.

The resultant tree is the spanning tree.

Q13. Mention the functions of Hub.**Answer :**

April/May-18(R13), Q1(c)

The functions of Hub are,

1. Hub allows adding, deleting or moving of workstations.
2. It enlarges the network length.
3. It offers centralized management services.
4. It also offers multiple interfaces.

Q14. What is repeater?

(Model Paper-I, Q1(d) | May/June-19(R15), Q1(c))

OR

Explain the function of repeaters.

Answer :

A repeater is a device used to amplify signals. The most important functions of repeater are,

- (i) The repeater function at physical layer of OSI model
- (ii) They regenerate the baseband signals.
- (iii) They does not filter the packets
- (iv) They keep the signal constant
- (v) They passes a broadcast.

March-17(R13), Q1(d)

PART-A SHORT QUESTIONS WITH SOLUTIONS

Q1. Write the responsibilities of network layer.

Answer :

The following are the responsibilities of the network layer,

1. Logical Addressing

Network layer defines an addressing system responsible for distinguishing source and destination system when a packet is sent across the network's boundary. It also adds a header to the packet received from upper layer. This header contains certain information such as the logical address of both sender and receiver.

2. Routing

Routing technique is used to select the optimal path or shortest path for sending packet from source to destination. There are various routing algorithms such as hierarchical routing, distance vector routing, link state routing, flow-based routing, etc. Network layer also solves the problem of congestion which degrades the performance of network by using various congestion control algorithms such as leaky-bucket, token bucket, choke-packet, etc.,

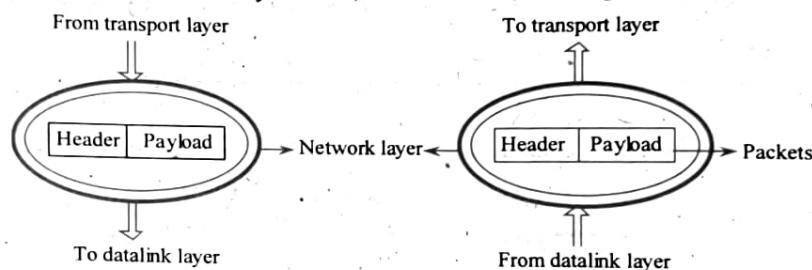


Figure: Network Layer

Q2. Mention the design issues of network layer.

Answer :

The following are the design issues of network layer,

(Model Paper-I, Q1(e) | Nov./Dec.-16(R13), Q1(e))

1. Providing services to the transport layer
2. Internal design of the subnet.

1. Providing Services to the Transport Layer

The function of the network layer is to provide services to the transport layer. These services are provided at the network-transport layer interface. This interface is important because it acts as a frequent medium between the carrier (the boundary of the subnet) and the customers. The job of the carrier is to send all the packets passed to it by the customers. Therefore, it must be designed well.

The network layer services are designed such that they are independent of the subnet organization, the details of subnet topology is hidden from the transport layer and the uniform network addresses are available to the transport layer across LANs and WANs.

2. Internal Design of the Subnet

Next issue in the design of network layer is the internal organization of the communication subnet. A communication subnet (or subnet) consists of transmission lines and switching elements (routers).

Q3. What are the metrics used by routing protocols?

Answer :

The metrics used by routing protocols are as follows,

1. Number of hops (hop count)
2. Path reliability
3. Path bandwidth
4. Latency (delay)
5. Speed of the path
6. Load
7. Cost.

March-17(R13), Q1(e)

Q4. Explain briefly about flooding.**Answer :**

(Model Paper-II, Q1(e) | May/June-19(R15), Q1(f))

Flooding is a static algorithm which consider all the incoming data packets and broadcast them among all the outgoing paths excluding the current path on which it is present. By doing so, it produces a huge amount (infinite) of duplicate packets and hence some effort needs to be applied in order to stop this process of duplication.

However, there exist certain prevention techniques such as use of hop counter and tracking of packets already flooded. In the first technique i.e., use of hop counter, a hop counter included in the header of packets which carry the hop number (or) the length of path typically the number of hops from source to the destination. In case that the destination path is not known, the hop counter is allotted with the full length of the subnet.

The second method of preventing the duplication is to keep track the packets that are already flooded. By this, the duplication is avoided simply by referring the list of packets already flooded.

Q5. What is the difference between router and gateway?**Answer :**

Nov./Dec.-16(R13), Q1(c)

Router	Gateway
1. Router is a device used for connecting two or more networks having similar protocol.	1. Gateway is a device used for translating information among different network data formats.
2. It is used at the network layer.	2. It is used at the application layer.
3. It is not capable of converting protocols.	3. It is capable of converting protocol.
4. It is simple.	4. It is complex.

Q6. Discuss various goals of routing algorithm.**Answer :**

(Model Paper-I, Q1(f) | Nov./Dec.-18(R15), Q1(f))

The goals of routing algorithms are,

1. To decide the path to be used for routing packet from source router to destination router.
2. To determine the best path from various interlinked router.
3. To ensure that the network is simple, robust, stable and optimal.

Q7. Define Broadcasting.**Answer :**

Dec.-19(R16), Q1(e)

The process of sending a packet to all the nodes on the network at same instant is called broadcasting. The algorithms used for broadcasting are called broadcast routing. Various methods for broadcast routing are,

1. Distinct point-to-point routing
2. Flooding
3. Multi-destination routing
4. Use of spanning tree
5. Reverse path forwarding.

Q8. What are the three main elements of distance vector routing algorithm?**Answer :**

April/May-18(R13), Q1(f)

The three main elements/aspects of distance vector routing algorithm are as follows,

1. Complete Network Information

Every individual router present in the network possesses some information about the network. So, each router is responsible for sharing the information with other routers. Hence, routers collect enormous information about the entire network.

2. Information Sharing among its Neighbouring Routers

Every individual router shares the information regarding the network among the routers which are directly connected to it (i.e., neighbouring router).

3. Sharing of Information at Regular Time Intervals

Every individual router shares the updated information with its neighbouring routers despite of any alterations in the network conditions. This sharing of information is done at specified regular time intervals (eg: for every 30 sec).

Q9. What is congestion? State general principles of congestion control.

Dec.-19(R16), Q1(f)

OR

What is congestion control? May/June-19(R15), Q1(e)

(Refer Only Topic: General Principles of Congestion Control)

OR

What is congestion?

(Refer Only Topic: Congestion)

Answer :

Nov./Dec.-18(R15), Q1(e)

Congestion

Congestion is the state in which network performance decreases. This happens when a network is holding too many packets which are much more than the network's capability.

There are various reasons for congestion to occur. Few of them are listed below.

1. If the traffic on the network is very high.
2. If the C.P.U's processing speed is slow.
3. If there is insufficient amount memory to hold the packets.

General Principles of Congestion Control

Congestion control is concerned about controlling traffic entry into a network so as to avoid congestion by taking resource reducing steps such as reducing the rate of sending packets.

Congestion control strategy is divided into two types.

1. Open loop congestion control
2. Closed loop congestion control.

Q10. How does netid differ from a network address?

Answer :

March-17(R13), Q1(f)

NetID stands for Network Identification which is also called as Network ID or Network Address. Network address is the unique identifier for a network which can be used by other networks inorder to identify it across the globe. Network address is represented by a certain number of bits on the left most side of an IP address.

Q11. Explain about Packet Fragmentation.

Answer : (Model Paper-II, Q1(f) | March-17(R13), Q1(h))

In Internet working, it is possible that a larger size packet can appear on a small sized network. This is done by dividing the original packet into smaller fragments which are treated as independent packets and are routed over the small sized network. Thus, dividing the larger packet into smaller independent packets is called fragmentation.

There are two strategies used for recombining the fragment into its original packet. They are as follows,

1. Transparent fragmentation
2. Non-transparent fragmentation.

Q12. Explain about IPv6 extension headers.

Nov./Dec.-18(R15), Q1(h)

Answer :

The following figure shows the format of an IPv6 header.

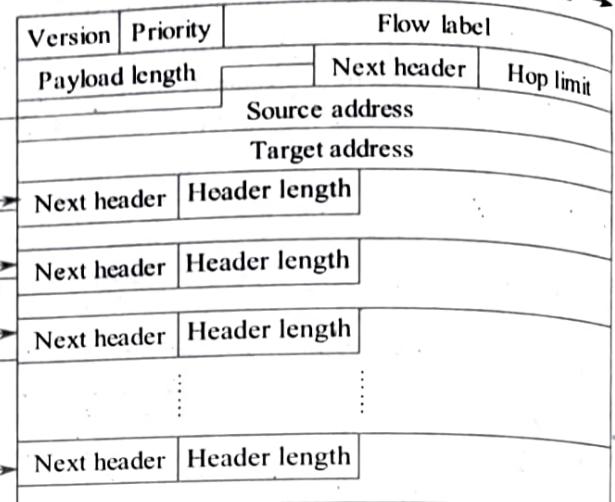


Figure: Format of an IPv6 Header

The base header of an IPv6 header has the following fields,

- (i) Version
- (ii) Priority
- (iii) Flow Label
- (iv) Payload Length
- (v) Next Header
- (vi) Hop Limit
- (vii) Source Address
- (viii) Target Address.

Q13. What are the disadvantages of IPv4?

Answer :

May/June-19(R15), Q1(h)

- Following are some of the disadvantages of using IPv4.
1. It offers limited amount of addresses which depletes the available addresses when number of devices increases exponentially.
 2. It does not provide security features.
 3. It lacks in providing quality of service with respect to bandwidth and delay requirements.

Q14. Explain about CIDR.

Answer :

Nov./Dec.-16(R13), Q1(g)

Supernetting is also called as Classless Inter Domain Routing (CIDR). It is a way to allocate and specify the Internet addresses used in interdomain routing more flexibly than with the original system of Internet protocol address classes. The original Internet protocol defines IP addresses in four major classes i.e., class A, B, C, D. Each of these classes allocates one portion of a 32-bit Internet address format to a network specified by the address.

One of the most commonly used classes is class B, which allocates space for upto 65,533 host address. A company who needs more than 254 host machines, but far less than 65,533 host addresses possible, would essentially be wasting most of the block of addresses allocated. For this reason, the Internet was running out of address space. CIDR effectively solved the problem by specifying a new way to specify the network addresses in routers.

Q15. Write about Tunneling.

Nov./Dec.-17(R13), Q1(h)

OR

Explain Tunneling.

Answer :

April/May-18(R13), Q1(g)

Tunneling is a method of transmitting data that is intended for use only within a private network through a public network in such a way that the routing nodes in the public network are unaware that the transmission is part of private network. Tunneling is generally done by encapsulating the private network data and protocol information within the public network transmission units, so that the private network protocol information appears to the public network as data. Tunneling allows the use of internet, which is a public network to convey data on behalf of a private network.

Q16. What is the purpose of Subnetting?

Answer :

April/May-18(R13), Q1(e)

A subnet (subnetwork) is a small network within a large network which is usually separated by a bridge or a router. Hosts or machines of a subnets shares a common address component.

The main purpose of subnetting is to keep network free from congestion.

A subnet is recognized as an isolated feature of an organizations network. Usually, a common subnet is the one where all the machines are connected to a common Local Area Network (LAN) at a particular location. It is also possible to have a connection to the Internet with a single shared network address by dividing the organizations network into various subnets, where as, an organization without any subnets require various Internet connections for each of its subnetwork. The problem in doing so, would be the unnecessary use of the restricted network numbers that the Internet need to assign. Then, the Internet routing tables are also needed on gateways which located outside the organization, so as to understand and control the routing that need to be handled within the organization. The figure below represents the subnets within a large network of an organization.

Q17. Define Firewall.

Answer :

Dec.-19(R16), Q1(i)

A firewall can be viewed as an information security program located at a network gateway server. It protects the confidential information present in the network against attacks or by other insecure networks. It acts as a barrier that allows only the authorized network traffic to pass and through and stops the unauthorized traffic. In simple terms, firewalls are designed to function either as a filter or as a security device. It is installed on a system so as to prevent the unauthorized users from accessing the secure networks. In case of mobile users, firewalls use secure procedures and authentication keys to allow remote access into the secure network.

Q18. Discuss in brief about DHCP.

Answer :

Nov./Dec.-18(R15), Q1(g)

Dynamic Host Configuration Protocol (DHCP) is mainly used for the simplification of installation and maintenance of network computers. If a new computer is connected to a network, DHCP provides it with all necessary information for full system integration into the network, e.g., address of a DNS server and the default router, the subnet mask, the domain name and an IP address.

DHCP mainly used as mobile IP as a source since it has the capability of providing an IP address. DHCP mechanisms are quite simple. Since, many options are available. DHCP is based on a client/server model.

PART-A SHORT QUESTIONS WITH SOLUTIONS**Q1. What is a transport layer?****Answer :**

- Transport layer is the fourth layer in the OSI reference model. It lies between the Network layer and session layer.
1. The transport layer is responsible for accepting data from the session layer, dividing it into small pieces (TPDUS), if required and passing these pieces to the network layer and assure the correct reception of data at the other end.
 2. It sets up and terminates the connections across the network thereby, regulating the flow of information.
 3. It also multiplexes the data and establishes multiple connections, when a high throughput is desired.

The transport layer allows the reliable transfer of data from source to destination. The layer defines two end-to-end protocols namely, TCP (Transmission Control Protocol) and UDP (User Datagram Protocol) to interact with other layers in the model.

Q2. List the transport service primitives.**Answer :**

The various transport service primitives are as follows,

(Dec.-19(R16), Q1(g))

- | | |
|-------------------|--|
| LISTEN | : Server is waiting for connection request. |
| CONNECT | : Client sends the connection request TPDU, requesting for connection. |
| SEND | : Transfer the data. |
| RECEIVE | : Receive the data. |
| DISCONNECT | : Terminates the connection using DISCONNECT TPDU. |

Q3. Explain the functions of transport layer.**Answer :**

(Model Paper-I, Q1(g) | Nov./Dec.-16(R13), Q1(h))

The functions of transport layer are as follows,

1. It is responsible for accepting data from the session layer, dividing it into small pieces (TPDUS) if required and passing these pieces to the network layer and assure the correct reception of data at the other end.
2. It sets up and terminates the connections across the network thereby, regulating the flow of information.
3. It also multiplexes the data and establishes multiple connections, when a high throughput is desired.

Q4. What are the services provided by transport layer protocol?**Answer :**

Transport layer is the fourth layer of ISO/OSI model. The primary objective of this layer is to provide reliable and efficient end-to-end delivery of a message. In order to achieve this goal, it is necessary for transport layer to utilize the services provided by its lower layer i.e., network layer. Transport entity is responsible for carrying out the operations within the transport layer. Similar to network layer, transport layer even provides two types of transport services. They are,

1. Connection oriented services
2. Connectionless services.

The functionality of these services is very much similar to the services provided by the network layer i.e., connection-oriented transport services are similar to connection-oriented network services, and connectionless transport services are similar to connectionless network services.

Q5. What is crash recovery?

May/June-19(R15), Q1(g)

OR**Explain briefly about crash recovery.****Answer :**

If a host present in a layer N crashes, then it is recovered by layer N + 1 using the status information present in the layer. This process of recovering from the crash is referred to as 'Crash Recovery'. The process becomes difficult if both host as well as the routers crashes. In order to understand the recovery process performed after the host crashes, let us consider a situation in which client and server communicate using stop-and-wait protocol. This protocol guarantees that the client will send another packet only after receiving the acknowledgement for the previously transmitted packet has received. The client transmits the transport entity (i.e., TPDU) to the server via the network layer on the client. This entity passes through all the layers on the client and then goes to the layers on the server. The transport layer on the server after receiving this entity from the network layer transmits it to the higher layer. Now, during this transmission, let us assume that the server crashes.

March-17(R13), Q1(g)



Publishers and Distributors Pvt. Ltd.

Q6. What is multiplexing? Give different types of multiplexing?**Answer :****Multiplexing**

The data chunks collected from different sockets at the source host are encapsulated with header information to create segments and the process of sending these segments to the network layer is known as multiplexing.

Different Types of Multiplexing

There are two types of multiplexing. They are,

1. Connection-oriented multiplexing
2. Connectionless multiplexing.

Connection-Oriented Multiplexing

The protocol which provides a reliable, connection-oriented service to the application is TCP (Transmission Control Protocol). The difference between UDP socket and TCP socket is UDP socket is a two tuple whereas TCP socket is four tuple. The four values of TCP socket include source address, source port number, destination IP address and destination port number, which are used by the receiving host to direct the segment to the appropriate socket unlike UDP two TCP segments having different source IP address or source numbers are sent to the two different sockets.

Connectionless Multiplexing

The protocol which provides unreliable connectionless service to the application is UDP (User Datagram Protocol).

UDP multiplexing and demultiplexing can be understood by the port numbers assigned to UDP sockets.

Q7. Difference between connectionless and connection-oriented networks.**Answer :**

(Model Paper-II, Q1(h) | Nov./Dec.-16(R13), Q1(f))

Connectionless Service	Connection-oriented Service
<ol style="list-style-type: none"> 1. In connectionless service, connection is neither established nor released. 2. Packets are not numbered. 3. There is no acknowledgement. 4. Packets may be delayed or lost or may arrive out of sequence. <p>Examples: Include, IP and UDP.</p> <ol style="list-style-type: none"> 5. It may (or) may not contain reliability transfer of data. 6. It doesnot require any authentication before sending data. 	<ol style="list-style-type: none"> 1. In connection oriented service, connection is first established and released at the end of the data transmission. 2. Packets are numbered with a randomly generated number. 3. The sender is acknowledged. 4. There is no loss of data or delay because the packets are transmitted in order from sender to receiver in one single connection. <p>Examples: Include, TCP and SCTP.</p> <ol style="list-style-type: none"> 5. It contains reliability in transfer of data. 6. It requires authentication of the destination node before sending data.

Q8. What is TCP?**Answer :**

TCP is a connection oriented protocol and most commonly used protocol in the transport layer. It supports the connection management facilities of the Internet.

TCP can be used to setup a logical connection between two entities and to transfer a sequence of bytes between them. A key feature of TCP is that it provides connection oriented user-to-user byte stream service. Every byte in a TCP connection consists of a unique 32-bit sequence number that is used for acknowledgments.

The exchange of data between any two TCP entities is done using segments. The TCP segment has a fixed 20-byte header and an optional part which is followed by data bytes. The length of a segment is determined by TCP software.

Q9. Explain the socket primitive of TCP.**Answer :**

April/May-18(R13), Q1(h)

The various primitives used for TCP are,

- SOCKET** : Create a new connection.
- BIND** : Assigns address to new socket.
- LISTEN** : Waits for the incoming connection request.
- ACCEPT** : Accepts the connection.
- CONNECT** : Connection is being established.
- SEND** : Transmit data over the connection.
- RECEIVE** : Receives data over the connection.
- CLOSE** : Terminates the connection.

Q10. What are the fields that are present in the UDP header?**Answer :**

(Model Paper-I, Q1(h) | Dec.-19(R16), Q1(h))

UDP header consists of four fields each of two bytes in length.

(i) Source Address

It specifies the port number of the sender which describes where a reply packet is to be sent. This can actually be set to zero if it is not used. For example if a user don't require a reply packet, then the source address for that packet can be set to zero.

(ii) Destination Address

It specifies the port number of the receiver where the packet is to be transmitted. If the destination host is a server, then the port numbers are reserved.

(iii) UDP Length

It specifies number of bytes comprising the combined UDP header information and payload data. The total length of UDP user datagram is 65,535 bytes, but as the datagram is stored within the IP packet, the length of UDP datagram is, $65535 - 20 = 65515$ bytes.

$$\text{i.e., UDP length} = \text{IP length} - \text{IP header length}$$

(iv) UDP Checksum

This checksum is the same kind of checksum used in TCP header except that it contains a different set of data. It is computed in the same way as that of TCP. A checksum is used to verify that end-to-end data that has not been corrupted by routers or bridges in the network. If checksum is not required, the value zero is placed in this field in which case the data is not checked by the receiver, checksum comprises of pseudoheader, UDP header and UDP data. The pseudoheader serves the same purpose as that of TCP. But for UDP, the value for protocol is 17.

PART-A SHORT QUESTIONS WITH SOLUTIONS

Q1. Write short notes on application layer and WWW.

Answer :

Model Paper-I, Q1(i)

Application Layer

Application layer provides interface between user and computer hardware. It contains the implementation of various protocols used for user interaction such as Telnet, FTP, SMTP etc.

WWW

The World Wide Web (WWW), or the web is a repository that spreads information all over the world and linked together. The WWW has a unique combination of flexibility, portability and user-friendly features that distinguish it from other services provided by the Internet. The WWW is a distributed client-server service, in which a client using a browser can access a service using a server. However, the service provided is distributed over many locations called websites.

Q2. What are the services offered by application layer?

Answer :

May/June-19(R15), Q1(j)

- The services offered by Application layer are as follows,
- (i) It offers security of messages using cryptography.
- (ii) It represents the names as IP addresses using DNS.
- (iii) It offers SNMP service, which specifies the process of management in the internet.
- (iv) It helps sending and receiving electronic mails.
- (v) It offers file transfer access and management by using FTP.
- (vi) It provides distributed database sources allowing access to global information.
- (vii) It provides HTTP services to fetch the web pages on the WWW.
- (viii) Authentication of the genuine users.

Q3. Write the application layer paradigms.

Answer :

Nov./Dec.-16(R13), Q1(j)

Application layer paradigms are the standards used by the two application programs to communicate with each other. Application layer uses three types of paradigms. They are as follows,

1. Traditional paradigm/client-server
2. New paradigm/peer-to-peer
3. Mixed paradigm.

Q4. What is DNS? Write its properties.

Answer :

Nov./Dec.-17(R13), Q1(i)

DNS

The Domain Name Space (DNS) is specified as a hierarchical, distributed method of organizing the name space of the Internet. The DNS administratively clusters hosts into a hierarchy of authority allowing addressing and other information to be widely distributed and maintained. A key advantage of the DNS is that it eliminates the dependence across centrally maintained file that maps host names to addresses. DNS is supported via set of network-resident servers called as Domain Name Servers.

Properties of DNS

(i) DNS Servers

The domain name space contains a huge amount of information that can't be stored on a single server. Thus it is distributed among multiple computers, each computer is called a DNS server.

(ii) Zone

The complete domain name hierarchy is divided among multiple servers. Each server handles one domain. The responsibility of a server for a particular domain is called a zone.

Q5. What are the two main categories of DNS messages?**Answer :**

March-17(R13), Q1(j)

The messages of Domain Name System (DNS) are divided into two categories, namely,

- The query message
- The response message.

A query message is composed of two fields,

- Header and
- Question records.

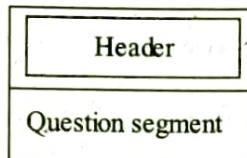


Figure (i): Query Message Fields

A response message is composed of five fields namely,

- Header
- Question records
- Answer records
- Authoritative records
- Additional records.

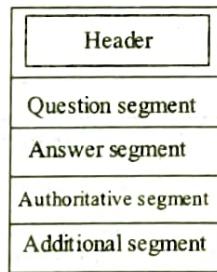


Figure (ii): Response Message Fields

Q6. Write short notes on SNMP.**Answer :**

The TCP/IP protocol suite has come up with the concept of the Simple Network Management Protocol (SNMP). It resides at the application layer and therefore, is does not depend on underlying protocols and hardware specific details. It provides a set of fundamental operations for monitoring and maintaining the Internet.

Q7. In e-mail system, where the e-mail messages are stored and why?**Answer :**

Nov./Dec.-18(R15), Q11(b)

E-mail messages are stored in the user's private electronic mailbox. A mailbox refers to a local hard drive component, a special file associated with permission restrictions so that only the owner i.e., the authorized user may have the capability of accessing it. The messages are stored until the recipient checks their electronic mailboxes (i.e. opens and reads them). Thus, the user should check the electronic mailbox regularly. However, most of the systems provide an alert whenever a mail is received. After the e-mail message has been read, the user can store it (in the form of a text file), reply to it, forward it (to the other users), delete it copy it or take a print of it. Since, mailboxes are not very stable, the e-mail message can be saved by copying it to a file or a document.

Q8. What are the basic functions of email systems?

(Model Paper-II, Q1(I) | March-17(R13), Q1(I))

Answer :
E-mail system has five functions. They are,

- Compose
- Send
- Report
- Display
- Disposition.

(a) Compose

The compose function allows the users to write their message in the message box.

(b) Send

The transfer (or) send function forwards the messages from source to destination automatically.

(c) Report

The Report function is like a feedback, which tells the sender about the message.

(d) Display

Display function allows the users to read their e-mail.

(e) Disposition

Disposition function gives the information about the message after received by the receiver.

Q9. Explain MIME header.

Answer :

Nov./Dec.-17(R13), Q1(j)

The following are the message header fields added by MIME.

- MIME-Version
- Content-Type
- Content-Transfer-Encoding
- Content-ID
- Content-Description.

Header	Meaning
(i) MIME-Version	This header is used to identify the version of the MIME message format.
(ii) Content-Type	It describes the type and format of the content. There are six types of content namely Application, Audio, Image, Message multipart, Text and Video.
(iii) Content-Transfer-Encoding	It indicates how the structure of message is encoded for transmission. i.e., it indicates the encoding method used to transform the document into seven bit format for transmission. Options are: 7-bit data, 8-bit characters, BASE 64, Binary, Quoted-Printable, X-Token.
(iv) Content-ID	It defines a unique identifier. This means, it allows a body of information to refer another message.
(v) Content Description	This header consists of string which gives the information regarding message.

Q10. Explain the status codes of HTTP client error:

Answer :

HTTP client error is provided with status codes in the response and caching of resource at server. The different status codes are,

400 : It represents a bad request,
 401 : It represents an unauthorized request,
 402 : It represents that the request needs payment before response feasible
 403 : It represents the request is for forbidden resource
 404 : It represents that the URL is not found.

April/May-18(R13), Q1(I)

Q11. Compare HTTP and FTP.

Answer :

(Model Paper-II, Q1(j) | April/May-18(R13), Q1(j))

HTTP	FTP
1. HTTP allows transfer of web pages from server to client.	1. FTP allows transfer of files from client to server and vice versa.
2. It uses a port number 80 i.e., single port connection.	2. It uses port number 20 and 21 i.e., two different port connections.
3. It is a stateless protocol.	3. It manages user's information.
4. It transfers its control information "in-band".	4. It transfers its control information "out of band".

Q12. Give the HTTP message format.

Answer :

May/June-19(R15), Q1(i)

Http Request

The request made to web server by client is called HTTP request. The HTTP request message format is shown in the following figure.

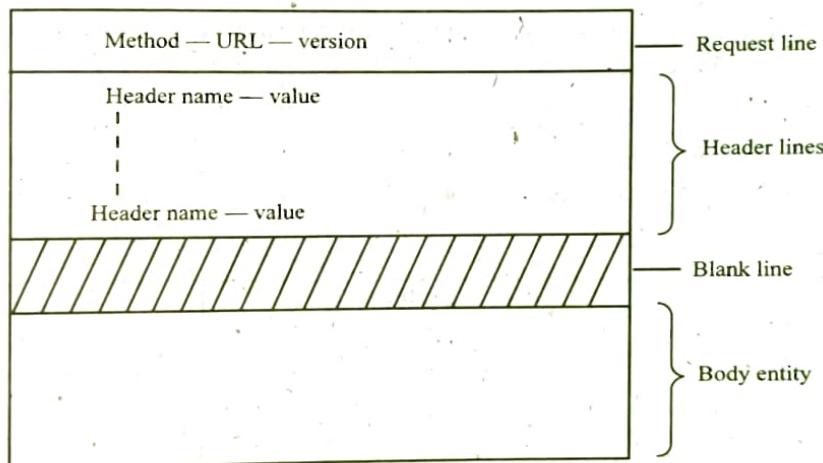


Figure: HTTP Request Message Format

Http Response

The response made from web server to client is called HTTP response. The HTTP response message format is shown in the following figure.

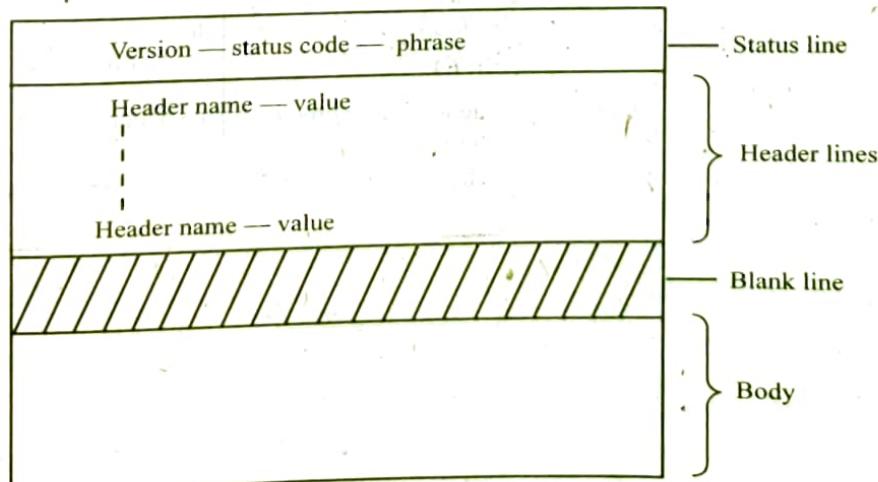


Figure: HTTP Response Message Format

Q13. Define URL.**Answer :****URL**

Model Paper-I, Q1(j)

Uniform Resource Locator (URL) specifies the address of an arbitrary resources (i.e., file or services) on the server so that, the client can easily access the required resource. It is a standard means of specifying any sort of information on the Internet.

Components of URL

The following are the basic components of URL,

1. Protocol
2. Host computer
3. Port
4. Path.

Q14. What is multimedia?**Answer :**

Multimedia is basically a media that makes use of combination of various content forms such as video, images, animation etc. Usually computerized and electronic devices utilize multimedia for recording and playing games, displaying accessing data. Multimedia is different from fixed media, because the form include the audio content. Multimedia can be classified into two categories based on navigational control.

Q15. Write the differences between I-frames, P-frames, B-frames.**Answer :**

S.No.	Intracoded frame (I-frame)	Predicted frame (P-frame)	Bidirectional frame (B-frame)
1.	It is an independent frame not relative to any other frame.	It is relative to previous I-frame or P-frame.	It is relative to preceding P-frame or I-frame.
2.	These frames are least compressible, thus other video frames are not required for decomposition.	Less compressible than I-frames and can share data from previous frames for decompression.	These frames provide higher amount of data compression these frames can share previous and forward frames for referencing the data.
3.	It is an intra-coded picture having the complete picture. P and B-frames hold part of this frame information.	It is a predicted picture which holds only modification in the image from the previous frame thereby consuming less space.	It is a Bi-predictive picture that saves a lot of space by having differences between the current frame and both previous and following frames.
4.	They contain only intra macroblocks.	They contain either intra or predicted macroblocks.	They contain either intra or predicted or bi-predicted macroblocks.