

9.4.3. Flooding

This is another static algorithm. In this algorithm, every incoming packet is sent out on every outgoing line except the line on which it has arrived. One disadvantage of flooding is that it generates a large number of duplicate packets. Infact, it produces infinite number of duplicate packets unless we somehow damp the process. There are various damping techniques such as,

- ✓ (i) Using a hop counter.
- ✓ (ii) To keep a track of packets which have been flooded.
- ✓ (iii) Selective flooding.

Hop-Count –

- A hop counter may be contained in the packet header which is decremented at each hop.
with the packet being discarded when the counter becomes zero
- The sender initializes the hop counter. If no estimate is known, it is set to the full diameter of the subnet.
- Keep track of the packets which are responsible for flooding using a sequence number. Avoid sending them out a second time.

2. Another technique is to keep the track of the packets that have been flooded, to avoid sending them a second time. For this, the source router put a sequence number in each packet it receives from its hosts. Each router then needs a list per source router telling which sequence numbers originating at that source have already been seen. If an incoming packet is on the list, it is not flooded.

3. Another solution is to use **selective flooding**. In selective flooding the routers do not send every incoming packet out on every output line. Instead packet is sent only on those lines which are approximately going in the right direction.

Characteristics –

- All possible routes between Source and Destination is tried. A packet will always get through if path exists
- As all routes are tried, there will be atleast one route which is the shortest
- All nodes directly or indirectly connected are visited

Limitations –

- Flooding generates vast number of duplicate packets
- Suitable damping mechanism must be used