Network layer :

The role of network is simple but a complex process .It is done by :

- Forwarding. When a packet arrives at a router's input link, the router must move the packet to the appropriate output link. For example, a packet arriving from Host H1 to Router R1 must be forwarded to the next router on a path to H2.
- Routing. The network layer must determine the route or path taken by packets as they flow from a sender to a receiver. The algorithms that calculate these paths are referred to as routing algorithms. A routing algorithm would determine, for example, the path along which packets flow from H1 to H2.

Computer networks that provide only a connection service at the network layer are called virtual-circuit (VC) networks; computer networks that provide only a connectionless service at the network layer are called datagram networks.

Virtual circuit networks

- VC consists of : (1) a path (that is, a series of links and routers) between the source and destination hosts, (2) VC numbers, one number for each link along the path, and (3) entries in the forwarding table in each router along the path. A packet belonging to a virtual circuit will carry a VC number in its header. Because a virtual circuit may have a different VC number on each link, each intervening router must replace the VC number of each traversing packet with a new VC number. The new VC number is obtained from the forwarding table

  three identifiable phases in a virtual circuit:

  - VC setup. During the setup phase, the sending transport layer contacts the network layer, specifies the receiver's address, and waits for the network to set up the VC. The network layer determines the path between sender and receiver, that is, the series of links and routers through which all packets of the VC will travel. The network layer also determines the VC number for each link along the path.
  - Data transfer once the VC has been established, packets can begin to flow along the VC.
  - VC teardown. This is initiated when the sender (or receiver) informs the network layer of its desire to terminate the VC. The network layer will then typically inform the end system on the other side of the network of the call termination and update the forwarding tables in each of the packet routers on the path to indicate that the VC no longer exists.

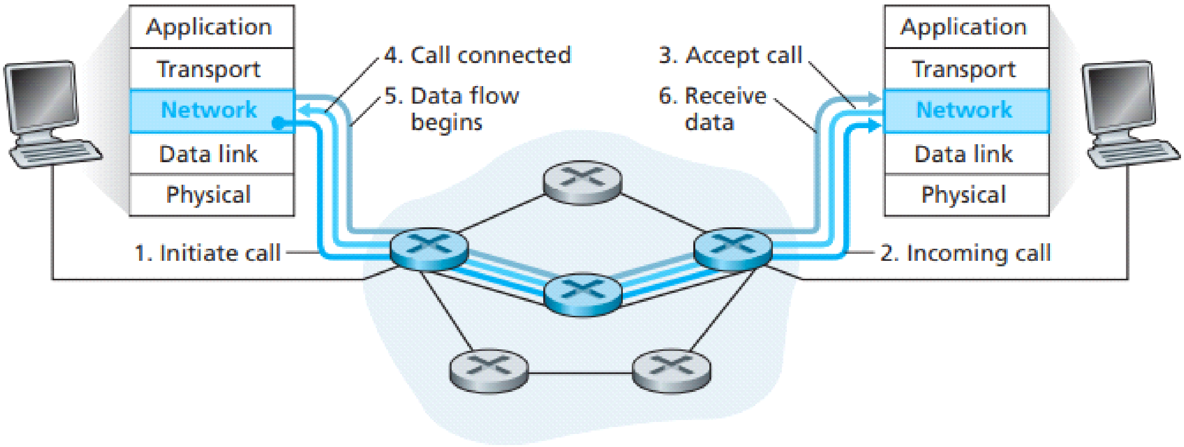
- 

Figure 4.4 ♦ Virtual-circuit setup

Datagram networks:

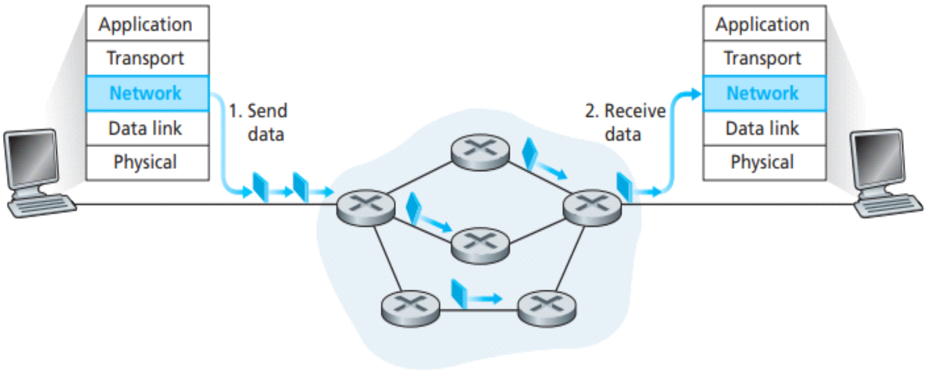
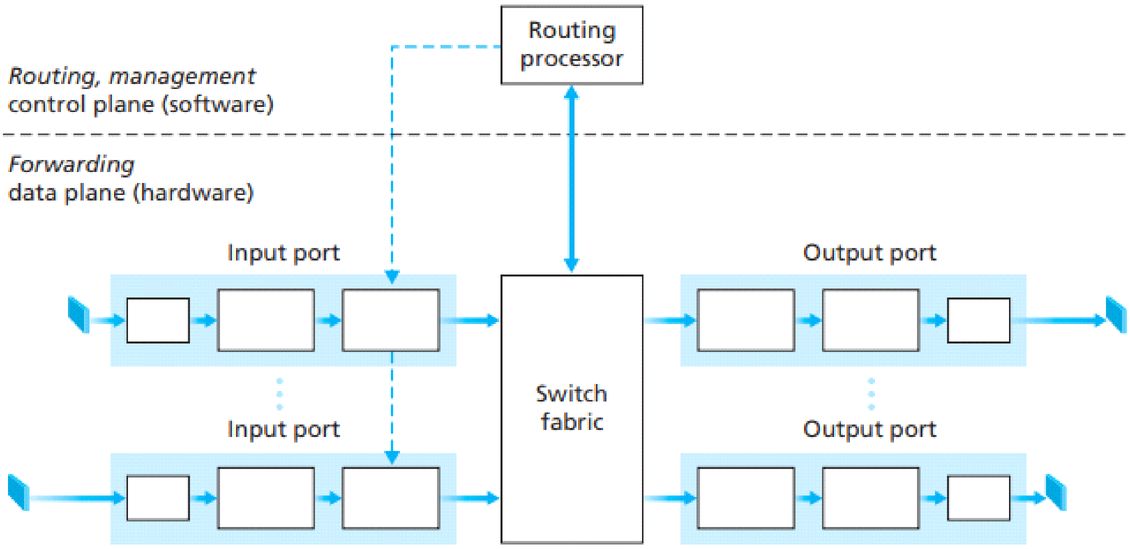
- In a datagram network, each time an end system wants to send a packet, it stamps the packet with the address of the destination end system and then pops the packet into the network. there is no VC setup and routers do not maintain any VC state information . As a packet is transmitted from source to destination, it passes through a series of routers. Each of these routers uses the packet's destination address to forward the packet. Specifically, each router has a forwarding table that maps destination addresses to link interfaces; when a packet arrives at the router, the router uses the packet's destination address to look up the appropriate output link interface in the forwarding table. The router then intentionally forwards the packet to that output link interface.
- 

Figure 4.5 ♦ Datagram network

- In a datagram network the forwarding tables are modified by the routing algorithms, which typically update a forwarding table every one-to five minutes or so. In a VC network, a forwarding table in a router is modified whenever a new connection is set up through the router or whenever an existing connection through the router is torn down.


Routing processor
Routing, management control plane (software)
Forwarding data plane (hardware)
Input port
Input port
Switch fabric
Output port
Output port

Principles or 4 components of router are:

- input processing:

  Line Termination Function and Link-Layer Processing: These implement the physical and link layers for each individual input link.

  Lookup: This is a central operation in the router. The router uses the forwarding table to determine the output port to which an incoming packet will be forwarded via the switching fabric. The forwarding table is computed and updated by the routing processor, with a shadow copy typically stored at each input port.

  Forwarding Table: This table is copied from the routing processor to the line cards over a separate bus. With a shadow copy, forwarding decisions can be made locally, at each input port, without invoking the centralized routing processor on a per-packet basis, thus avoiding a centralized processing bottleneck.

  Packet Blocking and Queuing: In some designs, a packet may be temporarily blocked from entering the switching fabric if packets from other input ports are currently using the fabric. A blocked packet will be queued at the input port and then scheduled to cross the fabric at a later point in time.

  Other Actions: Apart from lookup, many other actions must be taken such as physical- and link-layer processing, checking and rewriting the packet's version number, checksum and time-to-live field, and updating counters used for network management.

- Switching:

  Switching via Memory: In this method, the router's CPU has direct control over the switching between input and output ports. When a packet arrives at an input port, it signals the routing processor via an interrupt. The packet is then copied from the input port into processor memory. The routing processor extracts the destination address from the header, looks up the appropriate output port in the forwarding table, and copies the packet to the output port's buffers. This method limits the overall forwarding throughput, as only one memory read/write over the shared system bus can be done at a time.

Switching via a Bus: In this approach, an input port transfers a packet directly to the output port over a shared bus, without intervention by the routing processor. The input port adds a switch-internal label (header) to the packet indicating the local output port to which this packet is being transferred and transmits the packet onto the bus. The packet is received by all output ports, but only the port that matches the label will keep the packet. The label is then removed at the output port. This method is often sufficient for routers operating in small local area and enterprise networks, but its speed is limited by the bus speed.

Switching via inter connection network: This method is used to overcome the bandwidth limitation of a single, shared bus. It involves using a more sophisticated interconnection network, similar to those used to interconnect processors in a multiprocessor computer architecture. A key component of this method is a crossbar switch, an interconnection network consisting of 2N buses that connect N input ports to N output ports. Unlike the previous two switching approaches (memory and bus), crossbar networks are capable of forwarding multiple packets in parallel.

- Output processing: Output port processing, takes packets that have been stored in the output port’s memory and transmits them over the output link. This includes selecting and de-queueing packets for transmission, and performing the needed link layer and physical-layer transmission functions

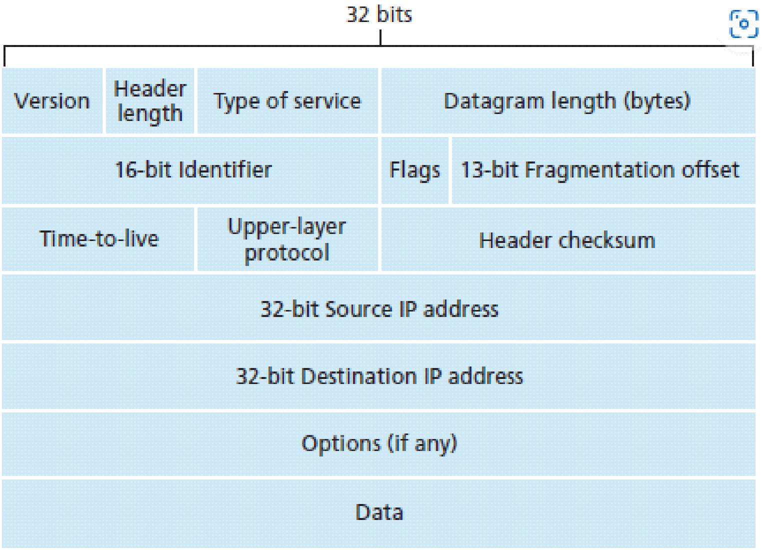
IPv4

- Each IP address is 32 bits long (equivalently, 4 bytes), and there are thus a total of 2^32 possible IP addresses. By approximating 210 by 103, it is easy to see that there are about 4 billion possible IP addresses. These addresses are typically written in so-called dotted-decimal notation, in which each byte of the address is written in its decimal form and is separated by a period (dot) from other bytes in the address.

IPv4	**IPv6**
IPv4 has a 32-bit address length	IPv6 has a 128-bit address length
It Supports Manual and DHCP address configuration	It supports Auto and renumbering address configuration
In IPv4 end to end, connection integrity is Unachievable	In IPv6 end-to-end, connection integrity is Achievable
It can generate 4.29×109 address space	The address space of IPv6 is quite large it can produce 3.4× 1038 address space
The Security feature is dependent on the application	IPSEC is an inbuilt security feature in the IPv6 protocol
Address representation of IPv4 is in decimal	Address Representation of IPv6 is in hexadecimal
Fragmentation performed by Sender and forwarding routers	In IPv6 fragmentation is performed only by the sender
In IPv4 Packet flow identification is not	In IPv6 packet flow identification

available	are Available and uses the flow label field in the header
In IPv4 checksum field is available	In IPv6 checksum field is not available
It has a broadcast Message Transmission Scheme	In IPv6 multicast and anycast message transmission scheme is available
In IPv4 Encryption and Authentication facility not provided	In IPv6 Encryption and Authentication are provided
IPv4 has a header of 20-60 bytes.	IPv6 has a header of 40 bytes fixed
IPv4 can be converted to IPv6	Not all IPv6 can be converted to IPv4
IPv4 consists of 4 fields which are separated by addresses dot (.)	IPv6 consists of 8 fields, which are separated by a colon (:)
IPv4's IP addresses are divided into five different classes. Class A , Class B, Class C, Class D , Class E.	IPv6 does not have any classes of the IP address.
IPv4 supports VLSM(Variable Length subnet mask).	IPv6 does not support VLSM.
Example of IPv4: 66.94.29.13	Example of IPv6: 2001:0000:3238:DFE1:0063:0000:0000:FEFB

- DHCP, which stands for Dynamic Host Configuration Protocol, is a network management protocol used on Internet Protocol (IP) networks. It automatically provides an Internet Protocol (IP) host with its IP address and other related configuration information such as the subnet mask and default gateway
-



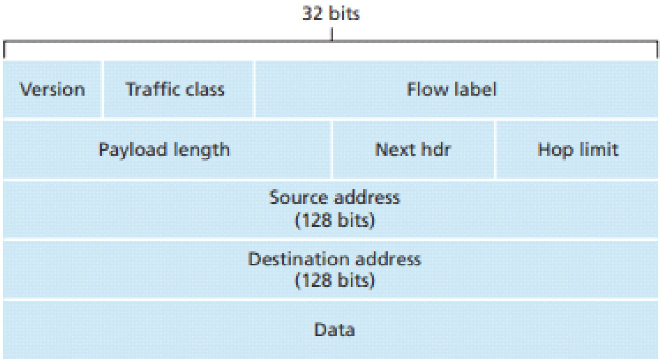
- 

Figure 4.24 ♦ IPv6 datagram format

Routing algorithm:

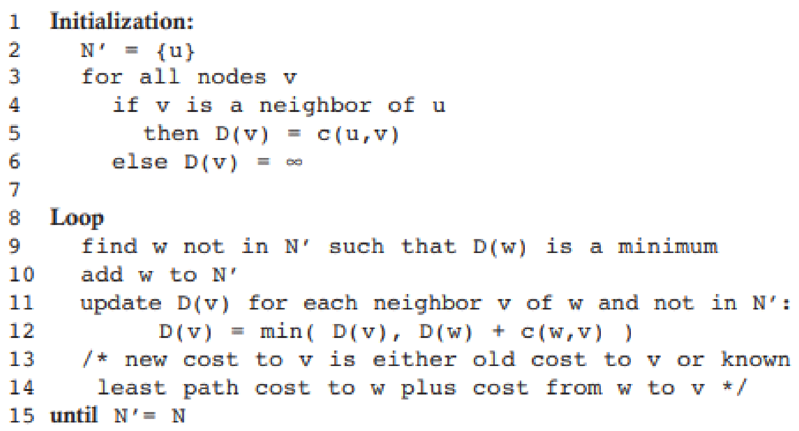
The purpose of a routing algorithm is then simple: given a set of routers, with links connecting the routers, a routing algorithm finds a "good" path from source router to destination router. Typically, a good path is one that has the least cost

- Link state algorithm:
  In a link-state algorithm, each node in the network has a complete, identical view of the network's topology and all link costs. This is achieved by having each node broadcast link-state packets to all other nodes in the network. Each link-state packet contains the identities and costs of its attached links.

  Dijkstra's algorithm is an iterative algorithm that computes the least-cost path from a source node (referred to as 'u') to all other nodes in the network. After the kth iteration of the algorithm, the least-cost paths are known to k destination nodes, and among the least-cost paths to all destination nodes, these k paths will have the k smallest costs.

  The algorithm uses the following notation:

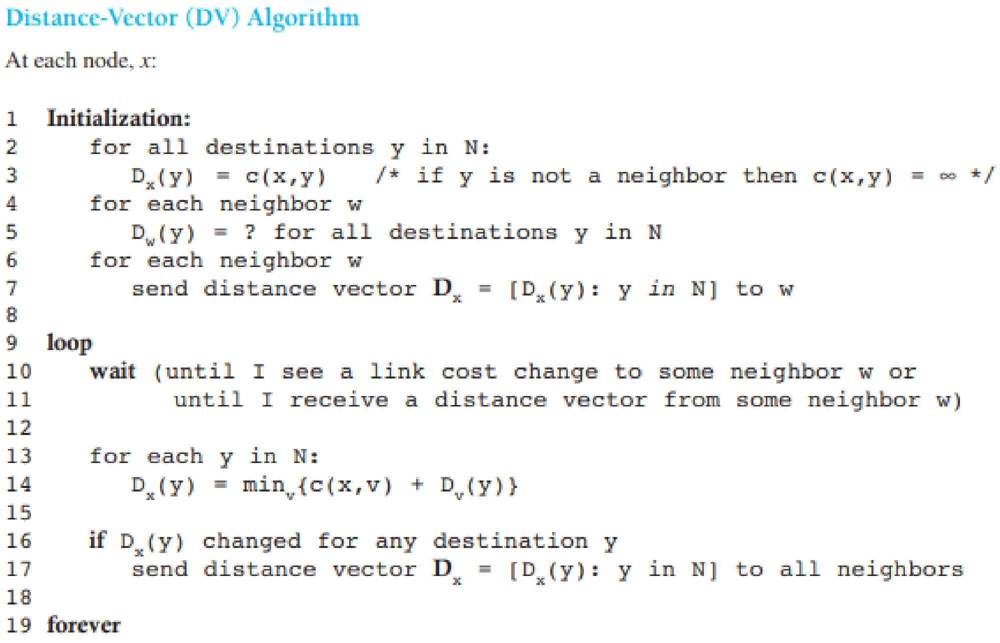
  D(v): The cost of the least-cost path from the source node to destination 'v' as of the current iteration of the algorithm.
  p(v): The previous node (neighbor of 'v') along the current least-cost path from the source to 'v'.
  N': A subset of nodes; 'v' is in N' if the least-cost path from the source to 'v' is definitively known.
  The algorithm consists of an initialization step followed by a loop. The loop is executed a number of times equal to the number of nodes in the network. Upon termination, the algorithm will have calculated the shortest paths from the source node 'u' to every other node in the network.

- 

```
Initialization:
  N' = {u}
  for all nodes v
    if v is a neighbor of u
      then D(v) = c(u,v)
    else D(v) = ∞

Loop
  find w not in N' such that D(w) is a minimum
  add w to N'
  update D(v) for each neighbor v of w and not in N':
        D(v) = min( D(v), D(w) + c(w,v) )
  /* new cost to v is either old cost to v or known
   least path cost to w plus cost from w to v */
until N'= N
```

- Distance vector algorithm:
  In DVR, each router maintains a routing table. It contains only one entry for each router. It contains two parts – a preferred outgoing line to use for that destination and an estimate of time (delay). Tables are updated by exchanging the information with the neighbor's nodes.
  Each router knows the delay in reaching its neighbors (Ex – send echo request).
  Routers periodically exchange routing tables with each of their neighbors.
  It compares the delay in its local table with the delay in the neighbor's table and the cost of reaching that neighbor.
  If the path via the neighbor has a lower cost, then the router updates its local table to forward packets to the neighbor.



Distance-Vector (DV) Algorithm

At each node, *x*:

```
Initialization:
   for all destinations y in N:
      $D_x(y)$ = c(x,y)    /* if y is not a neighbor then c(x,y) = ∞ */
   for each neighbor w
      $D_w(y)$ = ? for all destinations y in N
   for each neighbor w
      send distance vector $\mathbf{D}_x$ = [$D_x(y)$: y in N] to w

loop
   wait (until I see a link cost change to some neighbor w or
         until I receive a distance vector from some neighbor w)

   for each y in N:
      $D_x(y)$ = $\min_v\{c(x,v) + D_v(y)\}$

   if $D_x(y)$ changed for any destination y
      send distance vector $\mathbf{D}_x$ = [$D_x(y)$: y in N] to all neighbors

forever
```

Quality of Service (QoS)
QoS is a set of techniques to manage network resources by prioritizing certain types of traffic, ensuring that applications requiring real-time data transmission, like video conferencing or online gaming, have the necessary bandwidth and low latency.

Components of QoS:
Bandwidth Management: Allocating sufficient bandwidth to prevent jitter and delay for sensitive applications.
Latency and Jitter Control: Minimizing delay and variation in packet arrival

times to ensure smooth data flow.
Loss Management: Reducing packet loss which can significantly affect the quality of streaming media and real-time communications2.