UNIT-3

NETWORK LAYER

The network Layer is the third layer in the OSI model of computer networks. Its main function is to transfer network packets from the source to the destination. It involves both the source host and the destination host.

Key among these services are packetizing, routing, and forwarding. Packetizing involves encapsulating data into packets suitable for transmission. Routing determines the optimal path for these packets through the network, ensuring they navigate through multiple nodes and networks efficiently. Forwarding is the process of directing these packets to their next hop along the selected path.

In this article, we will discuss these topics in detail, along with the services provided by the network layer, etc.

What is the Network?

A network is a group of two or more connected computers or devices. These devices usually connect to a central hub, like a router. Networks can also have subnetworks, which are smaller sections of the main network. Subnetworks help large networks, such as those used by Internet Service Providers (ISPs), manage many IP addresses and devices.

The Internet is like a network of networks. Computers connect within their own networks and then connect to other networks. This allows computers to communicate with each other, no matter where they are.

What is the Network Layer?

The network layer is a part of the communication process in computer networks. Its main job is to move data packets between different networks. It helps route these packets from the sender to the receiver across multiple paths and networks. Network-to-network connections enable the Internet to function. These connections happen at the “network layer,” which sends data packets between different networks. In the 7-layer OSI model, the network layer is layer 3. The Internet Protocol (IP) is a key protocol used at this layer, along with other protocols for routing, testing, and encryption.

Features of Network Layer

- The main responsibility of the Network layer is to carry the data packets from the source to the destination without changing or using them.
- If the packets are too large for delivery, they are fragmented i.e., broken down into smaller packets.
- It decides the route to be taken by the packets to travel from the source to the destination among the multiple routes available in a network (also called routing).

- The source and destination addresses are added to the data packets inside the network layer.

Services Offered by Network Layer

The **services** which are offered by the network layer protocol are as follows:

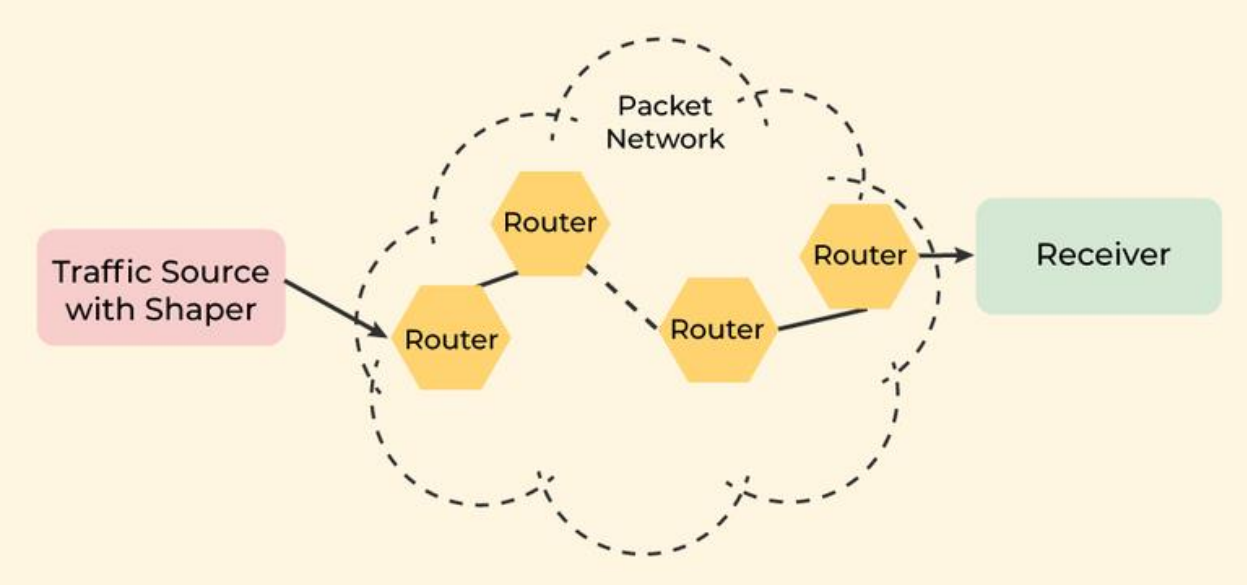
- Packetizing
- Routing
- Forwarding

1. Packetizing

The process of encapsulating the data received from the upper layers of the network (also called payload) in a network layer packet at the source and decapsulating the payload from the network layer packet at the destination is known as packetizing.

The source host adds a header that contains the source and destination address and some other relevant information required by the network layer protocol to the payload received from the upper layer protocol and delivers the packet to the data link layer.

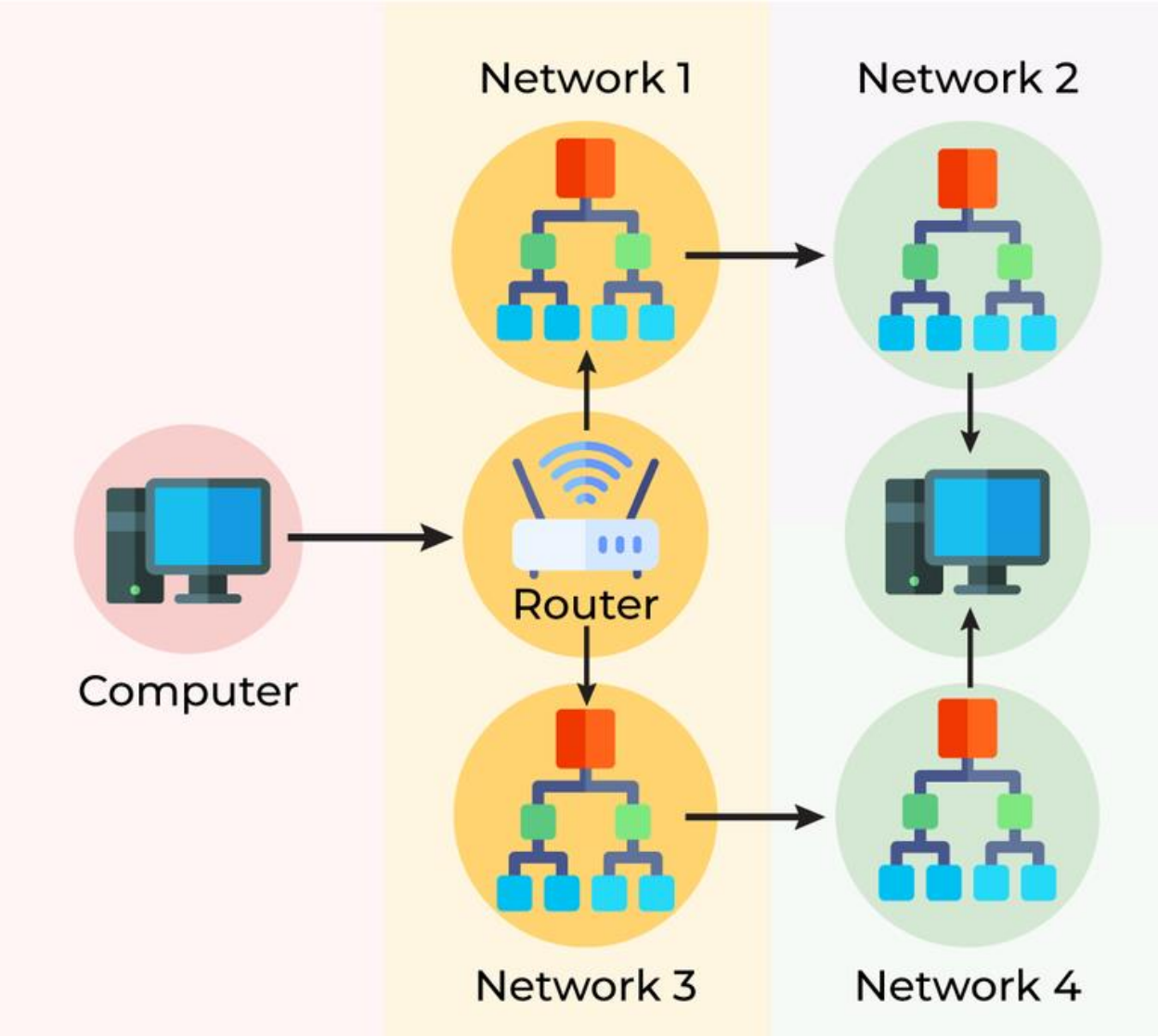
The destination host receives the network layer packet from its data link layer, decapsulates the packet, and delivers the payload to the corresponding upper layer protocol. The routers in the path are not allowed to change either the source or the destination address. The routers in the path are not allowed to decapsulate the packets they receive unless they need to be fragmented.



Packetizing

2. Routing

Routing is the process of moving data from one device to another device. These are two other services offered by the network layer. In a network, there are a number of routes available from the source to the destination. The network layer specifies some strategies which find out the best possible route. This process is referred to as routing. There are a number of routing protocols that are used in this process and they should be run to help the routers coordinate with each other and help in establishing communication throughout the network.

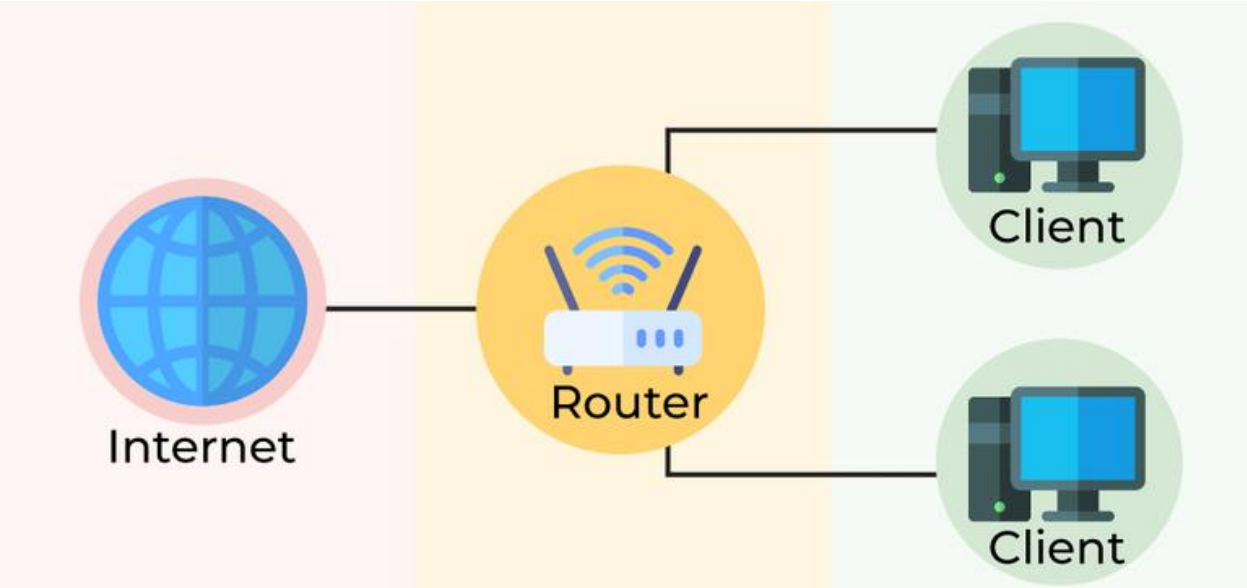


Routing

3. Forwarding

Forwarding is simply defined as the action applied by each router when a packet arrives at one of its interfaces. When a router receives a packet from one of its attached networks, it needs to forward the packet to another attached network (unicast routing) or to some attached networks (in the case of multicast routing). Routers are used on the network for forwarding a packet from

the local network to the remote network. So, the process of routing involves packet forwarding from an entry interface out to an exit interface.



Forwarding

Differences Between Routing and Forwarding

Routing	**Forwarding**
Routing is the process of moving data from one device to another device.	Forwarding is simply defined as the action applied by each router when a packet arrives at one of its interfaces.
Operates on the Network Layer.	Operates on the Network Layer.
Work is based on Forwarding Table.	Checks the forwarding table and work according to that.
Works on protocols like Routing Information Protocol (RIP) for Routing.	Works on protocols like UDP Encapsulating Security Payloads

Other Services Expected from Network Layer

- Error Control
- Flow Control

- Congestion Control

1. Error Control

Although it can be implemented in the network layer, it is usually not preferred because the data packet in a network layer may be fragmented at each router, which makes error-checking inefficient in the network layer.

2. Flow Control

It regulates the amount of data a source can send without overloading the receiver. If the source produces data at a very faster rate than the receiver can consume it, the receiver will be overloaded with data. To control the flow of data, the receiver should send feedback to the sender to inform the latter that it is overloaded with data.
There is a lack of flow control in the design of the network layer. It does not directly provide any flow control. The datagrams are sent by the sender when they are ready, without any attention to the readiness of the receiver.

3. Congestion Control

Congestion occurs when the number of datagrams sent by the source is beyond the capacity of the network or routers. This is another issue in the network layer protocol. If congestion continues, sometimes a situation may arrive where the system collapses and no datagrams are delivered. Although congestion control is indirectly implemented in the network layer, still there is a lack of congestion control in the network layer.

Advantages of Network Layer Services

- Packetization service in the network layer provides ease of transportation of the data packets.
- Packetization also eliminates single points of failure in data communication systems.
- Routers present in the network layer reduce network traffic by creating collision and broadcast domains.
- With the help of Forwarding, data packets are transferred from one place to another in the network.

Network Switching

A switch is a dedicated piece of computer hardware that facilitates the process of switching i.e., incoming data packets and transferring them to their destination. A switch works at the Data Link layer of the OSI Model. A switch primarily handles the incoming data packets from a source computer or network and decides the appropriate port through which the data packets will reach their target computer or network.

A switch decides the port through which a data packet shall pass with the help of its destination MAC(Media Access Control) Address. A switch does this effectively by maintaining a switching table, (also known as forwarding table). A network switch is more efficient than a network Hub or repeater because it maintains a switching table, which simplifies its task and reduces congestion on a network, which effectively improves the performance of the network.

Process of Switching

The switching process involves the following steps:

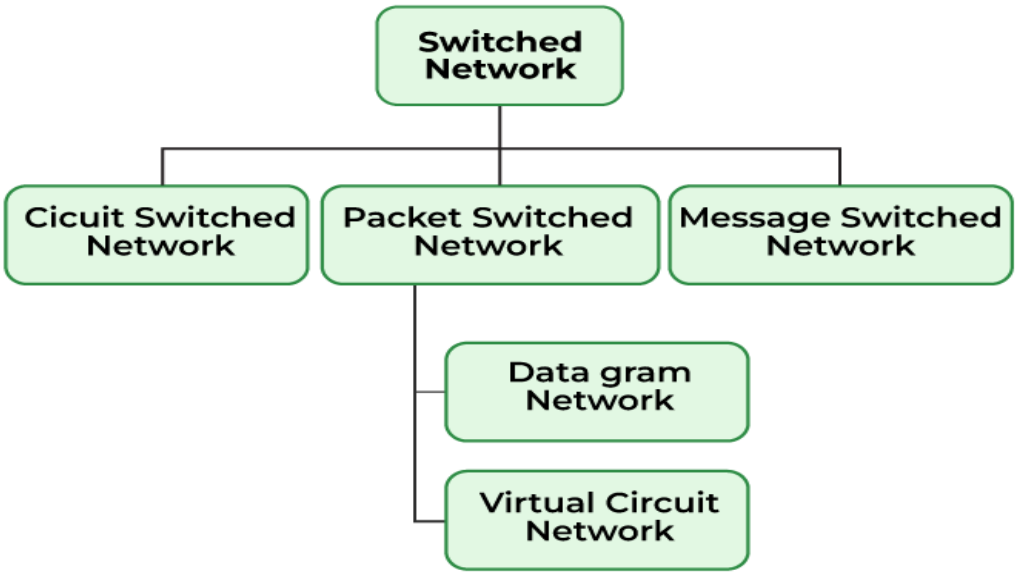
- **Frame Reception:** The switch receives a data frame or packet from a computer connected to its ports.
- **MAC Address Extraction:** The switch reads the header of the data frame and collects the destination MAC Address from it.
- **MAC Address Table Lookup:** Once the switch has retrieved the MAC Address, it performs a lookup in its Switching table to find a port that leads to the MAC Address of the data frame.
- **Forwarding Decision and Switching Table Update:** If the switch matches the destination MAC Address of the frame to the MAC address in its switching table, it forwards the data frame to the respective port. However, if the destination MAC Address does not exist in its forwarding table, it follows the flooding process, in which it sends the data frame to all its ports except the one it came from and records all the MAC Addresses to which the frame was delivered. This way, the switch finds the new MAC Address and updates its forwarding table.
- **Frame Transition:** Once the destination port is found, the switch sends the data frame to that port and forwards it to its target computer/network.

Types of Switching

There are three types of switching methods:

- Message Switching
- Circuit Switching
- Packet Switching
    - Datagram Packet Switching

- Virtual Circuit Packet Switching



Let us now discuss them individually:

Message Switching: This is an older switching technique that has become obsolete. In message switching technique, the entire data block/message is forwarded across the entire network thus, making it highly inefficient.

Circuit Switching: In this type of switching, a connection is established between the source and destination beforehand. This connection receives the complete bandwidth of the network until the data is transferred completely.
This approach is better than message switching as it does not involve sending data to the entire network, instead of its destination only.

Packet Switching: This technique requires the data to be broken down into smaller components, data frames, or packets. These data frames are then transferred to their destinations according to the available resources in the network at a particular time.
This switching type is used in modern computers and even the Internet. Here, each data frame contains additional information about the destination and other information required for proper transfer through network components.

Datagram Packet Switching: In Datagram Packet switching, each data frame is taken as an individual entity and thus, they are processed separately. Here, no connection is established before data transmission occurs. Although this approach provides flexibility in data transfer, it may cause a loss of data frames or late delivery of the data frames.

Virtual-Circuit Packet Switching: In Virtual-Circuit Packet switching, a logical connection between the source and destination is made before transmitting any data. These logical connections are called virtual circuits. Each data frame follows these logical paths and provides a reliable way of transmitting data with less chance of data loss.

Logical addressing (IPV4, IPV6)

IP addresses and MAC addresses are essential for data communication. Assume there are two networks. The first network has three devices: A, B, C and the second network has three devices: X, Y, Z. If a device A from the first network wishes to send data to a device Y in the second network, it must first determine where Y is located in the second network, which requires learning the IP address/ logical address, because the connection is subject to change and is not permanent due to the nature of the Packet Switched Network (Logical). However, in order to send data to that device, it must pass the data across physical communication links, for which a MAC Address/Physical address is utilized.

An IP address is a logical address assigned to a device on a network, whereas a MAC address is a physical address hardcoded into the network interface card (NIC) of a device.

1. An IP address is used to identify and communicate with devices on a network. It is assigned to a device by the network administrator or a DHCP (Dynamic Host Configuration Protocol) server. An IP address consists of two parts: network ID and host ID. The network ID identifies the network on which the device is connected, and the host ID identifies the specific device within the network. IP addresses are hierarchical and can be subnetted, allowing for more efficient use of address space and better management of networks.
2. On the other hand, a MAC address is a physical address tied to the hardware of the NIC. It is a unique identifier hardcoded by the device manufacturer and consists of six pairs of hexadecimal digits. The MAC address is used to identify the device on a physical network, such as an Ethernet LAN. The MAC address is used for low-level communication between devices on the same network, such as data transfer and network discovery.

The difference between logical and physical addresses is that logical addresses, such as IP addresses, are assigned by software protocols and can be changed or reconfigured, whereas physical addresses, such as MAC addresses, are hardcoded into the hardware of the device and cannot be changed. Logical addresses are used for higher-level network communication, such as routing and addressing, whereas physical addresses are used for low-level communication, such as data transfer.

IPV4

IP stands for **Internet Protocol version v4** stands for **Version Four** (IPv4), is the most widely used system for identifying devices on a network. It uses a set of four numbers, separated by periods (like 192.168.0.1), to give each device a unique address. This address helps data find its way from one device to another over the internet.

IPv4 was the primary version brought into action for production within the ARPANET in 1983. IP version four addresses are 32-bit integers which will be expressed in decimal notation. Example- 192.0.2.126 could be an IPv4 address.

Parts of IPv4

IPv4 addresses consist of three parts:

- **Network Part**: The network part indicates the distinctive variety that's appointed to the network. The network part conjointly identifies the category of the network that's assigned.
- **Host Part**: The host part uniquely identifies the machine on your network. This part of the IPv4 address is assigned to every host.
  For each host on the network, the network part is the same, however, the host half must vary.
- **Subnet Number**: This is the nonobligatory part of IPv4. Local networks that have massive numbers of hosts are divided into subnets and subnet numbers are appointed to that.

Characteristics of IPv4

- IPv4 could be a 32-bit IP Address.
- IPv4 could be a numeric address, and its bits are separated by a dot.
- The number of header fields is twelve and the length of the header field is twenty.
- It has Unicast, broadcast, and multicast-style addresses.
- IPv4 supports VLSM (Virtual Length Subnet Mask).
- IPv4 uses the Post Address Resolution Protocol to map to the MAC address.
- RIP may be a routing protocol supported by the routed daemon.
- Networks ought to be designed either manually or with DHCP.
- Packet fragmentation permits from routers and causes host.

Advantages of IPv4

- IPv4 security permits encryption to keep up privacy and security.
- IPV4 network allocation is significant and presently has quite 85000 practical routers.
- It becomes easy to attach multiple devices across an outsized network while not NAT.
- This is a model of communication so provides quality service also as economical knowledge transfer.
- IPV4 addresses are redefined and permit flawless encoding.
- Routing is scalable and economical as a result of addressing its collective more effectively.

- Data communication across the network becomes a lot of specific in multicast organizations.
    - Limits net growth for existing users and hinders the use of the net for brand-new users.
    - Internet Routing is inefficient in IPv4.
    - IPv4 has high System Management prices and it's labor-intensive, complex, slow & prone to errors.
    - Security features are nonobligatory.
    - The difficulty to feature support for future desires as a result of adding it on is extremely high overhead since it hinders the flexibility to attach everything over IP.

IPV6

The Internet Protocol version 6, or IPv6, is the latest version of the Internet Protocol (IP), which is the system used for identifying and locating computers on the Internet. IPv6 was developed by the Internet Engineering Task Force (IETF) to deal with the problem of IPv4 exhaustion. IPv6 is a 128-bit address having an address space of 2128, which is way bigger than IPv4. IPv6 uses a Hexa-Decimal format separated by a colon (:).

What is IP?

An IP address, which stands for Internet Protocol address, is like a home address for your computer or any device connected to the internet. Just as your home address lets mail find its way to your house, an IP address helps information find its way to your device.

Components in Address Format

- There are 8 groups and each group represents 2 Bytes (16-bits).
- Each Hex-Digit is of 4 bits (1 nibble)
- Delimiter used – colon (:)

Need For IPv6

The Main reason of IPv6 was the address depletion as the need for electronic devices rose quickly when Internet Of Things (IOT) came into picture after the 1980s & other reasons are related to the slowness of the process due to some unnecessary processing, the need for new options, support for multimedia, and the desperate need for security. IPv6 protocol responds to the above issues using the following main changes in the protocol:

- **Large Address Space:** An IPv6 address is 128 bits long .compared with the 32 bit address of IPv4, this is a huge(2 raised 96 times) increases in the address space.
- **Better Header Format**: IPv6 uses a new header format in which options are separated from the base header and inserted, when needed, between the base header and the upper layer data . This simplifies and speeds up the routing process because most of the options do not need to be checked by routers.
- **New Options**: IPv6 has new options to allow for additional functionalities.
- **Allowance for extension**: IPv6 is designed to allow the extension of the protocol if required by new technologies or applications.
- **Support For Resource Allocation**: In IPv6,the type of service field has been removed, but two new fields , traffic class and flow label have been added to enables the source to request special handling of the packet . this mechanism can be used to support traffic such as real-time audio and video.

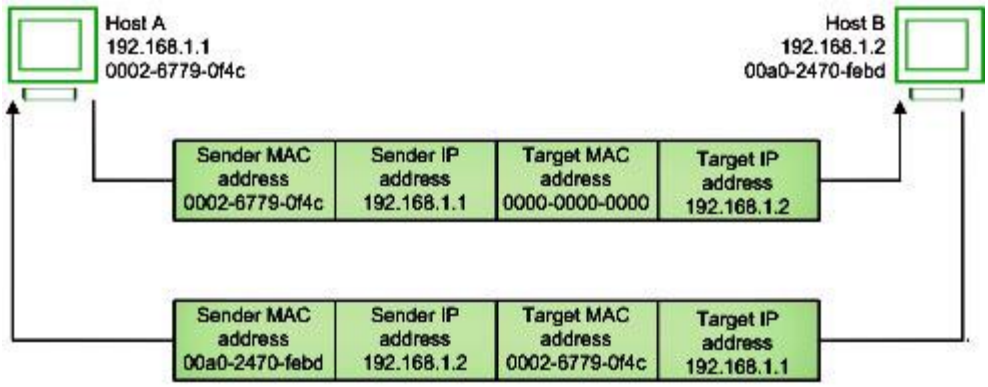
Advantages of IPv6

- **1. Realtime Data Transmission :** Realtime data transmission refers to the process of transmitting data in a very fast manner or **immediately**. Example : Live streaming services such as cricket matches, or other tournament that are streamed on web exactly as soon as it happens with a maximum delay of 5-6 seconds.
- **2. IPv6 supports authentication:** Verifying that the data received by the receiver from the sender is exactly what the sender sent and came through the sender only not from any third party. Example : Matching the hash value of both the messages for verification is also done by IPv6.
- **3. IPv6 performs Encryption:** Ipv6 can encrypt the message at network layer even if the protocols of application layer at user level didn't encrypt the message which is a major advantage as it takes care of encryption.
- **4. Faster processing at Router:** Routers are able to process data packets of Ipv6 much faster due to smaller **Base header** of fixed size – 40 bytes which helps in decreasing processing time resulting in more efficient packet transmission. Whereas in Ipv4, we have to calculate the length of header which lies between 20-60 bytes.

Address Mapping (ARP, Reverse ARP(RARP))

1. Address Resolution Protocol (ARP) –

Address Resolution Protocol is a communication protocol used for discovering physical address associated with given network address. Typically, ARP is a network layer to data link layer mapping process, which is used to discover MAC address for given Internet Protocol Address. In order to send the data to destination, having IP address is necessary but not sufficient; we also need the physical address of the destination machine. ARP is used to get the physical address (MAC address) of destination machine.



Before sending the IP packet, the MAC address of destination must be known. If not so, then sender broadcasts the ARP-discovery packet requesting the MAC address of intended destination. Since ARP-discovery is broadcast, every host inside that network will get this message but the packet will be discarded by everyone except that intended receiver host whose IP is associated. Now, this receiver will send a unicast packet with its MAC address (ARP-reply) to the sender of ARP-discovery packet. After the original sender receives the ARP-reply, it updates ARP-cache and start sending unicast message to the destination.