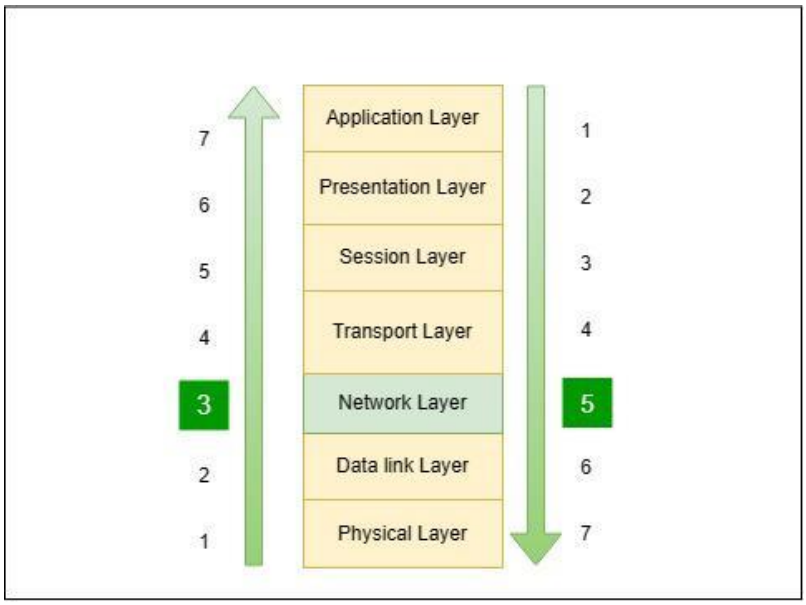
Network Layer in OSI Model

OSI stands for Open Systems Interconnection. It was developed by the ISO – 'International Organization for Standardization', in the year 1984. It is a 7-layer architecture with each layer having specific functionality to perform. All these 7 layers work collaboratively to transmit the data from one person to another across the globe.

What is a Network Layer?

The Network Layer is the 5th Layer from the top and the 3rd layer from the Bottom of the OSI Model. It is one of the most important layers which plays a key role in data transmission. The main job of this layer is to maintain the quality of the data and pass and transmit it from its source to its destination. It also handles routing, which means that it chooses the best path to transmit the data from the source to its destination, not just transmitting the packet. There are several important protocols that work in this layer.

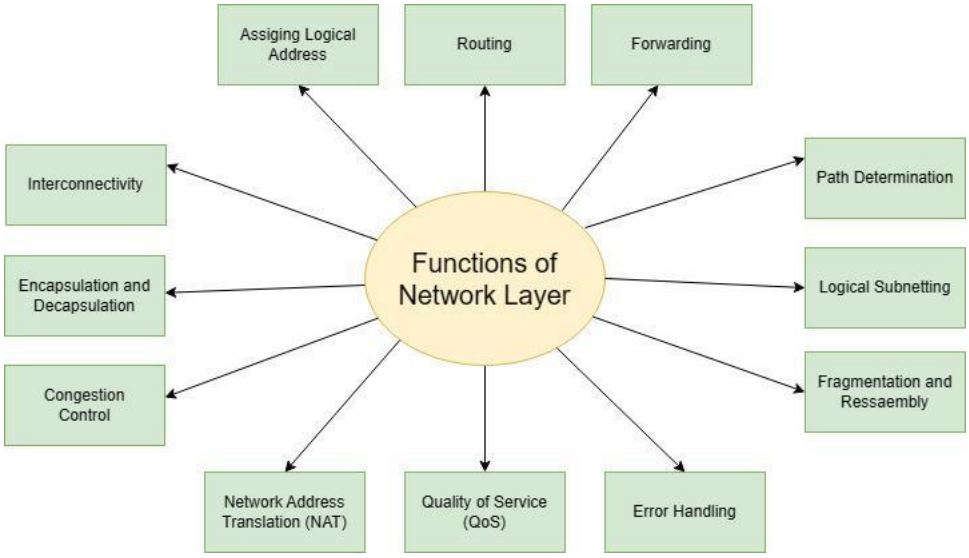


Entire OSI Model and the Location of Network Layer

Data is transmitted in the form of packets via various logical network pathways between various devices. In the seven-layer open system interconnection paradigm, the network layer is the third layer. It offers routes for data packet transfers across the network. The network layer is also responsible for organising and controlling the available paths for data transfer.

Functions of Network Layer

Network Layer serves various important functions in the data transport mechanism. It is also responsible for the routing mechanism in which it selects the best path to transfer the data from source to it's destination. It divides the entire data into smaller packets which eases the transfer procedure. It is also responsible for attaching the logical address to the devices between which the data transmission is happening, so that the packets reach correct destination and the destination can confirm that it is the same packet it was looking for. Some of the most important functions of the network layer is given below.



1. Assigning Logical Address

Network layer is solely responsible for assigning logical addresses to devices which are either sending or receiving data packets. It is useful to uniquely identify each devices in a certain network. The data packets sent or received consists the IP address of both the sender device and the receiver device. It is useful to confirm that the packets are sent or received by the desired parties. There are two part in an IP address, a Host ID and Network ID, using the Host ID it can be confirmed that the packets were sent by the authorized sender and it has successfully reached the desired receiver.

2. Routing

Routing is the process of identifying the best path to transmit the packets, Network Layer not only just sends packets from sender to receiver, but also determines the best route to send them. Numerous routers are used to find out the best and safest route to transmit the data packets. Various routing algorithms are used to determine the best path, like link state routing, Distance Vector Routing, Flooding, Random Walk etc. The header of each data packet holds the information regarding the path they need to follow to reach their destination via different routers. Usually there are multiple routers between the sender and the receiver, so the data packets are routed by using all these available routers.

3. Host-to-Host delivery

Host-to-Host delivery also known as Forwarding is the process in which the network layer transmits or forwards the data packets via routers, after determining the best path/route. In some cases it takes more than one router to reach the destination, Network Layer takes care of those too, it forwards packets from each router to the another router until it reaches the destination securely.

4. Logical Subnetting

Network Layer also allows a bigger network to be divided into smaller chunks of network known as Logical Subnetting. It helps the IP addresses to be used more efficiently and less amount of IP address will be wasted. It is also helpful to manage a larger network more efficiently. Due to smaller networks, it would be easier to find the device if any troubleshooting is needed.

5. Fragmentation and Reassembly

Each device / node has a maximum capacity to receive data (it may differ from Node to Node), which is called Maximum Transmission Unit (MTU). If the total size of data packets exceedes that size limit, then those data packets are fragmented into more smaller packets / fragmented so that they can fit the MTU. After fragmentation those packets are being send to the receiver, and at the receiving end all

those fragmented packets are rearranged to create the actual data in order. The fragmentation is taken care by the routers.

6. Error Handling

Network Layer also check for errors and handles them. Network Layer uses various error detection techniques like Cylic Redundancy Check (CRC) , Checksums etc. Apart from just detecting, it also handle those errors using different approaches like Forward Error Correction (FEC), Hamming Code, Reed-Solomon Codes etc. It also re-transmit the packets which are either erroneous or didn't reach the receiver. It uses the ACK messages to determine whether a packet has been successfully reached the receiver or not, if there is a Negative ACK, then it means that there is some error with the packet, and the receiver will ask the sender to resend that packet.

7. Quality of Service (QoS)

Network layer also keep track of the important data or the particular quality of data which is needed to be send first. Based on the QoS settings, it determines and prioritize the important data types which needed to be send first. It ensures that there is no delay in receiving the important data in any condition.

8. Network Address Translation (NAT)

Network Layer also takes care of the Network Address Translation (NAT), means that it converts any private IP address into a public IP address which is required to communicate between the sender and the receiver.

9. Congestion Control

Just like MTU, if there is an excessive load on the network which it can't handle, the network become congested. Due to which the entire process of sending and receiving data comes to a pause. Congestion can be dealt with using different algorithms like Leaky Bucket Algorithm and Token Bucket Algorithm. In case of the leaky bucket algorithm, whatever might be the speed or amount of data flow into the bucket, the data leaks at a constant rate, which reduces the congestion in the network. In case of the Token Bucket Algorithm, tokens are being added into the bucket one by one, until it has reached the maximum capacity, then one by one according the token sequence each data packet is transmitted.

10. Encapsulation and Decapsulation

Network Layer encapsulates the data coming from the Transport Layer, and also adds important header parts to the packets, which consists of the necessary information like source IP address and destination IP address. After receiving the data packets on the destination side it decapsulates those and make them of original size.

Working of Network Layer

The network layer will initially receive data from the OSI model's transport layer as part of the data flow between that layer and other OSI levels. These data packets are handled by the network layer by include their source and destination addresses. Additionally, it incorporates the network protocols for proper transfer to the data-link layer over the network channel.

Responsibilities of the Network Layer

In the network channel and communication channel, the network layer is in charge of the responsibilities listed below:

- It is in charge of managing the network channel's quickest routing path for the data packet.
- The network layer packages the data that has been received for transmission.

- maintains the network traffic in the channel by handling the network layer protocols.

Protocols Used at Network Layer

A protocol is a set of rules for data structuring that enables communication and mutual understanding between two or more devices. At the network layer, a variety of protocols enable connections, testing, routing, and encryption, including:

- IP
- IPsec
- ICMP
- IGMP
- GRE

Problems with the Network layer design

- The decision of how to direct packets is a pivotal aspect of network layer design. It holds great significance as it sets the groundwork for the protocol governing the transmission of packets between nodes in a network.
- In the nodes, data transmission can be facilitated through either static tables or dynamic tables. These tables serve as the routes for the transmission of information. The paths may be pre-established or subject to frequent alteration.
- The smooth flow of data in the network can be disrupted unexpectedly if there is an overwhelming abundance of packets being transmitted or present on the network. Consequently, the network might encounter bottlenecks causing a decline in its performance.
- Separate protocols are needed to enable communication between the two networks.

Advantages of Network Layer

- Using the network layer in the OSI paradigm offers a multitude of advantages. Let's delve into some of these benefits:
- The network layer takes the data and breaks it down into packets, which makes transmitting the data over the network easier. This process also eliminates any weak points in the transmission, ensuring that the packet successfully reaches its intended destination.
- Router is the important component of the network layer . Its role is to reduce network congestion by facilitating collisions and broadcasting the domains within the network layer.
- Used to send data packets across the network nodes, the forwarding method is various.

Disadvantages of Network Layer

- There is no flow control mechanism provided by the network layer design.
- There may be times when there are too many datagrams in transit over the network, causing congestion. This could put further strain on the network routers. In some circumstances, the router may lose some data packets if there are too many datagrams. Important data may be lost in the process of transmission as a result of this.
- Indirect control cannot be implemented at the network layer since the data packets are broken up before being sent. Additionally, this layer lacks effective error control systems.

Difference Between Routing and Flooding

Routing	**Flooding**
A routing table is required.	No Routing table is required
May give the shortest path.	Always gives the shortest path.
Routing is less reliable	Flooding is more reliable
Traffic is less in Routing	Traffic is more in Flooding
Duplicate packets are not present	Duplicate packet are present