NAME	
ROLL NUMBER	
PROGRAM	**MASTER OF COMPUTER APPLICATIONS (MCA)**
SEMESTER	**2nd**
COURSE CODE	**DCA6204**
COURSE NAME	**Advanced Computer Network**

SET - I

Q.1.a) Compare and contrast the OSI model with the TCP/IP reference model, highlighting their similarities and differences in terms of layering and functionality.

Answer .:- Both OSI (Open Systems Interconnection) and TCP/IP (Transmission Control Protocol/Internet Protocol) are models that describe network communication, but they serve different purposes.

Layering:

- **OSI:** A theoretical framework with 7 well-defined layers, each with specific functions. It provides a clear separation of concerns, making it easier to understand network communication.
- **TCP/IP:** A practical model with 4 layers, which are more focused on actual protocols used on the internet.

Functionality:

- **OSI:** Focuses on *what* needs to be done at each layer, not *how*. This allows for flexibility in choosing protocols at each layer. (Think of it as a blueprint)
- **TCP/IP:** Defines specific protocols for each layer. This ensures interoperability between devices using TCP/IP. (Think of it as a pre-built house plan)

Similarities:

- Both models break down network communication into smaller, manageable pieces.
- The top 3 layers (Application, Presentation, Session) have similar functions in both models.
- The core functionality of data transfer is handled by the middle layers (Transport and Network).

Differences:

- OSI has more layers, providing a more granular view of network communication.
- TCP/IP is more widely used and directly maps to real-world protocols.
- OSI is protocol-independent, while TCP/IP is protocol-dependent.

In essence:

- OSI is a theoretical guide for understanding network communication.
- TCP/IP is a practical implementation used for internet communication.

Q.1.b) Discuss the differences between Ethernet and Token Ring LAN technologies, focusing on their architectures and access methods

Answer .:- Ethernet vs. Token Ring: A Battle of Architectures and Access

Ethernet and Token Ring, once rivals in the LAN arena, offer distinct approaches to connecting devices.

Architecture:

- **Ethernet:** Utilizes a bus or star topology. Devices connect to a central hub (bus) or switch (star) and compete for access to the shared medium.
- **Token Ring:** Employs a ring topology. Devices are wired in a closed loop, with data traveling sequentially.

Access Method:

- **Ethernet:** Relies on Carrier Sense Multiple Access with Collision Detection (CSMA/CD). Devices listen for activity before transmitting. If a collision occurs (two devices transmit simultaneously), both halt and re-transmit after a random delay.
- **Token Ring:** Leverages a token passing mechanism. A special packet, the token, circulates around the ring. A device can only transmit data when it possesses the token.

Impact on Performance:

- **Ethernet:** Performance can fluctuate depending on network traffic. Collisions can lead to delays and re-transmissions.
- **Token Ring:** Offers more predictable performance. Since only one device transmits at a time, collisions are eliminated. However, waiting for the token can introduce latency.

Other Considerations:

- **Cost:** Ethernet is generally cheaper to install and maintain due to simpler cabling and components.
- **Scalability:** Ethernet scales more easily to larger networks compared to Token Ring, which has limitations on the number of connected devices.

Ethernet's flexibility, lower cost, and continuous speed improvements have cemented its dominance as the go-to LAN technology. Token Ring, with its deterministic performance, offered advantages in specific scenarios, but its limitations ultimately led to its decline.

Q.2.a) Explain the concept of Multiplexing. How does Wavelength Division Multiplexing (WDM) differ from Frequency Division Multiplexing (FDM)?

Answer .:- Multiplexing is a technique that allows for the transmission of multiple signals over a single physical medium, maximizing its capacity. Imagine a highway with multiple lanes – each lane carries a separate stream of traffic (data) without interfering with the others.

There are different types of multiplexing, but two common ones are Frequency Division Multiplexing (FDM) and Wavelength Division Multiplexing (WDM).

FDM:

- Works like dividing a highway into lanes with designated frequencies (radio channels on a spectrum).
- Each signal is assigned a specific frequency range and modulated (encoded) onto a carrier wave within that range.
- Multiple signals with different carrier frequencies can be transmitted simultaneously without interference.
- Used in radio and television broadcasting, where different channels occupy distinct frequency bands.

WDM:

- Operates like using multiple colored lights on the same fiber optic cable.
- Each signal is modulated onto a different wavelength of light.
- Light pulses of various colors (wavelengths) can travel together on the same fiber without interacting.
- Primarily used in high-bandwidth fiber optic communication systems.

Key Differences:

- **Medium:** FDM works on electrical signals (radio waves), while WDM utilizes light pulses in fiber optics.
- **Division method:** FDM divides the available frequency spectrum, while WDM divides the light spectrum into distinct wavelengths.
- **Applications:** FDM is suitable for radio and TV broadcasting, while WDM is ideal for high-capacity data transmission in fiber optic networks.

Multiplexing helps us efficiently utilize communication channels by allowing multiple data streams to coexist. FDM and WDM achieve this by dividing

resources (frequency or wavelength) to create separate channels for independent data transmission.

Q.2.b) Explain in detail the different types of network topology used in computer networks.

Answer .:- The layout of devices and connections in a network is called its topology.

- **Bus Topology:** Imagine a single cable acting as a highway. All devices connect directly to this central bus. Data travels from one device to all others on the network. This is a simple and inexpensive setup, but prone to issues if the central cable fails or there's too much traffic.
- **Star Topology:** Devices connect to a central hub or switch, like spokes on a wheel. Data packets are sent directly to the intended recipient, reducing collisions compared to bus topology. This is the most common topology due to its scalability and ease of troubleshooting.
- **Ring Topology:** Devices are wired in a closed loop, forming a ring. Data travels in one direction around the ring, passing through each device. A token (special packet) controls access – only the device holding the token can transmit. This offers predictable performance, but a break in the ring disrupts the entire network.
- **Mesh Topology:** Devices connect to each other in a web-like fashion, creating multiple pathways for data to travel. This redundancy ensures reliability even if a connection fails. However, mesh networks are complex to set up and manage.
- **Hybrid Topology:** Combines different types to leverage their strengths. For example, a network might have a star topology for basic connections and a mesh topology for critical devices requiring extra redundancy.

Choosing the right topology depends on factors like network size, budget, desired performance, and scalability needs.

- Bus and star are good for smaller networks with moderate traffic.
- Star is the most versatile and widely used.
- Ring offers predictable performance but lower flexibility.
- Mesh is ideal for critical applications requiring high reliability.
- Hybrid provides a customized solution for specific needs.

Q.3.a) Explain the Internet Protocol (IP) and Transmission Control Protocol (TCP)

Answer .:- The internet relies on two key protocols working together to ensure reliable data delivery: Internet Protocol (IP) and Transmission Control Protocol (TCP).

IP (Internet Protocol):

- Acts like the postal service – it handles addressing and routing data packets across the internet.
- Assigns a unique IP address (like a street address) to every device connected to the internet.
- Works at the Network Layer (Layer 3) of the TCP/IP model.
- Breaks down data into packets and adds headers containing the source and destination IP addresses.
- Doesn't guarantee order or error-free delivery – it's a best-effort service.

TCP (Transmission Control Protocol):

- Ensures reliable data transmission – like a certified courier service.
- Operates at the Transport Layer (Layer 4) of the TCP/IP model.
- Establishes a connection between sender and receiver before data transfer.
- Sequentially numbers data packets and acknowledges their receipt.
- Retransmits missing or corrupted packets for error-free delivery.
- Guarantees data arrives in the correct order at the destination.

Working Together:

- When you request a web page, your computer breaks the data down into packets.
- TCP adds sequence numbers and establishes a connection with the web server.
- IP adds the IP addresses and routes the packets to the server.
- The server reassembles the packets and sends the data back using the same process.
- TCP ensures all packets arrive and are in order before delivering the complete webpage to your browser.
- IP handles addressing and routing data packets across the internet.
- TCP guarantees reliable data delivery by establishing connections, sequencing packets, and checking for errors.

Q.3.b) Explain the operation of Circuit Switching and Packet Switching. Discuss the advantages and disadvantages of each

Answer .:-

Data travels across networks using two main methods: circuit switching and packet switching. Let's delve into their operations, advantages, and disadvantages.

Circuit Switching:

Imagine a dedicated phone line – that's circuit switching in action. It establishes a temporary, exclusive connection between sender and receiver before data transmission begins.

- **Operation:**
    1. Sender requests a connection.
    2. Network establishes a dedicated path between sender and receiver.
    3. Data flows continuously over the dedicated circuit.
    4. Connection is terminated when communication ends.
- **Advantages:**
    - Guaranteed bandwidth: Consistent data flow with no interruptions.
    - Low latency: Ideal for real-time applications like voice calls.
    - Ordered delivery: Data arrives in the exact sequence it was sent.
- **Disadvantages:**
    - Inefficient for bursty traffic: Unused bandwidth during pauses is wasted.
    - Connection setup time: Delays communication initiation.
    - Scalability limitations: Difficult to accommodate many simultaneous connections.

Packet Switching:

Think of sending a letter – that's similar to packet switching. Data is broken down into smaller packets, each containing addressing information and the data itself. Packets travel independently over the network, taking the most efficient route.

- **Operation:**
    1. Data is divided into packets.
    2. Each packet is addressed and sent individually.
    3. Packets travel independently over the network, taking different paths.
    4. Packets are reassembled at the destination.

- **Advantages:**
  - Efficient bandwidth utilization: Shares bandwidth dynamically among users.
  - Scalability: Handles bursty traffic and many users efficiently.
  - No connection setup delay: Faster for short data transfers.
- **Disadvantages:**
  - Variable latency: Packets can arrive out of order, causing delays for reassembly.
  - Lower predictability: Performance can vary depending on network congestion.
  - More complex processing: Requires additional processing overhead for routing and reassembly.

SET - II

Q.4.a) Describe the operation of BGP in inter-domain routing. How does BGP differ from intra-domain routing protocols like OSPF and RIP?

Answer .:- **BGP: The Big Picture of Inter-Domain Routing**

The Border Gateway Protocol (BGP) is the kingpin of internet routing, handling traffic exchange between different autonomous systems (AS) – large networks like internet service providers (ISPs). Here's how it operates:

- **BGP Peers:** Routers at the edge of each AS establish peering sessions with routers from other ASes. These peers exchange routing information.
- **Path Attributes:** BGP goes beyond simple hop count (distance) like intra-domain protocols (OSPF, RIP). It considers various path attributes like network policy, load balancing, and even cost.
- **Best Path Selection:** BGP routers advertise their available routes to their peers. Each router analyzes the path attributes and selects the "best" route based on its configuration and policies. This allows for intelligent routing decisions.

BGP vs. Intra-Domain Routing Protocols:

Feature	BGP (Inter-Domain)	OSPF/RIP (Intra-Domain)
Scope	Between ASes	Within a single AS
Route selection	Based on policy & attributes	Primarily hop count
Configuration	More complex	Easier to configure
Convergence	Slower	Faster

Key Differences:

- **Scope:** BGP focuses on routing between different networks (ASes) on the internet. Intra-domain protocols handle routing within a single network.
- **Policy-based:** BGP allows for considering network policies and preferences when selecting routes, making it more flexible for inter-domain communication.
- **Complexity:** BGP configuration is more complex due to the need for policy definition and peering agreements.
- **Convergence:** BGP convergence (reaching a stable routing state) can be slower due to complex decision-making and information exchange between multiple ASes.

Q.4.b) Explain the concept of Integrated Service Digital Network (ISDN). How does Basic Rate Interface (BRI) differ from Primary Rate Interface (PRI)?

Answer .:- **ISDN: A Blast from the Past of Digital Communication**

Integrated Services Digital Network (ISDN) was an early attempt to provide digital communication services over traditional phone lines. It aimed to integrate voice, data, and video transmission on a single line, a significant leap from analog phone technology.

ISDN Channels:

ISDN utilizes two types of channels to carry information:

- **Bearer Channels (B-channels):** These handle digital data transmission at 64 kbps each. They can be used for voice calls, fax transmissions, or internet access.
- **D channel (Delta channel):** This lower-speed channel (16 kbps) is used for signaling and control purposes, managing call setup, data flow, and synchronization.

BRI vs. PRI: Catering to Different Needs

ISDN comes in two main flavors, catering to varying bandwidth requirements:

- **Basic Rate Interface (BRI):** The most common option for homes and small businesses. It provides two B-channels (128 kbps total) for simultaneous voice and data and one D-channel for control.
- **Primary Rate Interface (PRI):** Designed for high-volume users like businesses with heavy internet traffic. It offers 23 B-channels (1.47 Mbps total) for data and one D-channel for control. PRI can also be configured to bundle multiple B-channels for even higher bandwidth.

Key Differences:

Feature	BRI	PRI
Number of B-channels	2	23 (configurable)
Total Bandwidth	144 kbps	1.47 Mbps (or higher)
Ideal for	Homes, small businesses	Large businesses

ISDN's Decline:

While ISDN offered a step forward in digital communication, it faced limitations. Its bandwidth pales in comparison to modern technologies like cable or fiber internet. Additionally, complex setup and higher costs compared to traditional phone lines hampered its widespread adoption. Today, ISDN is being phased out in favor of more advanced solutions.

Q.5.a) Discuss the operation of the Simple Network Management Protocol (SNMP) in network management. How does SNMPv3 enhance security compared to SNMPv2?

Answer .:- **SNMP: Keeping Your Network in Check**

Simple Network Management Protocol (SNMP) is a workhorse protocol for network management. It allows administrators to monitor and manage network devices like routers, switches, and servers. Here's how it operates:

- **SNMP Entities:** Think of network devices as SNMP "entities" with an SNMP agent and potentially one or more SNMP managers.
- **Management Information Base (MIB):** Each device has a built-in MIB – a database containing information about its configuration, performance, and status.
- **SNMP Messages:** SNMP managers communicate with agents using Get, Set, and Trap messages.
    - **Get:** Retrieves specific data from the MIB.
    - **Set:** Modifies values within the MIB (changing configurations).
    - **Trap:** Alerts the manager about critical events on the device.

SNMP Versions and Security:

SNMP has evolved over time, with security being a major focus:

- **SNMPv1 and v2c:** These earlier versions offered weak security. They relied on community strings (like weak passwords) for authentication, making them vulnerable to eavesdropping and manipulation.
- **SNMPv3:** This version addressed the security concerns. It introduces:
    - **User-based Security Model (USM):** Enables user accounts with passwords and encryption for secure communication.
    - **Authentication:** Verifies the identity of the SNMP manager before allowing access.
    - **Encryption:** Scrambles data transmission to prevent eavesdropping.

Benefits of SNMPv3 Security:

- **Confidentiality:** Data exchanged between the manager and agent remains encrypted, protecting sensitive information.
- **Integrity:** Ensures data hasn't been tampered with during transmission.

- **Authentication:** Guarantees only authorized users can access and manage network devices.

SNMP provides a standardized way to monitor and manage network devices. While earlier versions lacked robust security, SNMPv3 offers a significant improvement by implementing user-based authentication, encryption, and data integrity checks, making network management more secure.

Q.5.b) Describe the ATM protocol architecture. How are virtual channel connections established in ATM networks?

Answer .:- **Unveiling ATM: Architecture and Virtual Connections**

Asynchronous Transfer Mode (ATM) was a cell-based switching technology designed for high-speed, low-latency data transfer.

ATM Architecture:

- **Layered Approach:** ATM operates on top of the Physical layer, providing its own higher-level functionalities.
- **Cells:** Data is segmented into fixed-size cells (53 bytes) for efficient transmission. Each cell has a header containing information like Virtual Path Identifier (VPI) and Virtual Channel Identifier (VCI) for routing.
- **Switches:** ATM switches route cells based on the VPI/VCI information in the header.

Virtual Connections:

ATM offers two types of virtual connections for data flow:

- **Virtual Path (VP):** Represents a logical path between two ATM end-points. It can carry multiple virtual channels, allowing for efficient bandwidth utilization for related traffic streams (e.g., voice and data for a single user).
- **Virtual Channel (VC):** Defines a unidirectional flow of data between two specific applications on the network. It's the basic unit for data transfer in ATM.

Establishing Virtual Connections:

1. **Signaling Protocol:** A separate signaling protocol (like Q.2931) negotiates the establishment and deletion of virtual connections.

2. **Connection Request:** The sender initiates the process by sending a connection request message containing desired VPI/VCI values and Quality of Service (QoS) parameters.
3. **Path and Channel Negotiation:** Network elements like switches negotiate the availability and configuration of the requested VPs and VCs along the path.
4. **Connection Confirmation:** Once a path is established and VC resources are allocated, a confirmation message is sent back to the sender, allowing data transfer to begin.

Benefits of Virtual Connections:

- **Scalability:** VPs can bundle multiple VCs, allowing efficient bandwidth allocation for diverse traffic types.
- **QoS Support:** ATM can prioritize traffic based on QoS parameters specified during connection setup.
- **Connection-Oriented:** Provides reliable data transfer once a connection is established.

Q.6) Discuss the requirements for Web Security and the role of Secure Socket Layer (SSL) in ensuring secure communication over the Internet.

Answer .:- **Web Security: A Fortress in the Digital Age**

The internet has revolutionized communication and commerce, but it also presents security risks. Sensitive information like credit card details and login credentials need protection as they travel across the web. This is where web security comes in, establishing a set of requirements to safeguard data and ensure a trusted online environment.

Essential Web Security Requirements:

- **Confidentiality:** Guarantees that only authorized users can access sensitive data. Imagine sending a confidential letter sealed with a wax stamp – only the intended recipient can open it.
- **Integrity:** Ensures that data remains unaltered during transmission. Think of a document with a digital signature – any changes would invalidate the signature, indicating tampering.

- **Authentication:** Verifies the identity of parties involved in communication. It's like checking someone's ID before granting them access to a secure area.
- **Non-repudiation:** Provides proof that a specific party sent or received a message. Imagine a signed receipt for a package – it confirms delivery and who received it.

SSL: The Encryption Guardian

Secure Sockets Layer (SSL), now succeeded by its more robust version, Transport Layer Security (TLS), plays a vital role in achieving these web security requirements. Here's how:

- **Encryption:** SSL establishes a secure tunnel between a web server and a user's browser. Data traveling within this tunnel is encrypted using a complex algorithm, making it unreadable to anyone intercepting it. This is like scrambling the message in your sealed letter, ensuring only the recipient with the decryption key can decipher it.
- **Digital Certificates:** SSL uses digital certificates issued by trusted authorities to verify the server's identity. These certificates act like electronic passports, guaranteeing you're communicating with the legitimate website and not a fraudulent one impersonating it.
- **Secure Communication Channels:** With SSL/TLS, communication between the browser and server is secured. This prevents eavesdropping, where attackers might try to steal information like login credentials or credit card details.

Benefits of SSL/TLS:

- **Protects Sensitive Information:** Encrypted data transmissions minimize the risk of unauthorized access to confidential details.
- **Builds Trust:** Verified server identities through digital certificates foster trust in online transactions.
- **Enhances Online Security:** Secure communication channels reduce the vulnerability of data to interception and manipulation.

Beyond SSL/TLS:

While SSL/TLS forms a strong foundation for web security, it's just one piece of the puzzle. Additional measures like strong passwords, user education on phishing attempts, and secure coding practices are crucial for comprehensive web security.