The network layer is responsible for packet forwarding including routing through intermediate routes.

1. Need of Network layer (functions):
   (1) Host addressing
   (2) Message Forwarding
   (3) Keeps tracks of MAC address
   (4) Connectionless Communication is possible.

2. Service provided by network layer are:
   - Connectionless service and connection oriented service

3. Design Issues of Network layer:
   (1) Store and forward packet switching
   (2) Service provided to transport layer
      - Service should be independent of network topology.
      - Transport layer should be shielded from the number, type, and topology of the routes present.
      - Network addresses should be made available to the transport with a uniform numbering plan.

4. Implementation of connectionless service
5. Implementation of connection oriented service
6. Comparison of virtual circuit and datagram networks

Routing Algorithms -

4. **Least Cost Routing algorithm (shortest path algorithm)**
   (1) Dijkstra’s Algorithm

   **STEP 1:** Source node is initialized and can be indicated as a filled circle.

   **STEP 2:** Initial path cost to neighboring nodes (adjacent nodes) or link cost is computed and these nodes are relabeled considering source node.

   **STEP 3:** Examine the all adjacent nodes and find the smallest label, make it permanent.
STEP-4 - The smallest labeled node is now working node, then step 2 and step 3 are repeated till the destination node reaches.

(2) Bellman-Ford Algorithm -
It is used to find all shortest path in a graph from one
point to all other nodes.

5) Hierarchical Routing -
The routes are divided into regions. It contains all the
details about how to route packets to destination within its own
region.

<table>
<thead>
<tr>
<th>Region 1</th>
<th>Region 2</th>
<th>Region 3</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>B</td>
<td>C</td>
</tr>
<tr>
<td>B</td>
<td>C</td>
<td>A</td>
</tr>
<tr>
<td>C</td>
<td>A</td>
<td>B</td>
</tr>
</tbody>
</table>

Hierarchical Table for:

<table>
<thead>
<tr>
<th>Dest</th>
<th>Link</th>
<th>Hop</th>
</tr>
</thead>
<tbody>
<tr>
<td>1A</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>1B</td>
<td>1B</td>
<td>1</td>
</tr>
<tr>
<td>1C</td>
<td>1C</td>
<td>1</td>
</tr>
<tr>
<td>2</td>
<td>1B</td>
<td>2</td>
</tr>
</tbody>
</table>

6) Broadcast Routing -
Transmitting data to the multistation simultaneously called
broadcasting. Various methods are -
(1) Flooding - Transmitted to all nodes and so on
(2) Multidestination Routing -
Route generated new copy of packet for each links with
selected destination addresses
(3) Reverse Path Forwarding -
The route checks the forwarder whether it is from preferred
path and route sends it on the best route path. A tree like
structure is formed.
Multicast Routing - (Using spanning tree)

To send messages to well defined groups that are numerically large in size but small compared to the network as a whole.

Congestion Control Algorithms -

Congestion control is a process of maintaining the number of packets in a network below a certain level at which performance falls off. It makes sure that the network is able to carry the offered traffic.

General principles of congestion control -

Divided into two categories -

1. Open loop solutions - By good design, prevention of congestion
2. Closed loop solutions - Removing the congestion

Congestion Avoidance Policies -

1. Data link layer policies -
   a. Flow control
   b. Acknowledgement
   c. Re-transmission
   d. Out of order recovery
2. Network layer policies -
   a. Routing algorithm
   b. Packet queuing and service
   c. Packet lifetime management
   d. Packet discard
   e. Virtual circuit versus datagram inside the network
3. Transport layer policies -
   a. Flow control
   b. Acknowledgement
   c. Re-transmission
   d. Out of order recovery
   e. Timeout determination
10. Congestion control in virtual circuits networks - Difficult
   Remove all the paths leading to congestion and redraw a
   alternate access path from source to destination.

11. Congestion control in datagram networks - Using Warning bit and
   Routes use a bit in the packet header to signal the
   warning state. The receiver copies the warning bit from the packet
   header to the ACK message. The receiver, on receiving ACK
   with warning bit will adjust transmission rate accordingly.

12. IP Protocol -
   It is a connectionless datagram protocol with no guarantee
   of reliability. It does not provide any error control or flow control.
   It can detect errors and discard the packet if it is corrupted.

13. IP Addresses -
   They are 32 bit long and they are used in the source
   address and destination address fields of the IP header. Two part
   Network IP and Host IP.

13. Comparative Study of IPv4 and IPv6 -

<table>
<thead>
<tr>
<th>IPv4</th>
<th>IPv6</th>
</tr>
</thead>
<tbody>
<tr>
<td>12^32 possible addresses</td>
<td>2^128 possible addresses</td>
</tr>
<tr>
<td>It is written by dotted decimal notation e.g. - 121.2.8.12</td>
<td>It is hexadecimal and consists of 8 quartets e.g. - AC77:1884:2222:FACEB</td>
</tr>
<tr>
<td>Basic header length is 20 bytes</td>
<td>Basic header length is 40 bytes</td>
</tr>
<tr>
<td>Source and destination</td>
<td>Source and destination</td>
</tr>
<tr>
<td>Addresses are 32 bit in length</td>
<td>are 128 bit in length</td>
</tr>
<tr>
<td>IPsec support is optional</td>
<td>IPsec support is required</td>
</tr>
<tr>
<td>Address resolution protocol is used</td>
<td>Neighbour Solicitation messages are used</td>
</tr>
<tr>
<td>Must be configured either manually or through DHCP</td>
<td>Does not require manual configuration or DHCP</td>
</tr>
</tbody>
</table>
Mobile IP -

It is the underlying technology for support of various mobile data applications and the networking applications.

It is designed to allow mobile device users to move from one network to another while maintaining a permanent IP address.