Parul® University

Computer Networks (203105255)

Prof. Manish Kumar

Assistant Professor

Computer Science & Engineering

Parul®
University

DIGITAL LEARNING CONTENT

CHAPTER-3

Network Layer

Parul® University

DIGITAL LEARNING CONTENT

Outline

- **Topics to be covered:**
- **Switching**
- **Logical Addressing- IPv4 and IPv6**
- **Address Mapping- ARP, RARP, BOOTP and DHCP**
- **Delivery-Forwarding**
- **Unicast Routing**

Switching techniques

- In large networks, there can be multiple paths from sender to receiver.
- The switching technique will decide the best route for data transmission.
- Switching technique is used to connect the systems for making one-to-one communication.
- Classification Of Switching Techniques

1) **Circuit Switching**
2) **Packet Switching**
3) **Message Switching**

Switching Techniques

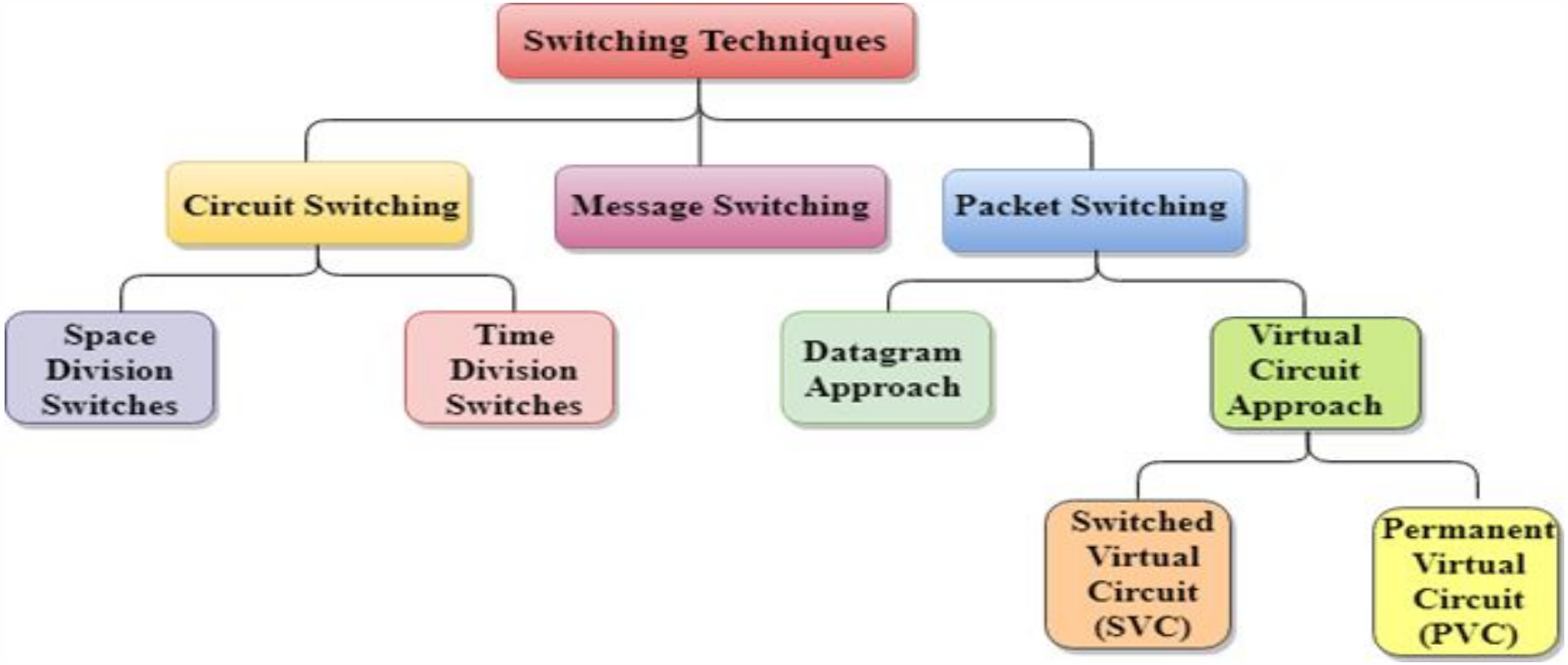


Figure: 3.1 Switching Techniques

Circuit Switching

- **Circuit switching** is a switching technique that establishes a dedicated path between sender and receiver.
- In the Circuit Switching Technique, once the connection is established then the dedicated path will remain to exist until the connection is terminated.
- Circuit switching in a network operates in a similar way as the telephone works.

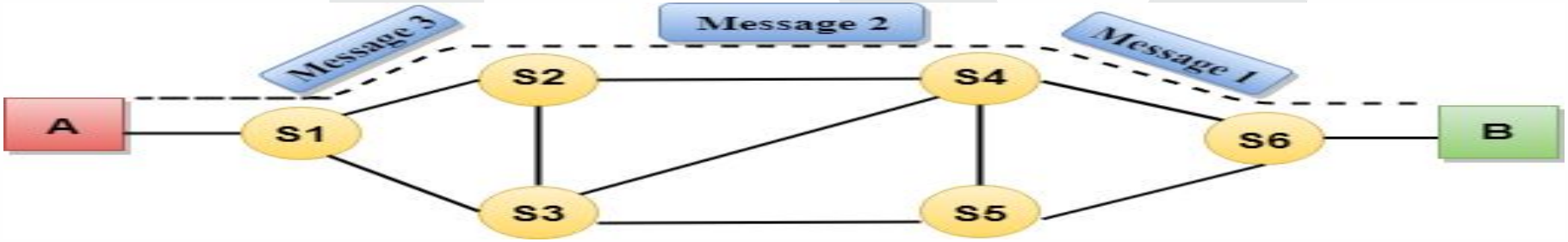


Figure: 3.2 Circuit Switching

Contd.

- **Advantages Of Circuit Switching**:

1) In the case of Circuit Switching technique, the communication channel is dedicated.
2) It has fixed bandwidth.

- **Disadvantages Of Circuit Switching:**

1) It takes a long time to establish a connection approx 10 seconds during which no data can be transmitted.
2) It is more expensive than other switching techniques as a dedicated path is required for each connection.
3) It is inefficient to use because once the path is established and no data is transferred, then the capacity of the path is wasted.

Message Switching

- **Message switching** is a switching technique in which a message is transferred as a complete unit and routed through intermediate nodes at which it is stored and forwarded.
- Each and every node stores the entire message and then forward it to the next node. This type of network is known as store and forward network.
- Message switching treats each message as an independent entity.

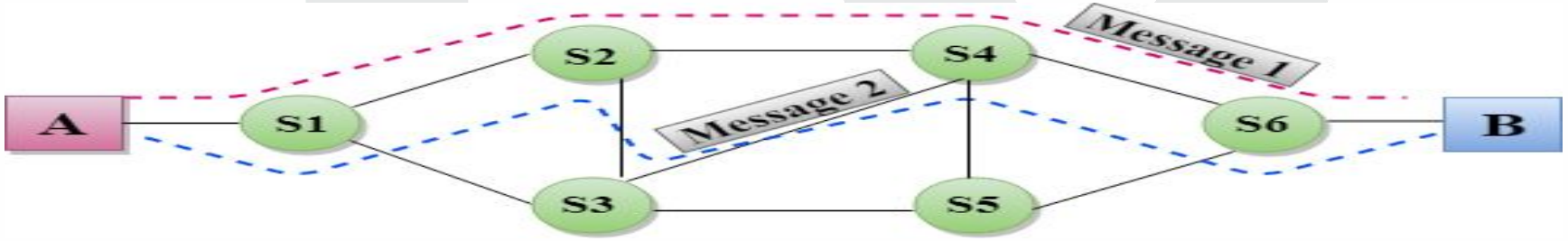


Figure: 3.3 Message Switching

Contd.

- **Advantages Of Message Switching**:

1) Data channels are shared among the communicating devices that improve the efficiency of using available bandwidth.
2) Traffic congestion can be reduced because the message is temporarily stored in the nodes.
3) Message priority can be used to manage the network

- **Disadvantages Of Message Switching:**

1) The message switches must be equipped with sufficient storage to enable them to store the messages until the message is forwarded.
2) The Long delay can occur due to the storing and forwarding facility provided by the message switching technique.

Packet Switching

- **Packet switching** in which the message splits into smaller pieces known as packets and is sent in one go, packets are given a unique number to identify their order at the receiving end.
- Packets will travel across the network, taking the shortest path as possible. All the packets are reassembled at the receiving end in correct order. If any packet is missing or corrupted, then the sender resend the message. If the correct order of the packets is reached, then the acknowledgment message will be sent.

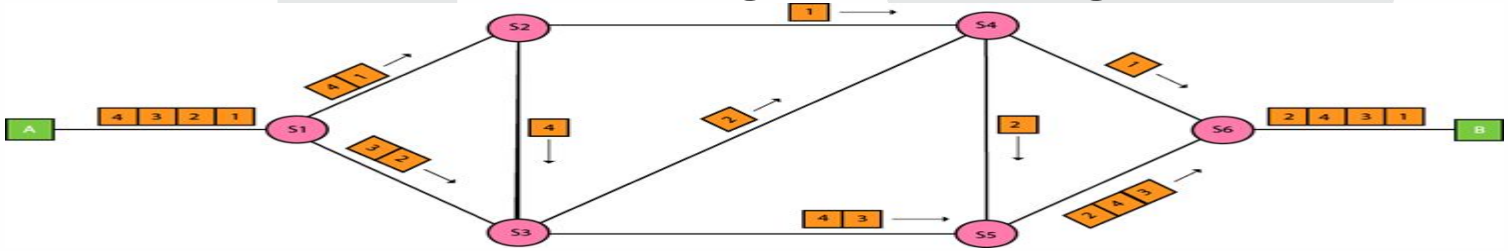


Figure: 3.4 Packet Switching

Contd.

- **Advantages Of Packet Switching**:

1) Cost-effective
2) Reliable
3) Efficient

- **Disadvantages Of Packet Switching:**

1) Packet Switching technique cannot be implemented in those applications that require low delay and high-quality services.
2) The protocols used in a packet switching technique are very complex and requires high implementation cost.
3) If the network is overloaded or corrupted, then it requires retransmission of lost packets. It can also lead to the loss of critical information if errors are nor recovered.

Logical Addressing

- **IPv4 ADDRESSES:** An IPv4 address is a **32-bit address** that uniquely and universally defines the connection of a device (for example, a computer or a router) to the Internet**.**
- Two devices on the Internet can never have the same address at the same time.
- The address space of IPv4 is **2^32** or 4,294,967,296.
- Notations:

1) **Binary: 01110101 10010101 00011101 00000010**
2) **Dotted- Decimal: 117.149.29.2**

Classful Addressing

- An IP address is 32-bit long. An IP address is divided into sub-classes:

1) Class A
2) Class B
3) Class C
4) Class D
5) Class E

- An IP address is divided into two parts:
- **Network ID**: It represents the number of networks.
- **Host ID**: It represents the number of hosts.

Logical Addressing

- Each class have a specific range of IP addresses.

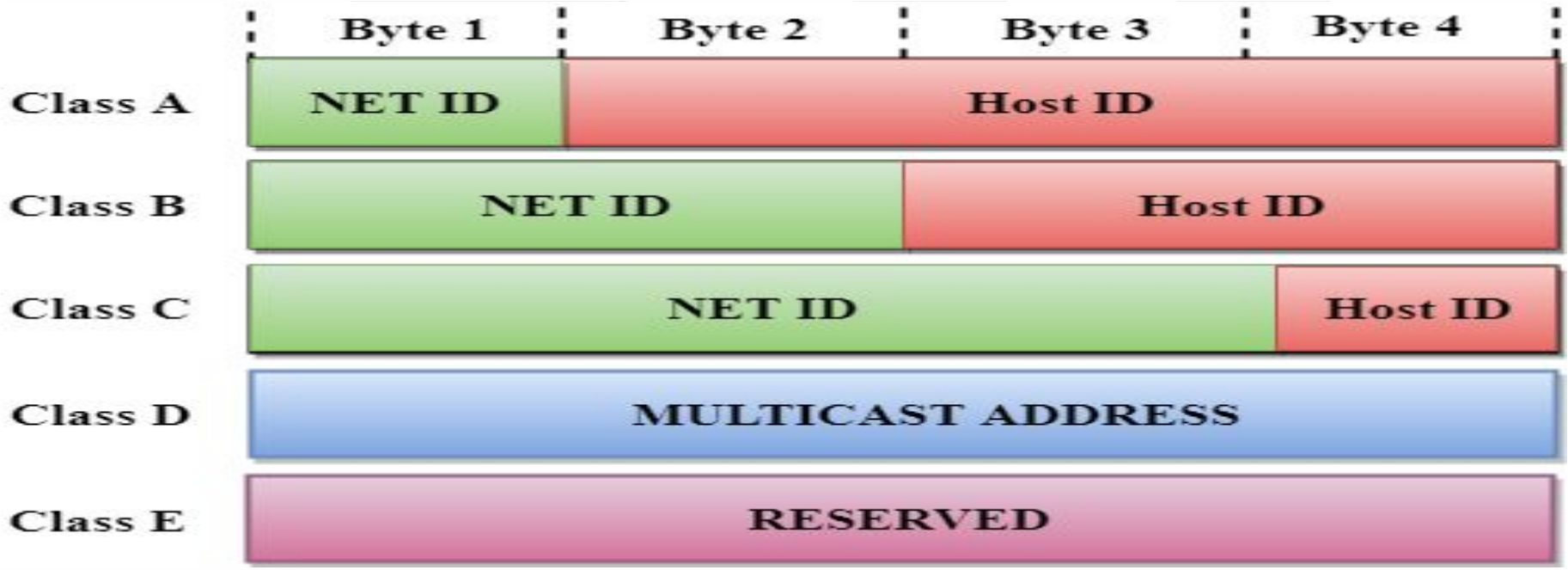


Figure: 3.5 IP Address Classes

Class A

- The **network ID** is 8 bits long. The **host ID** is 24 bits long.
- IP address is assigned to those networks that contain a **large number of hosts.**
- In Class A, the first bit in higher order bits of the first octet is always set to 0 and the remaining 7 bits determine the network ID. The 24 bits determine the host ID in any network.
- The total number of networks in Class A = 2^7 = 128 network address. The total number of hosts in Class A = 2^24 - 2 = 16,777,214 host address.

Figure: 3.6 Class A Format

Class B

- The **network ID** is 16 bits long. The **host ID** is 16 bits long.
- An IP address is assigned to those networks that range from **small-sized to large-sized networks**.
- In Class B, the higher order bits of the first octet is always set to 10, and the remaining14 bits determine the network ID. The other 16 bits determine the Host ID.
- The total number of networks in Class B = 2^14 = 16384 network address. The total number of hosts in Class B = 2^16 - 2 = 65534 host address.

Figure: 3.7 Class B Format

Class C

- The **Network ID** is 24 bits long.
- The **host ID** is 8 bits long..
- An IP address is assigned to only **small-sized** networks.
- In Class C, the higher order bits of the first octet is always set to 110, and the remaining 21 bits determine the network ID. The 8 bits of the host ID determine the host in a network.
- The total number of networks = 2^21 = 2097152 network address.
- The total number of hosts = 2^8 - 2 = 254 host address

Figure: 3.8 Class C Format

Class D and Class E

- **In Class D,** an IP address is reserved for **multicast addresses.** It does not possess subnetting.
- The higher order bits of the first octet is always set to **1110,** and the remaining bits determines the host ID in any network.
- **In Class E,** an IP address is used for the **future use** or for the research and development purposes. It does not possess any subnetting. The higher order bits of the first octet is always set to **1111,** and the remaining bits determines the host ID in any network.

Figure: 3.9 Class D and E Format

Need For IPv6

- **Subnetting**: If an organization was granted a large block in class A or B, it could divide the addresses into several contiguous groups and assign each group to smaller networks (called **subnets**) or, share part of the addresses with neighbors.
- **Supernetting:** In supernetting, an organization can combine several class C blocks to create a larger range of addresses. Supernetting decreases the number of Is in the mask. For example, if an organization is given four class C addresses, the mask changes from /24 to /22.
- **Address Depletion:** Fast growth of the Internet led to the near depletion of the available addresses.

Classless Addressing

- In this scheme, there are no classes, but the addresses are still granted in blocks.
- In classless addressing, when an entity, small or large, needs to be connected to the Internet, it is granted a block (range) of addresses. The size of the block (the number of addresses) varies based on the nature and size of the entity.
- Despite all short-term solutions, such as classless addressing, Dynamic Host Configuration Protocol (DHCP) address depletion is still a long-term problem for the Internet.

IPv6

- An IPv6 address consists of 16 bytes (octets) and it is 128 bits long.
- **Hexadecimal Colon Notation:** In this notation, 128 bits is divided into eight sections, each 2 bytes in length. Two bytes in hexadecimal notation requires four hexadecimal digits. Therefore, the address consists of 32 hexadecimal digits, with every four digits separated by a colon.

Figure: 3.10 IPv6 Address

Cont..

- **Address Space:** IPv6 has a much larger address space 2^128 addresses are available.
- **Unicast Addresses:** unicast address defines a single computer. The packet sent to a unicast address must be delivered to that specific computer.
- **Multicast Addresses:** Multicast addresses are used to define a group of hosts instead of just one. A packet sent to a multicast address must be delivered to each member of the group.
- **Reserved Addresses:** Another category in the address space is the reserved address. These addresses start
- with eight Os (type prefix is 00000000).

Internet Protocol v4 Header

- Internet Protocol being a layer-3 protocol (OSI) takes data Segments from layer-4 (Transport) and divides it into packets. IP packet encapsulates data unit received from above layer and add to its own header information.

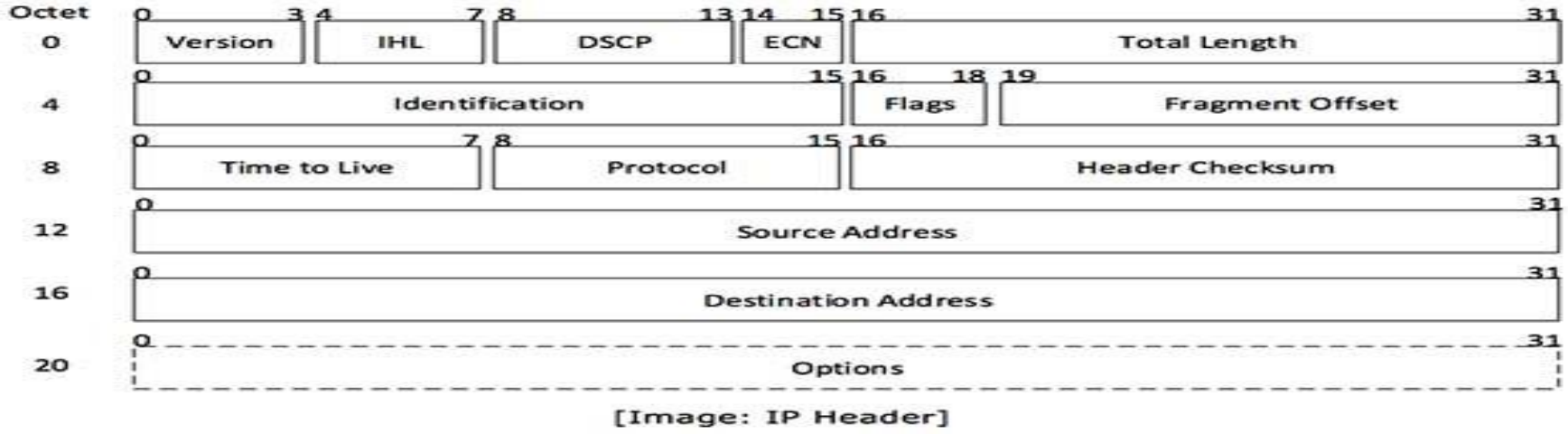


Figure: 3.11 IPv4 Header Format

Internet Protocol v4 Shortcomings

- Pv4 has some deficiencies that make it unsuitable for the fast-growing Internet.
- Despite all short-term solutions, such as subnetting, classless addressing, and NAT, address depletion is still a long-term problem in the Internet.
- The Internet must accommodate real-time audio and video transmission. This type of transmission requires minimum delay strategies and reservation of resources not provided in the IPv4 design.
- The Internet must accommodate encryption and authentication of data for some applications. No encryption or authentication is provided by IPv4

IPv6 Header

- Each packet is composed of a mandatory base header followed by the payload. The payload consists of two parts: optional extension headers and data from an upper layer. The base header occupies 40 bytes, whereas the extension headers and data from the upper layer contain up to 65,535 bytes of information.

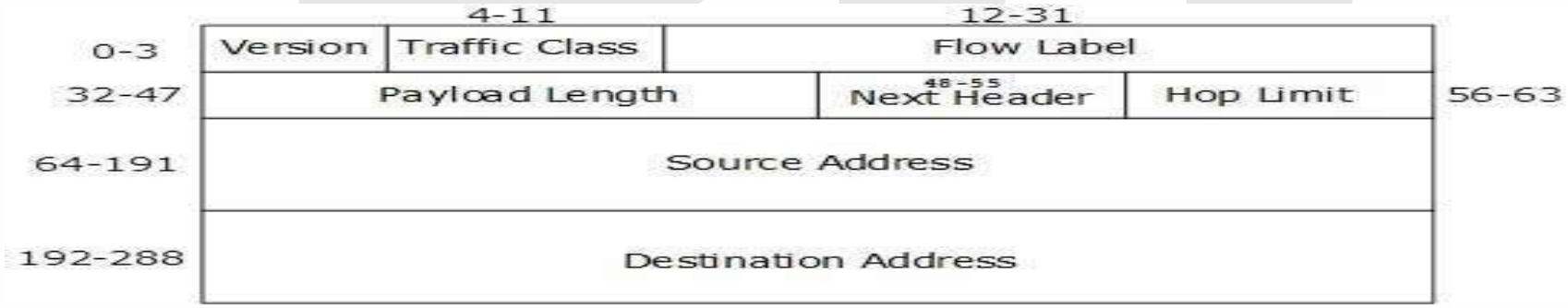


Figure: 3.12 IPv6 Header Format

TRANSITION FROM IPv4 TO IPv6

- Three transition strategies:

1) Dual Stack
2) Tunneling
3) NAT Protocol Translation

- **Dual Stack:** A router can be installed with both IPv4 and IPv6 addresses configured on its interfaces pointing to the network of relevant IP scheme.

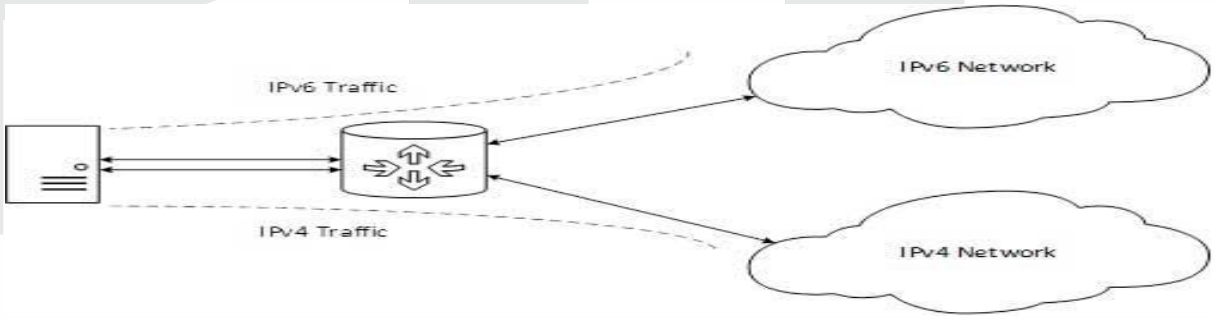


Figure: 3.13 Dual Stack

Cont..

- **Tunneling:** In a scenario where different IP versions exist on intermediate path or transit networks, tunneling provides a better solution where user's data can pass through a non-supported IP version.

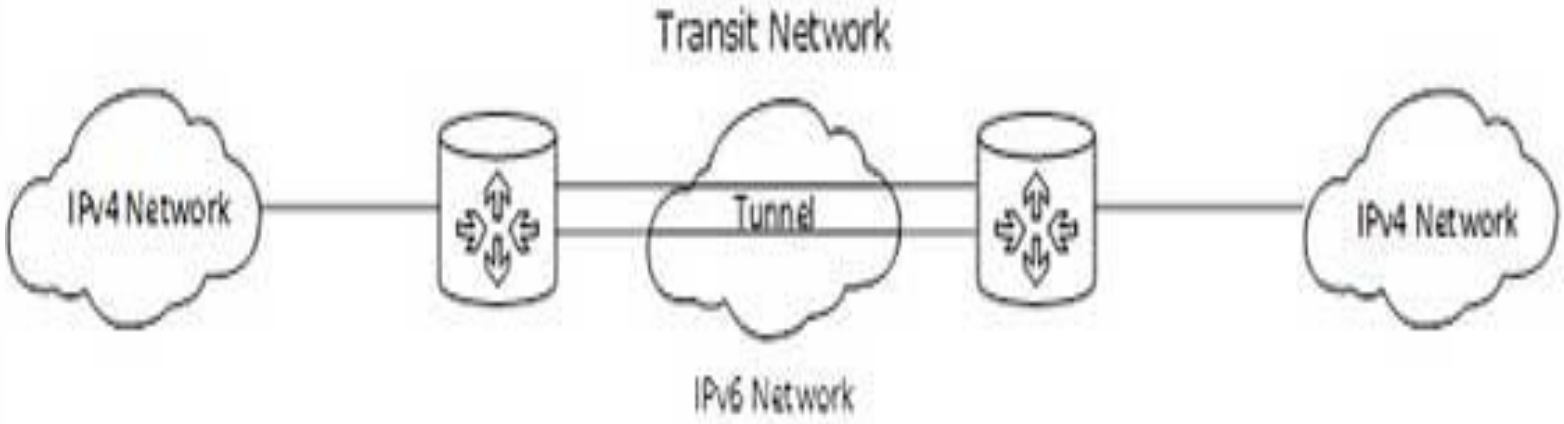


Figure: 3.14 Tunneling

Cont..

- **NAT Protocol Translation:** This is another important method of transition to IPv6 by means of a NAT-PT (Network Address Translation – Protocol Translation) enabled device. With the help of a NAT-PT device, actual can take place happens between IPv4 and IPv6 packets and vice versa.

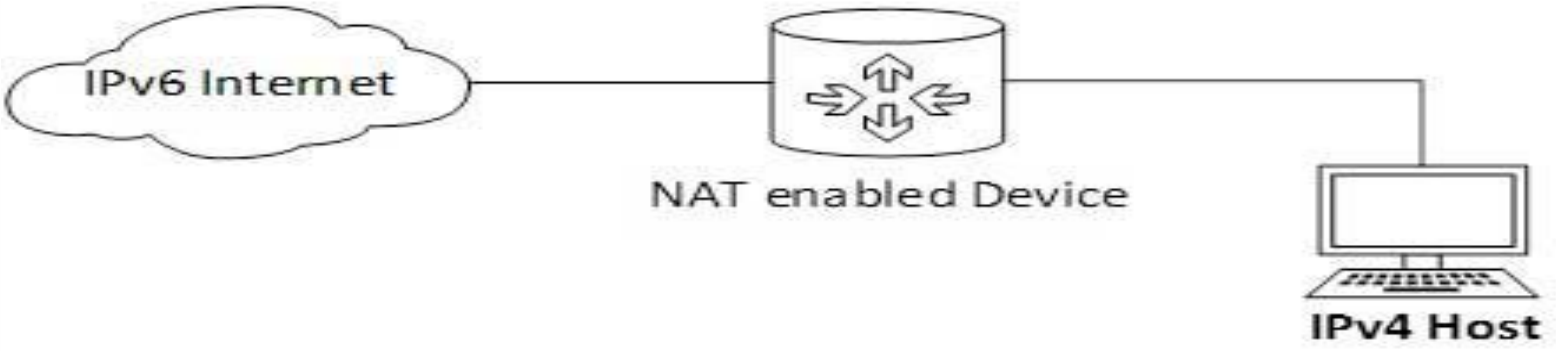


Figure: 3.15 NAT Translation

Address Resolution Protocol(ARP)

- While communicating, a host needs Layer-2 (MAC) address of the destination machine which belongs to the same broadcast domain or network. A MAC address is physically burnt into the Network Interface Card (NIC) of a machine and it never changes.

- On the other hand, IP address on the public domain is rarely changed. If the NIC is changed in case of some fault, the MAC address also changes. This way, for Layer-2 communication to take place, a mapping between the two is required.

Cont..

- To know the MAC address of remote host on a broadcast domain, a computer wishing to initiate communication sends out an ARP broadcast message asking, “Who has this IP address?” Because it is a broadcast, all hosts on the network segment (broadcast domain) receive this packet and process it.
- ARP packet contains the IP address of destination host, the sending host wishes to talk to. When a host receives an ARP packet destined to it, it replies back with its own MAC address.

Cont..

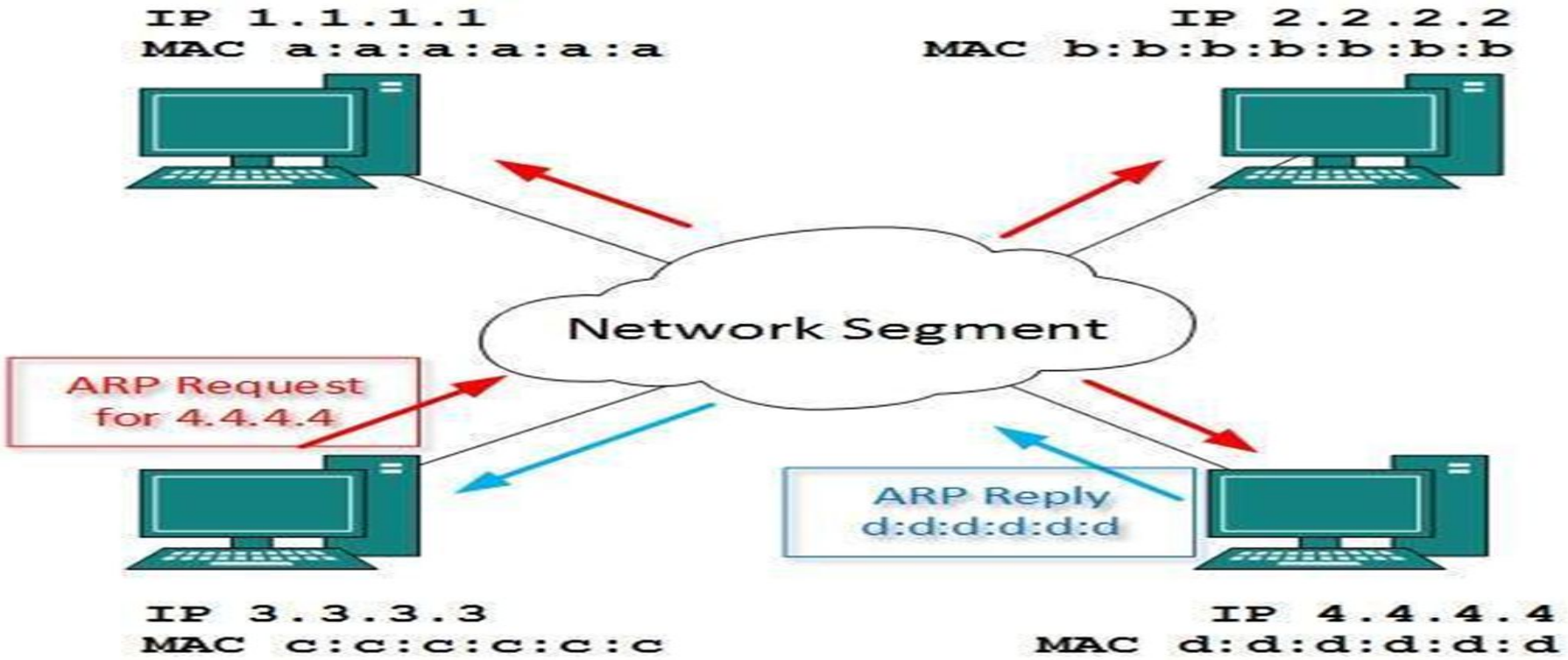


Figure: 3.16 Address Resolution Protocol

Cont..

- Once the host gets destination MAC address, it can communicate with remote host using Layer-2 link protocol.
- This MAC to IP mapping is saved into ARP cache of both sending and receiving hosts. Next time, if they require to communicate, they can directly refer to their respective ARP cache.

- **Reverse ARP** is a mechanism where host knows the MAC address of remote host but requires to know IP address to communicate.

Dynamic Host Configuration Protocol

- Dynamic Host Configuration Protocol (DHCP) is a network management protocol used to dynamically assign an IP address to nay device, or node, on a network so they can communicate using IP (Internet Protocol). DHCP automates and centrally manages these configurations. There is no need to manually assign IP addresses to new devices. Therefore, there is no requirement for any user configuration to connect to a DHCP based network.
- DHCP can be implemented on local networks as well as large enterprise networks. DHCP is the default protocol used by the most routers and networking equipment. DHCP is also called RFC (Request for comments) 2131

Bootstrap Protocol (BOOTP)

- The Bootstrap Protocol is a networking protocol used to by a client for obtaining an IP address from a server. It was originally defined as specification RFC 951 and was designed to replace the Reverse Address Resolution Protocol (RARP), also known as RFC 903.
- Bootstrap protocol was intended to allow computers to find what they need to function properly after booting up. BOOTP uses a relay agent, which allows packet forwarding from the local network using standard IP routing, allowing one BOOTP server to serve hosts on multiple subnets.

Delivery

- The network layer supervises the handling of the packets by the underlying physical networks. We define this handling as the delivery of a packet.
- **Direct Delivery:** In a direct delivery, the final destination of the packet is a host connected to the same physical network as the deliverer.
- **Indirect Delivery:** If the destination host is not on the same network as the deliverer, the packet is delivered indirectly. In an indirect delivery, the packet goes from router to router until it reaches the one connected to the same physical network as its final destination.

Forwarding

- Forwarding means to place the packet in its route to its destination. Forwarding requires a host or a router to have a routing table. When a host has a packet to send or when a router has received a packet to be forwarded, it looks at this table to find the route to the final destination.
- However, this simple solution is impossible today in an internetwork such as the Internet because the number of entries needed in the routing table would make table lookups inefficient.
- **Next-Hop Method Versus Route Method**
- **Network-Specific Method Versus Host-Specific Method**

Routing

- A Routing is a process of selecting path along which the data can be transferred from source to the destination. Routing is performed by a special device known as a router.
- A router is a networking device that forwards the packet based on the information available in the packet header and forwarding table.
- **Types of Routing:**
- Routing can be classified into three categories:

1) **Static Routing**
2) **Default Routing**
3) **Dynamic Routing**

Routing

- **UNICAST ROUTING PROTOCOLS**
- A routing table can be either static or dynamic. A static table is one with manual entries.
- A dynamic table, on the other hand, is one that is updated automatically when there is a change somewhere in the internet**.**
- **Intra- and Interdomain Routing:**
- An autonomous system (AS) is a group of networks and routers under the authority of a single administration. Routing inside an autonomous system is referred to as **intradomain** routing. Routing between autonomous systems is referred to as **interdomain** routing

Routing

- **Types OF Routing Protocols**

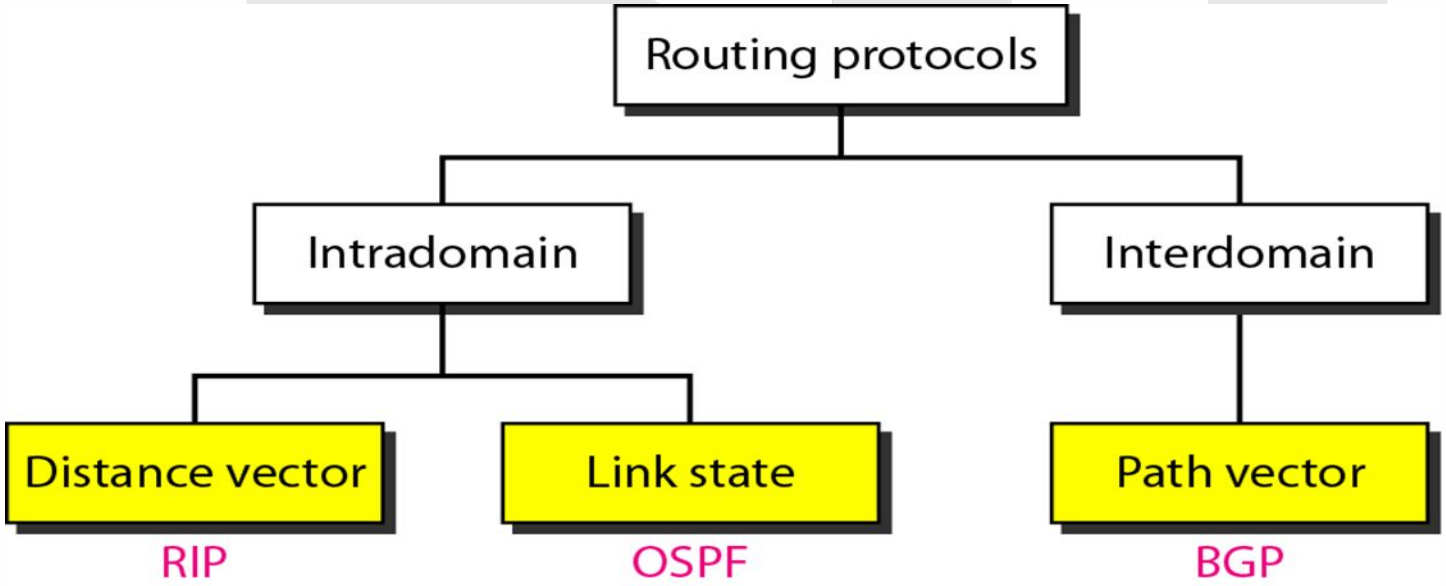


Figure: 3.17 Routing Protocols

Distance vector routing

- In distance vector routing, the least-cost route between any two nodes is the route with minimum distance. In this protocol, as the name implies, each node maintains a vector (table) of minimum distances to every node.
- The table at each node also guides the packets to the desired node by showing the next stop in the route (next-hop routing).

Distance vector routing

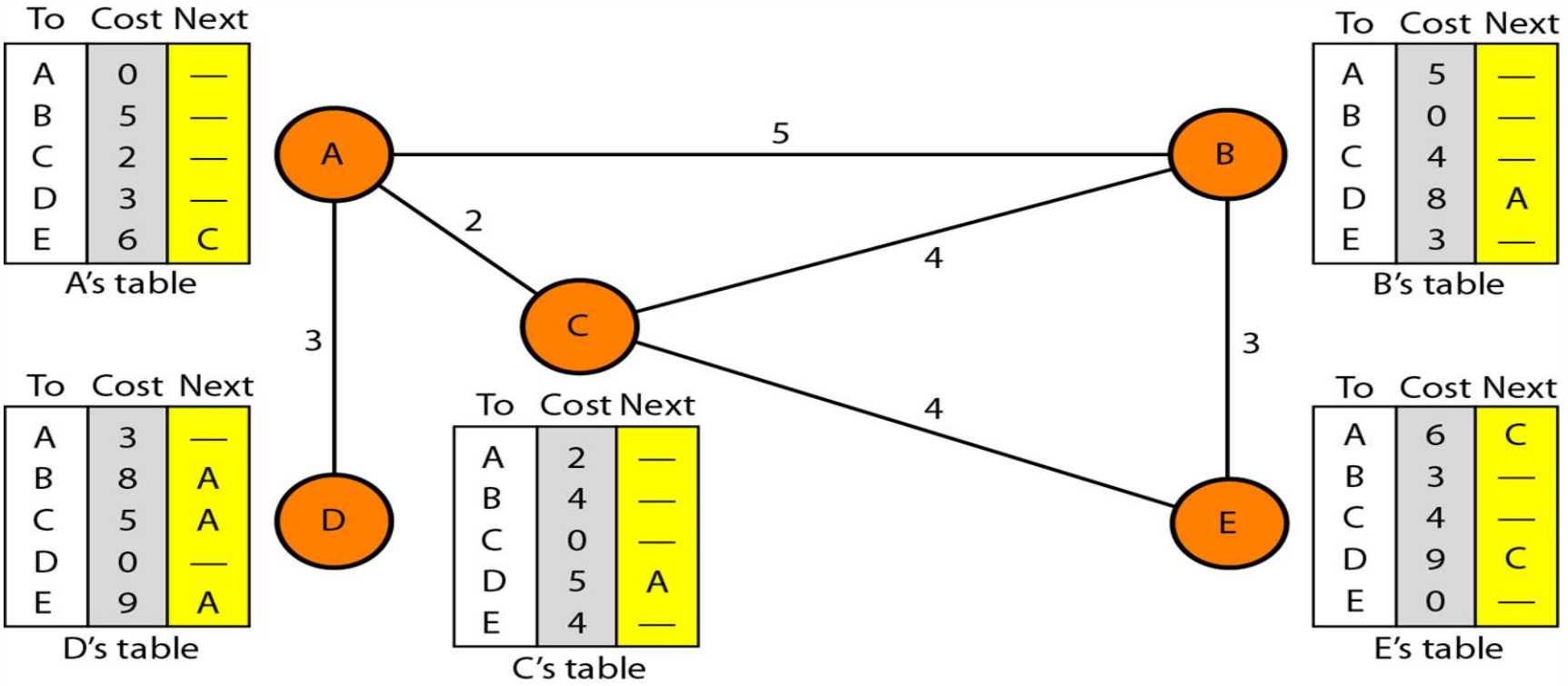


Figure: 3.18 Distance Vector Routing

Distance vector routing

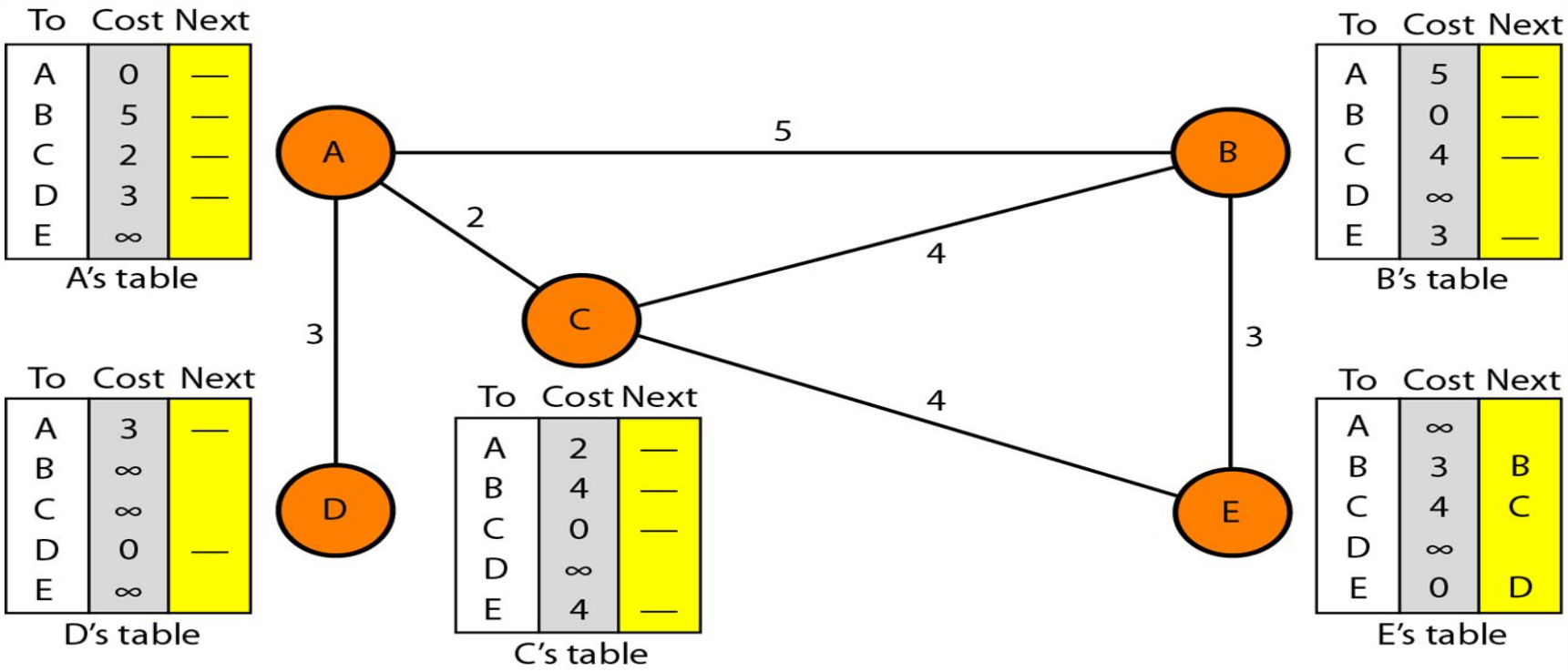


Figure: 3.19 Distance Vector Routing

Distance vector routing

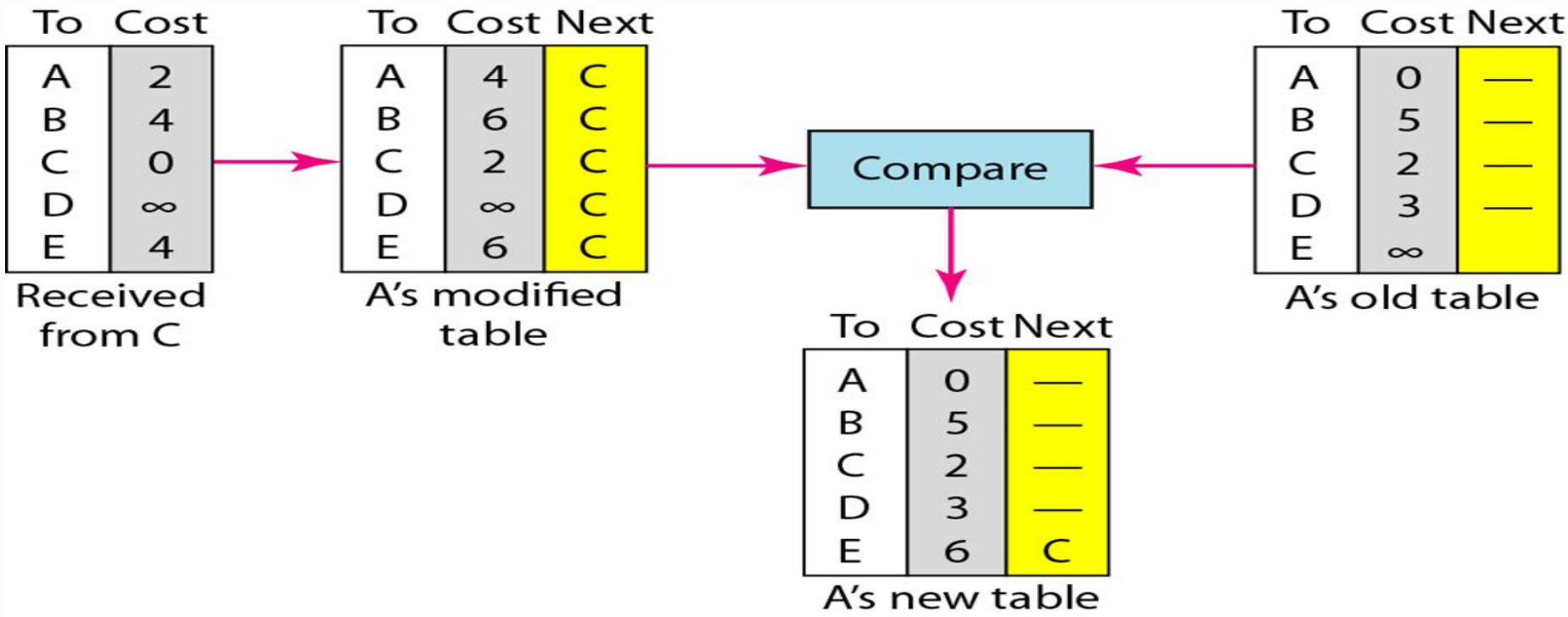


Figure: 3.20 Distance Vector Routing

Distance vector routing

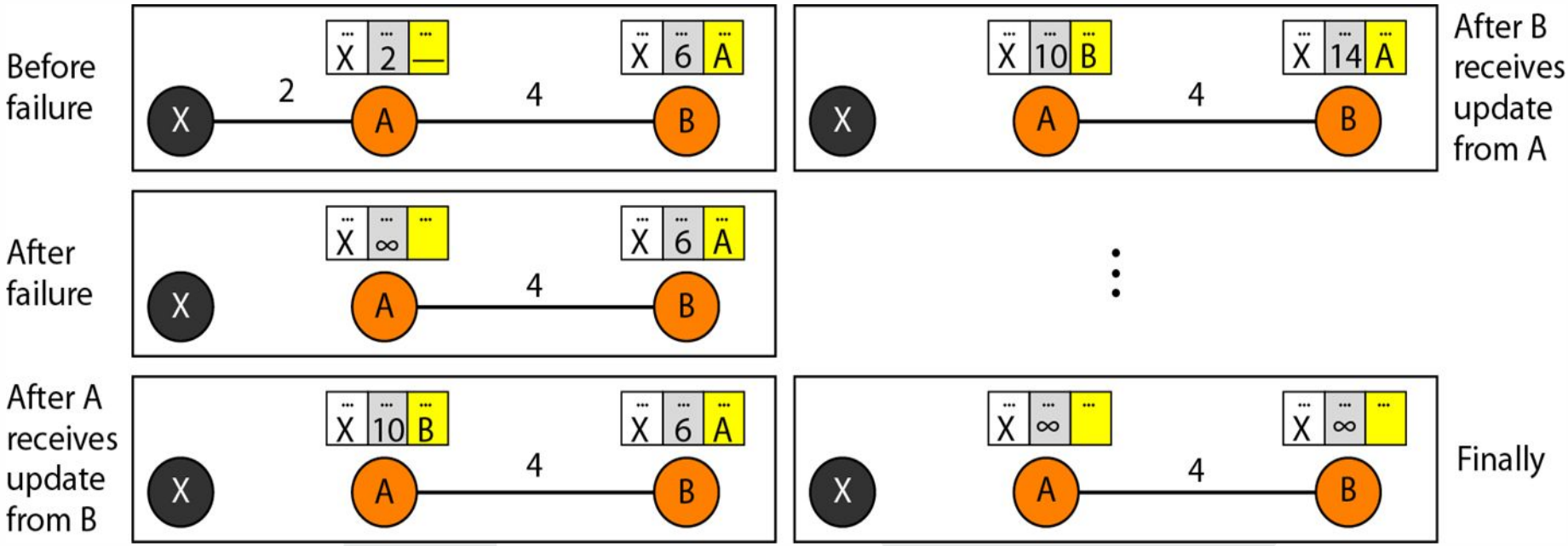


Figure: 3.21 Issues In Distance Vector Routing

Distance vector routing

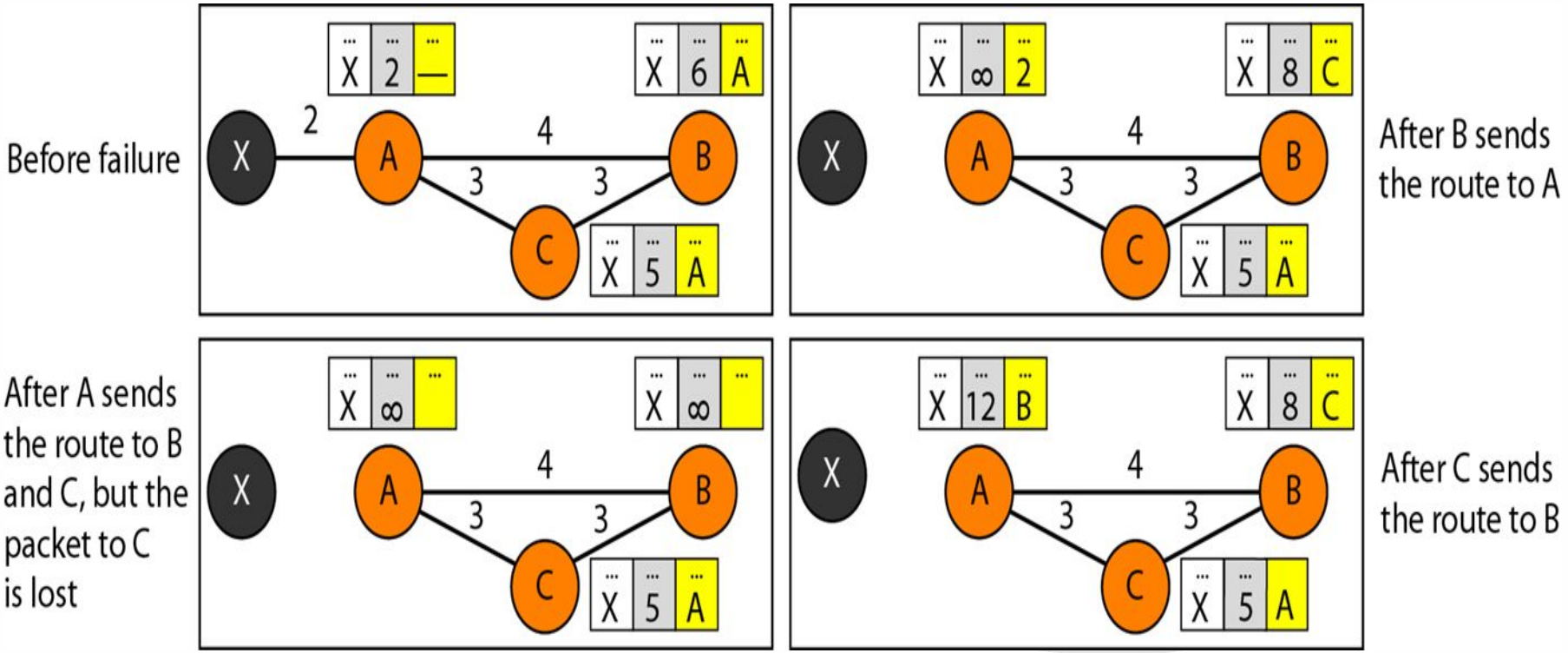


Figure: 3.22 Issues In Distance Vector Routing

Link State Routing

- In link state routing, if each node in the domain has the entire topology of the domain the list of nodes and links, how they are connected including the type, cost (metric), and condition of the links (up or down)-the node can use Dijkstra's algorithm to build a routing table.
- Each node uses the same topology to create a routing table, but the routing table for each node is unique because the calculations are based on different interpretations of the topology.

Link State Routing

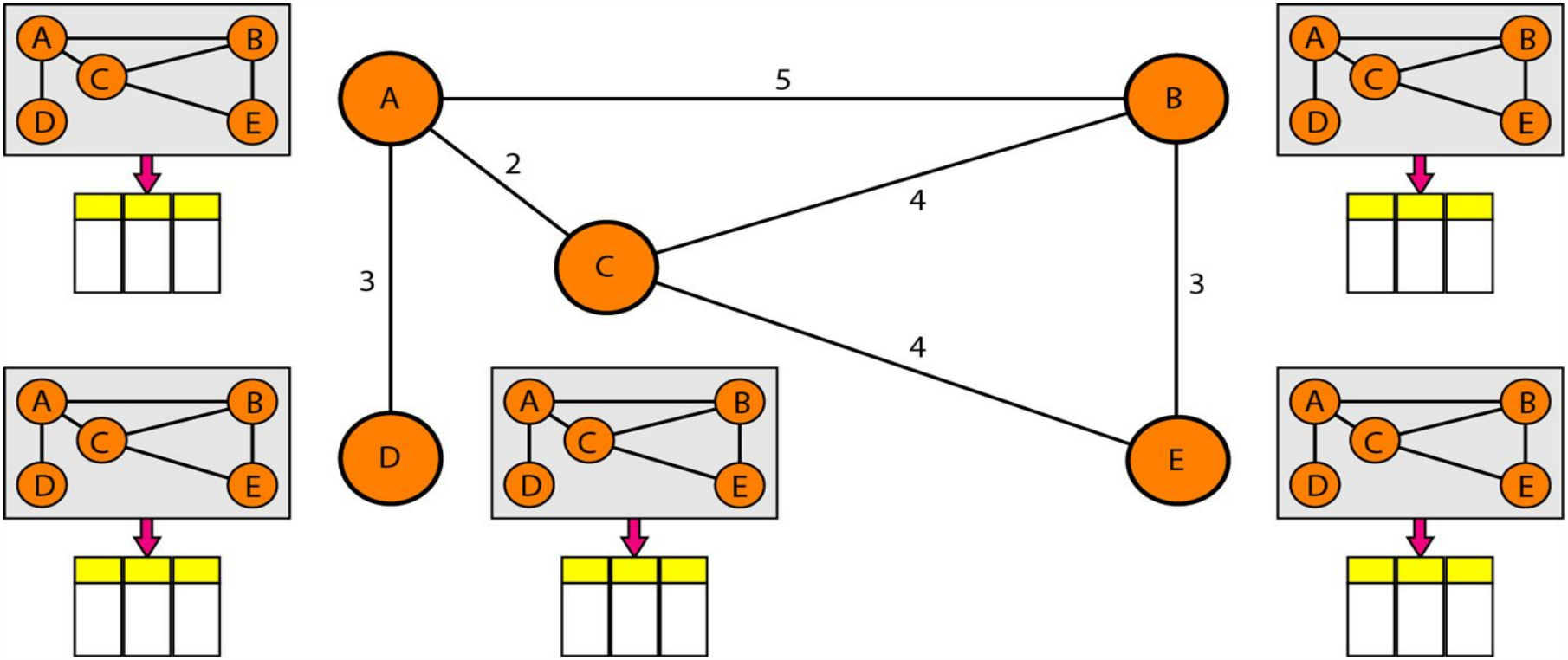


Figure: 3.23 Link State Routing

Link state knowledge

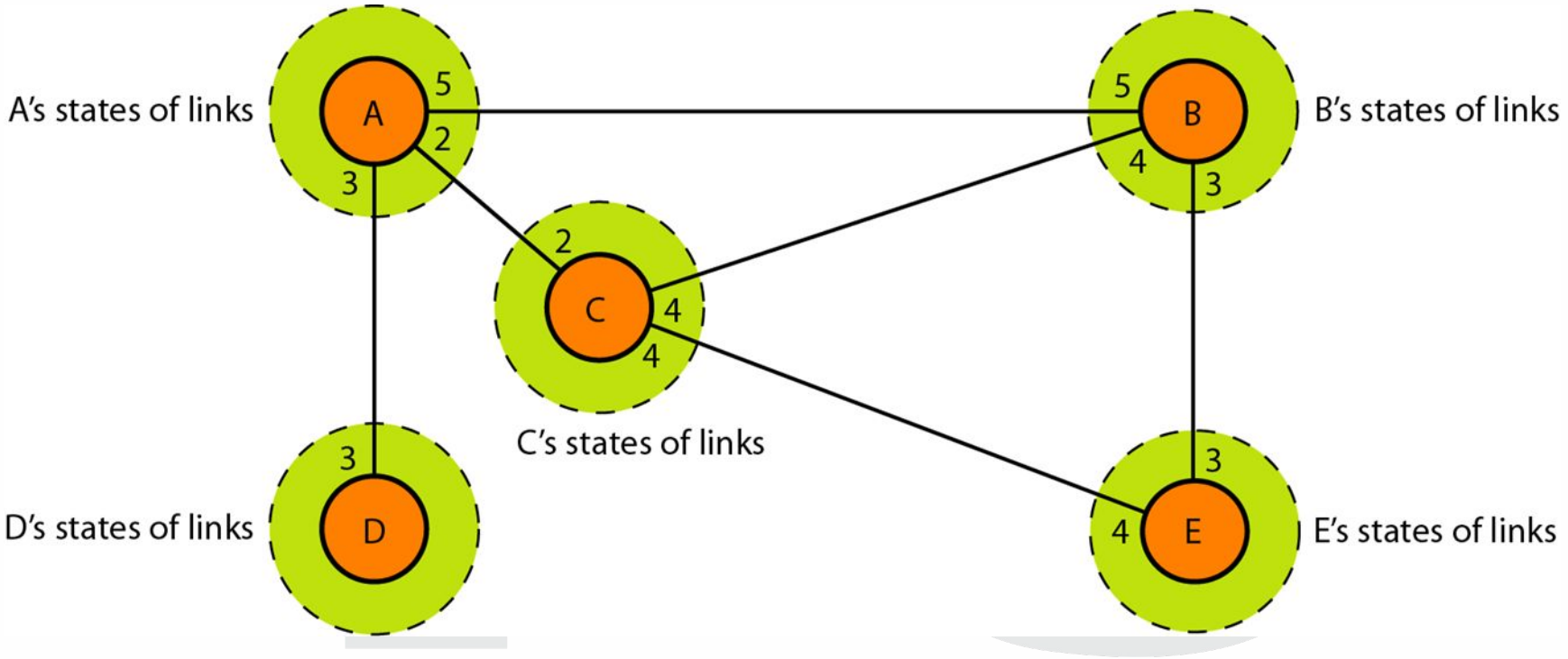


Figure: 3.24 Link State Routing

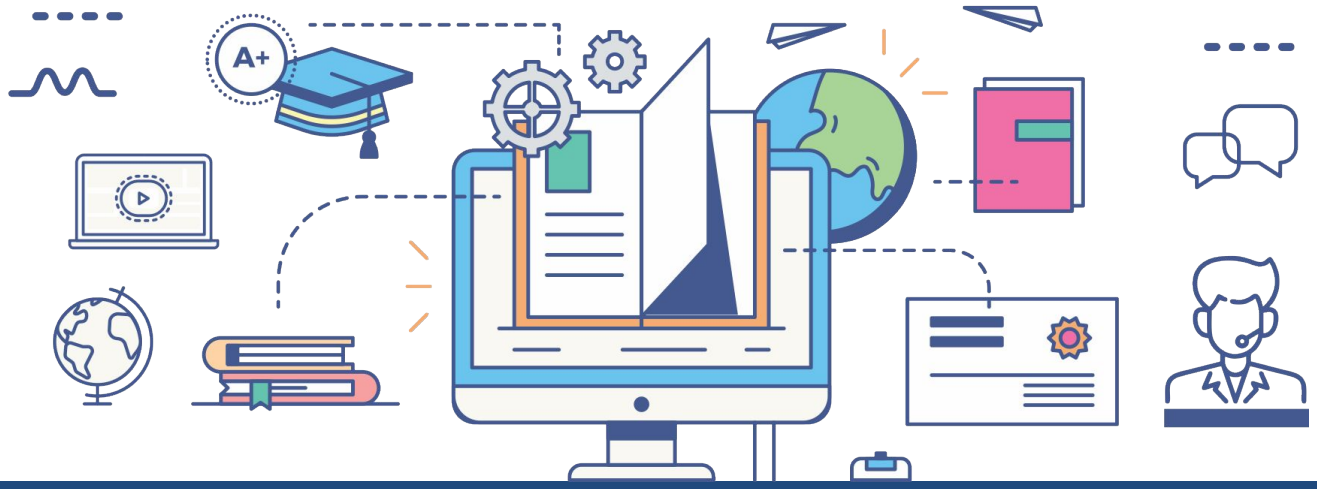
Path Vector Routing

- Distance vector and link state routing are both intradomain routing protocols. They can be used inside an autonomous system, but not between autonomous systems. These two protocols are not suitable for interdomain routing mostly because of scalability.
- Both of these routing protocols become intractable when the domain of operation becomes large. Distance vector routing is subject to instability if there are more than a few hops in the domain of operation. Link state routing needs a huge amount of resources to calculate routing tables. It also creates heavy traffic because of flooding. There is a need for a third routing protocol which we call **path vector routing.**

Path Vector Routing

- Path vector (PV) protocols, such as BGP, are used across domains aka autonomous systems.
- In a path vector protocol, a router does not just receive the distance vector for a particular destination from its neighbor; instead, a node receives the distance as well as path information (aka BGP path attributes), that the node can use to calculate (via the BGP path selection process) how traffic is routed to the destination AS.

DIGITAL LEARNING CONTENT



Parul® University

www.paruluniversity.ac.in