black N White

BLACK N WHITE

Learn Today Lead Tomorrow

jag...

NAME	
ROLL NUMBER	
SEMESTER	4th
COURSE CODE	DCA2201
COURSE NAME	COMPUTER NETWORKING

Q.1) Why is layered model used for computer networks? Explain OSI referenced model .

Answer .:-

In computer networks, a layered model is used to **simplify the design, implementation, and maintenance** of complex communication systems. The primary purpose of using a layered architecture is to **divide the entire networking process into smaller, manageable parts** or layers, where each layer handles a specific function and communicates only with its adjacent layers. This approach promotes **modularity**, allowing developers to make changes in one layer without affecting the entire system.

One major advantage of the layered model is that it supports **interoperability** between different hardware and software vendors. Since each layer follows a defined set of protocols and rules, devices from different manufacturers can communicate effectively if they adhere to the standard. Moreover, a layered model helps in **troubleshooting and debugging**, as network administrators can isolate problems by analyzing individual layers. It also provides **scalability and flexibility**, enabling the addition of new services or technologies without redesigning the entire network structure.

To implement these ideas, the **OSI (Open Systems Interconnection)** reference model was introduced by the **International Organization for Standardization (ISO)**. It is a conceptual framework that standardizes the functions of a telecommunication or computing system into **seven distinct layers**, from physical transmission to user interface.

The Seven Layers of the OSI Model:

1. **Physical Layer (Layer 1):**
   This layer is responsible for the actual transmission of raw bits over a physical medium such as cables, switches, and connectors. It defines hardware elements, signal modulation, and data rates.
2. **Data Link Layer (Layer 2):**
   It ensures **reliable transmission** of data frames between two nodes connected by a physical layer. It handles **error detection**, **correction**, and **flow control**. It includes protocols like Ethernet and PPP.
3. **Network Layer (Layer 3):**
   This layer manages **logical addressing** and routing of data across different networks. It determines the **best path** for data transfer using IP addresses. Protocols like IP, ICMP, and ARP operate here.
4. **Transport Layer (Layer 4):**
   It ensures **end-to-end communication**, reliability, and proper sequencing of data. Protocols like **TCP** and **UDP** function at this level to handle data segmentation and reassembly.
5. **Session Layer (Layer 5):**
   The session layer manages and controls the **dialogues (connections)** between computers. It establishes, maintains, and terminates sessions.
6. **Presentation Layer (Layer 6):**
   This layer is responsible for **data translation, encryption, and compression**. It acts as a translator between the application and the network format.

7. **Application Layer (Layer 7):**
   The topmost layer interacts directly with the user and provides **network services like email, file transfer, and web browsing** through protocols like HTTP, FTP, and SMTP.

   The layered approach of the OSI model not only organizes the network communication process but also promotes standardization, ease of development, and compatibility. It remains a foundational concept in networking despite the dominance of other models like TCP/IP.

Q.2) Discuss the working of stop and wait protocol in a noisy channel with the help of an example .

Answer .:-

The **Stop and Wait protocol** is one of the simplest flow control mechanisms used in data communication. It operates at the **data link layer** and ensures reliable transmission of frames between sender and receiver, especially in **noisy channels**, where errors can occur during data transfer.

In Stop and Wait, the sender **sends one frame at a time** and then **waits for an acknowledgment (ACK)** from the receiver before sending the next frame. If the sender does not receive an ACK within a certain **timeout period**, it assumes that either the frame or the ACK was lost or corrupted and **resends the same frame**. This process continues until the sender successfully receives the ACK.

Working in a Noisy Channel:

A **noisy channel** is a communication medium where **errors like data corruption, loss of frames, or damaged acknowledgments** can occur due to interference, hardware issues, or transmission faults.

Example:

Let’s consider a sender (S) and receiver (R) communicating over a noisy channel using the Stop and Wait protocol.

1. **S sends Frame 0 to R.**
   The frame is transmitted, and R receives it correctly.
2. **R sends ACK 0.**
   But due to noise, the ACK gets **lost** in the channel and doesn’t reach S.
3. **S waits for a timeout.**
   Since ACK 0 is not received in time, S **resends Frame 0** thinking it was lost.
4. **R receives Frame 0 again.**
   Now R has already processed Frame 0 earlier, but since Stop and Wait doesn’t include complex sequence handling, R **may process it again or discard it**, depending on implementation.
5. **R sends ACK 0 again.**
   This time, it reaches the sender successfully.
6. **S now sends Frame 1.**
   The process repeats.

Issues in Noisy Channel:

- If **frames or ACKs get corrupted**, the sender must **retransmit**, which causes **delays** and **reduces efficiency**.

- Duplicate frames may be received due to **lost ACKs**, so **sequence numbers (0 and 1)** are often used to identify duplicates.
- Only **one frame is in transit at any time**, which leads to **low channel utilization**, especially in long-distance communication.

Key Features:

- Simple and easy to implement.
- Reliable in handling **frame loss and errors**.
- Poor performance in high-latency or high-error environments due to frequent retransmissions and idle waiting time.

The Stop and Wait protocol provides a basic mechanism for **error control** in noisy channels by ensuring that every frame is acknowledged before sending the next. While it guarantees **reliable delivery**, its performance suffers in high-noise environments due to **retransmissions and idle time**. For better efficiency, more advanced protocols like **Sliding Window** are preferred in real-world systems.

Q.3) Give a contrast between unicast, multicast and broadcast. Also explain the way they implemented.

Answer .:-

In computer networking, **data transmission** can occur in different modes depending on the number of receivers and the method of data delivery. The three primary types are **Unicast**, **Multicast**, and **Broadcast**. Each of these modes serves a distinct purpose and is implemented differently.

1. Unicast

Definition:

Unicast is a **one-to-one communication** between a sender and a single receiver.

Example:

When you open a website in your browser, your system sends a unicast request to the server's IP address.

Working:

- The sender uses the **IP address of the specific receiver**.
- A **unique path** is established between the sender and the receiver.
- Only the target device processes the packet; others ignore it.

Implementation:

- Commonly used in **TCP/IP networks**.
  - Protocols like **TCP** and **UDP** support unicast.
  - Routers forward unicast packets based on **destination IP**.

2. Multicast

Definition:

Multicast is a **one-to-many** communication method where data is sent from one source to **multiple selected receivers** who have expressed interest in receiving the data.

Example:

Live video streaming or real-time stock market updates sent to subscribed users.

Working:

- The sender sends data to a **multicast group address**.
- Only devices that **join the group** receive the data.
- It avoids unnecessary traffic to uninterested nodes.

Implementation:

- Uses **Class D IP addresses** (224.0.0.0 to 239.255.255.255).
- Routers manage group memberships using protocols like **IGMP (Internet Group Management Protocol)**.
- Used in applications like **IPTV, conferencing, and video broadcasting**.

3. Broadcast

Definition:

Broadcast is a **one-to-all communication** where data is sent from one sender to **all devices** in the network segment.

Example:

When a device sends an ARP (Address Resolution Protocol) request to discover the MAC address of a given IP.

Working:

- The sender uses a **broadcast address**, such as 255.255.255.255 for IPv4.
- All devices on the local network **receive and process** the packet.

Implementation:

- Used in **local area networks (LANs)**.
- Broadcasts do not go beyond routers (i.e., they are **limited to subnet**).
- Protocols like **ARP, DHCP** use broadcasting.

Comparison Table:

Feature	**Unicast**	**Multicast**	**Broadcast**
Type	One-to-One	One-to-Many (selected)	One-to-All
Traffic Load	Medium	Low (to selected users)	High (to all devices)
IP Address Type	Unique IP	Multicast Group IP	Broadcast IP
Scope	Specific device	Subscribed devices	All devices in subnet
Usage Example	Web browsing	Live video streaming	ARP, DHCP

Unicast, multicast, and broadcast are essential data delivery methods in networking, each with its own advantages. **Unicast** is ideal for private communication, **multicast** is efficient for group-based services, and **broadcast** is best suited for network-wide announcements.

SET-II

Q.4) Explain various routing methods follow in network layer. Discuss their purpose in different environments.

Answer .:-

The **network layer** is responsible for the delivery of packets from the source to the destination across multiple networks. One of its key functions is **routing**, which determines the best path for data to travel. Different **routing methods** are used based on network size, topology, and performance requirements.

1. Static Routing

Definition:

In static routing, routes are manually configured by a network administrator. These routes do not change unless manually updated.

Purpose & Environment:

- Used in **small networks** with few devices and stable topology.
- Suitable where **minimal traffic changes** occur.
- Preferred for **predictable routing** and **tight control**.

Advantages:

- Simple and easy to implement.
- No routing overhead.

Disadvantages:

- Not scalable.
- Requires manual update in case of link failure.

2. Dynamic Routing

Definition:

Dynamic routing uses **routing protocols** that automatically adjust routes based on network conditions such as traffic load or failures.

Purpose & Environment:

- Ideal for **large and complex networks**.
- Used in **enterprise and ISP-level infrastructures**.
- Provides **fault tolerance and adaptability**.

Examples of Protocols:

- RIP (Routing Information Protocol)
- OSPF (Open Shortest Path First)
- EIGRP (Enhanced Interior Gateway Routing Protocol)

Advantages:

- Automatically updates routes.
- Adapts to changes in real time.

Disadvantages:

- Consumes bandwidth for updates.
- More complex configuration.

3. Default Routing

Definition:

Default routing is used when a router sends packets to a **default route** when no specific route is found in the routing table.

Purpose & Environment:

- Used in **small or stub networks** where there is only one exit point to the internet or another network.
- Common in **home or branch offices**.

Advantages:

- Reduces routing table size.
- Easy to configure.

Disadvantages:

- Not optimal for multiple exit paths.

4. Hierarchical Routing

Definition:

Hierarchical routing organizes routers in **levels or layers**, like core, distribution, and access layers.

Purpose & Environment:

- Common in **large enterprise networks**.
- Reduces complexity and increases manageability.

Advantages:

- Scalable and structured.
- Easy fault isolation and management.

Disadvantages:

- Needs proper planning.
- Slightly complex to implement initially.

5. Adaptive Routing (Adaptive Algorithms)

Definition:

Adaptive routing dynamically adjusts the routing decisions based on **current network conditions** like traffic congestion, link failure, or delay.

Purpose & Environment:

- Used in **mission-critical systems**, **military**, and **real-time communication**.

Advantages:

- Optimized performance.
- Real-time response to issues.

Disadvantages:

- High processing requirements.
- May create routing loops if not designed well.

Different routing methods serve specific purposes in networking. **Static routing** is best for small, stable networks, while **dynamic and adaptive routing** support larger, constantly changing environments. **Default routing** simplifies configuration in edge networks, and **hierarchical routing** supports large, multi-layered systems. Choosing the right method ensures **efficiency, reliability, and scalability** in data communication.

Q.5) Explain the process of controlling congestion in the transport layer in detail with the help of examples.

Answer .:-

In computer networks, **congestion** occurs when the amount of data sent to the network exceeds its capacity. This leads to **packet loss, delays, and degraded performance**. The **transport layer**, especially in protocols like TCP, plays a vital role in detecting and controlling congestion to ensure smooth data transmission.

What is Congestion?

Congestion refers to a situation where **too many packets** are present in the network, especially in routers or switches, causing **buffer overflow** and **packet drops**. It usually happens when multiple devices send data at high rates simultaneously.

Congestion Control Techniques in the Transport Layer

1. Slow Start

Purpose:

To gradually increase the rate of data transmission to avoid sudden overload.

How it works:

- The sender begins by sending **one segment** (usually 1 MSS - Maximum Segment Size).
- For each acknowledgment (ACK) received, the **congestion window (cwnd)** doubles.
- This continues until a threshold is reached or packet loss occurs.

Example:

If a sender starts with cwnd = 1 MSS, then next it becomes 2 MSS, then 4 MSS, then 8 MSS, and so on — until a limit or loss is encountered.

2. Congestion Avoidance

Purpose:

To maintain a stable flow once the network is near capacity.

How it works:

- After reaching a **slow start threshold (ssthresh)**, TCP increases **cwnd linearly** rather than exponentially.
- This avoids sudden congestion.

Example:

After cwnd reaches 16 MSS, instead of doubling to 32, it increases gradually to 17, 18, 19…

3. Fast Retransmit and Fast Recovery

Purpose:
To recover quickly from packet loss without restarting slow start.

How it works:

- If three duplicate ACKs are received (indicating a lost packet), TCP **immediately retransmits** the lost segment (Fast Retransmit).
- Instead of going back to 1 MSS, cwnd is reduced to **half of its size** (Fast Recovery), and grows linearly from there.

Example:
If cwnd was 20 MSS, and loss is detected, it reduces to 10 MSS instead of 1.

4. Explicit Congestion Notification (ECN)

Purpose:
To notify the sender of impending congestion **without dropping packets**.

How it works:

- Routers mark packets when congestion is about to happen.
- The receiver sees this mark and notifies the sender via TCP.
- The sender then reduces the sending rate.

Example:
Rather than discarding a packet, the router sets a **congestion bit**, prompting the sender to slow down.

Why is Congestion Control Important?

- Prevents **packet loss** and **network collapse**.
- Ensures **fairness** among multiple users.
- Helps maintain **high throughput** and **low latency**.

Congestion control in the transport layer is essential for **efficient and reliable data delivery**. Techniques like **slow start, congestion avoidance, fast retransmit**, and **ECN** ensure that the sender adapts to network conditions. By controlling the data flow intelligently, the transport layer ensures smooth communication even in heavily loaded networks.

Q.6) Compare between the lossy and lossless compression. Discuss the tradeoff between these.

Answer .:-

Compression is a process of reducing the size of data or files to save space or transmission time. It is mainly of two types:

1. **Lossy Compression**
2. **Lossless Compression**

Let's break down both methods to understand the key differences:

1. Lossy Compression

Definition:
In **lossy compression**, some data is lost during the compression process. The aim is to reduce file size by discarding some of the data, typically the parts that are least noticeable or less important. Once the data is compressed, it cannot be restored to its original form.

Characteristics:

- Significant **reduction in file size**.
- **Data loss** occurs, meaning the original quality is compromised.
- Common in **audio, image, and video files** (e.g., MP3, JPEG, MPEG).

Examples:

- **MP3 (audio)**: Some frequencies are removed based on human hearing limitations.
- **JPEG (image)**: Removes color details and textures that may not be noticeable to the human eye.
- **MPEG (video)**: Compresses video by reducing redundancy and ignoring less important visual details.

Advantages:

- **High compression ratios** (smaller file size).
- **Faster transmission** due to reduced file size.

Disadvantages:

- **Loss of quality** (irreversible).
- **Artifacts** like blurriness, distortion, or pixelation in images or videos.

2. Lossless Compression

Definition:
In **lossless compression**, no data is lost. The file can be perfectly reconstructed back to its original form after decompression. The goal is to reduce file size while preserving the full quality of the original data.

Characteristics:

- No **data loss**.
- Results in a **lower compression ratio** than lossy compression.
- Used in formats where **quality preservation** is critical (e.g., PNG, FLAC, ZIP).

Examples:

- **ZIP** files (for general file compression).
- **PNG (image)**: Maintains quality while reducing file size.
- **FLAC (audio)**: Compresses audio without losing any information.

Advantages:

- **No quality loss**, original data is preserved.
- Ideal for **archiving** and **textual data** where integrity is crucial.

Disadvantages:

- **Lower compression ratios** (files remain larger than lossy-compressed files).
- **Slower compression and decompression** speeds in some cases.

Trade-offs Between Lossy and Lossless Compression

Aspect	Lossy Compression	Lossless Compression
File Size	Smallest file size (high compression)	Larger file size compared to lossy
Data Integrity	Some data is lost; not recoverable	No data loss; perfect original file recovery
Compression Ratio	High (usually 70%-90% reduction)	Lower (typically 30%-60% reduction)
Quality	Reduced quality (depends on compression level)	No loss in quality
Use Case	Audio, video, streaming, web images	Archiving, documents, professional audio and images
Speed	Faster compression and decompression	Slower compression and decompression

Trade-offs:

- **File Size vs. Quality:**
  Lossy compression offers **smaller file sizes** at the cost of **quality loss**, while lossless compression preserves the **original quality** but at the expense of a larger file size.
- **Speed vs. Storage:**
  Lossy compression generally provides **faster processing** (both compression and decompression) because it reduces data by discarding less important information. Lossless compression, on the other hand, might be **slower** but ensures **complete data integrity**.
- **Application Choice:**
  Lossy compression is ideal for media such as music, movies, and web images where a slight degradation in quality is acceptable to save space. Lossless compression is perfect for applications like text documents, legal files, and images where **no loss of data** is acceptable.

The choice between **lossy** and **lossless compression** depends on the **purpose of the compression** and the importance of file **quality** versus **size**. **Lossy compression** is suitable when file size reduction is more important than preserving every bit of data (e.g., in streaming or multimedia), whereas **lossless compression** is ideal when the integrity of the data is critical, such as in professional and archival uses.