

# **Computer Communication and Networks**

**BCA III SEMESTER – NEP (2022-23)**

**UNIT-WISE**

**Comprehensive Question Bank**

**with Answers**

**UNIT-V**

## **2 Marks Questions**

### **1. Define transport layer.**

- The transport layer is a layer in the OSI (Open Systems Interconnection) and TCP/IP network models that provides end-to-end communication services for applications. Its main function is to ensure that data is reliably transferred between network devices by breaking it down into smaller packets and managing the delivery of those packets.

### **2. What are the elements of transport layer?**

- Port numbers
- Addressing
- Segmentation and reassembly
- Connection control
- Multiplexing and demultiplexing
- Quality of Service (QoS) control

### **3. List primitives for a transport service.**

*Table:4.1 - The primitives for a simple transport service.*

Primitive	Packet sent	Meaning
LISTEN	(none)	Block until some process tries to connect
CONNECT	CONNECTION REQ.	Actively attempt to establish a connection
SEND	DATA	Send information
RECEIVE	(none)	Block until a DATA packet arrives
DISCONNECT	DISCONNECTION REQ.	This side wants to release the connection

### **4. Define internet.**

- The Internet refers to the global network of interconnected computer networks that use standard protocols to communicate with each other. It is a vast network of networks that connects millions of computers, servers, and other devices around the world.
- The Internet allows users to access a wide range of information and services, such as email, social media, online shopping, streaming video, and more.

### **5. What is TCP.**

- TCP (Transmission Control Protocol) is a communication protocol used in computer networks. It is one of the main protocols in the Internet

Protocol (IP) suite and operates at the transport layer, providing reliable, ordered, and error-checked delivery of data between applications running on hosts communicating over an IP network.

**6. Define UDP.**

- UDP (User Datagram Protocol) is a communication protocol used in computer networks. It is one of the main protocols in the Internet Protocol (IP) suite and operates at the transport layer, providing a connectionless communication service.

**7. What is electronic mailing?**

- Electronic mailing, also known as email, is a method of exchanging digital messages between two or more people using electronic devices such as computers, smartphones, or tablets connected to the internet.

**8. What is World Wide Web?**

- The World Wide Web (WWW or the Web) is a global network of interconnected documents and resources, which are accessed via the internet.

**9. What is DNS.**

- DNS stands for Domain Name System. It is a system used on the internet to translate domain names, into IP addresses.

**10. What is TCP/IP protocol.**

- TCP/IP (Transmission Control Protocol/Internet Protocol) is a set of networking protocols that are used to establish and maintain communication between devices on the internet.
- TCP is responsible for establishing reliable connections between devices by dividing data into smaller packets and ensuring that they are transmitted and received correctly
- IP is responsible for routing data packets between devices on the internet.

**11. Define Web ?**

- The Web, short for World Wide Web, is a system of interconnected documents and resources, which are accessed via the internet using web browsers.

**12. Define mailing.**



- Mailing refers to the act of sending or receiving mail, which can be physical or digital.

## **5 Marks Questions**

### **1. Explain Elements of Transport Service.**

- Transport service is a service provided by the Transport Layer of the TCP/IP protocol suite to enable reliable and efficient data communication between networked devices.
- **Connection-Oriented and Connectionless Services:** The Transport Layer provides both connection-oriented and connectionless services.

In a **connection-oriented service**, a virtual circuit is established between the sender and the receiver before data transmission begins, and data is transmitted reliably over this circuit.

In a **connectionless service**, data is transmitted without establishing a virtual circuit, and the Transport Layer does not guarantee delivery or reliability.

- **Reliable Data Delivery:** The Transport Layer provides mechanisms to ensure reliable data delivery, even in the presence of errors or network congestion. This is achieved through error detection, retransmission of lost packets, and flow control mechanisms that prevent the receiver from being overwhelmed with too much data.
- **Segmentation and Reassembly:** The Transport Layer divides large data packets into smaller segments, which are easier to transmit over the network. The receiver then reassembles the segments back into the original packet.
- **Multiplexing and Demultiplexing:** The Transport Layer provides the ability to multiplex and demultiplex data from multiple applications running on a device. This allows multiple applications to use the network simultaneously, without interfering with each other.
- **Port Numbers:** The Transport Layer uses port numbers to identify different applications running on a device. Each application is assigned a

unique port number, which is used to route data to the correct application.

## 2. Explain UDP Header Format.

- **UDP (User Datagram Protocol)** is a simple transport protocol that is used for fast and efficient transmission of data over IP networks. The UDP header contains information that is used by the Transport Layer to ensure reliable and efficient data transmission. The format of the UDP header is as follows:

Source Port	Destination Port	Length	Checksum
2 bytes	2 bytes	2 bytes	2 bytes

**Source Port:** This field is 16 bits in length and contains the port number of the sender.

**Destination Port:** This field is 16 bits in length and contains the port number of the intended receiver.

**Length:** This field is 16 bits in length and specifies the length of the UDP datagram, including the header and data. The minimum value for this field is 8 bytes (the size of the UDP header), and the maximum value is 65,535 bytes.

**Checksum:** This field is 16 bits in length and is used to ensure the integrity of the UDP datagram. The checksum is calculated using a mathematical algorithm that takes into account the data in the UDP datagram.

## 3. Explain TCP Sockets.

- A **TCP (Transmission Control Protocol) socket** is a software endpoint that enables two-way communication between applications running on different devices over a network. The socket provides a reliable, stream-oriented, and connection-oriented interface between applications that allows for the transfer of data over a network.
- **TCP sockets are identified by a combination of an IP address and a port number.** The IP address identifies the device on the network, and the port number identifies the specific application running on that device.



- The TCP protocol provides a number of features to ensure reliable data transmission over the network, including:
- **Connection-oriented communication:** Before data can be exchanged between two applications using TCP sockets, a connection must be established between them.
- **Stream-oriented data transfer: TCP** provides a stream-oriented data transfer service, which means that data is sent and received as a continuous stream of bytes, rather than as individual packets.
- **Reliable data delivery:** TCP provides reliable data delivery by using mechanisms such as sequence numbers, acknowledgments, and retransmission of lost packets.
- **Flow control:** TCP provides flow control mechanisms to prevent the receiver from being overwhelmed with too much data. This is achieved through the use of sliding windows, where the receiver tells the sender how much data it can receive at any given time.

#### 4. Explain TCP timer management.

- TCP (Transmission Control Protocol) uses timers to manage various aspects of its operation. There are several different timers used by TCP, and each has its own purpose.

##### **Retransmission Timer:**

- When a TCP segment is sent, the sender starts a timer to track the amount of time that elapses before an acknowledgement is received. If no acknowledgement is received within this time, the segment is assumed to be lost, and the sender retransmits the segment. The retransmission timer is adjusted dynamically based on network conditions and the behavior of the receiver.

##### **Persist Timer:**

- This timer is used to ensure that a connection stays open when there is no data to be sent. If the sender has sent all of its data and has not received any acknowledgement, it will send a small message called a "window probe" to the receiver. The persist timer is started when the

window probe is sent, and if no acknowledgement is received within the time, the sender sends another window probe.

- **Keepalive Timer:**

This timer is used to detect when a connection has become idle. If no data is transmitted over the connection for a certain amount of time, the keepalive timer is started. If no response is received within a certain amount of time, the connection is assumed to be lost and closed.

- **Time-Wait Timer:**

When a TCP connection is closed, the endpoint that initiates the closure enters a state called TIME\_WAIT. During this time, the endpoint waits for any stray packets to arrive from the remote endpoint. The TIME\_WAIT timer determines the amount of time that the endpoint stays in this state before closing the connection completely.

## 5. Explain Addressing in TCP.

- TCP (Transmission Control Protocol) addressing is a way to identify the source and destination endpoints of a TCP connection. TCP uses IP (Internet Protocol) for addressing, which means that each endpoint has a unique IP address that is used to route data between them.
- When a TCP connection is established, each endpoint is assigned a port number that is used to distinguish between different applications running on the same IP address. The combination of the IP address and port number uniquely identifies the endpoint in the network.
- TCP addressing is important because it allows data to be sent between endpoints across the network. When data is sent from a source endpoint, the TCP protocol encapsulates the data in a segment that includes the IP address and port number of the destination endpoint. This segment is then sent over the network to the destination endpoint, which receives the segment and extracts the data.
- TCP addressing also allows for the establishment of multiple connections between two endpoints. Each connection is assigned a different port



number, allowing for multiple applications to communicate with each other simultaneously over the same IP address.

#### 6. Write a short note on DNS.

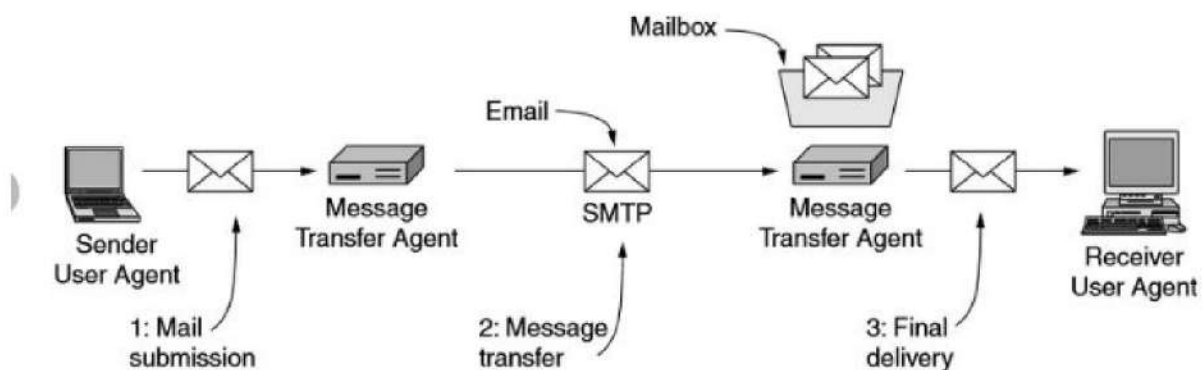
- DNS stands for Domain Name System. It is a hierarchical naming system that translates domain names, such as `www.example.com`, into IP addresses, which are used by computers to communicate with each other over the internet. DNS acts as a phonebook for the internet, allowing users to access websites by typing in easy-to-remember domain names, rather than having to remember long, complex IP addresses.
- DNS works by maintaining a distributed database of domain names and IP addresses. When a user enters a domain name into their web browser, the browser sends a request to a DNS resolver, which looks up the domain name in its database and returns the corresponding IP address. The browser can then use this IP address to connect to the web server that hosts the website.
- DNS plays a crucial role in the functioning of the internet, and its reliability and security are essential for ensuring that users can access websites and services without interruption. DNS also supports other important functions, such as email delivery and online security protocols like SSL/TLS.

#### 7. Explain Email Architecture.

- Email architecture is the framework of technologies and protocols used to send, receive, and manage email messages. The architecture consists of three main components: user agents, mail servers, and message transfer agents.
- **User Agents:**
- User agents, also known as email clients, are the software applications used by individuals to access and manage their email accounts. Examples of user agents include Gmail, Outlook, and Apple Mail. User agents provide a graphical user interface (GUI) for users to compose, read, and organize their emails.
-



- **Mail Servers:**
- Mail servers are responsible for storing and managing email messages. There are two types of mail servers: inbound mail servers and outbound mail servers. Inbound mail servers receive incoming emails and store them in the recipient's mailbox. Outbound mail servers send outgoing emails to the recipient's mail server. Examples of mail servers include Postfix, Exim, and Microsoft Exchange.
- **Message Transfer Agents:**
- Message Transfer Agents (MTAs) are responsible for transferring email messages between mail servers. MTAs use various protocols such as Simple Mail Transfer Protocol (SMTP), Post Office Protocol (POP), and Internet Message Access Protocol (IMAP) to move messages between mail servers. MTAs perform a series of checks on incoming emails to ensure they are legitimate and not spam or malicious.



#### 8. Explain SMTP Protocol.

- **SMTP stands for Simple Mail Transfer Protocol, which is a protocol used for sending and receiving email messages between mail servers. SMTP is responsible for the transmission of email messages from the sender's mail server to the recipient's mail server over the internet.**
- 
- **SMTP operates on the client-server model, where the sender's mail server is the client and the recipient's mail server is the server. When a user sends an email, their email client communicates with the sender's**

mail server, which then initiates the SMTP connection to the recipient's mail server. The SMTP protocol consists of a series of commands and responses exchanged between the two mail servers, which allows them to transfer email messages.

- 
- Here are the basic steps involved in an SMTP transaction
- **Connection Establishment:**
- The sender's mail server initiates a TCP connection with the recipient's mail server on port 25, which is the default port for SMTP.
- **Handshake:**  
The two mail servers identify themselves to each other and agree on the version of the SMTP protocol to use.
- **Message Transfer:**  
The sender's mail server sends the email message to the recipient's mail server using the SMTP "MAIL FROM", "RCPT TO", and "DATA" commands. These commands specify the sender's email address, the recipient's email address, and the actual email message, respectively.
- **Message Acceptance:**  
The recipient's mail server receives the email message and sends an SMTP "250 OK" response if the message was accepted. If there was an error, the recipient's mail server sends an appropriate error message.
- **Connection Termination:**  
The SMTP session ends with the sender's mail server sending a "QUIT" command, and the recipient's mail server responding with a "221" code to indicate that the session has been terminated.

#### 9. Write a Short Note on WWW.

- WWW stands for World Wide Web, which is a global system of interconnected hypertext documents accessed through the internet. It is a network of information resources and services that can be accessed using web browsers.
- The web is based on the principles of hypertext, which is a way of linking text together to create a non-linear navigation structure. Hypertext links

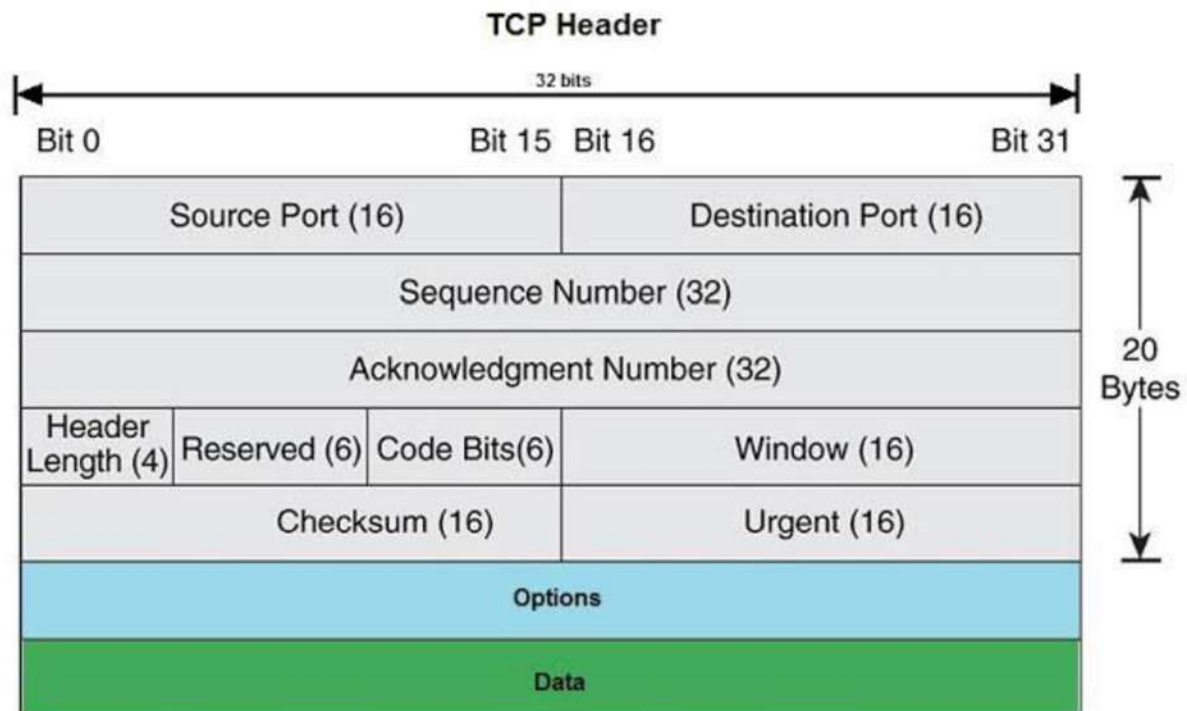
allow users to navigate between different web pages, which are connected through the use of URLs (Uniform Resource Locators).

- The web consists of millions of web pages that are hosted on web servers located around the world. Web pages are written using HTML (Hypertext Markup Language), which is a markup language used to structure content on the web. Web pages can contain various types of content, such as text, images, videos, and interactive elements such as forms and animations.
- Web browsers such as Google Chrome, Firefox, and Safari allow users to access web pages and interact with web-based services. Web browsers translate HTML code into visual representations of web pages and enable users to navigate between different pages using hyperlinks.
- The web has had a profound impact on society, revolutionizing the way we access and share information, communicate with each other, and conduct business. It has enabled the development of numerous web-based applications and services, such as social media, e-commerce, and online banking.

## **10 Marks Questions**

### **1. Explain TCP header Format.**





The TCP header consists of several fields, each of which contains important information about the TCP packet. Here is a breakdown of the TCP header format:

**Source Port (16 bits):**

This field specifies the source port number of the TCP packet. It is a 16-bit value that identifies the application that generated the packet on the sender's side.

**Destination Port (16 bits):**

This field specifies the destination port number of the TCP packet. It is also a 16-bit value that identifies the application that is supposed to receive the packet on the receiver's side.

**Sequence Number (32 bits):**

This field contains a 32-bit number that represents the sequence number of the first byte of data in the TCP packet. This number is used for reassembling the packet at the receiver's end.

**Acknowledgment Number (32 bits):**

This field contains a 32-bit number that represents the sequence number of the next expected byte of data. It is used to acknowledge the receipt of data from the sender and to request the retransmission of missing packets.

**Data Offset (4 bits):**

This field specifies the length of the TCP header in 32-bit words. It is used to indicate the start of the data section in the TCP packet.

**Reserved (6 bits):**

This field is reserved for future use.

**Flags (6 bits):**

This field contains various control flags that are used to manage the TCP connection, including URG, ACK, PSH, RST, SYN, and FIN.

**Window Size (16 bits):**

This field specifies the size of the receiver's buffer in bytes. It indicates the amount of data that the sender can transmit before receiving an acknowledgment from the receiver.

**Checksum (16 bits):**

This field contains a checksum that is used to verify the integrity of the TCP packet.

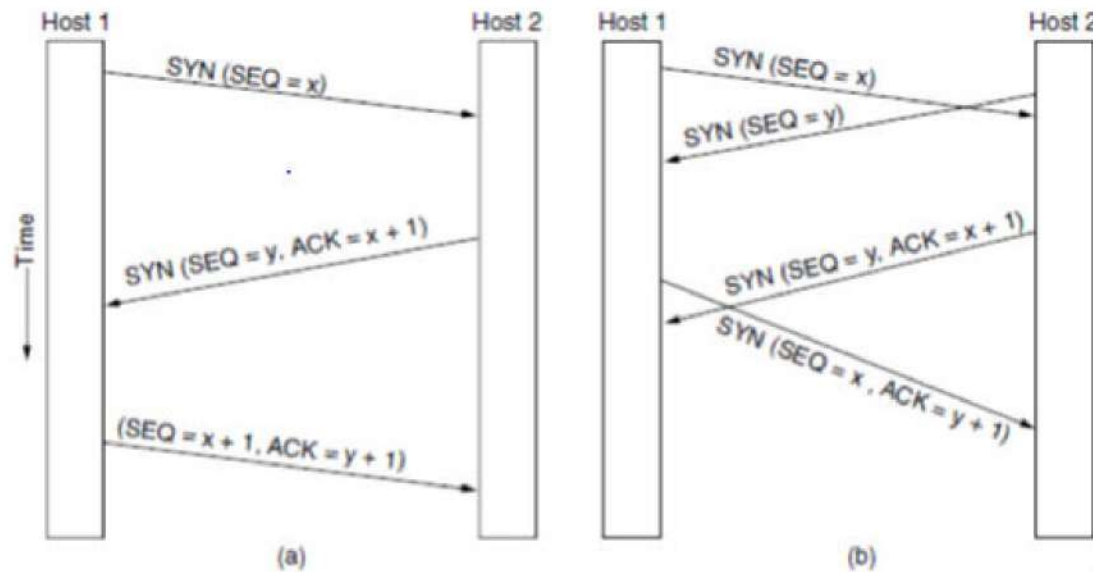
**Urgent Pointer (16 bits):**

This field is used to indicate the position of urgent data within the TCP packet. It is only used when the URG flag is set.

**Options (variable):**

This field is used to carry additional information that is necessary for the TCP connection, such as maximum segment size, selective acknowledgments, and timestamps.

**2. Explain TCP Connection Establishment and Connection release.**



a) TCP connection establishment in the normal case. (b) Simultaneous connection establishment on both sides.

### TCP Connection Establishment:

The client initiates the connection by sending a SYN (synchronize) packet to the server. The SYN packet contains a random sequence number and an initial window size value.

The server responds with a SYN-ACK (synchronize-acknowledge) packet. The SYN-ACK packet contains an acknowledgement number that is set to the client's sequence number + 1, and a server-generated sequence number.

The client sends an ACK (acknowledge) packet to the server, acknowledging the receipt of the SYN-ACK packet. The ACK packet contains an acknowledgement number that is set to the server's sequence number + 1.

At this point, the TCP connection is established, and data can be transmitted between the client and server.

### TCP Connection Release:

The client initiates the connection release by sending a FIN (finish) packet to the server. The FIN packet contains a sequence number.

The server responds with an ACK packet, acknowledging the receipt of the FIN packet.



The server sends a FIN packet to the client, containing a sequence number.

The client responds with an ACK packet, acknowledging the receipt of the FIN packet.

### 3. Explain Elements Transport Protocol.

Transport protocol is a protocol that is responsible for the end-to-end delivery of data between applications running on different hosts. The transport protocol provides several elements to ensure reliable and efficient data transmission. Here are the key elements of the transport protocol:

#### **Multiplexing and Demultiplexing:**

Multiplexing is the process of combining multiple data streams into a single communication channel, while demultiplexing is the reverse process of separating multiple data streams from a single communication channel. The transport protocol multiplexes and demultiplexes data streams using unique identifiers, called port numbers, which are used to identify the application that generated the data.

#### **Segmentation and Reassembly:**

The transport protocol segments data into smaller chunks to be transmitted over the network. This process is necessary because data generated by an application may be too large to be transmitted over the network in a single packet. At the receiving end, the transport protocol reassembles the data into its original form before delivering it to the application.

#### **Flow Control:**

Flow control is a mechanism used to regulate the rate of data transmission between two hosts. The transport protocol uses flow control to prevent the sender from overwhelming the receiver with data. The receiver can signal the sender to slow down the rate of transmission by adjusting the window size value in the TCP header.

#### **Error Control:**

The transport protocol ensures reliable data transmission by detecting and recovering from errors that may occur during data transmission. The transport protocol uses error detection codes, such as checksums, to verify

the integrity of data packets. If an error is detected, the transport protocol uses retransmission to recover the lost or corrupted data.

**Congestion Control:**

Congestion control is a mechanism used to regulate the rate of data transmission to prevent network congestion. The transport protocol uses congestion control to prevent the sender from overwhelming the network with data. The sender can adjust the rate of transmission by adjusting the congestion window value in the TCP header.

**Note:**

1. Refer Textbooks and Internet sources for depth and more.

**CCN Previous Year Question Papers: (Syllabus has been changed, extract questions based on syllabus).**

**ALL BCA Question Papers:**

<https://drive.google.com/drive/folders/1F0CEAtoFmji9Gx9snSGZYqEksw4VkjSW>