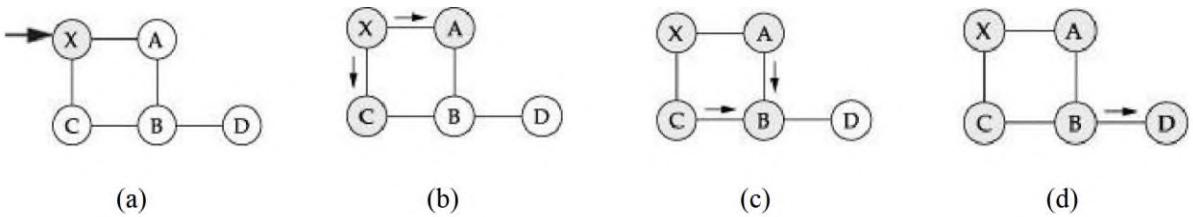
4.4 LINK STATE ROUTING (LSR) & OPEN SHORTEST PATH PROTOCOL (OSPF)

- Each node knows *state* of link to its neighbors and *cost*.
- Nodes create an update packet called *link-state packet* (LSP) that contains:
    1. ID of the node
    2. List of neighbors for that node and associated cost
    3. 64-bit Sequence number
    4. Time to live
- Link-State routing protocols rely on two mechanisms:
    1. ➢***Reliable flooding*** of link-state information to all other nodes
    2. ➢***Route calculation*** from the accumulated link-state knowledge

Reliable Flooding

- Each node *sends* its LSP out on each of its directly connected links.
- When a node receives LSP of another node, checks if it has an LSP already for that node.
- If not, it stores and forwards the LSP on all other links except the incoming one.
- Else if the received LSP has a *bigger* sequence number, then it is stored and forwarded. Older LSP for that node is *discarded*.
- Otherwise discard the received LSP, since it is not latest for that node.
- Thus recent LSP of a node eventually *reaches* all nodes, i.e., reliable *flooding*.
- Flooding of LSP in a small network is as follows:
    1. When node *X* receives *Y*'s LSP (*fig a*), it floods onto its neighbors *A* and *C* (*fig b*)
    2. Nodes *A* and *C* forward it to *B*, but does not sends it back to *X* (*fig c*).
    3. Node *B* receives two copies of LSP with same sequence number.
    4. Accepts one LSP and forwards it to *D* (*fig d*). Flooding is complete.
- LSP is generated either *periodically* or when there is a *change* in the topology



Route Calculation

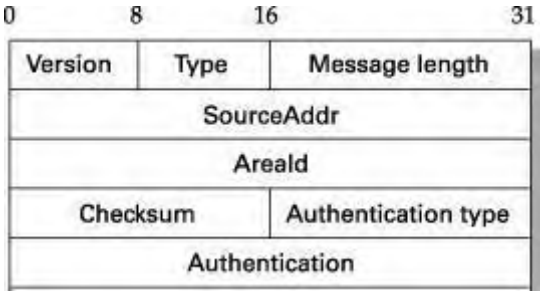
- Each node knows the entire topology, once it has LSP from every other node.
- Forward search algorithm is used to compute routing table from the received LSPs.

- Each node maintains two lists, namely Tentative and Confirmed with entries of the form (Destination, Cost, NextHop).

OPEN SHORTEST PATH FIRST PROTOCOL (OSPF)

- OSPF is a non-proprietary widely used link-state routing protocol. •OSPF Features are:
    1. **Authentication—**Malicious host can collapse a network by advertising to reach every host with cost 0. Such disasters are averted by authenticating routing updates.
    2. **Additional hierarchy—**Domain is partitioned into areas, i.e., OSPF is more scalable.
    3. **Load balancing—**Multiple routes to the same place are assigned same cost. Thus traffic is distributed evenly.

Link State Packet Format



1. **Version —** represents the current version, i.e., 2.
2. **Type —** represents the type (1–5) of OSPF message. Type 1 - "hello" message, Type 2 - request, Type 3 – send , Type 4 - acknowledge the receipt of link state messages , Type 5 - reserved
3. **SourceAddr —** identifies the sender
4. **AreaId —** 32-bit identifier of the area in which the node is located
5. **Checksum —** 16-bit internet checksum
6. **Authentication type —** 1 (simple password), 2 (cryptographic authentication).
7. **Authentication —** contains password or cryptographic checksum