USN | | | | | | | | | |

Internal Assessment Test 2
Dec 2024

Sub:	Computer Networks	Sub Code:	BCS502	Branch:	AINDS / CS (DS)

Date:		Duration:	90 minutes	Max Marks:	50	Sem	V	OBE

		Answer any FIVE Questions	MARKS	CO	RBT
1	a	i) A packet has arrived with an *M* bit value of 0. Is this the first fragment, the last fragment, or a middle fragment? Do we know if the packet was fragmented?	5	CO3	L3

he **M bit (More Fragments bit)** is part of the IPv4 header and is used to indicate whether more fragments of the same packet are expected to follow:

- **M = 1**: Indicates that more fragments are coming.
- **M = 0**: Indicates this is the last fragment or the packet was not fragmented at all.

Interpretation of M = 0:

1. **If the Fragment Offset is 0**:
   - This is the **only fragment**, meaning the packet was not fragmented. It is the original, unfragmented packet.
2. **If the Fragment Offset is greater than 0**:
   - This is the **last fragment** of a fragmented packet. The presence of a non-zero fragment offset indicates that the packet has been fragmented, and this fragment concludes the reassembly.

Summary:

- **M = 0** alone does not tell us if the packet was fragmented.
- You need to also check the **Fragment Offset**:
  - If **Fragment Offset = 0**, it is the only fragment (not fragmented).
  - If **Fragment Offset > 0**, it is the last fragment of a fragmented packet.

ii) A packet has arrived in which the offset value is 100, the value of HLEN is 5, and the value of the tota1length field is 100. What are the numbers of the first byte and the last byte?

Key Data:

1. **Offset Value**: 100 (measured in 8-byte units).

2. **HLEN**: 5 (represents the header length, measured in 32-bit words, meaning $5\times4=20$ bytes).
3. **Total Length**: 100 bytes (includes the header and the payload).

Step-by-Step Calculation:

1. **Payload Length**: The total length includes the header, so the payload size is:

   Payload Length=Total Length−Header Length=100−20=80 bytes

   First Byte Number: The fragment offset value indicates the starting position of the payload in the original unfragmented packet. Since the offset is measured in 8-byte units:

   First Byte Number=Offset×8=100×8=800

2. **Last Byte Number**: The last byte is calculated by adding the payload length to the first byte number (but subtracting 1 since the numbering starts from 0):

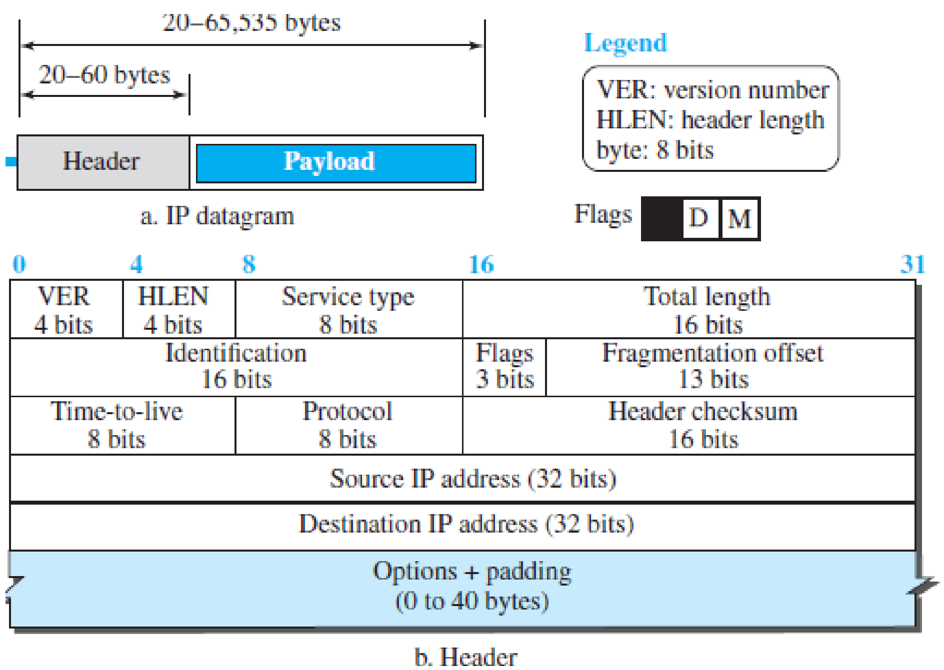
   Last Byte Number=First Byte Number+ Payload Length−1

   =800+80−1=879

Final Answer:

- **First Byte Number**: 800
- **Last Byte Number**: 879

b	Draw and explain IPV4 Packet format	5	CO3	L2



2		An organization is granted the block 130.56.0.0/16. The administrator wants to create 1024 subnets. a. Find the subnet mask. 1. **Calculate the number of bits needed for subnetting:** Calculate the number of bits needed for subnetting: • To create 1024 subnets, $2^n \geq 1024$, where n is the number of additiona • $n = 10$ (since $2^{10} = 1024$). 2. **Update the prefix length:** ○ Original prefix length: **16 bits**. ○ Adding 10 bits for subnetting: **16 + 10 = 26 bits**. 3. **Subnet mask:** ○ The subnet mask is /26 which corresponds to: ▪ **Binary:** 11111111.11111111.11111111.11000000 ▪ **Decimal:** 255.255.255.192 b. Find the number of addresses in each subnet. 1. The total number of bits in an IPv4 address is 32. 2. The host portion of each subnet is 32−26=6 bits. 3. The number of addresses per subnet 2^6 = 64. c. Find the first and last addresses in subnet 1. Subnet 1 is the first subnet, starting right after the network address. Range of subnet 1: Subnet 1 starts at 130.56.0.0. The block size is 64 64 addresses, so the last address is 130.56.0.63 130.56.0.63. First and last addresses: First address: 130.56.0.0 Last address: 130.56.0.63	10	CO3	L3

d. Find the first and last addresses in subnet 1024.

1. Subnet 1024 is the **last subnet**.
2. **Range of subnet 1024:**
   - Subnet 1024 starts at:

$$130.56.0.0 + (1024 - 1) \times 64 = 130.56.255.192$$

   - The block size is 64 addresses, so the last address is:

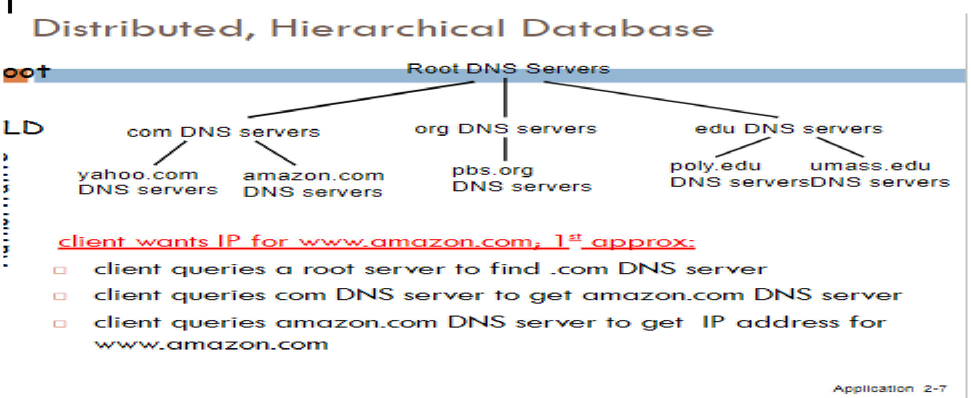
$$130.56.255.192 + 63 = 130.56.255.255$$

3. **First and last addresses:**
   - **First address:** 130.56.255.192
   - **Last address:** 130.56.255.255

3 a Difference between TCP and UDP | 4 | CO4 | L2

Feature	TCP	UDP
Connection Type	Connection-oriented	Connectionless
Reliability	Reliable	Unreliable
Speed	Slower due to overhead	Faster due to simplicity
Data Ordering	Guaranteed	Not guaranteed
Use Cases	Web, email, file transfers	Streaming, gaming, VoIP
Header Size	Larger (20-60 bytes)	Smaller (8 bytes)

b What are the three domains of the domain name space? | 6 | CO5 | L1



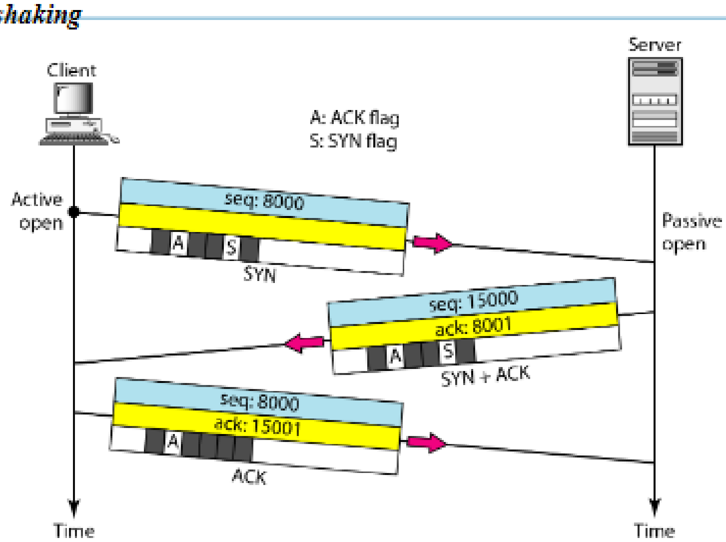
4 a What is the difference between local and remote log-in in TELNET? | 5 | CO5 | L1

Login: Authorization with user identification & password 1. Local login 2. Remote login

1. Local login: When user types at a terminal, keystrokes are accepted by terminal driver & passed to OS. OS in turn, interprets it to run desired utility or application program

2. Remote login:

User sends keystroke to terminal driver & then OS. But local OS does not understands it.

		The characters are sent to TELNET client, which transfers it to TCP/IP stack. TCP/IP converts it to NVT characters & sends to remote machine. OS at remote machine sends that to TELNET server, which changes NVT character to understandable format to OS. Pseudo terminal driver interprets & sends to application program			
	b	In electronic mail, what are the tasks of a user agent? The first component of an electronic mail system is the user agent (UA). It provides service to the user to make the process of sending and receiving a message easier. A user agent is a software package (program) that composes, reads, replies to, and forwards messages. It also handles local mailboxes on the user computers.	5	CO5	L1
5		Explain in detail with diagram connection establishment using 3way handshaking in TCP **Figure 23.18** ***Connection establishment using three-way handshaking*** 	10	CO4	L2

<table>
<tr>
<td></td>
<td></td>
<td>

Figure 23.20 *Connection termination using three-way handshaking*

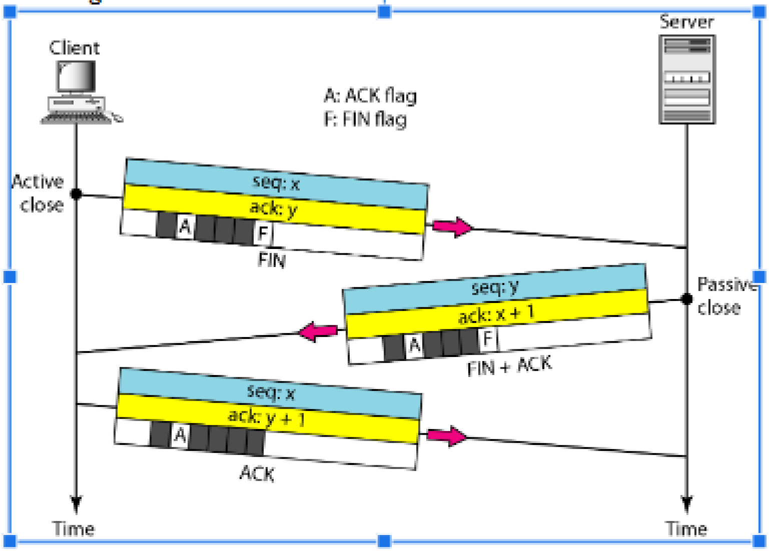
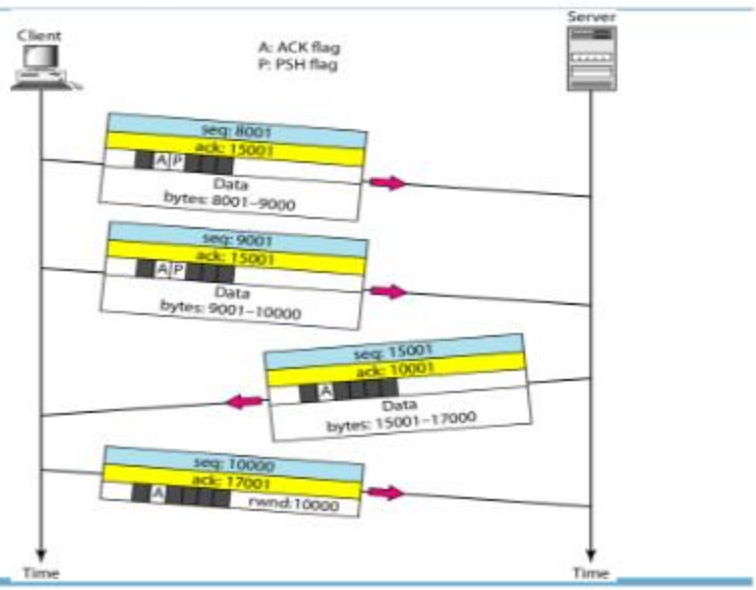


Figure 23.19 *Data transfer*



</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td></td>
<td>

Explain following:

i) FTP

Establishes two connections between the hosts. One connection is used for data transfer, the other for control information (commands and responses).

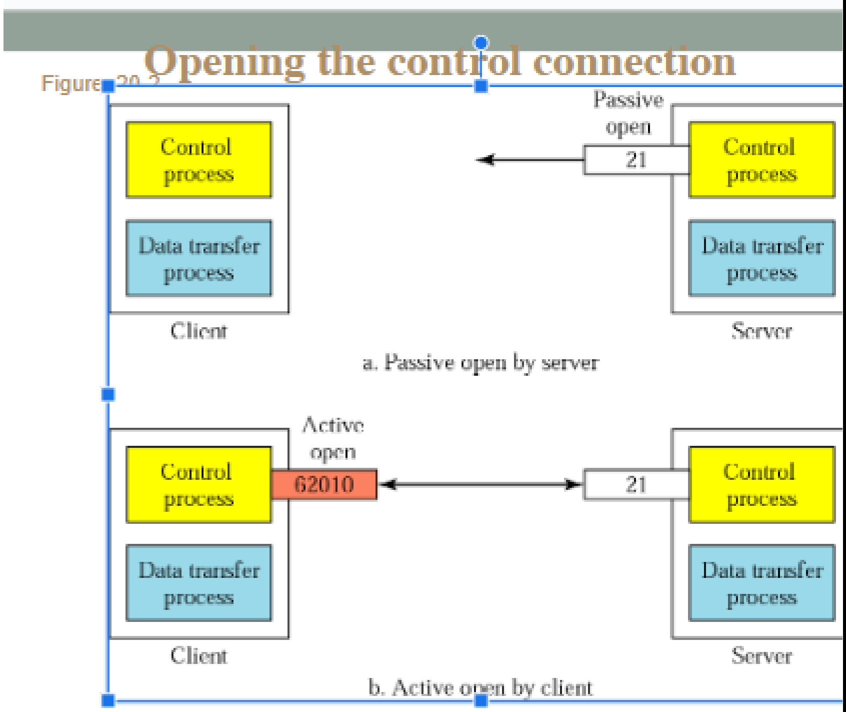
The control connection uses very simple rules of communication.

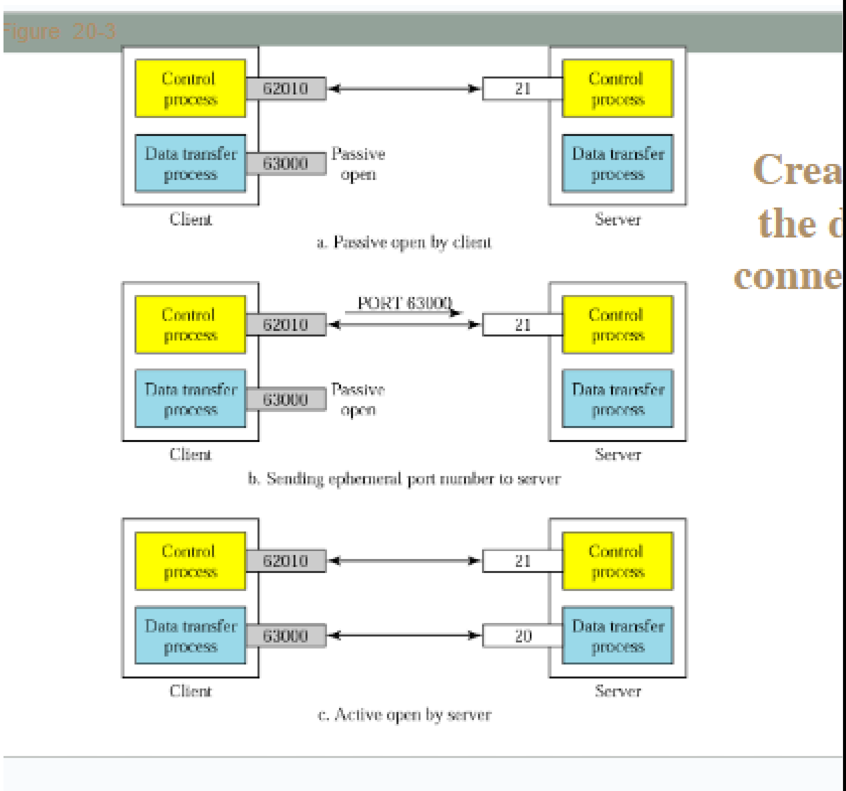
We need to transfer only a line of command or a line of response

</td>
<td>10</td>
<td>CO5</td>
<td>L1</td>
</tr>
</table>

at The data connection, needs more complex rules due to the variety of data types transferred.

FTP uses two well-known TCP ports:
Port 21 is used for the control connection, and
Port 20 is used for the data connection time.





ii) Persistent Versus Nonpersistent Connection wrt HTTP
In a non-persistent connection, one TCP connection is made for each request/response.
The following lists the steps in this strategy:

		1. The client opens a TCP connection and sends a request. 2. The server sends the response and closes the connection. 3. The client reads the data until it encounters an end-of-file marker; it then closes the connection. HTTP version 1.1 specifies a persistent connection by default. In a persistent connection, the server leaves the connection open for more requests after sending a response. The server can close the connection at the request of a client or if a time-out has been reached. The sender usually sends the length of the data with each response.			

CI CCI HOD