DEPARTMENT OF COMPUTER SCIENCE
Question Bank
ADVANCED NETWORKING MCA2

Chapter 1: Overview of Computer Networks

1. What *is* the Internet? What *is* a protocol?
2. What do we mean by the internet as a service?
3. Define three performance Characteristics of the internet and explain Delay in detail
4. List any four access networks that are used to connect end systems to edge routers.
5. Explain the network core and two key functions of the network core
6. Explain the Network under attack
7. Differentiate Packet switching versus circuit switching in a tabular format
8. With a well-labeled diagram explain the packet switching
9. Define the following in brief (2-3 sentences only):
    a) Authentication
    b) Confidentiality
    c) Integrity
    d) Firewall
10. Explain the TCP/IP protocol layers with a diagram and briefly explain the functions of each layer
11. Explain two types of communication links with 3 examples for each type

Chapter 2: The Application Layer

12. Explain client-server model in network application principle and give three network layer protocols that follows client-server model
13. What is P2P architecture
14. Explain HTTP
15. Why persistent http is better than non-persistent http? Compare in terms of RTT
16. What do the following HTTP response status codes mean:
    a) 200
    b) 301
    c) 400
    d) 404
    e) 500
17. Explain cookies and caching in web browsing with examples
18. Explain Email with a diagram showing how email message is shared between Alice and Bod through the internet
19. Explain DNS in detail
20. Explain how DNS resolution works in iterative query and recursive query
21. Explain Bit Torrent operation in P2P architecture
22. Explain video streaming (major consumer of Internet bandwidth), what are major challenges and their solution

23. Explain Spatial coding and temporal coding in multimedia with focus on video
24. What is CBR and VBR in video multimedia
25. Explain in brief Playout buffering and DASH
26. Explain Content Distribution Network
27. Explain the FTP, Telnet and SSH

SOLUTIONS TO CHAPTER 1 AND CHAPTER 2

1. What *is* the Internet? What *is* a protocol?

- **The Internet:** A vast global network of interconnected computer networks that facilitates communication and data exchange between devices worldwide. It operates without a central governing body, relying on standardized protocols to ensure seamless communication.
- **Protocol:** A set of rules and specifications that define how devices communicate over a network. Protocols govern data formatting, transmission, error handling, and flow control. Common internet protocols include TCP/IP (Transmission Control Protocol/Internet Protocol) suite, HTTP (Hypertext Transfer Protocol), and DNS (Domain Name System).

2. What do we mean by the internet as a service?

The Internet as a service refers to the provision of Internet connectivity and related services to users and businesses by Internet Service Providers (ISPs). These services include access to websites, email, online storage, communication tools, and various applications hosted on the Internet.

3. Define three performance Characteristics of the internet and explain Delay in detail

- **Three key performance characteristics:**
  - **Throughput:** The rate of successful data transfer across a network, typically measured in bits per second (bps) or Megabits per second (Mbps).
  - **Delay (Latency):** The time it takes for a data packet to travel from sender to receiver. Factors affecting delay include network congestion, physical distance, and processing time at intermediate points (routers). Delay is crucial for real-time applications like video conferencing and online gaming.
  - **Packet Loss:** The rate at which data packets fail to reach their destination due to network congestion, errors, or other issues. Packet loss can impact data integrity and require retransmission, increasing delay.
- **Delay (Latency) in detail:** Delay is a critical factor in internet performance, especially for real-time applications. It's influenced by several components:
  - **Propagation Delay:** The physical time it takes for a signal to travel through a medium like fiber optic cable or copper wire.
  - **Transmission Delay:** The time required to place the entire data packet onto the transmission medium.
  - **Queuing Delay:** The time packets spend waiting in queues at routers due to network congestion.

- **Processing Delay:** The time it takes for network devices (routers and switches) to process the header information in packets and route them appropriately.

4. List any four access networks that are used to connect end systems to edge routers

- Four common access networks connecting end systems (computers, phones, etc.) to edge routers:
- **Dial-up Access:** Uses a modem to transmit data over traditional phone lines. This is a low-bandwidth, legacy option.
- **Digital Subscriber Line (DSL):** Uses existing phone lines but transmits data at higher speeds compared to dial-up by separating voice and data signals.
- **Cable Modem:** Provides internet access via coaxial cables typically used for cable television. Offers higher bandwidth than DSL.
- **Data center network access:** Uses fiber optic cables for extremely high-speed data transmission with minimal signal degradation over long distances.
- **Enterprise networks**
- **Home networks**

5. Explain the network core and two key functions of the network core

1. The network core refers to the central part of a packet-switched network where data is routed. It typically consists of high-speed routers and switches interconnected by high-capacity communication links.
2. Two key functions of the network core are:
    - **Packet Forwarding:** The core routers and switches forward data packets from source to destination based on routing tables and algorithms.
    - **Packet Switching:** The network core employs packet switching, where data packets are routed independently based on destination addresses, allowing for efficient use of network resources.

6. explain the Network Under Attack

- A network under attack is a network that is being targeted by malicious actors attempting to gain unauthorized access, disrupt operations, steal data, or otherwise damage network resources. Common types of network attacks include:
- **Denial-of-Service (DoS) attacks:** Overwhelming a network with traffic to prevent legitimate users from accessing resources.
- **IP spoofing:** injection of a packet with a false source address
- **Packet sniffing:** broadcast media (shared Ethernet, wireless) promiscuous network interface reads/records all packets (e.g., including passwords!) passing by
- **Man-in-the-middle (MitM) attacks:** Eavesdropping on communication between two parties to steal data or impersonate one of them.
- **Malware attacks:** Exploiting software vulnerabilities to inject malicious code (viruses, worms, etc.) that can disrupt operations or steal data.

7. Differentiate Packet switching versus circuit switching in a tabular format

Feature	Packet Switching	Circuit Switching
Connection Setup	No dedicated path setup; packets routed dynamically	Dedicated path setup before communication starts
Resource Allocation	Shared resources; packets share available bandwidth	Dedicated resources allocated for the duration of call
Efficiency	More efficient use of network resources	Less efficient for bursty traffic but more suitable for constant bit rate applications
Flexibility	More flexible as bandwidth is dynamically allocated	Less flexible due to fixed bandwidth allocation
Example Technologies	Internet Protocol (IP), Asynchronous Transfer Mode (ATM)	Public Switched Telephone Network (PSTN), ISDN

8. With a well-labeled diagram explain packet switching and circuit Switching

9. explain the following in brief (2 to3 sentences)

a) **Authentication**: Authentication is the process of verifying the identity of a user or system. It ensures that the entity trying to access a network or resource is indeed who or what it claims to be.

b) Confidentiality: Confidentiality ensures that data is accessible only to authorized parties and protected from unauthorized access or disclosure. It's often achieved through encryption techniques.

c) Integrity: Integrity ensures that data remains unchanged and unaltered during transmission or storage. It verifies that data has not been tampered with or modified by unauthorized parties.

d) Firewall: A firewall is a network security device or software that monitors and controls incoming and outgoing network traffic based on predetermined security rules. It acts as a barrier

between a trusted internal network and untrusted external networks, such as the Internet, to prevent unauthorized access and protect against malicious activities.

10. Explain the TCP/IP protocol layers with a diagram and briefly explain the functions of each layer

The TCP/IP protocol suite consists of four layers:

- **Application Layer:** This layer interacts with the end-user applications, such as web browsers and email clients. It provides network services directly to user applications and includes protocols like HTTP, SMTP, and FTP.
- **Transport Layer:** The transport layer ensures end-to-end communication between applications. It's responsible for segmenting data from the application layer into smaller packets and ensuring reliable delivery. Key protocols include TCP (Transmission Control Protocol) and UDP (User Datagram Protocol).
- **Internet Layer:** The internet layer is responsible for addressing, routing, and packaging data packets for transmission across the network. It enables packets to be routed between different networks. The main protocol at this layer is IP (Internet Protocol).
- **Link Layer:** Also known as the network interface layer or data link layer, this layer deals with the physical transmission of data over the network. It includes protocols that define how data is formatted for transmission and how access to the network is controlled. Examples include Ethernet, Wi-Fi, and PPP (Point-to-Point Protocol).
- **Physical layer:** the physical layer of the TCP/IP protocol suite is responsible for the physical transmission of data bits over the network medium, defining characteristics such as encoding, signaling, transmission media, data rate control, synchronization, and physical topology.

11. Explain two types of communication links with 3 examples for each type

1. **Unguided Media:**

Unguided media, also known as wireless or unbounded media, transmits signals through the air or space without the need for physical connections. These media offer mobility and flexibility, making them ideal for mobile devices and applications where wired connections are impractical. Here are three examples of unguided media:

a) **Wi-Fi (Wireless Fidelity):**

Wi-Fi technology enables wireless communication between devices within a limited range, typically within a building or hotspot area. It operates on the IEEE 802.11 standard and uses radio waves for data transmission.

b) **Bluetooth:**

Description: Bluetooth technology enables short-range wireless communication between devices, typically within a range of 10 meters. It is commonly used for connecting peripherals, such as headphones, keyboards, and printers, to computers and mobile devices.

Example Applications:

1. Wireless Headsets
2. Wireless Speakers
3. Smart Home Devices

c) **Cellular Networks:**

Description: Cellular networks provide wireless communication over a wide geographic area by dividing it into smaller areas called cells. Mobile devices connect to nearby cellular towers, which relay signals to the core network infrastructure.

2. **Guided Media:**

Guided media, also known as wired or bounded media, use physical cables or wires to transmit signals between devices. These cables provide a pathway for signals to travel, offering a stable and reliable communication channel. Here are three examples of guided media:

a) **Twisted Pair Cable:**

Description: Twisted pair cables consist of copper wires twisted together in pairs, with each pair enclosed in insulation. They are widely used in telecommunications and computer networking.

Example Applications:

1. Ethernet LAN
2. Telephone Systems
3. DSL Internet

b) **Coaxial Cable:**

Description: Coaxial cables consist of a central conductor surrounded by insulation, a metallic shield, and an outer insulating layer. They offer higher bandwidth and better shielding compared to twisted pair cables.

Example Applications:

1. Cable Television:
2. CCTV Systems
3. Broadband Internet

c) **Fiber Optic Cable:**

Description: Fiber optic cables use light signals to transmit data over long distances. They consist of a core surrounded by cladding, which reflects light within the core, ensuring minimal signal loss.

Example Applications

1. Long distance communication
2. Data centers
3. Internet backbone

Chapter 2: Application Layer

12. Explain the client-server model in network application principle and give three network layer protocols that follow the client-server model

In the client-server model, network applications are structured into two distinct roles: the client and the server. The client initiates communication by making requests to the server, and the server responds to those requests by providing the requested resources or services. This model allows for efficient sharing of resources and centralized management of data.

server:

- always-on host
- permanent IP address
- often in data centers, for scaling

clients:

- contact, and communicate with the server
- may be intermittently connected
- may have dynamic IP addresses
- do *not* communicate directly with each other

Three network layer protocols that follow the client-server model are:

- HTTP (Hypertext Transfer Protocol)
- FTP (File Transfer Protocol)
- SMTP (Simple Mail Transfer Protocol)

13. What is P2P architecture

Peer-to-peer (P2P) architecture is a decentralized network model where participants in the network (peers) share resources directly with one another, rather than through a centralized

server. Each peer in the network can act as both a client and a server, allowing for distributed sharing of resources

14. Explain HTTP

HTTP is a protocol used for transferring hypertext requests and information on the World Wide Web. It is the foundation of data communication for the web. HTTP operates as a request-response protocol between a client and a server. Clients, typically web browsers, initiate requests for resources (such as web pages), and servers respond with the requested content.

- The web page consists of *objects*, each of which can be stored on different Web servers
- The object can be an HTML file, JPEG image, Java applet, or audio file

web page consists of a *base HTML file* that includes *several referenced objects, each* addressable by a *URL, and the collection of web pages is called a Website*

15. Why persistent http is better than non-persistent http? Compare in terms of RTT

Persistent HTTP	**Non-Persistent HTTP**
Maintains the TCP connection for multiple requests and responses, reducing the overhead of RTT	Establishes a new TCP connection for each request-response cycle. Hence several RTT
Suitable for scenarios where multiple resources need to be fetched from the same server.	Commonly used in situations where only a single resource needs to be retrieved.
Efficient in terms of reducing round-trip time (RTT) due to connection reuse.	This may lead to higher latency due to connection establishment overhead for each request.

16. What do the following HTTP response status codes mean:

200 OK

request succeeded, requested object later in this message

301 Moved Permanently

requested object moved, the new location specified later in this message (in Location: field)

400 Bad Request

request msg not understood by the server

404 Not Found

The requested document is not found on this server

505 HTTP Version Not Supported

17. Explain cookies and caching in web browsing with examples

- **Cookies**: Cookies are small pieces of data stored on a user's computer by websites they visit. They are used to track user preferences, session information, and other data. For example, a shopping website might use cookies to remember items in a user's shopping cart. *cookies can be used for:*
    - authorization
    - shopping carts
    - recommendations
    - user session state (Web e-mail)

- **Caching**: Caching involves storing copies of web resources (such as HTML pages, images, and scripts) closer to the user, typically in a web browser or proxy server. This helps reduce server load and speeds up subsequent requests for the same resources. For example, a web browser may cache images and CSS files to avoid downloading them again when revisiting a website.
    - reduce response time for client request
    - cache is closer to the client
    - reduce traffic on an institution’s access link

18. Explain Email with a diagram showing how email message is shared between Alice and Bod through the internet

Email communication involves the exchange of electronic messages between users over the Internet. Alice's email client sends the email message to her email server through SMTP. The email server routes the message through the Internet to Bob's email server. Bob's email server delivers the message to Bob's email client through IMAP

19. Explain DNS in detail

DNS is a hierarchical decentralized naming system for computers, services, or other resources connected to the Internet or a private network. It translates domain names (e.g., example.com) into IP addresses (e.g., 192.0.2.1) required for locating computer services and devices worldwide.

DNS services:

- **hostname-to-IP-address translation**
- **host aliasing**: Host aliasing refers to the ability to assign multiple domain names (aliases) to a single host. This allows a single server or network device to be accessible under different domain names
- **canonical, alias names:** It allows multiple domain names to resolve to the same IP address. For example, if "www.example.com" is a CNAME for "example.com," accessing "www.example.com" would ultimately resolve to the same IP address as "example.com."
- **mail server aliasing:** this involves configuring DNS to assign multiple domain names to a single mail server or multiple mail servers in a mail exchange (MX) record. This enables organizations to receive email addressed to different domain names using the same mail infrastructure**.**
- load distribution: replicated Web servers: many IP addresses correspond to one name

20. Explain how DNS resolution works in iterative query and recursive query

Iterative Query:

1. The client sends a DNS query to a DNS resolver within Local DNS server
2. The DNS resolver, if it doesn't have the requested information cached, sends an iterative query to the root DNS server.
3. The root DNS server responds with the authoritative DNS server for the top-level domain (TLD) of the requested domain.
4. The resolver sends a query to the TLD DNS server, which responds with the authoritative DNS server for the second-level domain.
5. The resolver sends a query to the authoritative DNS server for the second-level domain, which responds with the IP address associated with the requested domain.
6. The resolver caches the IP address and returns it to the client.

Recursive Query:

In a recursive query, the client asks the local DNS resolver to fetch the destination IP address directly or return an error message.

Here’s the breakdown:

1. Client Request: The client generates a DNS query (e.g., when you type a URL in your browser) e.g. google.com
2. Local DNS Resolver: The local resolver receives the query and forwards it to the local DNS server (your local ISP)

3. Local DNS Server: The local server recursively resolves the query by following the entire chain of referrals (root server, TLD server, authoritative server) until it obtains the IP address.
4. Response to Client: The local resolver delivers the IP address back to the client, completing the resolution process.
5. The resolver caches the IP address and returns it to the client.

21. Explain Bit Torrent operation in P2P architecture

In the context of peer-to-peer (P2P) architectures, "seeding" typically refers to the process of making a file available for download to other users in the network. It's commonly associated with BitTorrent, a popular P2P file-sharing protocol. Here's how seeding works in BitTorrent and similar P2P networks:

1. **Initial Seeding:** When a user creates a torrent file (which contains metadata about the file to be shared) and shares it on the network, they become the initial seeder. Initially, this seeder has the complete file available for sharing.
2. **Downloading:** Other users in the network, often referred to as leechers, connect to the network and start downloading the file. Initially, they may not have the complete file, so they request different parts of it from multiple sources.
3. **Seeding:** As users download parts of the file, they become seeders themselves for those parts. Once a user has downloaded the entire file, they can continue to seed it, making it available for download by other users.
4. **Ratio:** In many BitTorrent clients, there's a concept of a seeding ratio. Users are encouraged to continue seeding files they have downloaded until they've uploaded a certain amount of data (typically equal to or greater than what they downloaded). This helps distribute the file and maintain the health of the network.

22. Explain video streaming (major consumer of Internet bandwidth), what are major challenges and their solution

Video streaming refers to the delivery of video content over the internet in real-time. Major challenges in video streaming include:

- Bandwidth Limitations: High-quality video requires significant bandwidth, which can strain network infrastructure.
- Buffering and Latency: Buffering occurs when the video stream can't be delivered as fast as it's being consumed, leading to interruptions in playback. Latency refers to the delay between when content is requested and when it's actually viewed.
- Quality of Service: Ensuring consistent video quality across different devices and network conditions is crucial for a positive user experience.

- Solutions include adaptive bitrate streaming, content delivery networks (CDNs), and efficient video compression algorithms.

23. Explain Spatial coding and temporal coding in multimedia with focus on video

Spatial Coding: Spatial coding refers to the compression of video frames by exploiting spatial redundancy within each frame.

Temporal Coding: Temporal coding exploits temporal redundancy between consecutive frames in a video sequence. Predictive coding techniques, such as motion estimation and compensation, are used to predict future frames based on previously encoded frames, reducing redundancy and improving compression efficiency.

24. What is CBR and VBR in video multimedia

CBR (Constant Bit Rate): CBR encoding maintains a constant bitrate throughout the video stream, regardless of the complexity of the content. This ensures a consistent quality but may lead to inefficient use of bandwidth during scenes with low complexity.

VBR (Variable Bit Rate): VBR encoding dynamically adjusts the bit rate based on the complexity of the video content. It allocates more bits to complex scenes and fewer bits to simpler scenes, resulting in better overall compression efficiency and potentially higher quality at a lower average bitrate

25. Explain in brief Playout buffering and DASH

Playout Buffering: Playout buffering involves temporarily storing a portion of the video stream on the user's device before playback begins. This buffer helps smooth out fluctuations in network bandwidth and reduces the likelihood of buffering interruptions during playback.

DASH (Dynamic Adaptive Streaming over HTTP): DASH is a streaming protocol that dynamically adjusts video quality and bitrate based on the user's network conditions and device capabilities. It breaks the video content into small segments and offers multiple versions of each segment encoded at different bitrates. The client device can adaptively switch between these segments to maintain smooth playback without interruptions.

26. Explain Content Distribution Network

A CDN is a network of geographically distributed servers that work together to deliver content to users more efficiently. CDNs cache content closer to end-users, reducing latency and relieving the load on origin servers. When a user requests content, the CDN routes the request to the nearest server with the cached content, improving delivery speed and reliability. CDNs are commonly used for delivering web pages, streaming media, and other content-heavy applications.

27. Explain the FTP, Telnet and SSH

FTP (File Transfer Protocol):

FTP is a standard network protocol used to transfer files between a client and a server on a computer network, typically the Internet. It operates on the client-server model, where the client initiates a connection to the server to perform file transfer operations. Here's how FTP works:

1. **Authentication:** Users typically authenticate themselves using a username and password.
2. **Commands:** Once authenticated, the client can issue commands to the server to perform various file operations such as uploading, downloading, renaming, deleting, and listing files and directories.
3. **Data Transfer:** FTP uses separate connections for control (commands and responses) and data transfer. Data transfer can occur in two modes: active mode, where the server initiates the data connection, and passive mode, where the client initiates the data connection.

Telnet:

Telnet is a protocol used to establish a command-line connection to a remote computer or device over a network. It allows users to access the command-line interface (CLI) of a remote system and execute commands as if they were directly connected to it. Here's how Telnet works:

1. **Connection Establishment:** The client establishes a TCP connection to the Telnet port (typically port 23) of the remote server.
2. **Terminal Emulation:** Once the connection is established, the client emulates a terminal, providing a text-based interface for the user to interact with the remote system.
3. **Command Execution:** Users can execute commands on the remote system as if they were physically present at the terminal.

However, Telnet has security vulnerabilities as it transmits data, including login credentials, in plain text, making it susceptible to eavesdropping and interception. Hence, it's generally recommended to use more secure protocols like SSH instead of Telnet for remote access.

SSH (Secure Shell):

SSH is a cryptographic network protocol used to establish a secure, encrypted connection to a remote computer or device over a network. It provides secure authentication and encrypted data communication, making it suitable for secure remote access and file transfer. Here's how SSH works:

1. **Key Exchange:** The SSH client and server perform a key exchange to establish a secure connection.

2. **Authentication:** Users authenticate themselves using various methods such as passwords, public-key cryptography, or other authentication mechanisms supported by SSH.
3. **Encrypted Communication:** Once authenticated, SSH encrypts all communication between the client and server, including commands, data, and responses, to prevent eavesdropping and tampering.
4. **Secure File Transfer:** SSH includes protocols like SCP (Secure Copy Protocol) and SFTP (SSH File Transfer Protocol) for secure file transfer operations similar to FTP but with the added security provided by SSH encryption.

SSH is widely used for secure remote administration, secure file transfer, tunneling, and other secure network communication tasks, offering a significant improvement in security over protocols like Telnet.