

## Scheme of Evaluation for BCS502- Prepared by TIE TEAM

### MODULE 1

#### 1. Differentiate between data communications and networking. What are the key components required for effective data communication?

- **Data Communications:** Refers to the exchange of data between two devices via some form of transmission medium (e.g., wire, fiber optic cable, radio waves).<sup>1</sup> It focuses on the point-to-point transfer of information.
- **Networking:** Involves connecting multiple devices (computers, servers, etc.) together to share resources (files, printers, internet access) and communicate with each other.<sup>2</sup> It focuses on establishing a communication infrastructure.

#### Key components for effective data communication:

- **Sender:** The device that transmits the data.
- **Receiver:** The device that receives the data.
- **Transmission Medium:** The physical path through which data is transmitted (e.g., cable, wireless signal).
- **Message:** The information being transmitted (data).
- **Protocol:** A set of rules that govern data communication, ensuring proper transmission and reception.<sup>3</sup>

#### 2. Compare and contrast various network types (e.g., LAN, MAN, WAN, PAN) with real-world examples.

Feature	LAN (Local Area Network)	MAN (Metropolitan Area Network)	WAN (Wide Area Network)	PAN (Personal Area Network)
Scope	Limited geographical area (e.g., home, office, building)	Larger geographical area (e.g., city, metropolitan region)	Spans a large geographical area (e.g., country, continent, globe)	Very small area, typically within a person's immediate vicinity
Ownership	Usually	Often owned	Typically	Owned by an

Feature	LAN (Local Area Network)	MAN (Metropolitan Area Network)	WAN (Wide Area Network)	PAN (Personal Area Network)
	owned by a single organization	by a consortium or a single large organization	owned by multiple service providers	individual
<b>Technology</b>	Ethernet, Wi-Fi	High-speed connections like fiber optics, microwave links	Internet, leased lines, satellite links	Bluetooth, Infrared, NFC
<b>Speed</b>	High (e.g., 100 Mbps to 10 Gbps)	Moderate to high (e.g., 10 Mbps to 1 Gbps)	Lower than LAN/MAN (e.g., few Mbps to Gbps)	Relatively low (e.g., few Mbps)
<b>Examples</b>	Home network, office network, school network	City-wide Wi-Fi, cable TV networks, metropolitan Ethernet	Internet, corporate networks connecting offices in different cities	Bluetooth connection between phone and headphones, wireless keyboard and mouse

### 3. Explain the concept of protocol layering and discuss the advantages of using a layered approach in network models.

- **Protocol Layering:** Organizing network communication functions into distinct layers, where each layer performs a specific set of tasks. Data passes through these layers in a defined order, both on the sending and receiving ends.

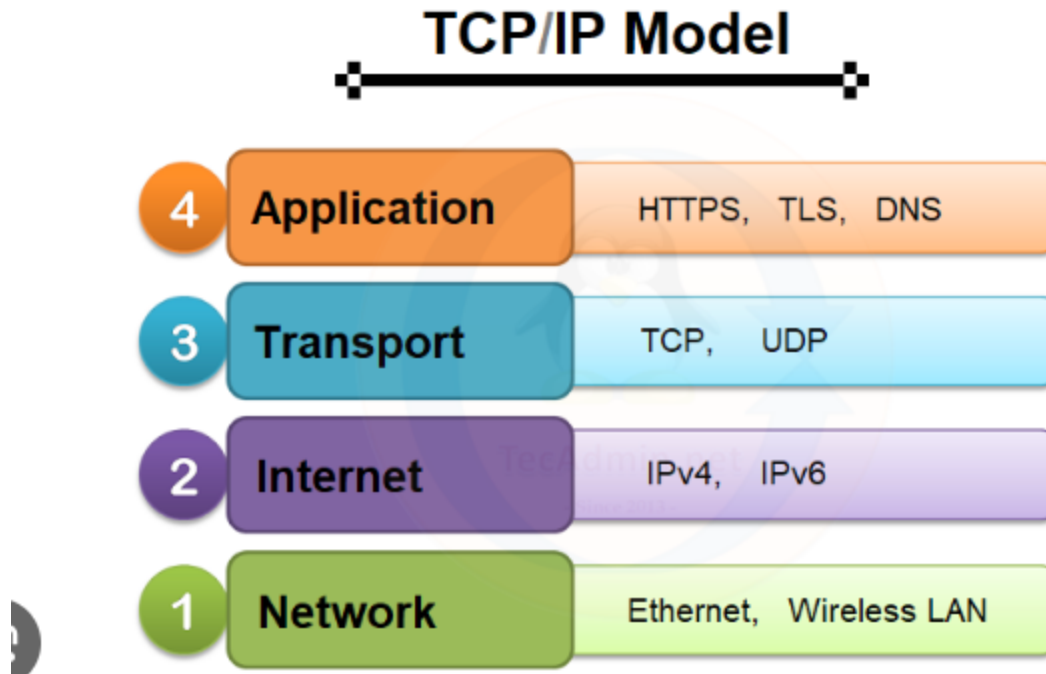
#### Advantages:

- **Modularity:** Easier to design, implement, and maintain network protocols as each layer has a specific function.
- **Flexibility:** Changes in one layer do not affect other layers, as long as the interfaces between

layers remain the same.<sup>4</sup>

- **Interoperability:** Allows different hardware and software from different vendors to communicate with each other, as long as they adhere to the same layered model.
- **Troubleshooting:** Simplifies troubleshooting by isolating problems to specific layers.

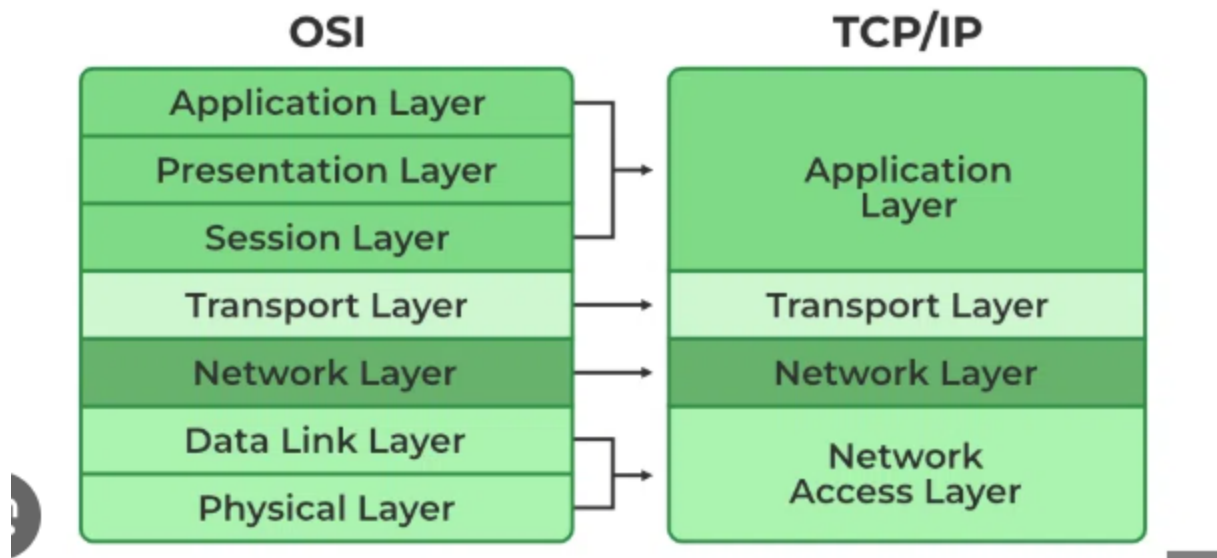
4. Describe the TCP/IP protocol suite and explain the functions of each layer.



The TCP/IP model has four layers (sometimes five, with the physical and data link layers combined into a single "link" layer):<sup>5</sup>

- **Application Layer:** Provides network services to applications (e.g., HTTP, FTP, SMTP).<sup>6</sup>
- **Transport Layer:** Provides end-to-end communication between applications, including reliable delivery (TCP) and unreliable delivery (UDP).<sup>7</sup>
- **Network (Internet) Layer:** Handles routing of data packets across networks (IP).<sup>8</sup>
- **Link (Network Interface) Layer:** Handles communication with the physical network medium.

5. Explain the OSI model and its seven layers. Compare the OSI and TCP/IP models, highlighting their similarities and differences.



The OSI (Open Systems Interconnection) model has seven layers:

1. **Physical Layer:** Deals with the physical transmission of bits over the medium.
2. **Data Link Layer:** Handles error-free transmission between adjacent nodes.
3. **Network Layer:** Handles routing of packets across networks.
4. **Transport Layer:** Provides end-to-end communication between applications.
5. **Session Layer:** Manages dialogues between applications.
6. **Presentation Layer:** Handles data formatting and encryption.
7. **Application Layer:** Provides network services to applications.<sup>10</sup>

#### Comparison:

- **Similarities:** Both models use a layered approach. The network, transport, and application layers have similar functions in both models.
- **Differences:** OSI has seven layers, while TCP/IP has four (or five).<sup>11</sup> OSI has separate session and presentation layers, which are combined into the application layer in TCP/IP. TCP/IP is the dominant model used in the internet, while OSI is more of a theoretical model.<sup>12</sup>

#### 6. Discuss the characteristics of guided transmission media, including twisted pair, coaxial cable, and fiber optics, and compare their advantages and disadvantages.

- **Twisted Pair:** Two insulated wires twisted together to reduce interference.<sup>13</sup>
  - **Advantages:** Inexpensive, easy to install.
  - **Disadvantages:** Limited bandwidth, susceptible to interference over long distances.
- **Coaxial Cable:** A central conductor surrounded by insulation, a metallic shield, and an outer jacket.<sup>14</sup>
  - **Advantages:** Higher bandwidth than twisted pair, better resistance to interference.<sup>15</sup>
  - **Disadvantages:** More expensive than twisted pair, less flexible.
- **Fiber Optics:** Transmits data as light pulses through thin glass or plastic fibers.<sup>16</sup>
  - **Advantages:** Very high bandwidth, immune to electromagnetic interference, long

transmission distances.<sup>17</sup>

- **Disadvantages:** Most expensive, requires specialized installation and equipment.

## 7. Explain unguided transmission media, focusing on wireless technologies and their applications.

- **Unguided Transmission Media:** Data is transmitted through the air or space without a physical conductor.<sup>18</sup>

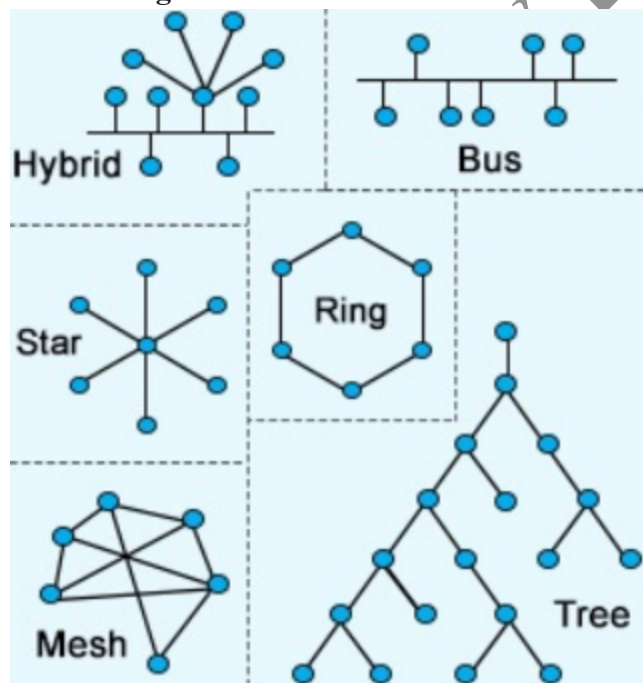
### Wireless Technologies and Applications:

- **Radio Waves:** Used for radio and television broadcasting, Wi-Fi, Bluetooth.
- **Microwaves:** Used for satellite communication, microwave ovens, WiMAX.
- **Infrared:** Used for short-range communication, such as remote controls.

## 8. Explain the concept of packet switching and differentiate between datagram and virtual circuit packet switching.

- **Packet Switching:** Data is divided into small units called packets, which are transmitted independently across the network.<sup>19</sup>
- **Datagram Packet Switching:** Each packet is treated independently and may take a different path to the destination. No connection is established beforehand.
- **Virtual Circuit Packet Switching:** A logical connection is established between the sender and receiver before data transmission. All packets follow the same path.

## 9. Discuss the four basic topologies used in networks, including their advantages and disadvantages.



- **Bus Topology:** All devices are connected to a single cable (the bus).
  - **Advantages:** Simple to install, inexpensive.

- **Disadvantages:** Single point of failure (the bus), difficult to troubleshoot, limited scalability.
- **Star Topology:** All devices are connected to a central hub or switch.
  - **Advantages:** Easy to install and troubleshoot, failure of one device does not affect the rest of the network.
  - **Disadvantages:** Central point of failure (the hub/switch), requires more cabling.
- **Ring Topology:** Devices are connected in a closed loop.<sup>20</sup>
  - **Advantages:** Relatively simple to implement, good performance under light loads.
  - **Disadvantages:** Failure of one device can affect the entire network, difficult to troubleshoot.
- **Mesh Topology:** Every device is connected to every other device.
  - **Advantages:** Highly redundant, very reliable.
  - **Disadvantages:** Very expensive, complex to implement.

## MODULE 2

**1. Explain the importance of error detection and correction at the data link layer. Describe the basic principles of block coding.**

- **Importance of Error Detection and Correction:** The data link layer is responsible for reliable communication over a single link. Errors can occur during transmission due to noise or interference. Error detection and correction mechanisms ensure that data is transmitted accurately between two directly connected nodes.
- **Basic Principles of Block Coding:** In block coding, the message is divided into blocks of  $k$  bits (data bits). Redundant bits ( $r$ ) are added to each block to form a codeword of  $n$  bits ( $n = k + r$ ). The redundant bits are calculated based on the data bits. At the receiver, the received codeword is checked for errors using the redundant bits.

**2. Explain cyclic codes with examples. How are they used for error detection and correction?**

- **Cyclic Codes:** A special type of block code where a cyclic shift (rotation) of a codeword results in another valid codeword. They are based on polynomial arithmetic.
- **Example:** Consider a dataword of 1011 ( $k=4$ ). Using a generator polynomial (a predefined polynomial), we can calculate the redundant bits. Let's say the generator polynomial is  $x^3 + x + 1$ . We represent the dataword as a polynomial ( $x^3 + x + 1$ ) and multiply it by  $x^{(n-k)}$  (in this case  $x^3$ ). Then, we divide the result by the generator polynomial. The remainder is the redundant bits.
- **Use for Error Detection and Correction:** Cyclic codes are very effective at detecting burst errors (multiple consecutive bits in error). The receiver performs the same division operation. If the remainder is zero, there are no detected errors. If the remainder is non-zero, an error is detected. More advanced cyclic codes (like CRC) can also correct some errors.

**3. Describe the key Data Link Control (DLC) services: framing, flow control, and error control, and explain their purposes.**

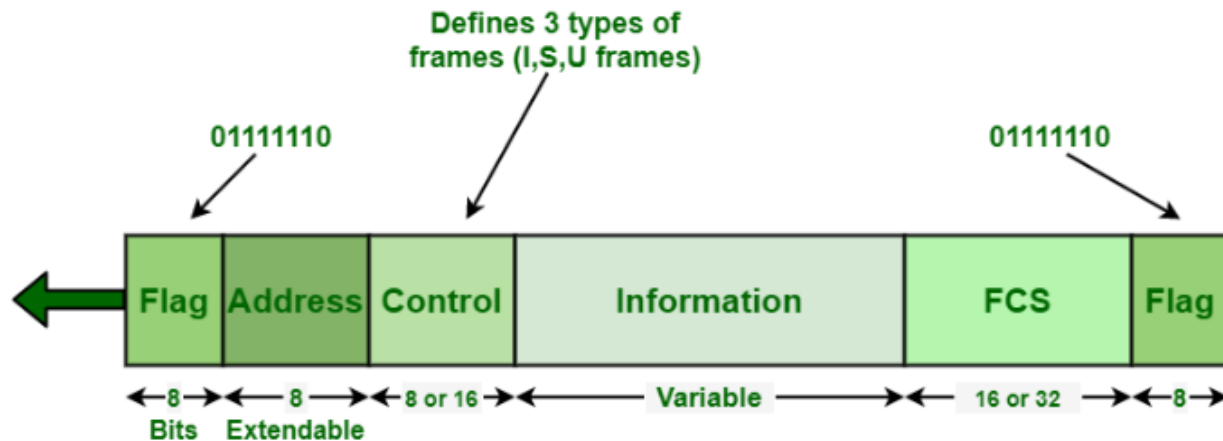
- **Framing:** Dividing the stream of bits received from the physical layer into manageable units called frames. This involves adding headers and trailers to delineate the start and end of each frame.
- **Flow Control:** Preventing a fast sender from overwhelming a slow receiver. Mechanisms like stop-and-wait or sliding window protocols are used.
- **Error Control:** Detecting and correcting errors that occur during transmission. This includes error detection techniques (like CRC) and error correction techniques (like retransmission or forward error correction).

**4. Compare and contrast connectionless and connection-oriented services at the data link layer with examples of protocols.**

Feature	Connectionless Service	Connection-Oriented Service
<b>Connection</b>	No prior connection establishment	Connection is established before data transfer
<b>Delivery</b>	Each frame is treated independently. No guarantee of delivery or order.	Frames are delivered in order and reliably.
<b>Overhead</b>	Lower overhead	Higher overhead due to connection establishment and maintenance
<b>Examples</b>	Ethernet (original implementation)	HDLC, PPP



5. Explain the functions and structure of the High-Level Data Link Control (HDLC) protocol and its modes of operation.



- **Functions:** HDLC is a bit-oriented protocol that provides reliable data transfer over point-to-point and multipoint links. It supports framing, flow control, and error control.
- **Structure:** An HDLC frame consists of:
  - **Flag:** Delimits the start and end of a frame.
  - **Address:** Identifies the secondary station in multipoint configurations.
  - **Control:** Contains control information, including frame type and sequence numbers.
  - **Data (Information):** Contains the user data.
  - **Frame Check Sequence (FCS):** Contains error detection information (typically CRC).
  - **Flag:** Delimits the end of the frame.
- **Modes of Operation:**
  - **Normal Response Mode (NRM):** Used in multipoint configurations where a primary station polls secondary stations.
  - **Asynchronous Balanced Mode (ABM):** Used in point-to-point configurations where both stations have equal status.
  - **Asynchronous Response Mode (ARM):** Rarely used.

6. Discuss different media access control methods: random access (e.g., ALOHA, CSMA/CD) and controlled access (e.g., reservation, polling, token passing), with examples.

- **Random Access:** Stations contend for access to the medium. Collisions can occur.
  - **ALOHA:** Stations transmit whenever they have data. High collision rate.
  - **CSMA/CD (Carrier Sense Multiple Access with Collision Detection):** Stations listen to the medium before transmitting. If a collision is detected, transmission is stopped and retransmission is attempted after a random backoff period. Used in Ethernet.
- **Controlled Access:** A central authority or a defined procedure controls access to the medium.
  - **Reservation:** Stations reserve time slots for transmission.
  - **Polling:** A primary station polls each secondary station to see if it has data to transmit.
  - **Token Passing:** A special packet called a token is passed from station to station. Only the station with the token can transmit. Used in Token Ring.



### 7. Explain the checksum method for error detection. What are its limitations?

- **Checksum Method:** The sender adds the data units (treated as binary numbers) and appends the complement of the sum (the checksum) to the data. The receiver performs the same addition and checks if the sum (including the received checksum) is all 1s.
- **Limitations:** Not very robust. It can fail to detect errors if the errors cancel each other out (e.g., if one bit is flipped from 0 to 1 and another bit is flipped from 1 to 0). It is less effective than CRC for detecting burst errors.

### 8. Describe the Point-to-Point Protocol (PPP), its key features, and applications.

- **PPP (Point-to-Point Protocol):** A data link layer protocol used for establishing direct connections between two nodes. Commonly used for dial-up internet access and VPNs.
- **Key Features:**
  - **Framing:** Uses byte stuffing to delimit frames.
  - **Link Control Protocol (LCP):** Establishes, configures, and tests the data link connection.
  - **Network Control Protocols (NCPs):** Negotiate network layer parameters (e.g., IP addresses).
- **Applications:** Dial-up internet access, DSL connections, point-to-point links between routers.

### 9. Explain bit-oriented framing, including byte stuffing and unstuffing with examples.

- **Bit-Oriented Framing:** Frames are delimited by bit patterns (flags) rather than byte counts. HDLC uses bit-oriented framing.
- **Byte Stuffing (Character Stuffing):** When a flag byte (e.g., 01111110) appears within the data, an escape byte is inserted before it. At the receiver, the escape byte is removed.
- **Example:**
  - **Data:** ABC 01111110 DEF
  - **Stuffed Data:** ABC ESC 01111110 DEF (where ESC is the escape byte).
- **Unstuffing:** The receiver detects the escape byte and removes it, restoring the original data.

## Module - 03

### 1. Describe the services provided by the network layer and its primary functions.

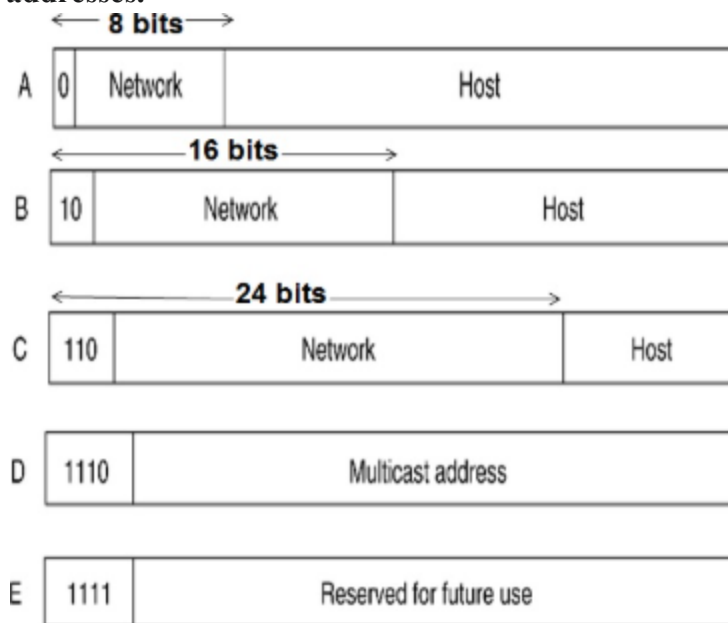
- **Services:** The network layer provides the service of delivering packets from a source host to a destination host across one or more networks. It is responsible for host-to-host delivery.
- **Primary Functions:**
  - **Routing:** Determining the best path for packets to travel from source to destination.
  - **Logical Addressing:** Assigning unique logical addresses (IP addresses) to devices.
  - **Packetizing (Fragmentation):** Dividing data from the transport layer into smaller packets for transmission.

- **Internetworking:** Providing a way for different networks to communicate with each other.

## 2. Explain the concept of packet switching at the network layer. How does it differ from packet switching at the data link layer?

- **Packet Switching at the Network Layer:** The network layer uses packet switching to route packets across multiple networks. Routers at each network make routing decisions based on the destination IP address in the packet header.
- **Difference from Data Link Layer Packet Switching:**
  - The data link layer handles packet switching within a single network (link), using MAC addresses. The network layer handles packet switching across multiple networks, using IP addresses.
  - The data link layer is concerned with physical addressing and media access control, while the network layer is concerned with logical addressing and routing.

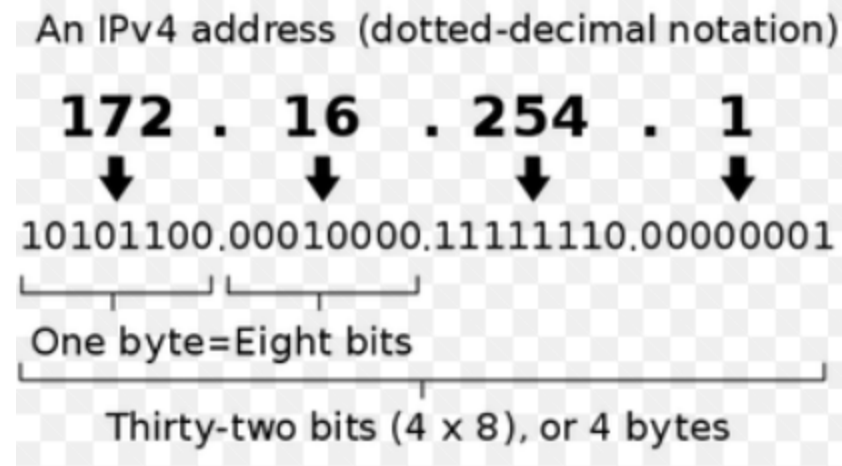
## 3. Explain the structure of an IPv4 address and describe the different classes of IPv4 addresses.



- **Structure of an IPv4 Address:** A 32-bit address represented in dotted decimal notation (e.g., 192.168.1.1). It consists of two parts:
  - **Network ID:** Identifies the network.
  - **Host ID:** Identifies a specific host within the network.
- **Classes of IPv4 Addresses:** Historically, IPv4 addresses were divided into classes:
  - **Class A:** Large networks (0-127 network ID).
  - **Class B:** Medium-sized networks (128-191 network ID).
  - **Class C:** Small networks (192-223 network ID).
  - **Class D:** Multicast addresses (224-239).
  - **Class E:** Reserved for future use (240-255).

Classful addressing is now obsolete and has been replaced by Classless Inter-Domain Routing (CIDR).

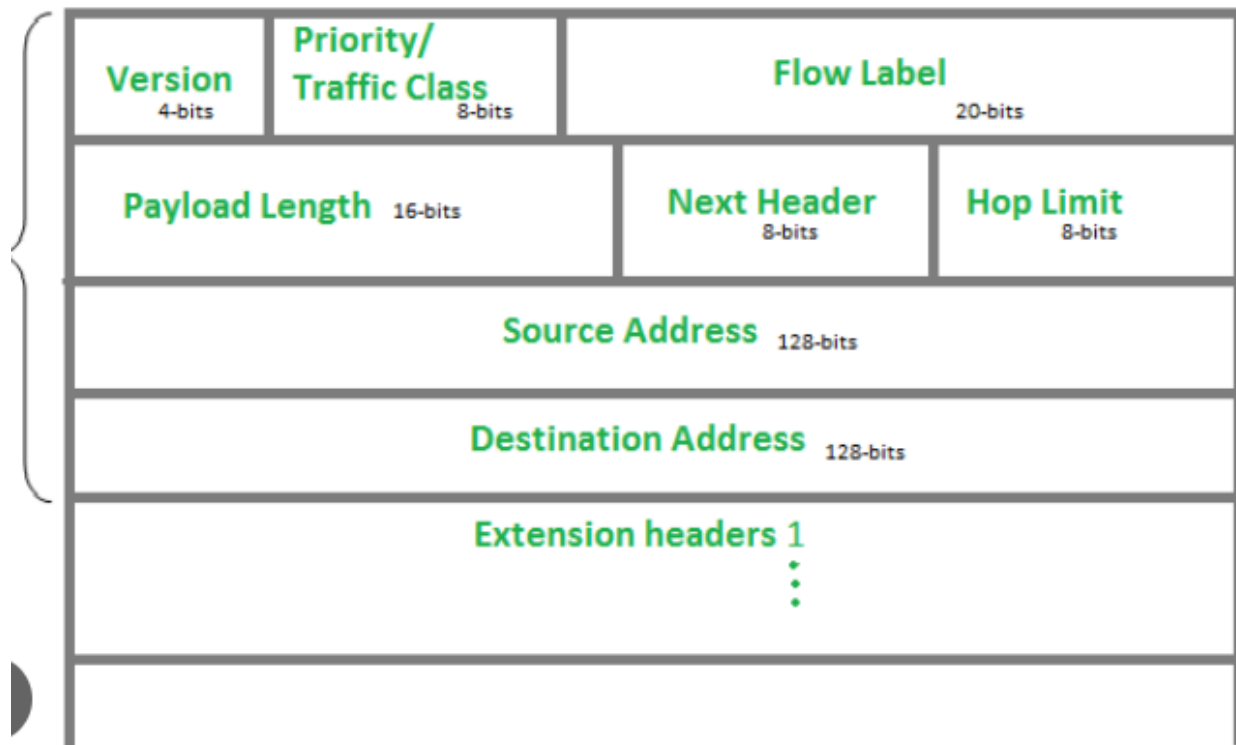
4. Describe the format of an IPv4 datagram and explain the key fields and their functions.



● **IPv4 Datagram Format:**

- **Version:** IP version number (4).
- **Header Length (IHL):** Length of the header in 32-bit words.
- **Type of Service (ToS) / Differentiated Services Code Point (DSCP):** Specifies the desired quality of service.
- **Total Length:** Total length of the datagram (header + data).
- **Identification:** Used for fragmentation and reassembly.
- **Flags:** Control fragmentation.
- **Fragment Offset:** Position of the fragment in the original datagram.
- **Time to Live (TTL):** Prevents packets from looping indefinitely.
- **Protocol:** Indicates the upper-layer protocol (e.g., TCP, UDP).
- **Header Checksum:** Checks for errors in the header.
- **Source IP Address:** IP address of the sender.
- **Destination IP Address:** IP address of the receiver.
- **Options:** Optional fields.
- **Data:** Payload from the upper layer.

5. Briefly explain the structure of an IPv6 datagram. Compare it with IPv4 and discuss the advantages of IPv6.



- **IPv6 Datagram Structure:**

- **Version:** IP version number (6).
- **Traffic Class:** Similar to ToS/DSCP in IPv4.
- **Flow Label:** Used for quality of service.
- **Payload Length:** Length of the payload.
- **Next Header:** Indicates the next header type.
- **Hop Limit:** Similar to TTL in IPv4.
- **Source IP Address:** 128-bit source address.
- **Destination IP Address:** 128-bit destination address.
- **Payload:** Data from the upper layer.

- **Comparison with IPv4:**

- **Address Length:** IPv6 uses 128-bit addresses, while IPv4 uses 32-bit addresses.
- **Header Format:** IPv6 has a simplified header format.
- **Address Autoconfiguration:** IPv6 supports stateless address autoconfiguration.
- **Security:** IPv6 has built-in security features (IPsec).

- **Advantages of IPv6:**

- Much larger address space.
- Simplified header format.
- Improved security.
- Better support for mobile devices.

## 6. Introduce the concept of routing algorithms and differentiate between static and dynamic routing.

- **Routing Algorithms:** Algorithms used by routers to determine the best path for packets to

reach their destination.

- **Static Routing:** Routing tables are manually configured by the network administrator.
  - **Advantages:** Simple to implement.
  - **Disadvantages:** Not adaptable to network changes, requires manual updates.
- **Dynamic Routing:** Routing tables are automatically updated by routing protocols.
  - **Advantages:** Adapts to network changes, less administrative overhead.
  - **Disadvantages:** More complex to implement, requires more processing power.

## 7. Compare and contrast Distance Vector Routing (DVR), Link State Routing (LSR), and Path Vector Routing (PVR).

Feature	Distance Vector Routing (DVR)	Link State Routing (LSR)	Path Vector Routing (PVR)
<b>Information Shared</b>	Distance vectors (distance and direction to other networks)	Topology information (link states of the network)	Path information (list of ASes to reach a destination)
<b>Routing Metric</b>	Hop count, cost	Cost, link characteristics	AS path length, policy
<b>Algorithm</b>	Bellman-Ford	Dijkstra's algorithm	Path vector algorithm
<b>Convergence</b>	Slow, prone to routing loops (count-to-infinity problem)	Fast, less prone to routing loops	Prevents routing loops between ASes
<b>Examples</b>	RIP	OSPF	BGP

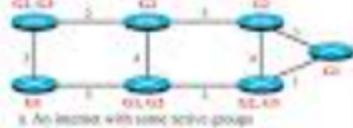
## 8. Explain the functionalities of RIP, OSPF, and BGP protocols.

- **RIP (Routing Information Protocol):** A distance-vector routing protocol. Uses hop count as the metric. Simple but has limitations (e.g., hop count limit of 15).
- **OSPF (Open Shortest Path First):** A link-state routing protocol. Uses Dijkstra's algorithm. More complex but more efficient than RIP.
- **BGP (Border Gateway Protocol):** A path-vector routing protocol used between autonomous systems (ASes). Used for internet routing.

### 9. Briefly discuss multicast routing using MOSPF.

**Multicast Open Shortest Path First (MOSPF)**

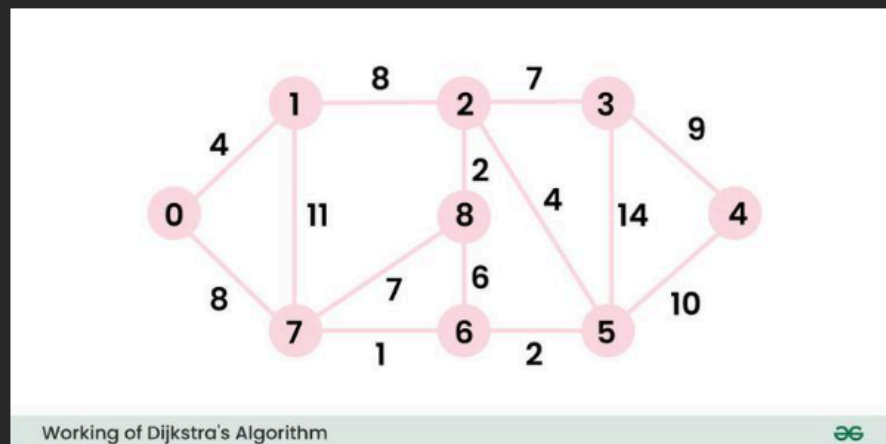
- Source-rooted tree algorithm
  - Extends unicasting to multicasting
  - Every router is linked to a database
  - Aim: to determine an interface with an active node
- Uses intra-area routing
  - All receivers must be one OSPF area – local group database
  - Router delivers datagrams to these members
- A designated router is used to:
  - Transmit host membership queries
  - Listen to membership reports
- Shortest path tree
  - Created on-demand upon receiving the initial message



- **MOSPF (Multicast Open Shortest Path First):** An extension of OSPF that supports multicast routing. It builds a shortest-path tree for each multicast group.

### 10. Solve an example using Dijkstra's algorithm to form a least-cost tree

**Input:**  $src = 0$ , the graph is shown below.



**Answer :** [Find Shortest Paths from Source to all Vertices using Dijkstra's Algorithm](#)

Source : Geeks for Geeks

- **Steps to be written in VTU EXAM**
  1. Assign a tentative distance value to every node: set it to zero for our initial node, and to infinity for all other nodes.

2. Mark the initial node as current.
3. For the current node, consider all of its unvisited neighbors and calculate their tentative<sup>1</sup> distances through the current node. Compare the newly calculated tentative distance to the current assigned value and assign the smaller one.<sup>2</sup>
4. When we are done considering all of the unvisited neighbors of the current node, mark the current node as visited. A visited node will<sup>3</sup> not be checked again.
5. Select the unvisited node that is marked with the smallest tentative distance, and set this as the new "current node" then go back to step 3.

## Module- 04

### 1. Explain the primary functions of the transport layer. How does it provide end-to-end communication between applications?

- **Primary Functions:** The transport layer is responsible for providing end-to-end communication between applications running on different hosts. It ensures that data is delivered reliably and in the correct order.
- **How it provides end-to-end communication:**
  - **Segmentation and Reassembly:** Divides data from the application layer into smaller segments for transmission and reassembles them at the destination.
  - **Port Addressing:** Uses port numbers to identify specific applications on a host.
  - **Connection Management:** Establishes and terminates connections between applications (in the case of TCP).
  - **Flow Control:** Prevents a fast sender from overwhelming a slow receiver.
  - **Error Control:** Detects and corrects errors in transmission.

### 2. Compare and contrast the characteristics of UDP and TCP.

Feature	UDP (User Datagram Protocol)	TCP (Transmission Control Protocol)
<b>Connection</b>	Connectionless	Connection-oriented
<b>Reliability</b>	Unreliable (no guarantee of delivery or order)	Reliable (guarantees delivery and order)
<b>Overhead</b>	Low overhead	Higher overhead due to connection management and reliability mechanisms



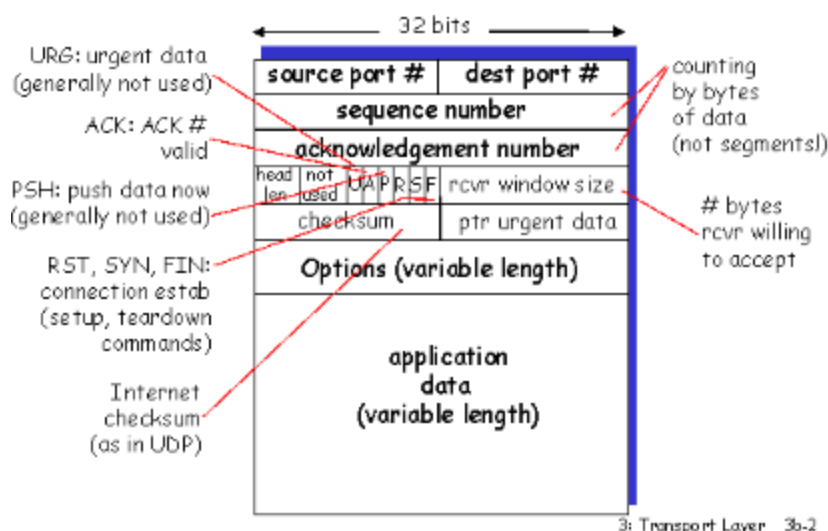
Feature	UDP (User Datagram Protocol)	TCP (Transmission Control Protocol)
<b>Speed</b>	Faster	Slower
<b>Use Cases</b>	Streaming media, online gaming, DNS	Web browsing, file transfer, email

### 3. Describe the services and features provided by TCP. How does it ensure reliable data delivery?

- **Services and Features:**
  - **Connection-oriented:** Establishes a connection before data transfer.
  - **Reliable delivery:** Guarantees delivery of data in the correct order.
  - **Flow control:** Prevents sender from overwhelming receiver.
  - **Error control:** Detects and corrects errors.
  - **Congestion control:** Prevents network congestion.
- **How it ensures reliable data delivery:**
  - **Sequence numbers:** Each segment is assigned a sequence number, which is used to reorder segments at the receiver.
  - **Acknowledgements (ACKs):** The receiver sends ACKs to acknowledge the receipt of segments.
  - **Retransmission:** If an ACK is not received within a timeout period, the sender retransmits the segment.
  - **Checksum:** Used to detect errors in segments.

### 4. Explain the structure of a TCP segment and describe the key fields and their functions.

#### TCP segment structure



- **TCP Segment Structure:**

- **Source Port:** Port number of the sending application.
- **Destination Port:** Port number of the receiving application.
- **Sequence Number:** Sequence number of the first byte in the segment.
- **Acknowledgement Number:** Next expected sequence number from the receiver.
- **Data Offset (Header Length):** Length of the header in 32-bit words.
- **Reserved:** Reserved for future use.
- **Control Bits (Flags):**
  - **URG:** Urgent data.
  - **ACK:** Acknowledgement.
  - **PSH:** Push data.
  - **RST:** Reset the connection.
  - **SYN:** Synchronize sequence numbers (used for connection establishment).
  - **FIN:** Finish the connection.
- **Window Size:** Size of the receiver's receive window.
- **Checksum:** Checksum for error detection.
- **Urgent Pointer:** Points to the end of urgent data.
- **Options:** Optional fields.
- **Data:** Payload from the application layer.

**5. Explain the concept of TCP connections, including the three-way handshake and connection termination.**

- **TCP Connections:** TCP is connection-oriented, meaning a connection must be established before data can be exchanged.
- **Three-Way Handshake:**
  1. **SYN:** The sender sends a SYN segment to the receiver, indicating its intention to establish a connection.
  2. **SYN-ACK:** The receiver responds with a SYN-ACK segment, acknowledging the sender's SYN and sending its own SYN.
  3. **ACK:** The sender sends an ACK segment to acknowledge the receiver's SYN-ACK.
- **Connection Termination:**
  1. **FIN:** One of the hosts sends a FIN segment to indicate that it is finished sending data.
  2. **ACK:** The other host acknowledges the FIN.
  3. **FIN:** The other host sends its own FIN.
  4. **ACK:** The original host acknowledges the second FIN.

**6. Describe TCP flow control mechanisms. How does TCP prevent the sender from overwhelming the receiver?**

- **TCP Flow Control:** Prevents a fast sender from overwhelming a slow receiver by limiting the amount of data the sender can transmit without receiving an acknowledgement.
- **Mechanisms:**
  - **Window Size:** The receiver advertises its receive window size in the TCP header. The sender can only send up to the advertised window size without receiving an ACK.
  - **Sliding Window:** The sender maintains a window of segments that can be sent without

waiting for ACKs. As ACKs are received, the window slides forward, allowing more segments to be sent.

### 7. Explain TCP error control mechanisms. How does TCP handle lost or corrupted segments?

- **TCP Error Control:** Ensures reliable delivery of data by detecting and correcting errors.
- **Mechanisms:**
  - **Checksum:** Used to detect corrupted segments.
  - **Acknowledgements (ACKs):** Used to acknowledge the receipt of segments.
  - **Retransmission Timeout:** If an ACK is not received within a timeout period, the sender retransmits the segment.
  - **Selective Repeat/Go-Back-N:** If a segment is lost, the sender retransmits only the lost segment (selective repeat) or all segments sent after the lost segment (Go-Back-N).

### 8. Describe TCP congestion control mechanisms. How does TCP prevent network congestion?

- **TCP Congestion Control:** Prevents network congestion by reducing the sending rate when congestion is detected.
- **Mechanisms:**
  - **Slow Start:** Starts with a small congestion window and increases it exponentially until congestion is detected.
  - **Congestion Avoidance:** After slow start, the congestion window is increased linearly.
  - **Fast Retransmit/Fast Recovery:** If three duplicate ACKs are received, it is assumed that a segment is lost, and the sender retransmits the segment without waiting for a timeout.

### 9. Explain the differences between stop-and-wait and selective-repeat protocols.

Feature	Stop-and-Wait	Selective Repeat
<b>Window Size</b>	Sender window = 1, Receiver window = 1	Sender window > 1, Receiver window > 1
<b>Efficiency</b>	Low efficiency (sender waits for ACK after each segment)	Higher efficiency (sender can send multiple segments)
<b>Complexity</b>	Simple	More complex
<b>Buffer</b>	Requires minimal buffer at	Requires larger buffer at sender and receiver to store

Feature	Stop-and-Wait	Selective Repeat
	sender and receiver	multiple out-of-order packets

### 10. Discuss the finite state machine (FSM) of Reno TCP.

- **Reno TCP FSM:** Reno is a version of TCP that includes congestion control mechanisms like fast retransmit and fast recovery. Its FSM describes the different states the TCP connection can be in and the transitions between those states.
- **Key States:**
  - **Closed:** No connection.
  - **Listen:** Waiting for a connection request.
  - **SYN-Sent:** Sent a SYN segment.
  - **SYN-Received:** Received a SYN segment.
  - **Established:** Connection is established.
  - **Fin-Wait-1/Fin-Wait-2:** Waiting for a FIN or ACK.
  - **Time-Wait:** Waiting for a sufficient time to ensure that all segments have been received.
  - **Close-Wait:** Waiting for the local application to close the connection.
  - **Last-ACK:** Waiting for the final ACK.

## Modula - 05

### 1. Describe the functions of the application layer and its interaction with user applications.

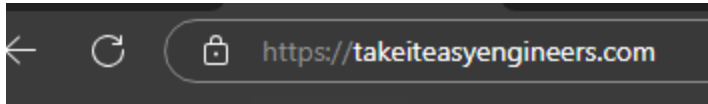
- **Functions:** The application layer is the top layer of the TCP/IP and OSI models. It provides network services to user applications, enabling them to communicate over the network. It does not provide services to any other layer.
- **Interaction with User Applications:** The application layer acts as an interface between user applications and the network. It provides protocols that applications use to request and receive network services. Examples include:
  - Web browsers using HTTP to access web pages.
  - Email clients using SMTP to send emails and POP3/IMAP to receive emails.
  - File transfer applications using FTP to transfer files.

### 2. Explain the client-server programming model, detailing the roles of the client and server.

- **Client-Server Programming Model:** A distributed application structure that partitions tasks or workloads between servers (providers of resources or services) and clients (requesters of services).
- **Roles:**
  - **Client:**
    - Initiates requests for services.
    - Sends requests to the server.

- Waits for a response from the server.
- Processes the response from the server.
- **Server:**
  - Listens for client requests.
  - Processes client requests.
  - Sends responses back to the client.
  - Provides services or resources to clients.

### 3. Explain the working of the World Wide Web (WWW) and the HTTP protocol. What are HTTP methods and status codes?



- **Working of the WWW:** The World Wide Web is a system of interconnected hypertext documents and other resources, accessed via the Internet. It is based on the client-server model, with web browsers acting as clients and web servers hosting websites.  
Ex: [www.takeiteasyengineers.com](https://www.takeiteasyengineers.com)- here www is connecting your favourite TAKEITEASY ENGINEERS to the Internet
- **HTTP (Hypertext Transfer Protocol):** The foundation of data communication for the World Wide Web. It defines how clients and servers exchange messages.
- **HTTP Methods:** These define the type of action a client wants to perform on a resource. Common methods include:
  - **GET:** Retrieves a resource.
  - **POST:** Submits data to be processed by a resource.
  - **PUT:** Updates a resource.
  - **DELETE:** Deletes a resource.
- **HTTP Status Codes:** These are three-digit codes sent by the server in response to a client request, indicating the status of the request. Common categories include:
  - **1xx (Informational):** Request received, continuing process.
  - **2xx (Success):** Request was successful. (e.g., 200 OK)
  - **3xx (Redirection):** Further action needs to be taken by the client.
  - **4xx (Client Error):** Client error. (e.g., 404 Not Found)
  - **5xx (Server Error):** Server error. (e.g., 500 Internal Server Error)

### 4. Describe the File Transfer Protocol (FTP) and its usage in transferring files between hosts.

- **FTP (File Transfer Protocol):** A standard network protocol used for transferring files between a client and a server over<sup>1</sup> a TCP/IP network.
- **Usage:**
  - A client establishes two connections to the server: a control connection (for commands) and a data connection (for file transfer).
  - The client sends commands to the server (e.g., to list files, upload files, download files).
  - The server responds with replies.
  - Files are transferred over the data connection.

## 5. Explain the workings of electronic mail and the key protocols involved (e.g., SMTP, POP3, IMAP).

- **Workings of Electronic Mail:** Email involves sending and receiving messages electronically over a network.
- **Key Protocols:**
  - **SMTP (Simple Mail Transfer Protocol):** Used for sending emails from a client to a mail server or between mail servers.
  - **POP3 (Post Office Protocol version 3):** Used for retrieving emails from a mail server to a client. Downloads emails to the client and typically deletes them from the server.
  - **IMAP (Internet Message Access Protocol):** Used for retrieving emails from a mail server to a client. Allows clients to access and manage emails on the server without necessarily downloading them.

## 6. Describe the Domain Name System (DNS) and how it translates domain names to IP addresses.

- **DNS (Domain Name System):** A hierarchical and distributed naming system for computers, services, or other resources connected to the Internet or a private network. It translates<sup>2</sup> human-readable domain names (e.g., <https://takeiteasyengineers.com/>) into IP addresses (e.g., 192.0.2.1).
- **Translation Process:**
  - A client queries a local DNS server (usually provided by the ISP).
  - If the local DNS server does not have the IP address, it queries a root DNS server.
  - The root DNS server directs the query to a top-level domain (TLD) server (e.g., .com, .org).
  - The TLD server directs the query to an authoritative name server for the domain.
  - The authoritative name server provides the IP address.
  - The local DNS server caches the IP address for future queries.

## 7. Explain the TELNET protocol, its uses, and security limitations.

- **TELNET:** A network protocol used to provide bidirectional interactive text-oriented communication using a virtual terminal connection.
- **Uses:** Used for remote administration of servers and network devices.
- **Security Limitations:** Transmits data in clear text, making it vulnerable to eavesdropping and interception. It is generally considered insecure and has been largely replaced by SSH.

## 8. Describe the Secure Shell (SSH) protocol and how it provides secure remote access to servers.

- **SSH (Secure Shell):** A cryptographic network protocol for operating network services securely over an unsecured network.
- **How it provides secure remote access:**
  - **Encryption:** Encrypts all communication between the client and server, protecting against eavesdropping.
  - **Authentication:** Provides strong authentication mechanisms to verify the identity of the client and server.

- **Integrity:** Ensures that data has not been tampered with during transmission.

### 9. Differentiate between persistent and non-persistent connections in HTTP with examples.

- **Non-Persistent Connections:** A new TCP connection is established for each request/response pair.
  - **Example:** A web page with multiple images. The browser establishes a separate connection for each image.
- **Persistent Connections:** A single TCP connection is used for multiple request/response pairs.
  - **Example:** A web page with multiple images. The browser establishes one connection and retrieves all images over that connection.
- **Advantages of Persistent Connections:** Reduced overhead due to fewer connection establishments, improved performance.

### 10. Explain iterative communication using TCP with examples.

- **Iterative Communication using TCP:** The server processes one client request at a time. While the server is processing a request from one client, other clients must wait.
- **Example:** A simple time server. A client connects to the server and requests the current time. The server sends the time and closes the connection. While the server is handling this request, other clients attempting to connect will be blocked. This is a basic example, most servers use concurrent methods to handle multiple clients simultaneously.