Model Question Paper

Course Code: CST 303

Course Name : Computer Networks

PART A

1. What does “negotiation" mean when discussing network protocols in alayered architecture? Give an example.

Negotiation in terms of network protocols can be done on established connection. the sender and receiver will make some negotiations on parameters which are used to transfer the data between both of them. Parameters are like QOS, which authentication, encryption technique will use, Maximum size of message etc.

2. Define simplex, half-duplex, and full-duplex transmission modes. Give one example for each.

Simplex mode	Half-duplex mode	Full-duplex mode
The communication is unidirectional.	The communication is bidirectional, but one at a time.	The communication is bidirectional.
A device can only send data but cannot receive it or it can only receive data but cannot send it.	Both the devices can send and receive the data, but one at a time.	Both the devices can send and receive the data simultaneously.
The lowest performance among the mods.	The performance is better than simplex but less than full duplex.	The highest performance among the mods.
Examples are radio, keyboard, and monitor.	Example is Walkie-Talkies.	Example is a telephone or mobile network.

3. Data link protocols almost always put the CRC in a trailer rather than in a header. Why?

The CRC is computed during transmission and appended to the output stream as soon as the last bit goes out onto the wire. If the CRC were in the header, it would be necessary to make a pass over the frame to compute the CRC before transmitting. This would require each byte to be handled twice— once for checksumming and once for transmitting. Using the trailer cuts the work in half.

4. An 8-bit byte with binary value 10101111 is to be encoded using an even-parity Hamming code. What is the binary value after encoding?

The procedure used by the sender to encode the message encompasses the following steps –

Step 1 − Calculation of the number of redundant bits.

Step 2 − Positioning the redundant bits.

Step 3 − Calculating the values of each redundant bit.

Refer step by step example here: https://www.geeksforgeeks.org/hamming-code-in-computer-network/

Solution to the given problem is :

12	11	10	9	8	7	6	5	4	3	2	1
1	1	1	1	0	0	1	0	0	1	0	1

5. Illustrate the Count to Infinity problem in routing.

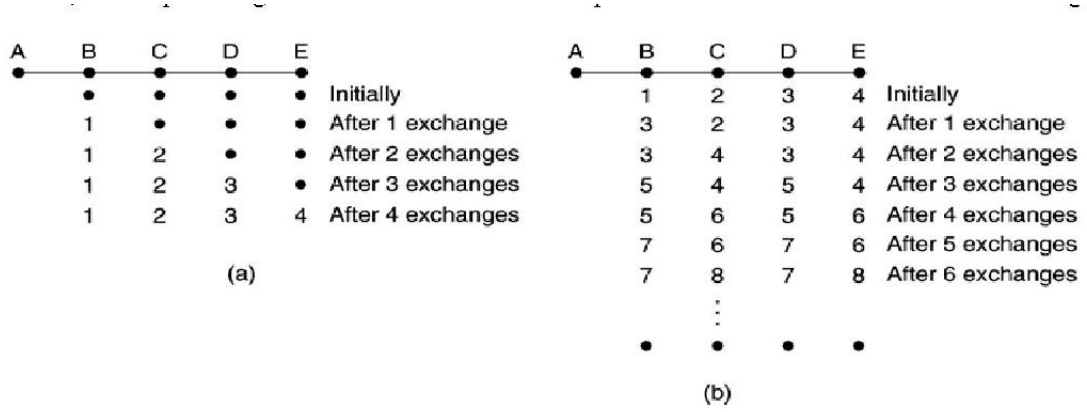


Figure 2. (a) Before and (b) After Count to infinity problem

Distance vector routing reacts rapidly to good news, but leisurely to bad news. Consider a router whose best route to destination X is long. If, on the next exchange, neighbor A suddenly reports a short delay to X, the router just switches over to using the line to A to send traffic to X. In one vector exchange, the good news is processed. (Figure on left side)

A goes down or the link between A and B is cut (which is effectively the same thing from B's point of view). At the first packet exchange, B does not hear anything from A. Fortunately, C says ''Do not worry; I have a path to A of length 2.'' Little does B suspect that C's path runs through B itself. For all B knows, C might have ten links all with separate paths to A of length 2. As a result, B thinks it can reach A via C, with a path length of 3. D and E do not update their entries for A on the first exchange. On the second exchange, C notices that each of its neighbors claims to have a path to A of length 3. It picks one of them at random and makes its new distance to A 4, as shown in the third row of Fig. fig(b). Subsequent exchanges produce the history shown in the rest of Fig(b). From this figure, it should be clear why bad news travels slowly.

6. Describe two major differences between the warning bit method and the Random Early Detection (RED) method.

These are two congestion control mechanisms.

Warning bit/DECBit method - the idea here is to more evenly split the responsibility for congestion control between the routers and the end nodes. Each router monitors

the load it is experiencing and explicitly notifies the end nodes when congestion is about to occur. This notification is implemented by setting a binary congestion bit in the packets that flow through the router, hence the name *DECbit*. The destination host then copies this congestion bit into the ACK it sends back to the source. Finally, the source adjusts its sending rate so as to avoid congestion.

RED - similar to the DECbit scheme in that each router is programmed to monitor its own queue length and, when it detects that congestion is imminent, to notify the source to adjust its congestion window.

2 Differences:

- The first is that rather than explicitly sending a congestion notification message to the source, RED is most commonly implemented such that it *implicitly* notifies the source of congestion by dropping one of its packets. The source is, therefore, effectively notified by the subsequent timeout or duplicate ACK.
- The second difference between RED and DECbit is in the details of how RED decides when to drop a packet and what packet it decides to drop. To understand the basic idea, consider a simple FIFO queue. Rather than wait for the queue to become completely full and then be forced to drop each arriving packet (the tail drop policy), we could decide to drop each arriving packet with some *drop probability* whenever the queue length exceeds some *drop level*. This idea is called *early random drop*.

7. The Protocol field used in the IPv4 header is not present in the fixed IPv6 header. Why?

<Draw IPv4 and IPv6 header structure>

The Protocol field tells the destination host which protocol handler to give the IP packet to. Intermediate routers do not need this information, so it is not needed in the main header. Actually, it is there, but disguised. The Next header field of the last (extension) header is used for this purpose.

8. How many octets does the smallest possible IPv6 (IP version 6) datagram contain?

1,280 octets

9. Can Transmission Control Protocol(TCP) be used directly over a network (e. g. an Ethernet) without using IP? Justify your answer.

Explain the need of network layer / IP – host-to-host delivery. The layer above it, transport layer is implemented with the help of services provided by network layer.

Ethernet – Data Link Layer

IP – Network Layer

TCP – Transport Layer

TCP depends on IP to deliver the data, even to another machine on the same network. The IP header contains the IP address to which the data is sent. Finally, there is a configured IP packet type code for the Ethernet header, but no TCP type code, so there is no way to put TCP directly on top of the Ethernet header.

10. When Web pages are sent out, they are prefixed by MIME headers. Why?

The question is regarding sending e-mails containing web pages.

- Initially email consisted messages containing simple text written in English and expressed in ASCII. It cannot be used for languages other than English (such as French, German, Hebrew, Russian, Chinese, and Japanese). Also, it cannot be used to send binary files or video or audio data.
- The basic idea of MIME (Multipurpose Internet Mail Extensions) is to add structure to the message body and define encoding rule for non- ASCII messages. MIME transforms non-ASCII data to ASCII data and vice-versa.
- MIME defines five headers that can be added to the original e-mail header section to define the transformation parameters:

Header	Meaning
1. MIME-Version	Identifies the MIME version
2. Content-Type	type/subtype
3. Content-Transfer-Encoding	encoding type
4. Content-Id	message id
5. Content-Description	textual explanation of nontextual contents

PART B

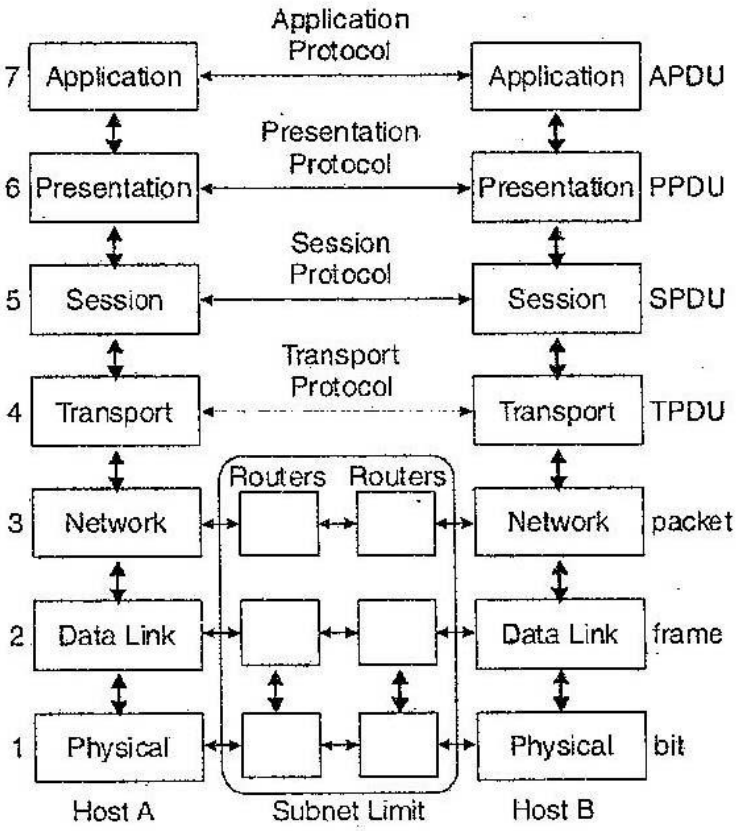
11. A) With a neat diagram, explain Open Systems Interconnection (OSI) Reference Model.

The main functions of each of the layers are as follows −

- **Physical Layer** − Its function is to transmit individual bits from one node to another over a physical medium.
- **Data Link Layer** − It is responsible for the reliable transfer of data frames from one node to another connected by the physical layer.
- **Network Layer** − It manages the delivery of individual data packets from source to destination through appropriate addressing and routing.
- **Transport Layer** −It is responsible for delivery of the entire message from the source host to destination host.

- **Session Layer** − It establishes sessions between users and offers services like dialog control and synchronization.
- **Presentation Layer** − It monitors syntax and semantics of transmitted information through translation, compression, and encryption.
- **Application Layer** − It provides high-level APIs (application program interface) to the users.

<More explanation required for high mark question. Refer text book. One quick ref link which provides explanation is https://www.techtarget.com/searchnetworking/definition/OSI



11. B) Compare Twisted Pair, Coaxial Cable and Optical Fibre guided transmission media.

Twisted pair cable	Co-axial cable	Optical fiber
1. Transmission of signals takes place in the electrical form over the metallic conducting wires.	1. Transmission of signals takes place in the electrical form over the inner conductor of the cable.	1. Signal transmission takes place in an optical forms over a glass fiber.
2. In this medium the noise immunity is low.	2. Coaxial having higher noise immunity than twisted pair cable.	2. Optical fiber has highest noise immunity as the light rays are unaffected by the electrical noise.
3. Twisted pair cable can be affected due to external magnetic field.	3. Coaxial cable is less affected due to external magnetic field.	3. Not affected by the external magnetic field.
4. Cheapest medium.	4. Moderate Expensive.	4. Expensive
5. Low Bandwidth.	5. Moderately high bandwidth.	5. Very high bandwidth
6. Attenuation is very high.	6. Attenuation is low.	6. Attenuation is very low.
7. Installation is easy.	7. Installation is fairly easy.	7. Installation is difficult.

12. A) Consider two networks providing reliable connection-oriented service. One of them offers a reliable byte stream and the other offers a reliable message stream. Are they identical? Justify your answer.

Reliable connection-oriented service has two minor variations: message sequences and byte streams. In the former variant, the message boundaries are preserved. When two 1024-byte messages are sent, they arrive as two distinct 1024- byte messages, never as one 2048-byte message. In the latter, the connection is simply a stream of bytes, with no message boundaries. When 2048 bytes arrive at the receiver, there is no way to tell if they were sent as one 2048-byte message, two 1024-byte messages, or 2048 1-byte messages. If the pages of a book are sent over a network to a phototypesetter as separate messages, it might be important to preserve the message boundaries. On the other hand, to download a DVD movie, a byte stream from the server to the user's computer is all that is needed. Message boundaries within the movie are not relevant.

So the output of given scenario will be:

Message stream – receive 1024 byes only at one time

Byte stream – full 2048 bytes as a whole.

12. B) Sketch the waveform in Manchester and Differential Manchester Encoding for the bitstream 11000110010.

Important points to note: State your initial signal level assumption for differential Manchester

Both are biphase schemes – your waves should cross the horizontal line through '0'.

First write the rules for both and then draw the waveform.

Manchester Encoding

- has transition in middle of each bit period
- low to high (i.e negative to positive voltage) represents one
- high to low (positive to negative) represents zero

Differential Manchester Encoding

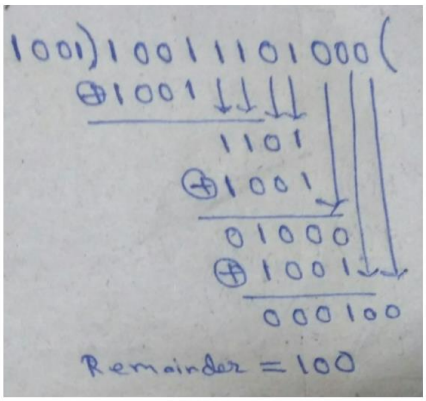
- If bit is 0,there is transition
- If bit is 1,there is no transition

13. A) A bit stream 10011101 is transmitted using the standard CRC method. The generator polynomial is $x^3 + 1$. Show the actual bit string transmitted. Suppose the third bit from the left is inverted during transmission. Show that this error is detected at the receiver's end.

    Start your answer with a short notes on CRC.

Generator polynomial=$x^3 + 1 = 1 * x^3 + 0 * x^2 + 0 * x^1 + 1 * x^0$=1001

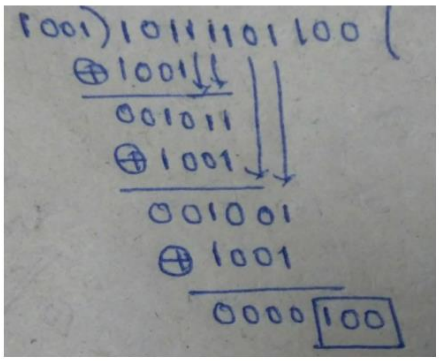
So we've to append three 0s at the end of message



Message transmitted=10011101100

The 3rd bit from left gets inverted. So receiver receives 10111101100

[both sender and receiver agrees on generating polynomial]



non-zero remainder indicates error

13. B) Explain the working of High-Level Data Link Control (HDLC) protocol.

<Refer page numbers 340 -346 of the text – Data communication and networking 4th edition – uploaded to CN drive>

Or

https://www.tutorialspoint.com/high-level-data-link-control-hdlc#:~:text=High%2Dlevel%20Data%20Link%20Control%20(HDLC)%20is%20a%20group,that%20verifies%20its%20successful%20arrival.

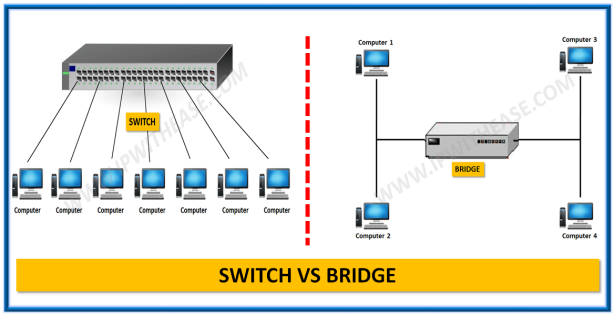
14. A) Explain the working of IEEE 802.11 MAC sublayer.

<Refer page numbers 423 of the text – Data communication and networking 4th edition – uploaded to CN drive>

Or

https://www.tutorialspoint.com/the-802-11-mac-sublayer-protocol#:~:text=The%20802.11%20MAC%20sublayer%20provides,frames%20and%20describing%20frame%20formats.

14. B) Distinguish between Bridges and Switches



BASIS FOR COMPARISON	BRIDGE	SWITCH
Basic	A bridge can connect fewer LAN.	A switch can connect more networks compared to the bridge.
Buffer	Bridges do not have buffers.	Switch has a buffer for each link connected to it.
Types	Simple bridge, multiport bridge and transparent bridge.	Store-and-forward switch and cut-through switch.
Error	Bridges do not perform error checking.	Switches perform error checking.

15. A) Illustrate Distance Vector Routing algorithm with an example.

<Refer slide of Module 3 – uploaded to CN drive>

15. B) Explain the characteristics of Routing Information Protocol (RIP).

<Refer page numbers 384 of the text – Computer Networking: a Top Down Approach – uploaded to CN drive>

16. A) A computer on a 6-Mbps network is regulated by a token bucket. The token bucket is filled at a rate of 1 Mbps. It is initially filled to capacity with 8 megabits. How long can the computer transmit at the full 6 Mbps?

<Write about token bucket algorithm with figure>

New tokens are added at the rate of r bits/sec which is 1Mbps in the given question.

Capacity of the token bucket (b) = 8 Mbits

Maximum possible transmission rate (M) = 6Mbps

So the maximum burst time = b/(M-r) = 8/(6-1) = 1.6 seconds

16. B) Explain how routing is performed for mobile hosts.

<Refer page numbers 410 of the text – Computer Networks by Andrew S Tannenbeum – uploaded to CN drive>

17. A) Explain the address resolution problem using Address Resolution Protocol (ARP) and Reverse Address Resolution Protocol (RARP)with an example network.

PARAMETERS	ARP	RARP
Abbreviation for	Address resolution protocol	Reverse Address Resolution Protocol
Broadcast MAC/IP	Nodes use ARP broadcast in LAN by using broadcast MAC address	RARP uses Broadcast IP address
Mapping	Maps IP address of node to its MAC Address	Maps 48 bit MAC address to IP address
Usage	Used by host or Router to find physical address of another host/Router in LAN.	Used by thin clients with limited facilities
Table maintained by	Local Host maintains ARP table	RARP Server maintains RARP table
Reply information	ARP reply is used to update ARP table	RARP reply is used to configure IP address in local host

ARP – Page 612, Data communication and networking 4th edition

RARP – Page 618, Data communication and networking 4th edition

17. B) A network on the Internet has a subnet mask of 255.255.240.0. What is the maximum number of hosts it can handle?

An IP address has 2 parts – Network Id and Host Id

Number hosts in a network = 2^no.of bits used for host id part – 2(reserved)

Here First 20 bits are network id and remaining (32-20=12bits) are host id.

Total hosts = 2^{12} - 2 = 4096 - 2 = 4094

18. A) How do you subnet the Class C IP address 195.1.1.0 so as to have 10 subnets with a maximum of 12 hosts in each subnet.

<For studying Subnetting, I have uploaded one more pdf in the drive titled “IP Addressing Detailed” >

Current mask= 255.255.255.0

Bits needs for 10 subnets =4 =2^4 =16 possible subnets

Bits needs for 12 hosts = 4 = 2^4 = 16-2=14 possible hosts.

So our mask in binary =**11110000**= **240** decimal

Final Mask =**255.255.255.240**

Hosts on Subnets 0,1,2,3,10

- Subnet 0 host 1 IP address = 195.1.1.1 **0000 0001**
- Subnet 1 host 1 IP address = 195.1.1.17 **0001 0001**
- Subnet 2 host 1 IP address = 195.1.1.33 **0010 0001**
- Subnet 3 host 1 IP address = 195.1.1.49 **0011 0001**
- Subnet 10 host 1 IP address = 195.1.1.161 **1010 0001**

18. B) Draw IPv6 Datagram format and explain its features.

IPv6 Packet Format

IPv6 datagram is a packet composed of the **base header**(**40** bytes) and **payload**(up to **65,536** bytes) Payload has **extension header** (optional) and **data packet**.

Base Header(40 bytes)	Payload (upto 65,535 bytes)

The **base header** consists of the following fields:

- **Version:** It defines the version number of IP which is 6 here. Its length is 4 bits.
- **Priority:** It defines the priority of the packet. Its length is 4 bits.
- **Flow label:** It helps in controlling the flow of data. The source device labels to the data packets so that the router route the packet in sequence efficiently. Its length is 24 bits.
- **Payload length:** It tells the entire length of the IP datagram except for the base header. Its length is 16 bits.
- **Next header:** It denotes the presence of any extension headers or if is not present then it denotes the protocol such as TCP or UDP.
- **Hop limit:** This works similarly as TTL as in IPv4. This is used to prohibit the data to go in an infinite loop in the system. At each hop, the value of TTL is decreased by 1 and when it reaches 0, the packet is abandoned. Its length is 8 bits.
- **Source address:** It has the IP address of the source. The length is 128 bits.
- **Destination address:** It has the IP address of the destination. The length is 128 bits.

Version	Priority	Flow Label		
Payload Length			Next Header	Hop Limit
Source IP Address				
Destination IP Address				

19. A) Distinguish the header formats of Transmission Control protocol (TCP) and User Datagram Protocol (UDP).

TCP Segment Header Format

Bit #	0 – 7	8 – 15	16 – 23	24 – 31
0	Source Port		Destination Port	
32	Sequence Number			
64	Acknowledgment Number			
96	Data Offset	Res	Flags	Window Size
128	Header and Data Checksum		Urgent Pointer	
160...	Options			

UDP Datagram Header Format

Bit #	0 – 7	8 – 15	16 – 23	24 – 31
0	Source Port		Destination Port	
32	Length		Header and Data Checksum	

<Explain the fields also.>

19. B) Explain the principal Domain Name System (DNS) resource record types for IPv4

Resource Records

Type	Meaning	Value
SOA	Start of Authority	Parameters for this zone
A	IP address of a host	32-Bit integer
MX	Mail exchange	Priority, domain willing to accept e-mail
NS	Name Server	Name of a server for this domain
CNAME	Canonical name	Domain name
PTR	Pointer	Alias for an IP address
HINFO	Host description	CPU and OS in ASCII
TXT	Text	Uninterpreted ASCII text

The principal DNS resource records types.

https://www.cloudflare.com/en-in/learning/dns/dns-records/#:~:text=DNS%20records%20(aka%20zone%20files,handle%20requests%20for%20that%20domain.

20. A) What is the role of Simple Mail Transfer Protocol (SMTP) in E- mail?

<Refer page numbers 623 of the text – Computer Networks by Andrew S Tannenbeum – uploaded to CN drive>

20. B) With the help of a basic model, explain the working of World Wide Web (WWW).

<Refer page numbers 646 of the text – Computer Networks by Andrew S Tannenbeum – uploaded to CN drive>