

Name - Akshat Negi

Sap ID: → 500106533

Roll No. → 2142880414

Subject: Data
communication and
Networks.

Assignment:

Q1. Identify and explain the key IEEE Standards for LAN and WAN.

Ans1. The IEEE (Institute of Electrical and Electronics Engineers) defines several standards to ensure interoperability and performance in LAN (Local Area Network) and WAN (Wide Area Network) systems. The most prominent standards for LAN are IEEE 802.3 and IEEE 802.11. IEEE 802.3 defines Ethernet, the foundation of most wired LANs, specifying physical layer and MAC layer operations, including speeds ranging from 10 Mbps to multi-Gbps. IEEE 802.11, commonly associated with WiFi, governs wireless LANs, supporting features like multiple frequency bands and secure access protocols. For WAN technologies, IEEE has indirectly influenced through standards such as IEEE 802.16 (WiFi MAX) for Metropolitan area networks, enabling broadband access over large distances. These standards ensure compatibility, scalability and reliability forming the backbone of modern communication networks.

Q2. Role of SNMP and RMON in Network Management.

A&2. Simple Network Management Protocol (SNMP) and Remote Network Monitoring (RMON) are critical tools for efficient network management. SNMP, a widely used protocol, facilitates the monitoring and management of devices in an IP network by collecting and organizing network data such as bandwidth usage, device status, and errors. It operates through agents and a central manager, enabling real-time troubleshooting and network optimization. RMON, an extension of SNMP, provides detailed network statistics and monitoring capabilities. It allows administrators to analyze traffic patterns, identify bottlenecks and monitoring anomalies at different network segments. Together, SNMP and RMON enhance network visibility, reduce downtime and ensure optimal performance by enabling proactive and comprehensive network management.

Q3. Write a short note on ICMP in about 150 words.

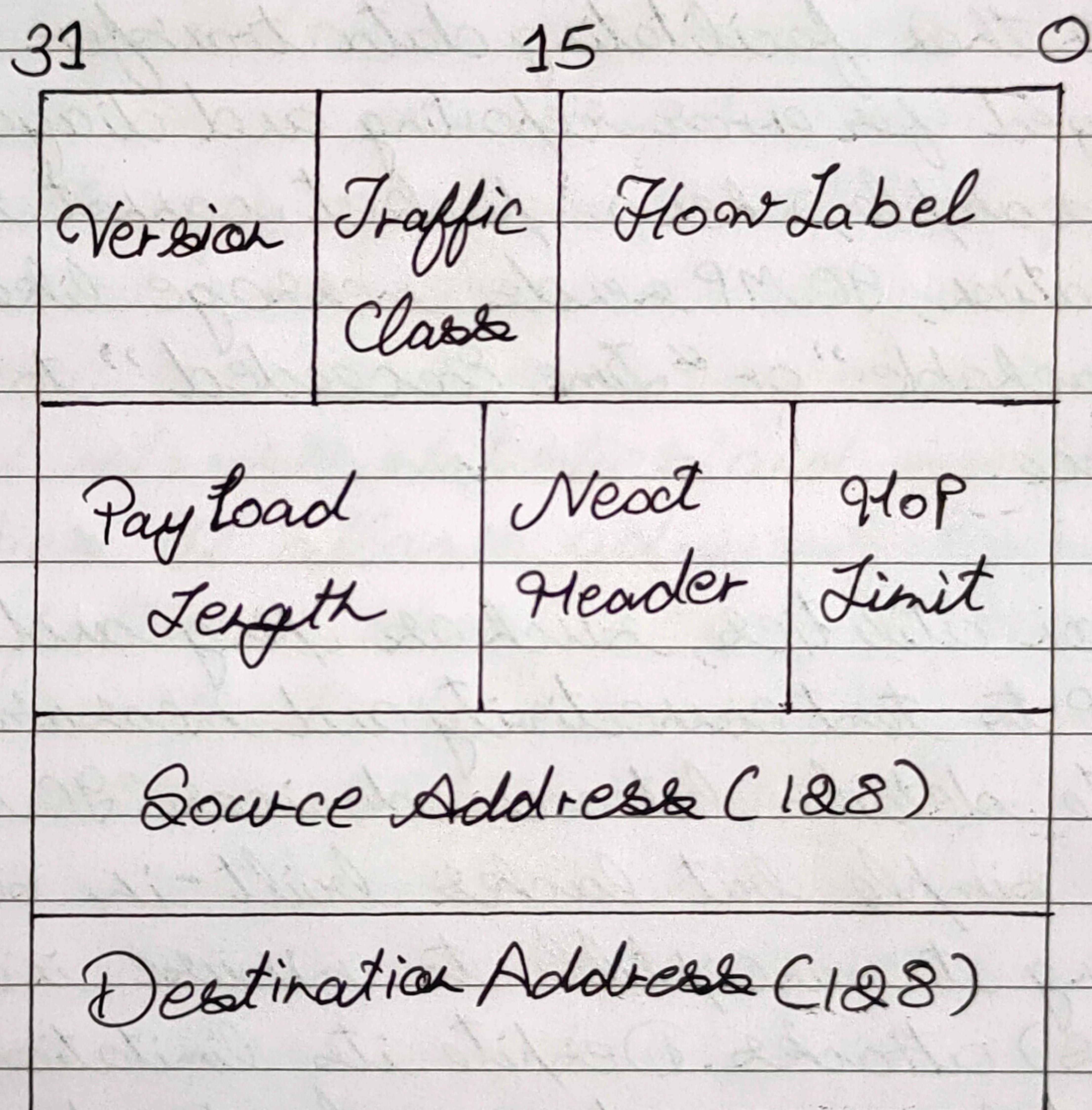
Ans.3. The Internet Control Message Protocol (ICMP) is a vital network layer protocol used for diagnosing and managing network performance in IP-Based systems. It operates as a control protocol, primarily providing feedback about issues in the communication environment rather than facilitating data transfer. ICMP is a widely employed for error reporting and diagnostic functions. For example, when a packet cannot reach its destination, ICMP sends message like "Destination unreachable" or "Time Exceeded" to notify the source.

Common utilities, such as ping and traceroute, use ICMP to test connectivity and measure latency or route details between devices. ICMP is lightweight and simple but lacks built-in security features, making it susceptible to misuse in denial-of-service (DoS) attacks. Despite its limitations, ICMP remains essential for maintaining robust network operations by enabling fault isolation and improving overall communication efficiency.

Q4. Draw and discuss in brief about the IPv6 datagram header format and write a table of comparison between IPv4 and IPv6 header's format.

Ans4.

IPv6 Header Format



It features the fixed size of 40 bytes.

- 1) Version: (4 bits) indicates the IP version (6 for IPv6)
- 2) Traffic Class (8 bits) specifies packet priority.
- 3) Flow Label (20 bits) identifies traffic flows requiring special handling.

- 4) Payload Length (16 bits) length of data following the header.
- 5) Next Header (8 bits) identifies the type of the next header.
- 6) Hop Limit (8 bits) replaces the TTL field of IPv4, indicating the maximum number of hops.
- 7) Source Address (128 bits) IPv6 address of the sender.
- 8) Destination Address (128 bits) IPv6 address of receiver.

Comparison between IPv4 and IPv6

Features	IPv4 Header	IPv6 Header
Header Length	Variable (20 - 60 bytes)	Fixed (40 bytes)
Address Size	32 bits	128 bits
Fragmentation	Handled in header	Moved to extension headers
Checksum	Present	Removed (handled by above layers)
Security	No strict security features	Support IPsec by default
Efficiency	Complex and less efficient	Simplified for faster processing.

Q5. Write a short note on key Application Layer Protocols:

- 1) WWW (World Wide Web): The WWW is a global system of interconnected documents and multimedia content accessible via the internet. It uses HTTP to transfer web pages and hyperlinks to connect information. It enables user-friendly access to resources through browsers.
- 2) Hypertext Transfer Protocol (HTTP): HTTP is the primary protocol for transferring hypertext documents on the web. It uses a request-response model between clients and servers and supports stateless communication, often paired with HTTPS for secure data transfer.
- 3) File Transfer Protocol (FTP): FTP is a protocol for transferring files between devices over a network. It uses separate control and data connections for efficient communication. Though secure alternatives like SFTP are preferred today, FTP remains widely used.
- 4) Domain Name System (DNS): DNS translates human-readable domain names into IP addresses, enabling devices to locate and connect with servers. It acts as the internet's phonebook.