Certainly! Here are the duties provided by the network layer in brief for 3 marks:

1. Addressing and Routing: Assigning unique addresses and determining the best path for data transmission.
2. Packet Encapsulation and Fragmentation: Packaging data into packets and breaking them into smaller units if needed.
3. Network Congestion Control: Monitoring and regulating traffic to prevent congestion and ensure efficient resource utilization.

Different Types of Data Communication:
1. Unicast: Communication between a single sender and a single receiver.
2. Multicast: Communication between a single sender and multiple receivers.
3. Broadcast: Communication from a single sender to all devices on a network.
4. Anycast: Communication to the nearest or most appropriate destination among a group of potential receivers.

Difference between Frames and Packets:
Frames:
- Used in data link layer.
- Contains control information like source and destination MAC addresses.
- Provides error detection and correction mechanisms.
- Transmitted over the physical network.

Packets:
- Used in network layer.
- Contains control information like source and destination IP addresses.
- Provides routing information to reach the destination.
- Transmitted over a network as a series of frames.

Format of Physical Address (MAC Address) with an Example:
A physical address, also known as a Media Access Control (MAC) address, is a unique identifier assigned to a network interface controller (NIC) by the manufacturer. It is a six-byte address expressed in hexadecimal notation. Here's an example of a MAC address: 00:1A:2B:3C:4D:5E.

Different Services provided by PPP Protocol:
The Point-to-Point Protocol (PPP) is a data link layer protocol used to establish a direct connection between two network nodes. It provides several services, including:
1. Authentication: Verifies the identity of the connecting devices.
2. Encryption: Ensures secure transmission of data.
3. Compression: Reduces the size of data for more efficient transmission.
4. Error Detection: Identifies and corrects transmission errors.
5. Multi-Protocol Support: Accommodates various network protocols, such as IP, IPX, and AppleTalk.

Packet Switching Technique:
Packet switching is a network transmission technique where data is divided into small packets before transmission. Each packet is individually addressed and routed across the network independently. The key characteristics of packet switching are:
1. Packets are independently routed based on the destination address.
2. Multiple packets can be transmitted simultaneously.
3. Packets can take different paths to reach the destination.
4. Packets are reassembled at the receiving end to reconstruct the original data.

Please note that the response provided here is aimed at addressing the question within the given word limit for 3 marks, and more elaborate explanations can be provided if needed.

Q1: Draw OSI reference model and explain the function of each layer (8 marks)

OSI Reference Model:

```
+-------------+
|  Application |
+-------------+
|  Presentation|
+-------------+
|   Session   |
+-------------+
|  Transport  |
+-------------+
|   Network   |
+-------------+
|  Data Link  |
+-------------+
|   Physical  |
+-------------+
```

1. Application Layer: Provides interfaces and protocols for user applications to communicate with the network. It enables services such as file transfer, email, and web browsing.

2. Presentation Layer: Handles data formatting, encryption, and compression. It ensures that data from the application layer can be properly interpreted by the receiving application.

3. Session Layer: Establishes, manages, and terminates communication sessions between applications. It provides functions like session checkpointing and recovery.

4. Transport Layer: Ensures reliable and efficient data transfer between hosts. It handles end-to-end error recovery, flow control, and segmentation/reassembly of data.

5. Network Layer: Responsible for logical addressing and routing of data packets. It determines the best path for data to reach the destination across different networks.

6. Data Link Layer: Provides error-free transmission of data frames between adjacent nodes on a network. It handles framing, error detection, and medium access control.

7. Physical Layer: Transmits raw bitstream over physical media. It defines the electrical, mechanical, and procedural aspects of communication.

The OSI model provides a structured framework for understanding and designing network protocols and enables interoperability between different network devices and technologies.

Q2: Describe WAN and MAN networks with a diagram and compare them (7 marks)

WAN (Wide Area Network):
- Covers a large geographical area, such as a city, country, or even globally.
- Uses public or private telecommunication networks to connect multiple LANs or other WANs.
- Typically owned and operated by service providers.
- Example: Internet

MAN (Metropolitan Area Network):
- Covers a smaller geographical area, such as a city or town.
- Connects multiple LANs within the same metropolitan area.
- Operated by private or public organizations.
- Example: Cable TV network

Comparison:
1. Geographical Coverage: WAN covers a larger area than MAN.
2. Ownership and Operation: WAN is typically owned and operated by service providers, while MAN can be owned by private or public organizations.
3. Connectivity: WAN connects multiple LANs across different regions or countries, while MAN connects LANs within the same metropolitan area.
4. Technologies: WAN uses various technologies like leased lines, fiber optics, and satellite links. MAN can use technologies like Ethernet, SONET, or wireless connections.
5. Speed and Bandwidth: WAN generally offers higher bandwidth and faster speeds compared to MAN due to the larger-scale infrastructure.
6. Cost: WAN infrastructure and connectivity are more expensive compared to MAN.
7. Examples: The Internet is an example of a WAN, while a cable TV network can be an example of a MAN.

Q3: Define bridge used in computer networks and explain the types of bridges (8 marks)

Bridge:
- A bridge is a network device that connects two or more separate network segments or LANs, allowing them to communicate with each other.
- It operates at the data link layer (Layer 2) of the OSI model.

Types of Bridges:
1. Transparent Bridge: Transparent bridges operate without any configuration. They learn and store MAC addresses from the connected networks and use this information to make forwarding decisions. They are commonly used to connect LAN segments.
2. Source Routing Bridge: Source routing bridges rely on information provided by the sender to determine the path for forwarding data. The sender specifies the complete route the packet should follow, and the bridge follows the given instructions

.
3. Learning Bridge: Learning bridges dynamically learn the MAC addresses of devices connected to their ports by analyzing the source addresses of received frames. They maintain a forwarding table to determine the destination port for each MAC address.
4. Source-Route Transparent (SRT) Bridge: SRT bridges combine the functionality of source routing and transparent bridges. They can handle source-routed frames and also function as transparent bridges for non-source-routed frames.

Bridges are used to increase the size and reach of networks, improve network performance, and segment LANs to enhance security and reduce collisions in Ethernet-based networks.

Q4: Differentiate between a switch and a router in detail (7 marks)

Switch:
- Operates at the data link layer (Layer 2) of the OSI model.
- Used to connect multiple devices within a network, such as computers, printers, and servers.
- Switches use MAC addresses to forward data packets to the appropriate destination.
- They provide high-speed data transfer within a LAN and perform frame forwarding based on MAC addresses.
- Switches improve network performance by reducing collisions and enabling simultaneous communication between multiple devices.
- They create separate collision domains for each port, increasing network efficiency.
- Switches are not aware of IP addresses and do not perform routing functions.

Router:
- Operates at the network layer (Layer 3) of the OSI model.
- Connects different networks together, such as LANs, WANs, or the Internet.

- Routers use IP addresses to forward data packets between networks.
- They make intelligent routing decisions based on network protocols, routing tables, and metrics.
- Routers perform functions like path determination, packet forwarding, and network address translation (NAT).
- They provide interconnectivity and route packets based on destination IP addresses.
- Routers can perform network segmentation, filtering, and security functions.
- They are capable of connecting networks with different protocols and have built-in firewall capabilities.

In summary, switches focus on connecting devices within a network and forwarding data based on MAC addresses, while routers handle the interconnection of different networks and forward data based on IP addresses, performing more complex routing functions.

Q4: Compare radio wave and microwave transmission media of the physical layer (8 marks)

Radio Wave:
- Uses electromagnetic waves in the frequency range of 3 kHz to 300 GHz.
- Can be used for wireless communication, including FM/AM radio, Wi-Fi, Bluetooth, and cellular networks.
- Radio waves have longer wavelengths and lower frequencies compared to microwaves.
- They have lower bandwidth and are more susceptible to interference and signal attenuation.
- Radio waves have a longer range and can propagate through obstacles like buildings and vegetation.
- Suitable for long-range communication but generally have lower data transfer rates.

Microwave:
- Uses electromagnetic waves in the frequency range of 300 MHz to 300 GHz.
- Often used in point-to-point communication, such as microwave links and satellite communication.
- Microwaves have shorter wavelengths and higher frequencies compared to radio waves.
- They have higher bandwidth and can support higher data transfer rates.
- Microwaves are more susceptible to atmospheric interference and obstacles like buildings and trees.
- Suitable for medium-range communication with higher data transfer rates.

In summary, radio waves are suitable for long-range wireless communication with lower data transfer rates, while microwaves provide higher bandwidth and data rates but are more affected by interference and obstacles.

Q4: Briefly explain the coaxial cable with a diagram (7 marks)

Coaxial Cable:

- A coaxial cable is a type of transmission medium consisting of a central conductor, an insulating layer, a metallic shield, and an outer insulating layer.
- It is commonly used in networking, cable television, and broadband connections.
- The central conductor carries the signal, surrounded by an insulating layer (dielectric) that prevents signal leakage and interference.
- The metallic shield acts as a ground and protects against external electromagnetic interference.
- The outer insulating layer provides further insulation and physical protection.

Diagram:

```
   Outer Insulating Layer
         |              (Plastic or Rubber)
         |
   Metallic Shield      (Braided or Foil)
         |
    Insulating Layer    (Dielectric)
         |
    Central Conductor   (Copper or Aluminum)
```

Coaxial cables provide high bandwidth and are capable of carrying both analog and digital signals. They offer better protection against interference compared to twisted pair cables.

Q5: Different sublayers of the Data Link Layer (DLL) and their functions (8 marks)

1. Logical Link Control (LLC) Sublayer:
- Provides interface between the MAC layer and the network layer.
- Handles flow control, error control, and sequencing of frames.
- Defines protocols for establishing, maintaining, and terminating data links.

2. Media Access Control (MAC) Sublayer:
- Controls access to the physical medium and manages data transmission.
- Handles addressing and synchronization between devices.
- Implements medium access control protocols like CSMA/CD (Ethernet) or CSMA/CA (Wi-Fi).

The DLL sublayers work together to ensure reliable and efficient data transfer across the data link layer.

Q5: Comparison of Pure ALOHA and Slotted ALOHA (7 marks)

Pure ALOHA:
- A random access protocol for shared communication channels.

- Stations transmit data whenever they have it, without checking for collisions.
- Collisions can occur if multiple stations transmit simultaneously, causing data loss.
- Stations perform a retransmission after a random time interval.
- Pure ALOHA has lower efficiency due to frequent collisions and resulting retransmissions.

Slotted ALOHA:
- Improves the efficiency of Pure ALOHA by dividing time into discrete slots.
- Stations transmit data only at the beginning of each time slot.
- Collisions can still occur, but the probability is reduced compared to Pure ALOHA.
- Stations perform retransmissions based on specific

time slots.
- Slotted ALOHA provides better channel utilization and efficiency compared to Pure ALOHA.

In summary, Pure ALOHA allows random transmission, resulting in frequent collisions, while Slotted ALOHA introduces time slots for synchronized transmission, reducing collision probability and improving efficiency.

Q6:
1) Two main protocols of the transport layer are:
- Transmission Control Protocol (TCP)
- User Datagram Protocol (UDP)

Explanation of TCP:
- TCP is a reliable and connection-oriented protocol.
- It provides a reliable data delivery mechanism through features like flow control, error detection, and retransmission of lost packets.
- TCP ensures that data is delivered in the correct order and without errors.
- It establishes a connection between sender and receiver before data transmission and releases the connection after communication.
- TCP implements a sliding window mechanism for flow control, allowing the sender to adjust the rate of data transmission based on the receiver's capacity.
- It uses acknowledgments and sequence numbers to ensure reliable and ordered delivery of data.
- TCP is widely used in applications such as web browsing, email, file transfer, and other applications that require reliable data delivery.

Q6:
2) WWW (World Wide Web) and its Architecture:

- The World Wide Web (WWW) is a system of interconnected hypertext documents accessible over the Internet.

- It is based on the client-server model, where clients (web browsers) request and retrieve information from web servers.
- The architecture of the WWW consists of three main components: web browsers, web servers, and web documents.

1. Web Browsers:
- Web browsers, such as Google Chrome, Mozilla Firefox, or Safari, are client applications used to access and view web content.
- They interpret and render HTML, CSS, and JavaScript to display web pages to users.
- Web browsers send HTTP requests to web servers and receive HTTP responses containing the requested web content.

2. Web Servers:
- Web servers are computers or systems that host websites and web applications.
- They store and serve web documents to client browsers upon request.
- Web servers receive HTTP requests from clients and send HTTP responses with the requested content.
- Popular web server software includes Apache HTTP Server, Nginx, and Microsoft IIS.

3. Web Documents:
- Web documents are files containing HTML, CSS, JavaScript, images, videos, and other resources that make up a web page.
- Web documents are stored on web servers and accessed by clients through URLs (Uniform Resource Locators).
- Hyperlinks within web documents enable navigation and linking to other web pages.

The WWW architecture allows users to access and navigate through interconnected web pages using hyperlinks. Clients (web browsers) make HTTP requests to servers, which respond with the requested web documents, enabling users to browse and interact with web content.

Q7: Short notes

1) Link State Routing Algorithm:
- Link State Routing Algorithm is a dynamic routing algorithm used by routers to exchange information about network topology.
- Each router constructs a complete map of the network by collecting information about its directly connected links and advertising this information to other routers.
- The routers exchange link state packets (LSPs) to build a consistent view of the network's topology.
- Based on the collected information, each router calculates the shortest path to reach destination networks using algorithms like Dijkstra's algorithm.
- Link State Routing Algorithm provides accurate and up-to-date routing information, but it requires more memory and processing power compared to distance vector algorithms.

2) HTTP protocol:

- HTTP (Hypertext Transfer Protocol) is a protocol used for communication between web browsers and web servers.
- It is the foundation of data communication on the World Wide Web.
- HTTP follows the client-server model, where clients (web browsers) send requests to web servers, and servers respond with requested content.
- HTTP uses a request-response model, where a client sends an HTTP request, and the server sends back an HTTP response.
- It operates on top of TCP/IP and uses port 80 for communication.
- HTTP supports various methods (GET, POST, PUT, DELETE) to perform different actions on web

 resources.
- HTTP is a stateless protocol, meaning each request is independent of previous requests, and servers do not maintain client state between requests.

3) Flooding:

- Flooding is a network communication technique where a message is sent to all network nodes without considering the network topology.
- In flooding, a node broadcasts a message to all its neighboring nodes, which further broadcast the message to their neighbors, and so on.
- Flooding is often used in network protocols for tasks like network discovery, broadcasting updates, or distributing routing information.
- While flooding ensures message delivery to all nodes, it can lead to excessive network traffic and can cause broadcast storms and duplication of messages.
- To prevent endless looping and reduce traffic, network protocols implementing flooding may use mechanisms like hop count limits or sequence numbers to control message propagation.