Basics of Networking

Computing for Internet of Things

Dr. Arijit Roy

Overview

Introduction

- Present era of data and information-centric operations, everything – starting from agriculture to military operations – relies heavily on information.
- The goodness of any particular information is as good as the variety and strength of the data, which generates this information.
- Networking refers to the networking of computers and communication network devices (also referred to as hosts), which interconnect through a network (Internet or Intranet) and are separated by unique device identifiers (IP addresses and MAC addresses).
- These hosts may be connected by a single path or through multiple paths for data sending and receiving.
- The data transferred between the hosts may be text, images, or videos, which are typically in the form of binary bit-streams.

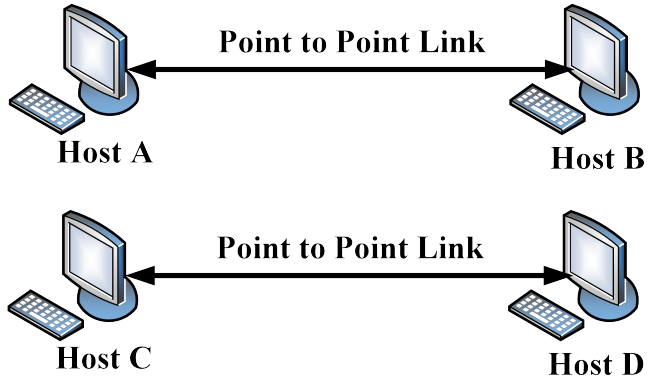
Network Types

Computer networks are classified according to -

- Type of Connection,
- Physical Topology,
- Reach of the Network.

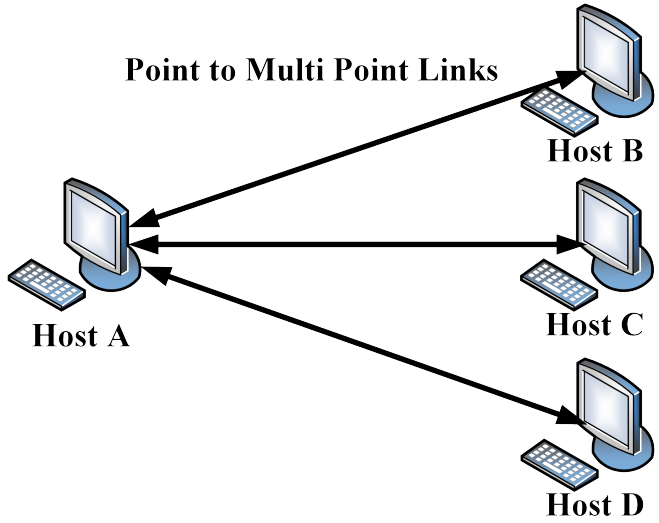
These classifications are helpful in deciding the requirements of network setup and provides insights into the appropriate selection of a network type for the setup.

Point to Point connection



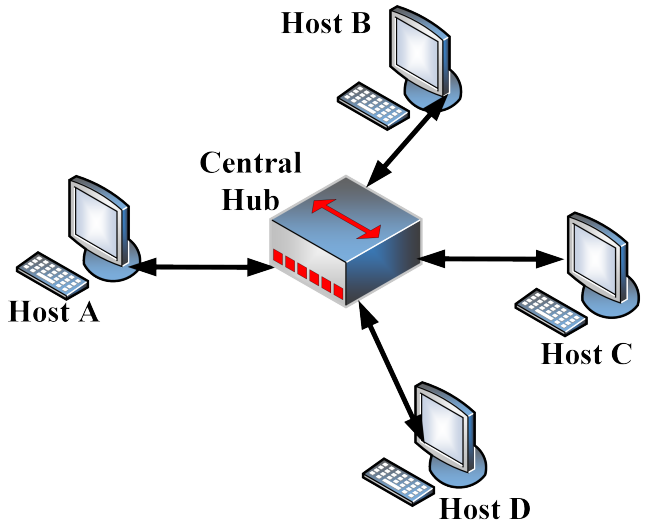
- Point to point connections are used to establish direct connections between two hosts.
- These networks were designed to work over duplex links, and are functional for both synchronous as well as asynchronous systems.
- Regarding computer networks, point to point connections find common usage for specific purposes such as in optical networks.

Point to Multipoint connection



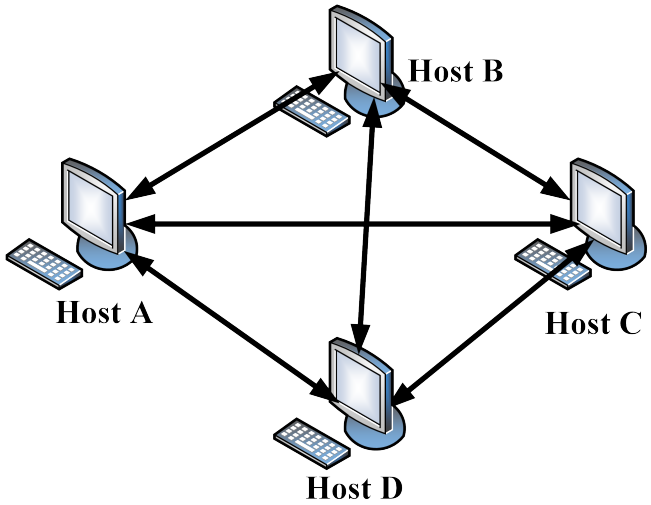
- More than two hosts share the same link. This configuration is similar to the one-to-many connection type.
- These types of connections find popular use in wireless networks and IP telephony.
- The channel is shared between the various hosts, either spatially (FDMA) or temporally (TDMA).

Star Topology



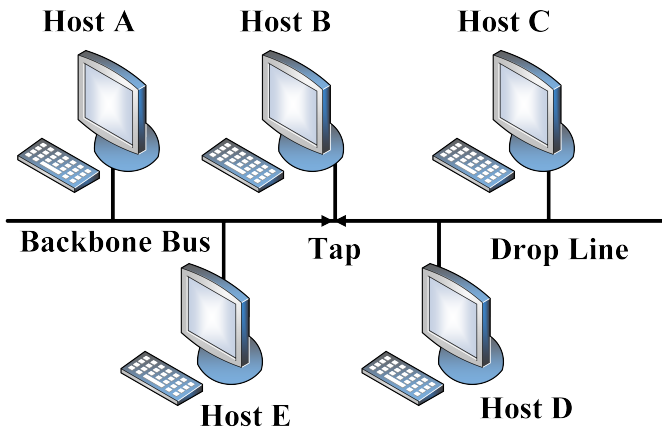
- For large-scale systems, the hub has to be essentially a powerful server to handle all the simultaneous traffic flowing through it.
- As there are fewer links (only one link per host), this topology is cheaper and easier to set up.
- The main advantage of the star topology is the easy installation of this network and the ease of fault identification within this network.

Mesh Topology



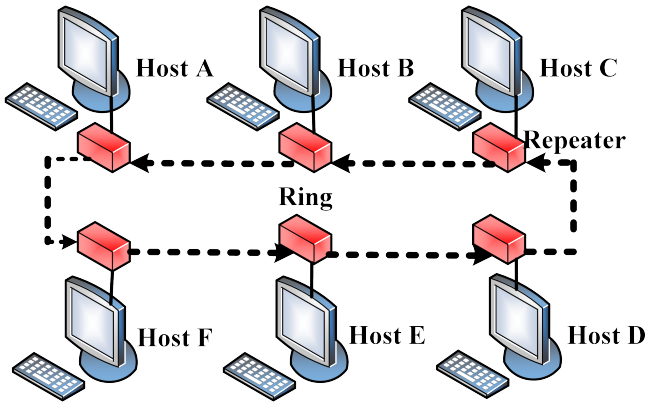
- This massive number of links makes this topology expensive.
- Allows for robustness and resilience of the system. Even in case a link is down or broken, the network is still fully functional as there remain other pathways for the traffic to flow through.

Bus Topology



- A backbone cable or bus serves as the primary traffic pathway between the hosts. The hosts are connected to the main bus employing drop lines or taps.
- The main advantage of this topology is the ease of its installation.
- There is a restriction on the length of the bus and the number of connections that can be simultaneously connected to the bus due to signal loss over the extended bus.

Ring Topology



- The repeaters at each host capture the incoming signal intended for other hosts, regenerates the bit-stream, and passes it onto the next repeater.
- The fault identification and setup of this topology is quite simple and straightforward.
- The main disadvantage of this system is the high probability of a single point of failure.

Network Reachability

Computer networks are divided into four broad categories based on network reachability as,

- Personal Area Networks
- Local Area Networks
- Wide Area Networks
- Metropolitan Area Networks

Personal Area Networks

- PANs, as the name suggests, are restricted to individual usage mostly.
- A good example of PANs may be connected wireless headphones, wireless speakers, laptops, smartphones, wireless keyboards, wireless mouse, and printers within a house.
- Generally, PANs are wireless networks, which make use of low-range and low-power technologies such as Bluetooth.
- The reachability of PANs lies in the range of a few centimeters to a few meters.

Local Area Networks (LAN)

- A LAN is a collection of hosts connected to a single network through wired or wireless connections.
- However, LANs are restricted to buildings, organizations, or campuses.
- Typically, few leased lines connecting to the Internet provide web access to an organization or a campus, which is further redistributed to multiple hosts within the LAN enabling hosts, which are much more than the actual direct lines to the Internet to access the web from within the organization. This also allows the organization to define various access control policies for web access within its hierarchy.
- Typically, the present-day data access rates within the LANs range between 100 Mbps to 1000 Mbps, with very high fault-tolerance levels.
- Commonly used network components in a LAN are servers, hubs, routers, switches, terminals, and computers.

Metropolitan Area Networks (MAN)

- The reachability of a MAN lies between that of a LAN and a WAN.
- Typically, MANs connect various organizations or buildings within a given geographical location or city.
- An excellent example of a MAN is an Internet Service Provider (ISP) supplying Internet connectivity to various organizations within the reaches of a city.
- As MANs are costly, they may not be owned by individuals or even single organizations.
- Typical networking devices/components in MANs are modems and cables. MANs tend to have moderate fault-tolerance levels.

Wide Area Networks (WAN)

- WANs typically connect diverse geographic locations. However, they are restricted within the boundaries of a state or country.
- The data rate of WANs is in the order of a fraction of the LAN's data rate.
- Typically WANs connecting two LANs or MANs may use Public Switched Telephone Networks (PSTNs) or satellite-based links.
- Due to the long transmission ranges, WANs tend to have more errors and noise during transmission and are very costly to maintain. The fault-tolerance of WANs are also generally low.

Layered Network Models

- The intercommunication between hosts in any computer network, be it a large-scale or a small-scale one, is built upon the premise of various task-specific layers.
- Two of the most commonly accepted and used traditional layered network models are the ISO-OSI reference model and the Internet protocol suite.

ISO-OSI Model

The ISO-OSI model is a conceptual framework, which partitions any networked communication device into seven layers of abstraction, each performing distinct tasks, based on the underlying technology and internal structure of the hosts. These seven layers in a bottom-up manner are

1. Physical layer
2. Data-link layer
3. Network layer
4. Transport layer
5. Session layer
6. Presentation layer
7. Application layer

Networking through OSI Model

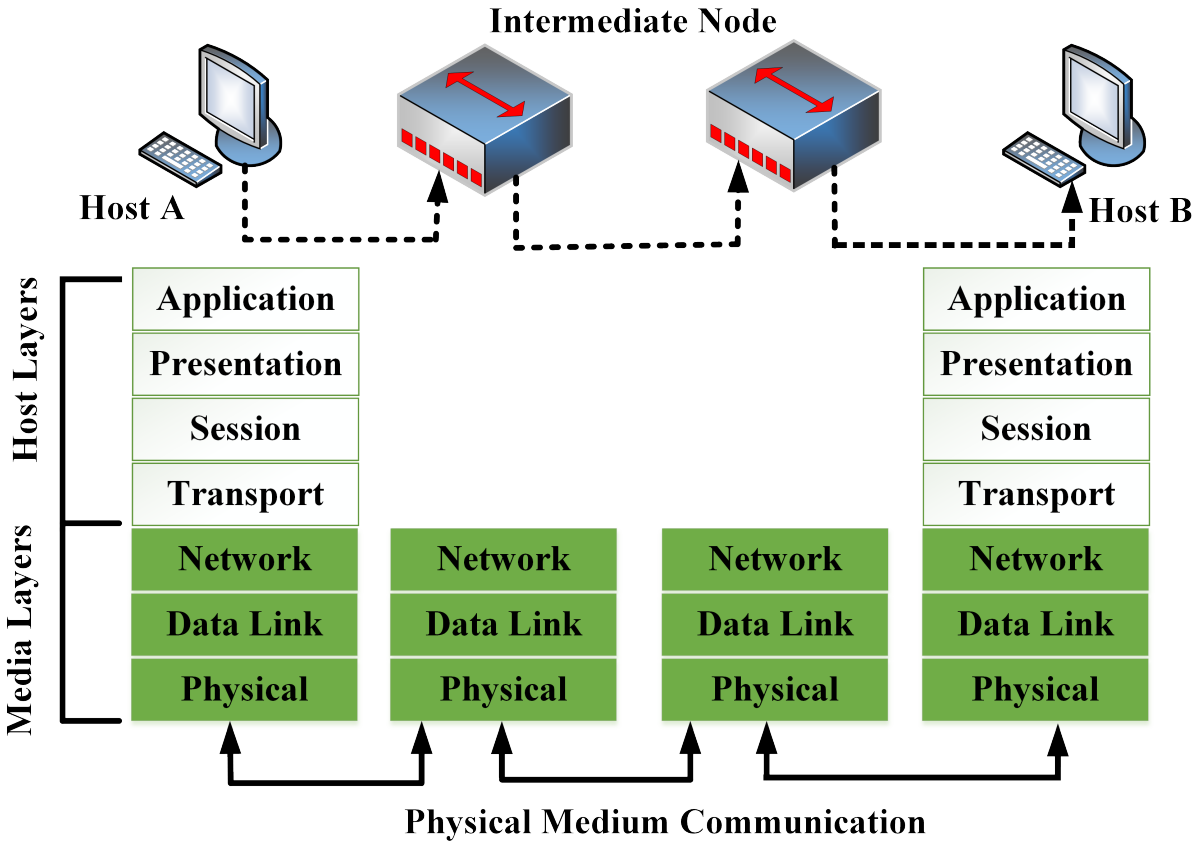


Figure: Networked communication between two hosts following the OSI model

ISO-OSI Model

The ISO-OSI model is a conceptual framework, which partitions any networked communication device into seven layers of abstraction, each performing distinct tasks, based on the underlying technology and internal structure of the hosts. These seven layers in a bottom-up manner are

1. Physical layer
2. Data-link layer
3. Network layer
4. Transport layer
5. Session layer
6. Presentation layer
7. Application layer

TCP/IP Suite

The Internet protocol suite is yet another conceptual framework, which provides levels of abstraction for ease of understanding and development of communication and networked systems on the Internet. However, the Internet protocol suite predates the OSI model and provides only four levels of abstraction,

1. Link layer
2. Internet layer
3. Transport layer
4. Application layer

This collection of protocols is commonly referred to as the TCP/IP protocol suite as the foundation technologies of this suite are Transmission Control Protocol (TCP) and Internet Protocol (IP)

TCP/IP Suite

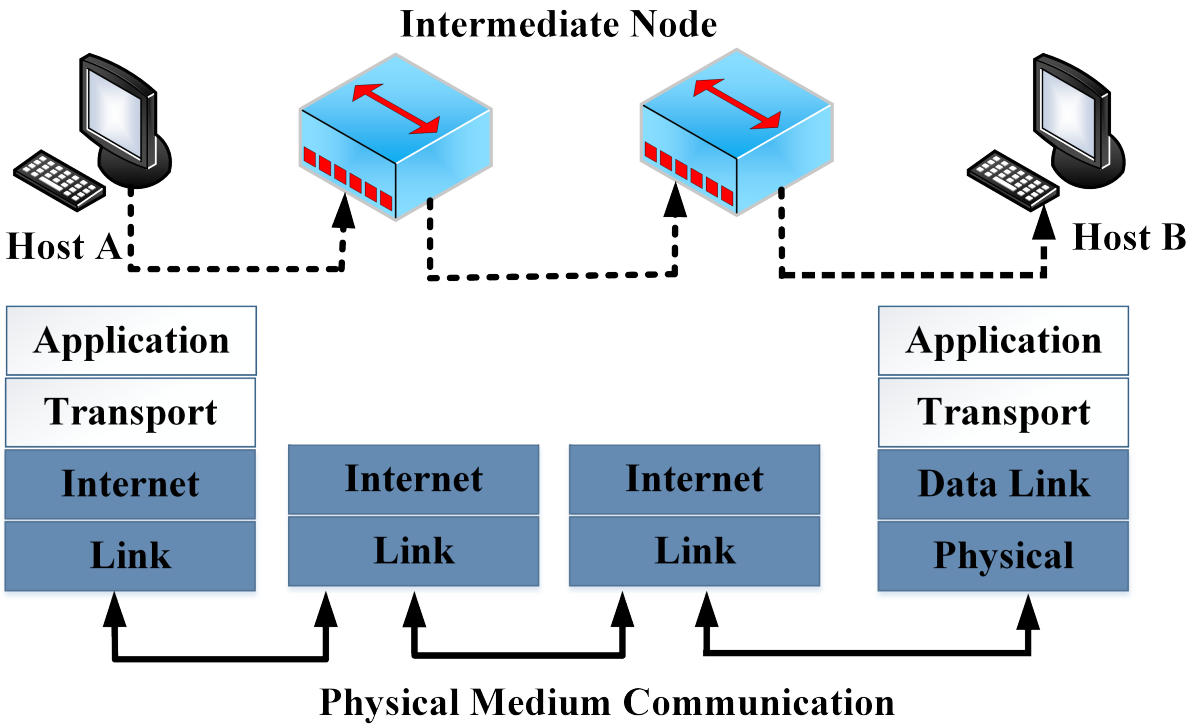


Figure: Networked communication between two hosts following the TCP/IP suite

Addressing

- The role of addressing in networked devices play a crucial role in ensuring the delivery of packets to the designated/intended receivers.
- The addressing scheme is synonymous with postal addresses used in real-life scenarios.
- We divide the addressing mechanisms into two parts
  1. Data-link layer addressing
  2. Network layer addressing

Data Link Layer Addressing

The data-link layer addressing deals with Media Access Control (MAC) addresses of devices, which work at the MAC sub-layer of the data-link layer.
MAC addresses are 48-bits long, in which the first 24-bits are organizational identifiers, while the last 24-bits are network interface controller identifiers. These addresses are unique globally.
Data-link layer addressing is broadly divided into three types:

1. **Unicast**: The data-flow from a transmitting host is restricted to only one receiving host in the link.
2. **Multicast**: The data-flow from a transmitting host is intended for multiple hosts within the same link.
3. **Broadcast**: The data from a transmitting host is received by all other hosts connected to that link.

Network Layer Addressing

- The network layer addressing is also termed as IP-based addressing or logical addressing. IPv4 addressing uses 32-bits long addresses, whereas IPv6 uses addresses that are 128-bits long.
- These addresses can identify the source or destination addresses from the address itself.

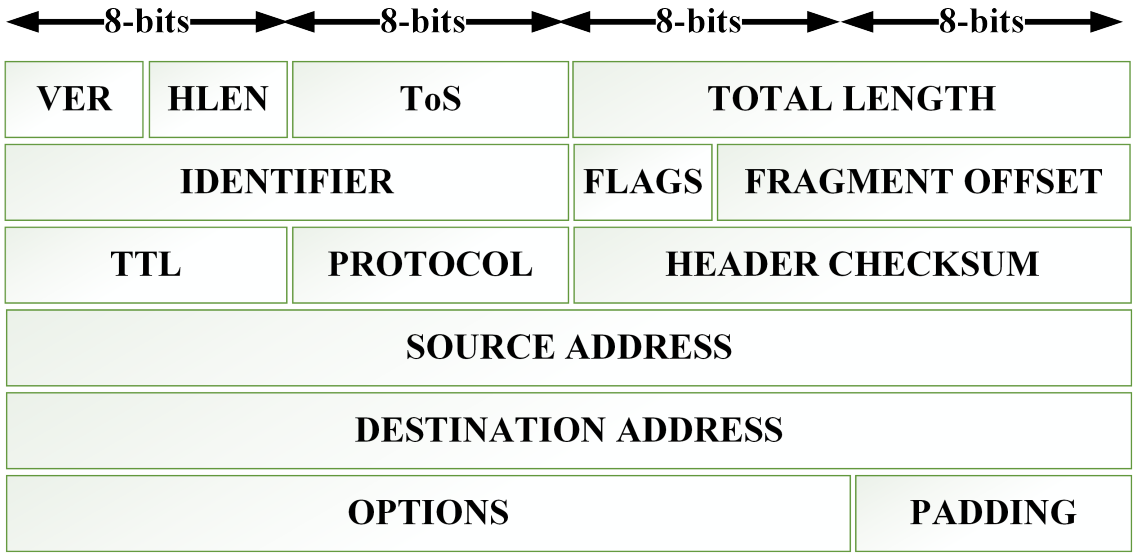


Figure: An IPv4 packet header structure

Network Layer Addressing

- The mapping of a device/host's logical address to its hardware address is done through a mechanism called Address Resolution Protocol (ARP).
- During transmission of a packet from a host, the IPv4 sends an IPv4 packet, the next-hop address, and the next-hop interface to the ARP.
- Direct delivery is performed by the ARP in case the destination address for delivery matches the next-hop address.
- In contrast, if the addresses do not match, the ARP performs an indirect delivery by forwarding the packet to a router or an intermediate node.
- The resolution of the mapping of a packet's next-hop address to its MAC address is made using broadcasting ARP requests.
- The returning ARP reply frame to the sender contains the MAC address corresponding to the packet's next-hop address.

Network Layer Addressing

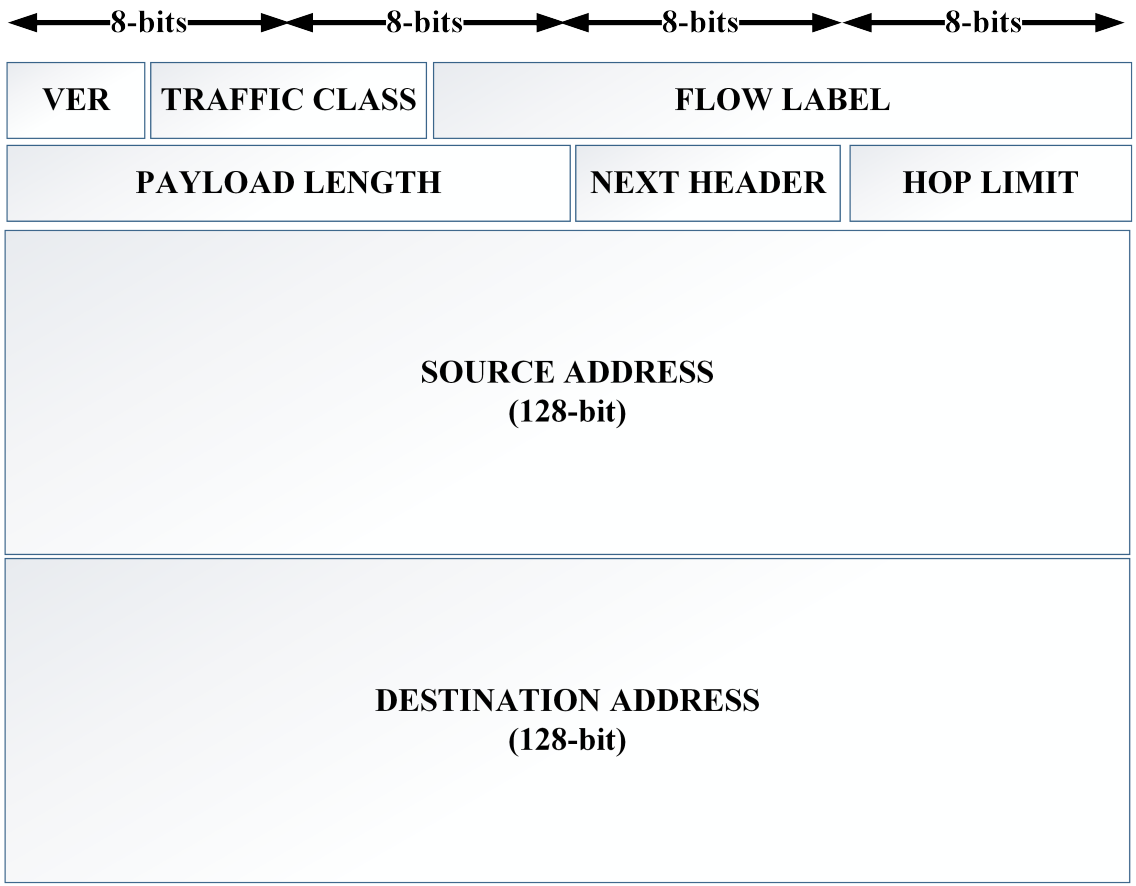


Figure: An IPv6 packet header structure

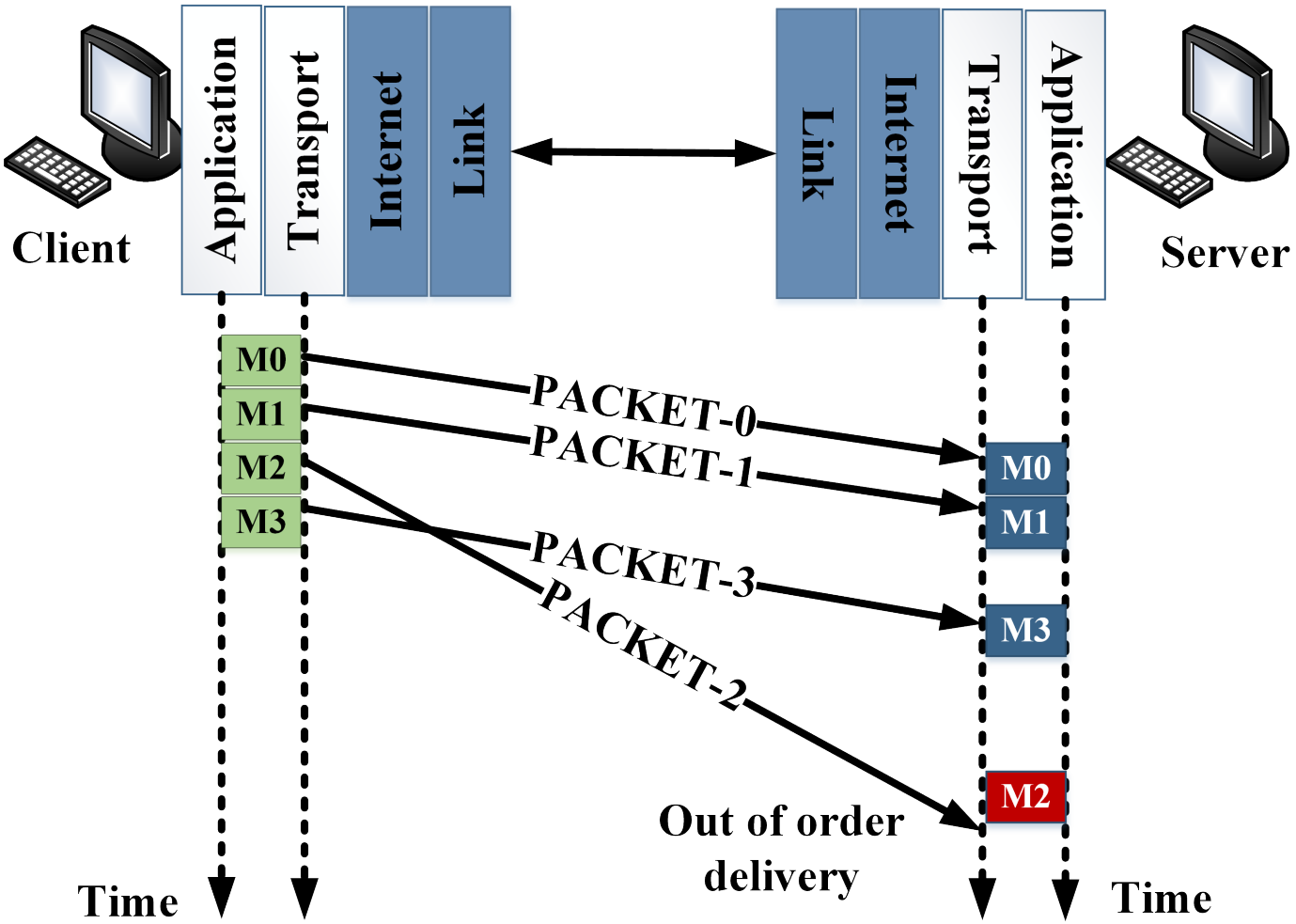
TCP/IP Transport Layer

- The transport layer is the third layer in the TCP/IP protocol suite and is an important connectivity entity as it acts as the interlocutor for the clients and servers in a client-server paradigm.
- This layer forms the core of the TCP/IP protocol suite as it provides logical mechanisms for data exchanges between two or more points over the Internet.
- The transport layer engages in networking functionalities such as
  1. process-to-process communication,
  2. encapsulation and decapsulation of data,
  3. multiplexing and demultiplexing of virtual pathways,
  4. flow control,
  5. error control
  6. congestion control

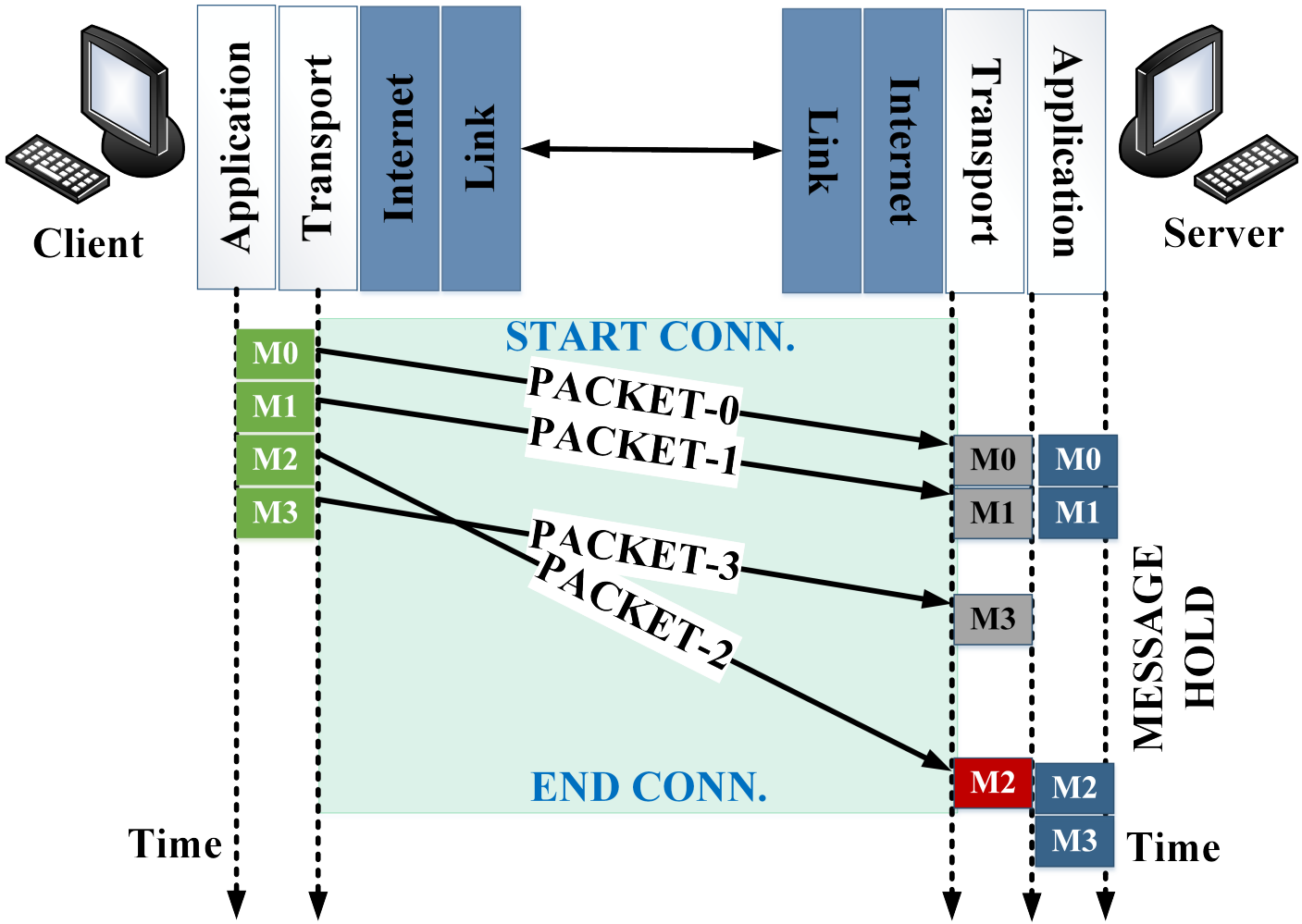
TCP/IP Transport Layer

- The transport layer provides two types of services
  1. Connectionless service
  2. Connection-oriented service
- These service types at the transport layer determine the degree of inter-dependence between transmitted packets.
- The application layer for both service types first divides a message into smaller chunks, which are acceptable by the transport layer for further transmission.
- These chunks are sequentially forwarded from the application layer to the transport layer.
- Upon receiving these chunks, the transport layer encapsulates these into packets for transmission.
- Generally, the packets in a connectionless transport-layer service are independent of one another, whereas the packets in a connection-oriented service are dependent on one another.

Connectionless Service



Connection-Oriented Service



The End