UNIT -4

NETWORK LAYER II

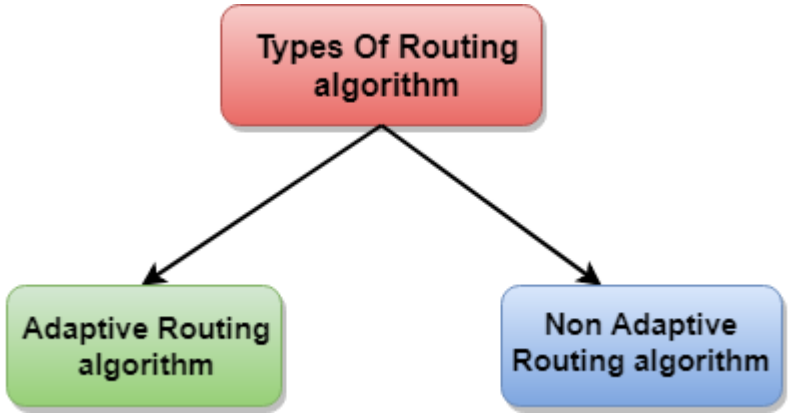
Routing

- Routing is the process of establishing the routes that data packets must follow to reach the destination.
- Routing is a process which is performed by layer 3 (or network layer) devices in order to deliver the packet by choosing an optimal path from one network to another
- In this process, a routing table is created which contains information regarding routes that data packets follow.
- Various routing algorithms are used for the purpose of deciding which route an incoming data packet needs to be transmitted on to reach the destination efficiently.

Routing

Types of Routing

Routing can be classified into three categories:



Routing

Nonadaptive Routing/ Static Routing

- Static Routing is also known as Nonadaptive Routing.
- It is a technique in which the administrator manually adds the routes in a routing table.
- A Router can send the packets for the destination along the route defined by the administrator.
- In this technique, routing decisions are not made based on the condition or topology of the networks

Routing

Advantages –

- No routing overhead for router CPU which means a cheaper router can be used to do routing.
- It adds security because only administrator can allow routing to particular networks only.
- No bandwidth usage between routers.

Disadvantages -

- For a large network, it is a hectic task for administrator to manually add each route for the network in the routing table on each router.
- The administrator should have good knowledge of the topology. If a new administrator comes, then he has to manually add each route so he should have very good knowledge of the routes of the topology.

Routing

Adaptive Routing

- It is also known as **Dynamic Routing**.
- It is a technique in which a router adds a new route in the routing table for each packet in response to the changes in the condition or topology of the network.
- Dynamic protocols such as RIP and OSPF are used to discover the new routes to reach the destination.
- If any route goes down, then the automatic adjustment will be made to reach the destination.

Routing

Advantages –

- Easy to configure.
- More effective at selecting the best route to a destination remote network and also for discovering remote network.

Disadvantage –

- Consumes more bandwidth for communicating with other neighbors.
- Less secure than static routing.

Routing

The Dynamic protocol should have the following features:

- All the routers must have the same dynamic routing protocol in order to exchange the routes.
- If the router discovers any change in the condition or topology, then router broadcast this information to all other routers.

TYPES OF ROUTING PROTOCOLS

Internet is divided into autonomous systems which is a group of networks and routers under the authority of a single administration.

Two types of Dynamic Routing are used in the Internet:

1) Intradomain routing

- Routing within a single autonomous system
  - Distance-vector algorithm using Routing Information Protocol (RIP)
  - Link-state algorithm using Open Shortest Path First (OSPF)

2) Interdomain routing

- Routing between autonomous systems.
  - Path-vector algorithm using Border Gateway Protocol (BGP)

Distance Vector Routing (DVR) Protocol

In distance-vector routing (DVR), each router is required to inform the topology changes to its neighboring routers periodically.

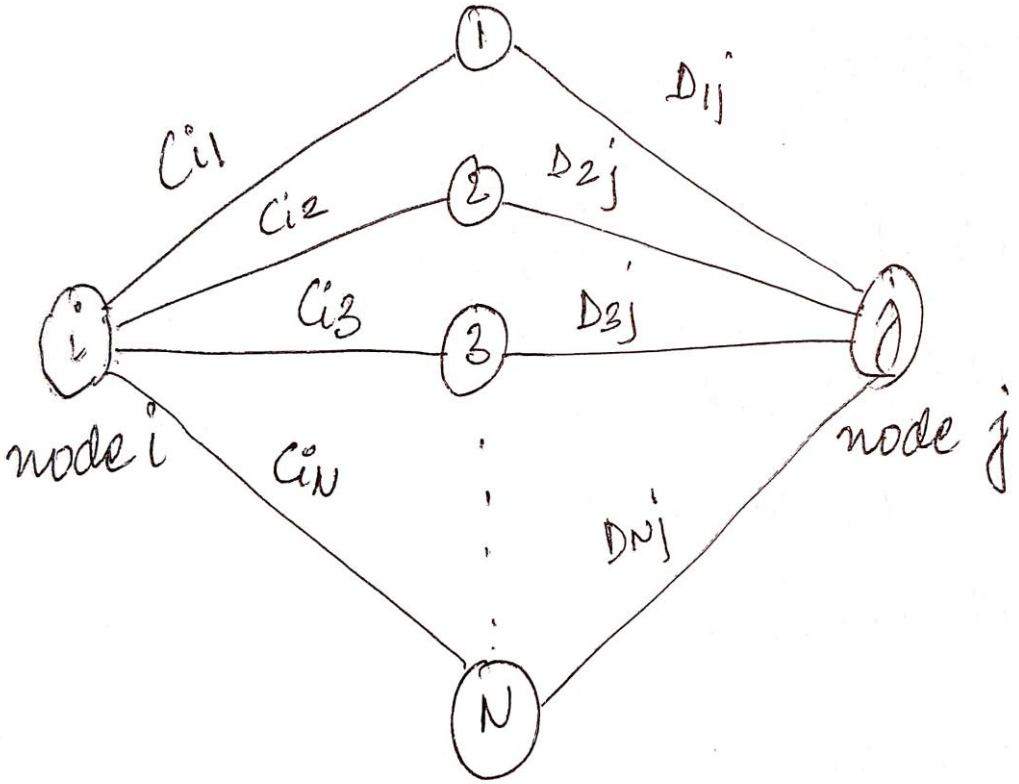
It is also known as Bellman-Ford algorithm after the researchers who developed it (Bellman, 1957; and Ford and Fulkerson, 1962). It was the original ARPANET routing algorithm and was also used in the Internet under the name RIP. .

Distance Vector Routing (DVR) Protocol

How the DVR Protocol Works

- In DVR, each router maintains a routing table which contains two parts −
  - a preferred outgoing line to use (next hop) for that destination and
  - an estimate of cost for each link (distance, number of hops, propagation delay etc.).
- Router tables are updated by exchanging the information with the neighbor's nodes.
- 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 neighbour.
- Eventually, every router knows the best link to reach each destination.

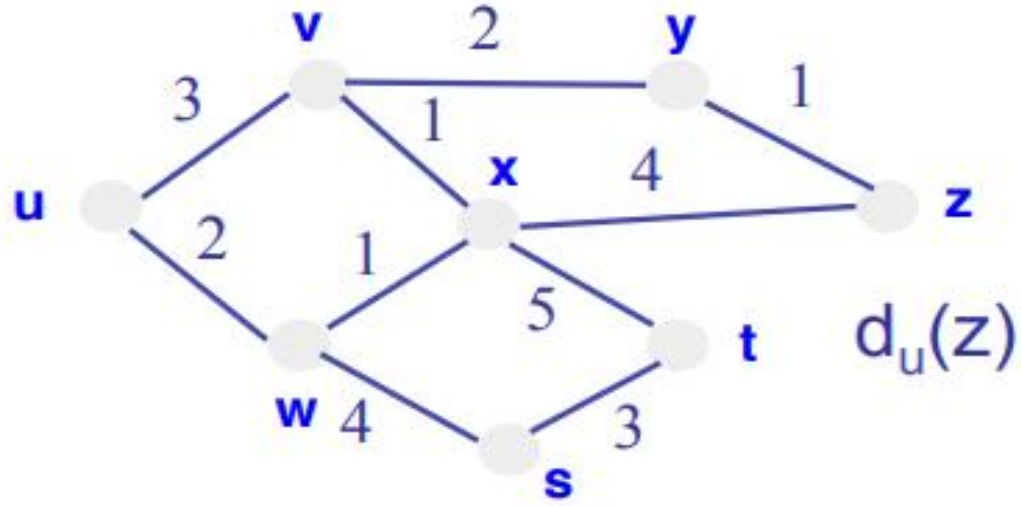
Bellman-Ford Algorithm



- Bellman-Ford algorithm states that the shortest distance between nodes i and j would be
- $\boldsymbol{D_{ij} = \min(C_{i1} + D_{1j}, C_{i2} + D_{2j}, \ldots, C_{iN} + D_{Nj})}$
- where
- C_{i1} is the cost of the direct link from i to node 1.
- D_{1j} is the estimate of the least cost from node 1 to j.

Bellman-Ford Algorithm

- Define distances at each node *X*
  - $d_x(y)$ = cost of least-cost *path* from *X* to *Y*
- Update distances based on neighbors
  - $d_x(y) = \min \{c(x,v) + d_v(y)\}$ over all neighbors *V*



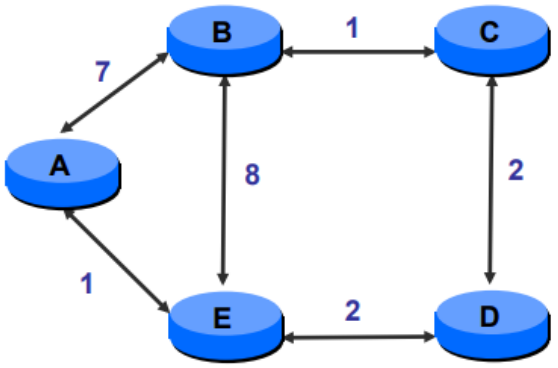
$$d_u(z) = \min\{c(u,v) + d_v(z), \; c(u,w) + d_w(z)\}$$

Step-by-Step

- $c(x,v)$ = cost for direct link from x to v
  - Node x maintains costs of direct links $c(x,v)$
- $D_x(y)$ = estimate of least cost from x to y
  - Node x maintains distance vector $\mathbf{D}_x = [D_x(y): y \in N]$
- Node x maintains its neighbors' distance vectors
  - For each neighbor v, x maintains $\mathbf{D}_v = [D_v(y): y \in N]$
- Each node v periodically sends D_v to its neighbors
  - And neighbors update their own distance vectors
  - $D_x(y) \leftarrow \min_v\{c(x,v) + D_v(y)\}$ for each node $y \in N$

Distance Vector Routing (DVR) Protocol

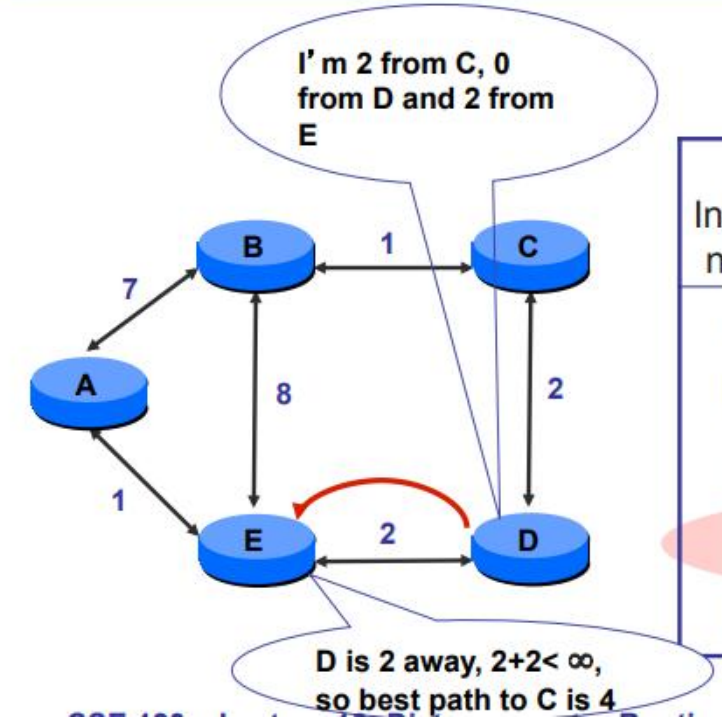
Example: Initial State



Info at node	Distance to Node				
	A	B	C	D	E
A	0	7	∞	∞	1
B	7	0	1	∞	8
C	∞	1	0	2	∞
D	∞	∞	2	0	2
E	1	8	∞	2	0

Distance Vector Routing (DVR) Protocol

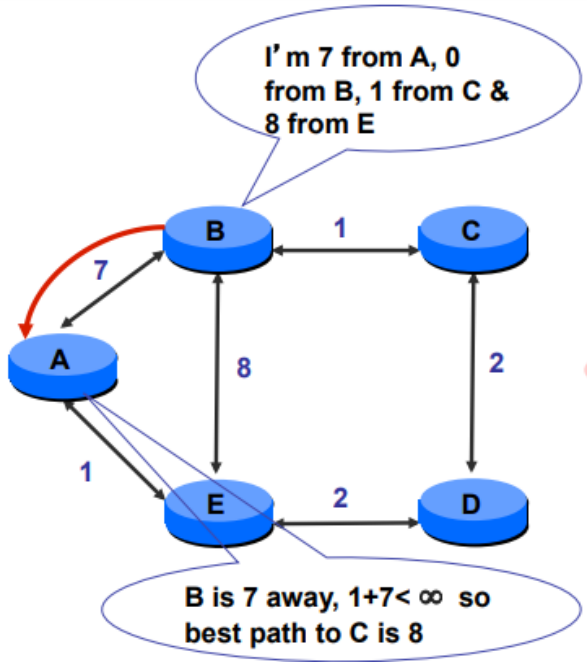
D sends vector to *E*



Info at node	Distance to Node				
	A	B	C	D	E
A	0	7	∞	∞	1
B	7	0	1	∞	8
C	∞	1	0	2	∞
D	∞	∞	2	0	2
E	1	8	**4**	2	0

Distance Vector Routing (DVR) Protocol

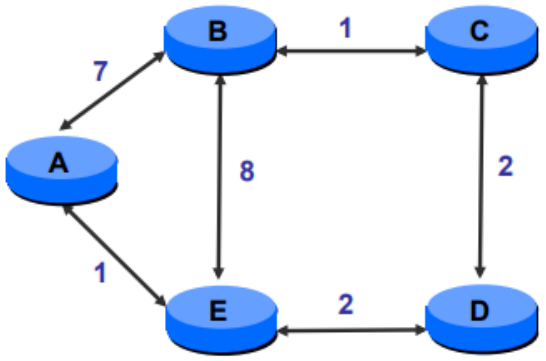
B sends vector to *A*



Info at node	Distance to Node				
	A	**B**	**C**	**D**	**E**
A	0	7	**8**	∞	1
B	7	0	1	∞	8
C	∞	1	0	2	∞
D	∞	∞	2	0	2
E	1	8	4	2	0

Distance Vector Routing (DVR) Protocol

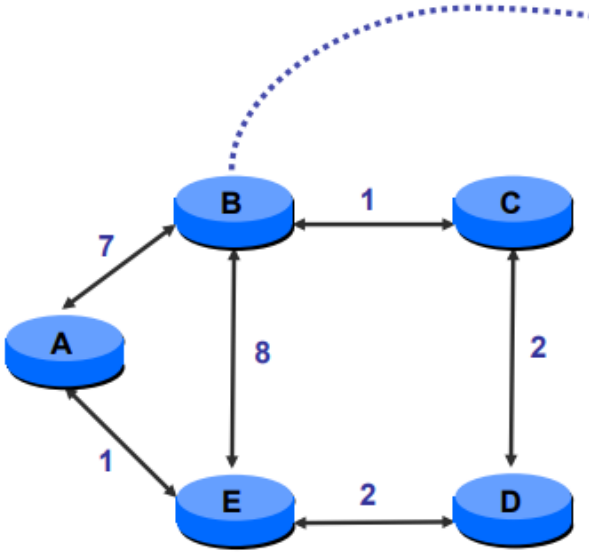
…until Convergence



Info at node	Distance to Node				
	A	B	C	D	E
A	0	6	5	3	1
B	6	0	1	3	5
C	5	1	0	2	4
D	3	3	2	0	2
E	1	5	4	2	0

Distance Vector Routing (DVR) Protocol

Node *B*'s distance vectors

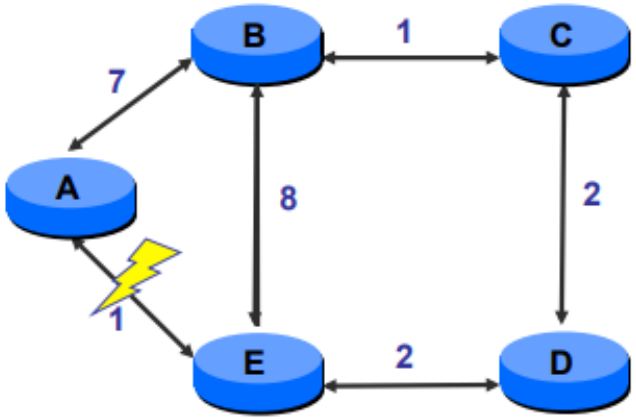


Dest	Next hop A	E	C
A	7	9	**6**
C	12	12	**1**
D	10	10	**3**
E	8	8	**5**

Distance Vector Routing (DVR) Protocol

Handling Link Failure

- A marks distance to E as ∞ , and tells B
- E marks distance to A as ∞ , and tells B and D
- B and D recompute routes and tell C, E and E
- etc… until converge

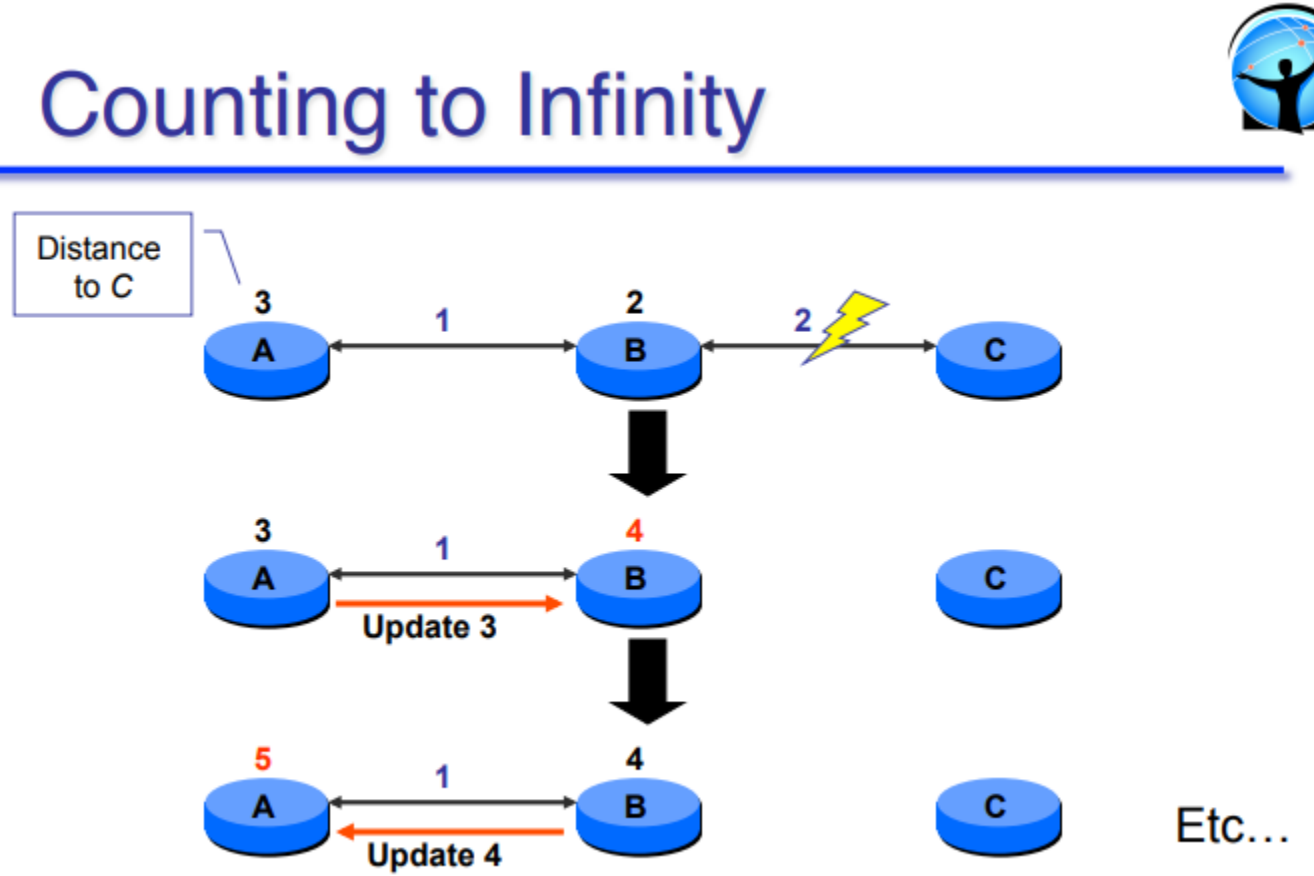


Info at node	Distance to Node				
	A	B	C	D	E
A	0	7	8	10	12
B	7	0	1	3	5
C	8	1	0	2	4
D	10	3	2	0	2
E	12	5	4	2	0

Limitations of Distance Vector Routing (DVR) Protocol

- The settling of routes to best paths across the network is called convergence.
- Distance vector routing is useful as a simple technique by which routers can collectively compute shortest paths, but it has a serious drawback in practice: although it converges to the correct answer, it may do so slowly.
  - In particular, it reacts rapidly to good news, but leisurely to bad news.
  - Leading to Count to infinity problem.

Distance Vector Routing (DVR) Protocol



RIP

- Routing Information Protocol (RIP) is a dynamic routing protocol that uses hop count as a routing metric to find the best path between the source and the destination network.

- It is a distance-vector routing protocol that has an AD value of 120 and works on the Network layer of the OSI model. RIP uses port number 520.

RIP

Hop Count

- Hop count is the number of routers occurring in between the source and destination network. The path with the lowest hop count is considered as the best route to reach a network and therefore placed in the routing table.

- RIP prevents routing loops by limiting the number of hops allowed in a path from source and destination.

- The maximum hop count allowed for RIP is 15 and a hop count of 16 is considered as network unreachable.

RIP

Features of RIP

1. Updates of the network are exchanged periodically.

2. Updates (routing information) are always broadcast.

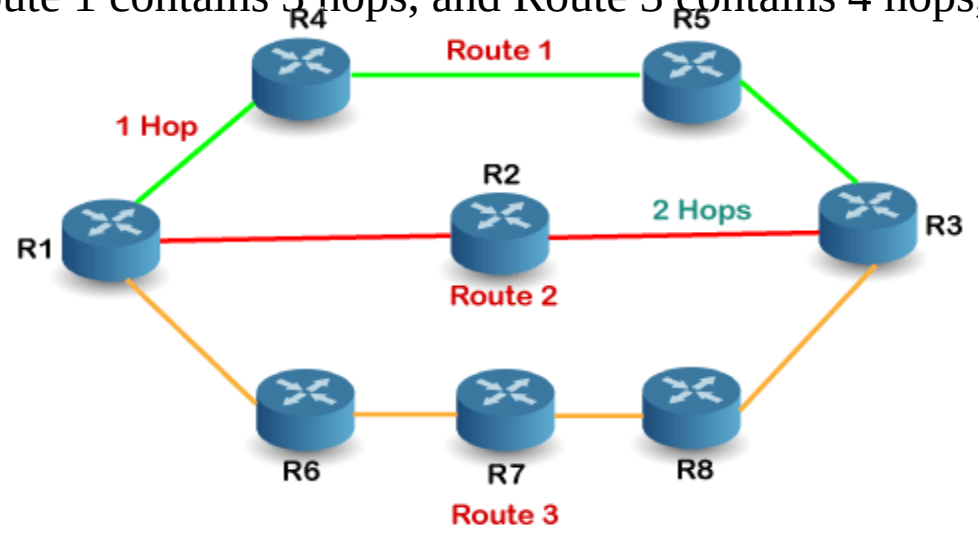
3. Full routing tables are sent in updates.

4. Routers always trust routing information received from neighbor routers. This is also known as Routing on rumors.

RIP

How does the RIP work?

If there are 8 routers in a network where Router 1 wants to send the data to Router 3. If the network is configured with RIP, it will choose the route which has the least number of hops. There are three routes in the above network, i.e., Route 1, Route 2, and Route 3. The Route 2 contains the least number of hops, i.e., 2 where Route 1 contains 3 hops, and Route 3 contains 4 hops, so RIP will choose Route 2.



Link State Routing

Link state routing is a technique in which each router shares the knowledge of its neighborhood with every other router in the internetwork.

The idea behind link state routing can be stated as five parts. Each router must do the following things to make it work:

1. Discover its neighbors and learn their network addresses: It accomplishes this goal by sending a special HELLO packet on each point-to-point line. The router on the other end is expected to send back a reply giving its name
2. Set the distance or cost metric to each of its neighbors

Link State Routing

4. Construct a packet telling all it has just learned: Once the information needed for the exchange has been collected, the next step is for each router to build a Link state packet (LSP) containing all the data. The packet contains the identity of the sender, list of neighbors, and the cost to each neighbor.

5. Send this packet to and receive packets from all other routers: These LSPs are distributed amongst all routers using Flooding.

6. Compute the shortest path to every other router: using Dijkstra's Algorithm

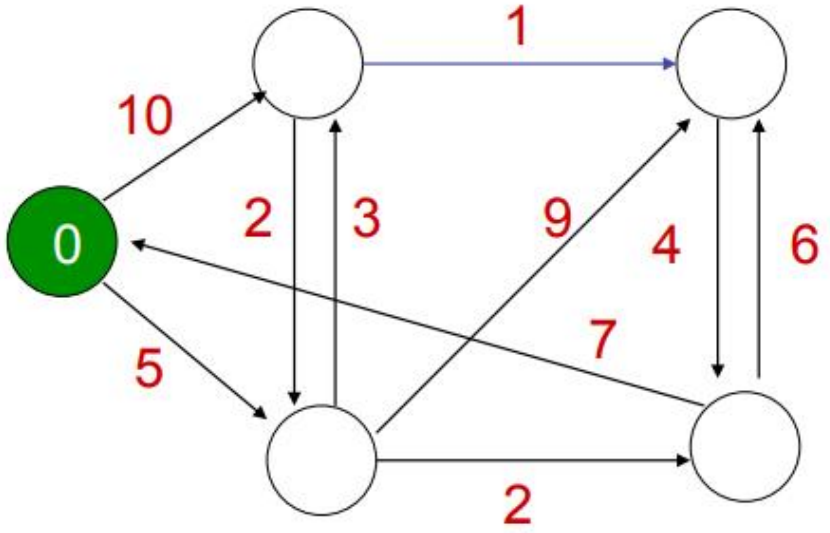
Link State Routing

Route Calculation

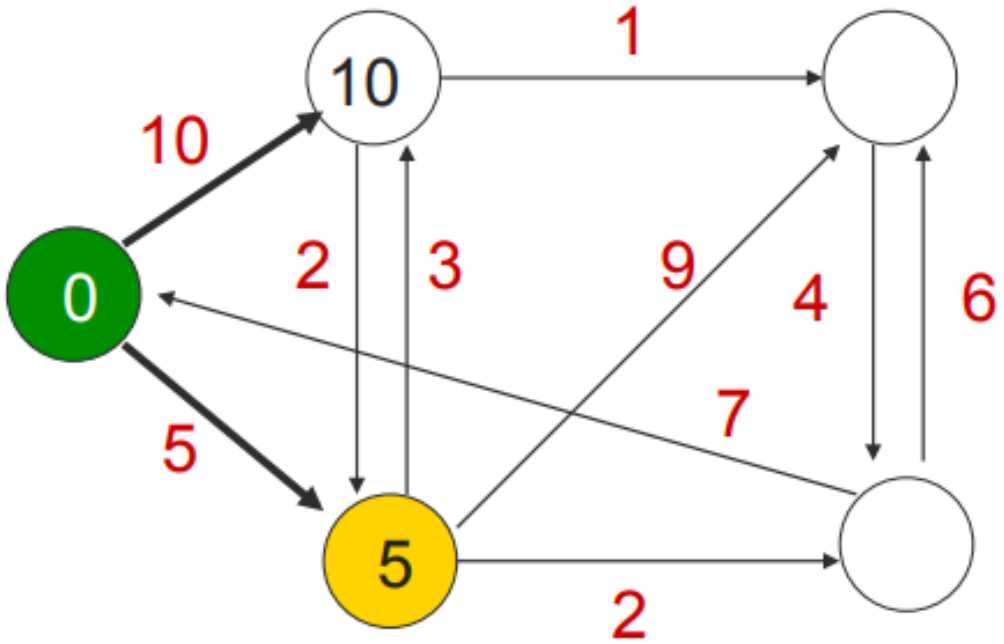
- The Link state routing uses Dijkstra's algorithm on the graph to calculate the optimal routes to all nodes.
- It computes single source shortest path tree.
- The Dijkstra's algorithm is an iterative, and it has the property that after k^{th} iteration of the algorithm, the least cost paths are well known for k destination nodes.

Dijkstra's Algorithm

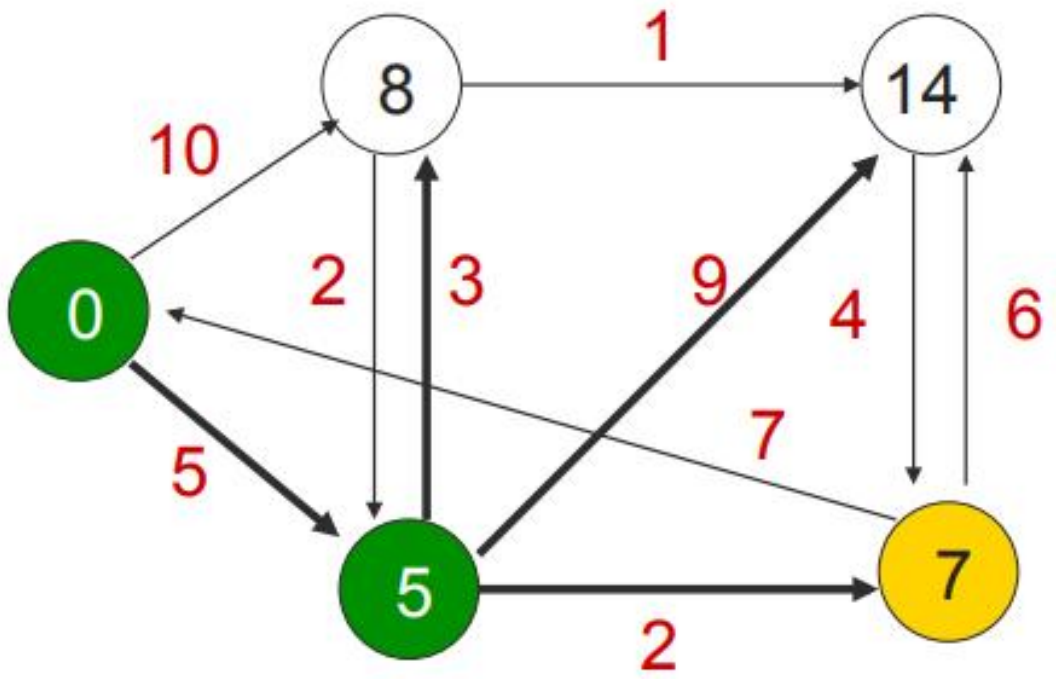
Example: Step 1



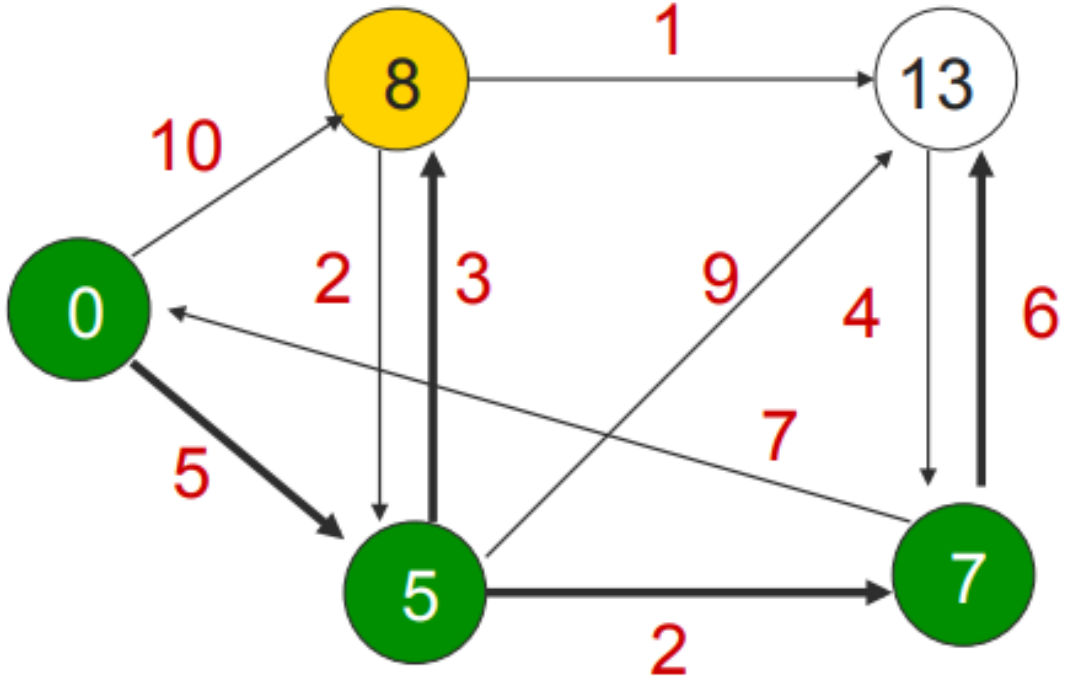
Example: Step 2



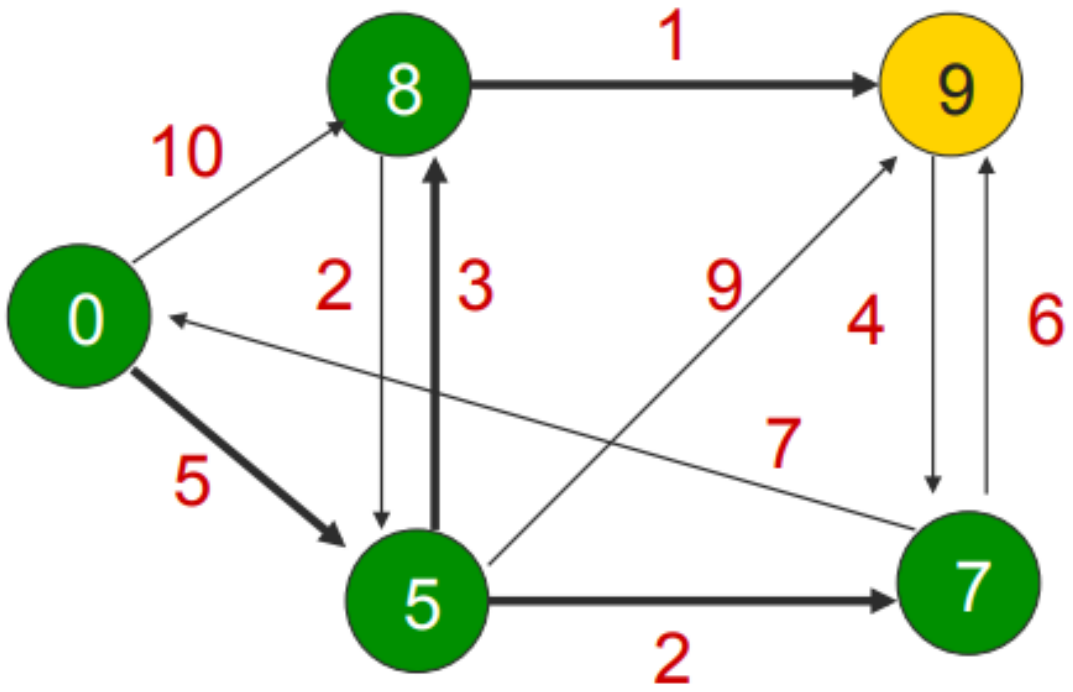
Example: Step 3



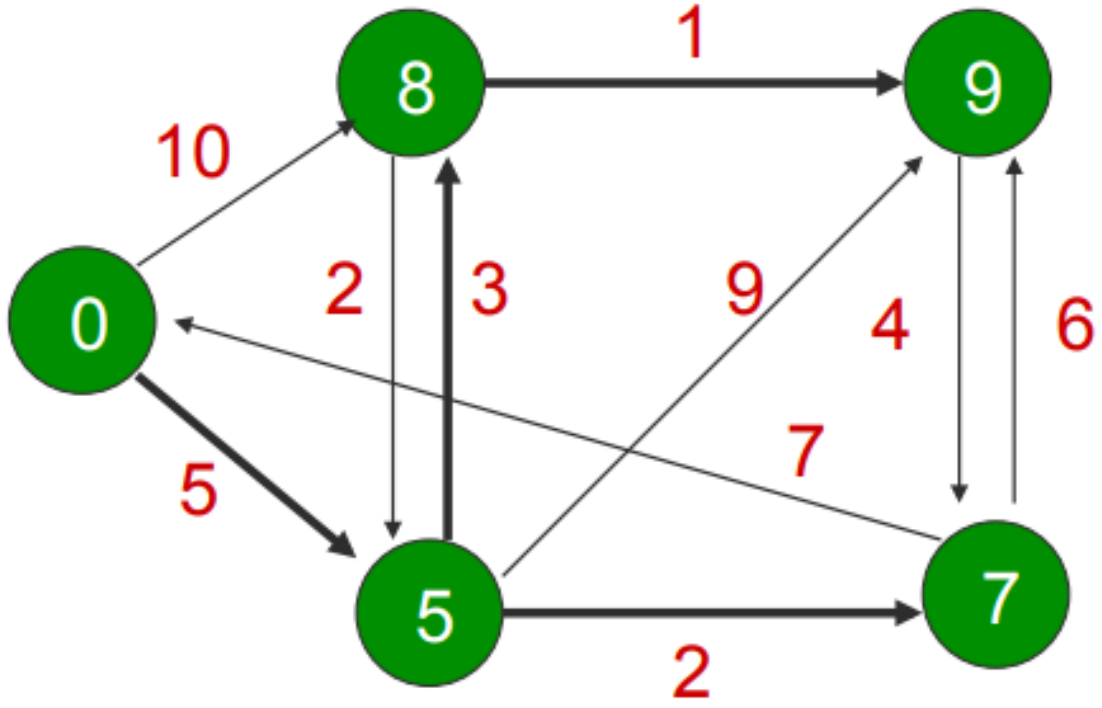
Example: Step 4



Example: Step 5



Example: Conclusion



Link State Routing

Protocols of Link State Routing

- Open Shortest Path First (OSPF)
- Intermediate System to Intermediate System (IS-IS)

Distance Vector Routing (DVR) Protocol

Distance Vector Routing	Link State Routing
--> Bandwidth required is less due to local sharing, small packets and no flooding.	--> Bandwidth required is more due to flooding and sending of large link state packets.
--> Based on local knowledge since it updates table based on information from neighbors.	--> Based on global knowledge i.e. it have knowledge about entire network.
--> Make use of Bellman Ford algo	--> Make use of Dijkastra's algo
--> Traffic is less	--> Traffic is more
--> Converges slowly i.e. good news spread fast and bad news spread slowly.	--> Converges faster.
--> Count to infinity problem.	--> No count to infinity problem.
--> Persistent looping problem i.e. loop will there forever.	--> No persistent loops, only transient loops.
--> Practical implementation is RIP and IGRP.	--> Practical implementation is OSPF and ISIS.

Open Shortest Path First (OSPF)

- Open shortest path first (OSPF) is a link-state routing protocol that is used to find the best path between the source and the destination router.

- OSPF is an Interior Gateway Protocol (IGP) that operates within a single routing domain, like an autonomous system. It's a dynamic routing protocol that can detect topological changes and calculate new routes.

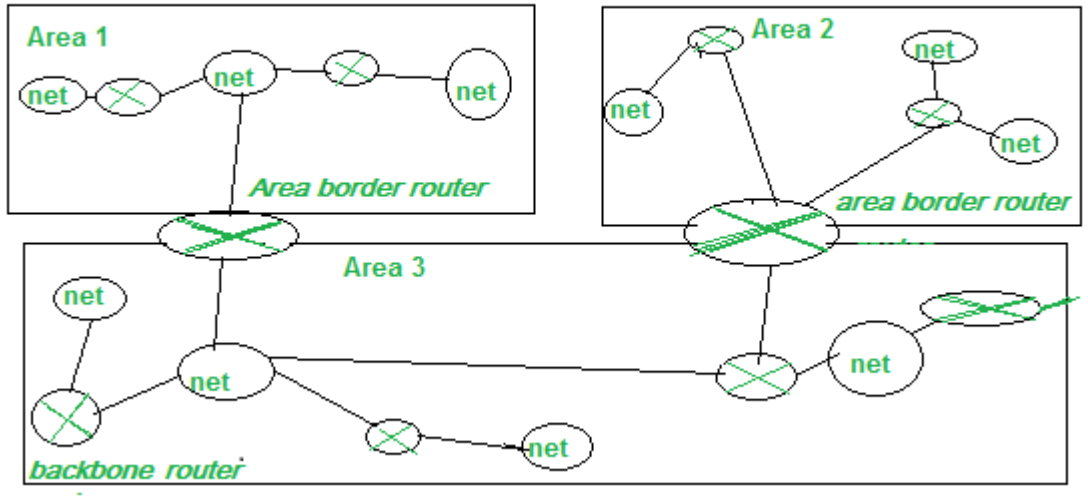
- A link-state routing protocol is a protocol that uses the concept of triggered updates, i.e., if there is a change observed in the learned routing table then the updates are triggered only, not like the distance-vector routing protocol where the routing table is exchanged at a period of time.

Open Shortest Path First (OSPF)

- Open Shortest Path First (OSPF) is a link-state routing protocol that is used to find the best path between the source and the destination router using its own Shortest Path First.
- OSPF is developed by Internet Engineering Task Force (IETF) as one of the Interior Gateway Protocol (IGP), i.e, the protocol which aims at moving the packet within a large autonomous system or routing domain.
- It is a network layer protocol which works on protocol number 89 and uses AD value 110. OSPF uses multicast address 224.0.0.5 for normal communication and 224.0.0.6 for update to designated router(DR)/Backup Designated Router (BDR).

Open Shortest Path First (OSPF)

- To handle routing efficiently and on time, this protocol divides an autonomous system into areas. Area is a collection of routers, hosts, networks all contained within an autonomous system.
- An autonomous system can be divided into many different areas, but at the same time, all networks inside an area must be connected.



Open Shortest Path First (OSPF)

Working of OSPF

OSPF protocol working can be understood in the following three steps:

Step 1: The first step in the working of the OSPF protocol is to become the OSPF neighbors. The two routers that are running on the same link and are connected establishes the neighbor relationship between them.

Step 2: Now the next step is to exchange the database information between the routers. When the router establishes the neighbor relationship they exchange the link-state database (LSDB) with each other.

Step 3: The third step in the working of the OSPF protocol is to select the best route. After an exchange of LSDB information, the router finds the best route for adding to the routing table.

Open Shortest Path First (OSPF)

Working of OSPF

OSPF protocol working can be understood in the following three steps:

Step 1: The first step in the working of the OSPF protocol is to become the OSPF neighbors. The two routers that are running on the same link and are connected establishes the neighbor relationship between them.

Step 2: Now the next step is to exchange the database information between the routers. When the router establishes the neighbor relationship they exchange the link-state database (LSDB) with each other.

Step 3: The third step in the working of the OSPF protocol is to select the best route. After an exchange of LSDB information, the router finds the best route for adding to the routing table.

Border Gateway Protocol (BGP)

- BGP stands for **Border Gateway Protocol**. It is a standardized gateway protocol that exchanges routing information across autonomous systems (AS). When one network router is linked to other networks, it cannot decide which network is the best network to share its data to by itself.

- Border Gateway Protocol considers all peering partners that a router has and sends traffic to the router closest to the data's destination.

- This communication is possible because, at boot, BGP allows peers to communicate their routing information and then stores that information in a Routing Information Base (RIB).

Border Gateway Protocol (BGP)

- The main goal of BGP is to find any path to the destination that is loop-free. This is different from intradomain routing protocols' common goals**: finding an optimal route to the destination based on a specific link metric.**

- The routers that connect other ASs are called border gateways. The task of the border gateways is to forward packets between ASs. Each AS has at least one BGP speaker. BGP speakers exchange reachability information among ASs.

Border Gateway Protocol (BGP)

Types

The types of BGP are as follows −

1. Internal BGP

- Routes are exchanged, and traffic is transmitted over the Internet using external BGP or eBGP. Autonomous systems can also use an internal BGP version to route through their internal networks, known as internal BGP.

- It should be noted that using internal BGP is NOT a requirement for using external BGP. Autonomous systems can choose from several internal protocols to connect the routers on their internal network.

Border Gateway Protocol (BGP)

2. External BGP

- External BGP is like international shipping; some specific standards and guidelines need to be followed when shipping a piece of mail internationally. Once that piece of mail reaches its destination country, it has to go through its local mail service to reach its final destination.

- Each country has its internal mail service that doesn’t necessarily follow the same guidelines as other countries.

- Similarly, each autonomous system can have its internal routing protocol for routing data within its network.

Mobile IP Data Encapsulation Techniques

- Data Encapsulation is a process of adding header to wrap the data flows through OSI model.
- The new headers specify how to send the encapsulated datagram to the mobile node's care-of address.
- Encapsulation is required because each datagram we intercept and forward needs to be resent over the network to the device's care-of address.
- The default encapsulation process used in Mobile IP is called IP Encapsulation Within IP, commonly abbreviated IP-in-IP.
- In addition to IP-in-IP, two other encapsulation methods may be optionally used:
  - Minimal Encapsulation Within IP
  - Generic Routing Encapsulation (GRE)
- To use either of these, the mobile node must request the appropriate method in its Registration Request
- The home agent must agree to use it. If foreign agent care-of addressing is used,
- The foreign agent also must support the method desired.

5 Steps of Data Encapsulation are :

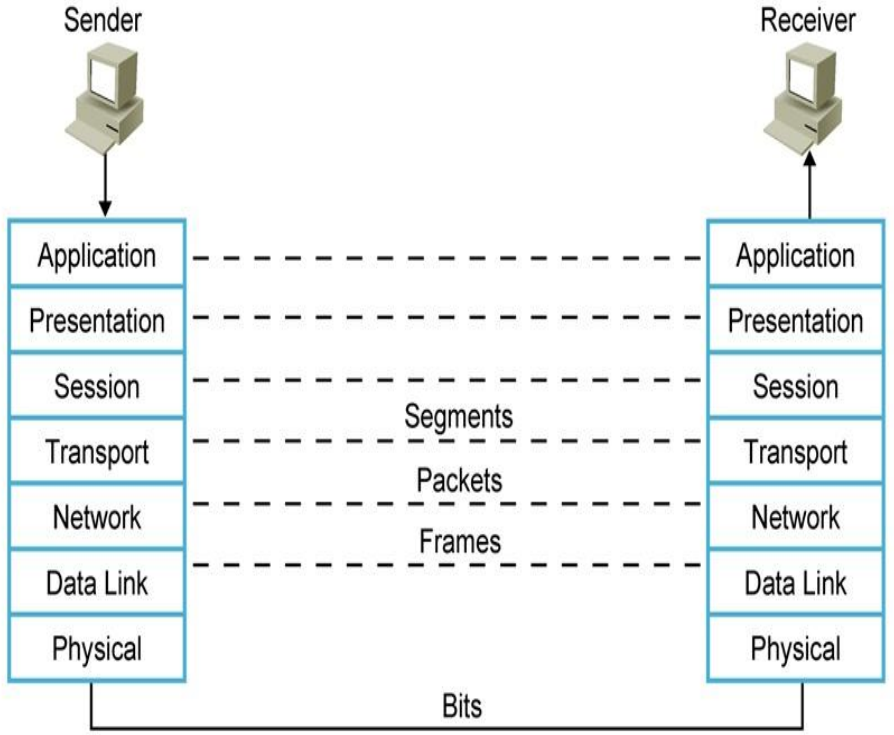
The Application, Presentation & Session layer creates DATA (Message) from user's input

The transport layer converts that data into SEGMENTS (User Datagram).

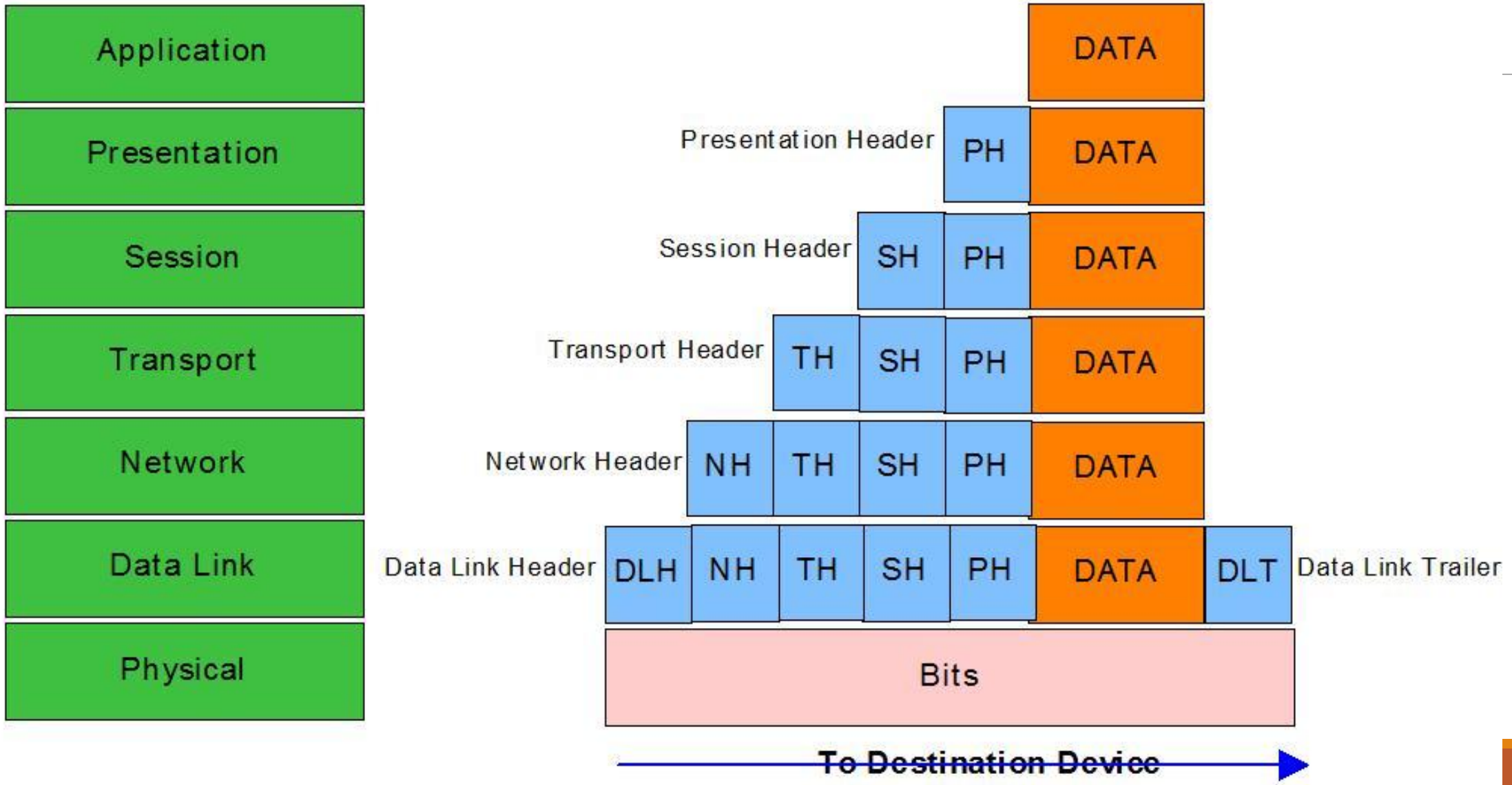
The Network layer converts this Segment into PACKETS (Datagram).

The Data link layer converts that Packet into FRAMES

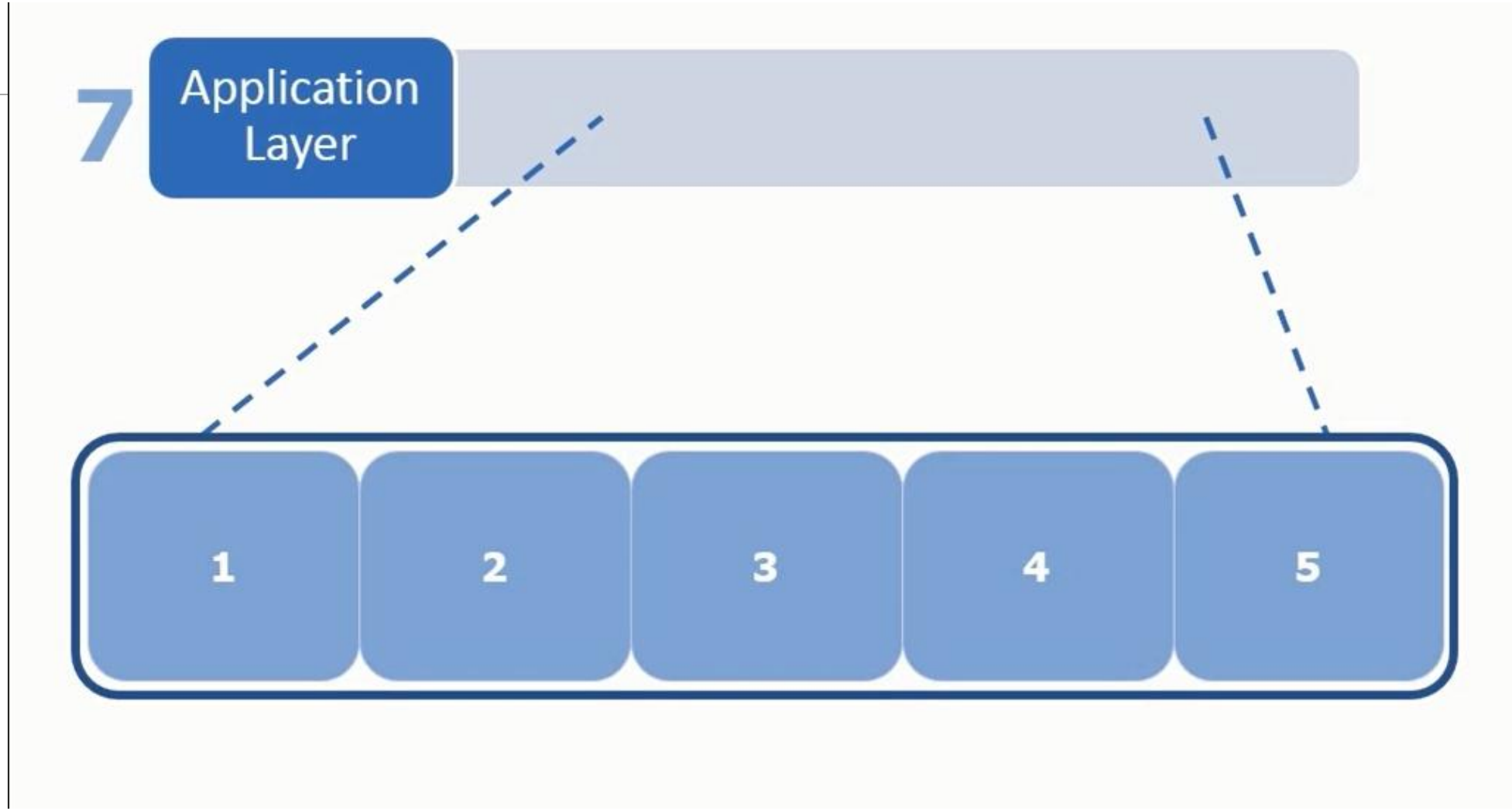
The Phyisical layer converts that Frames into BITS.



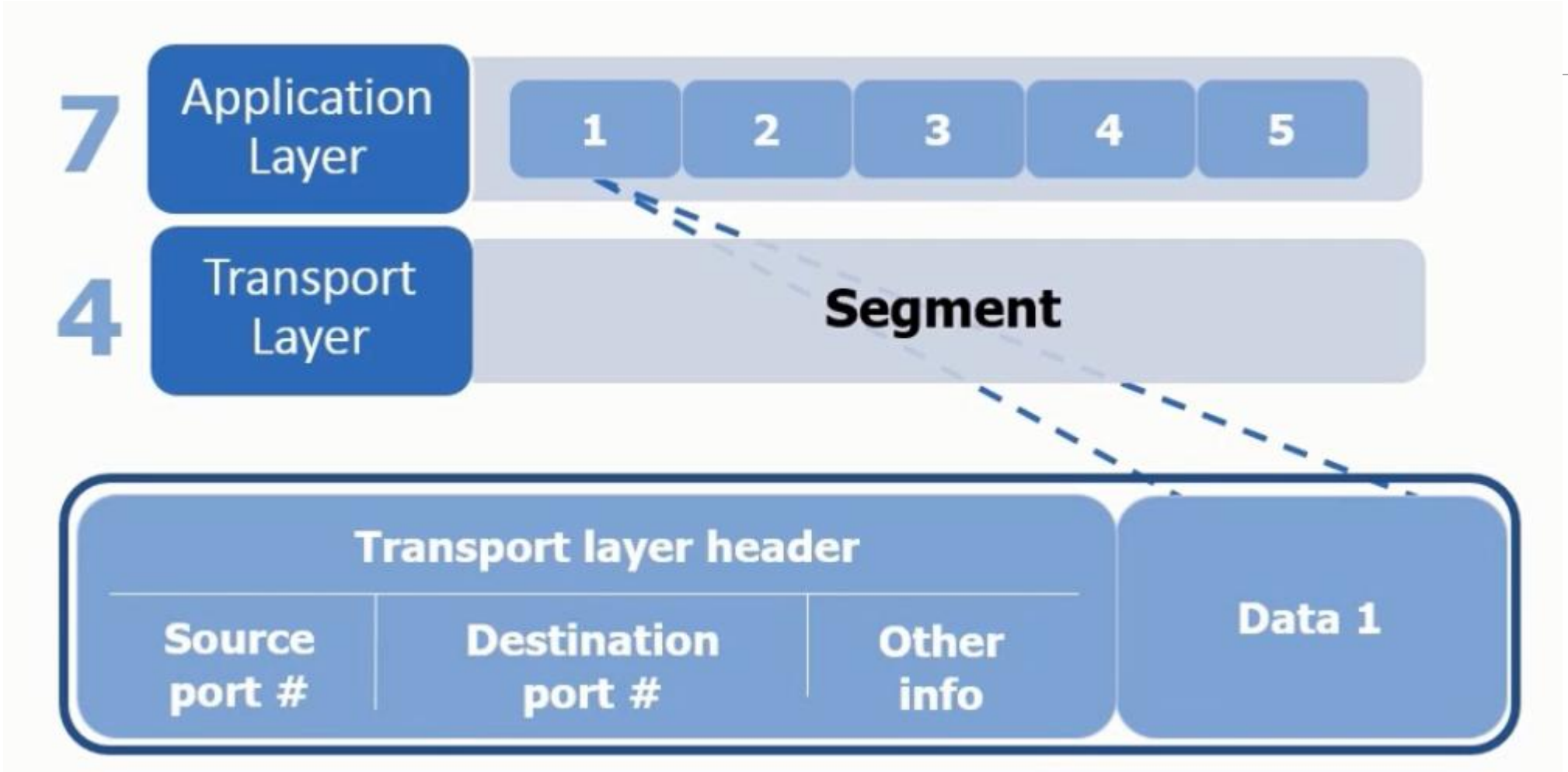
Encapsulation



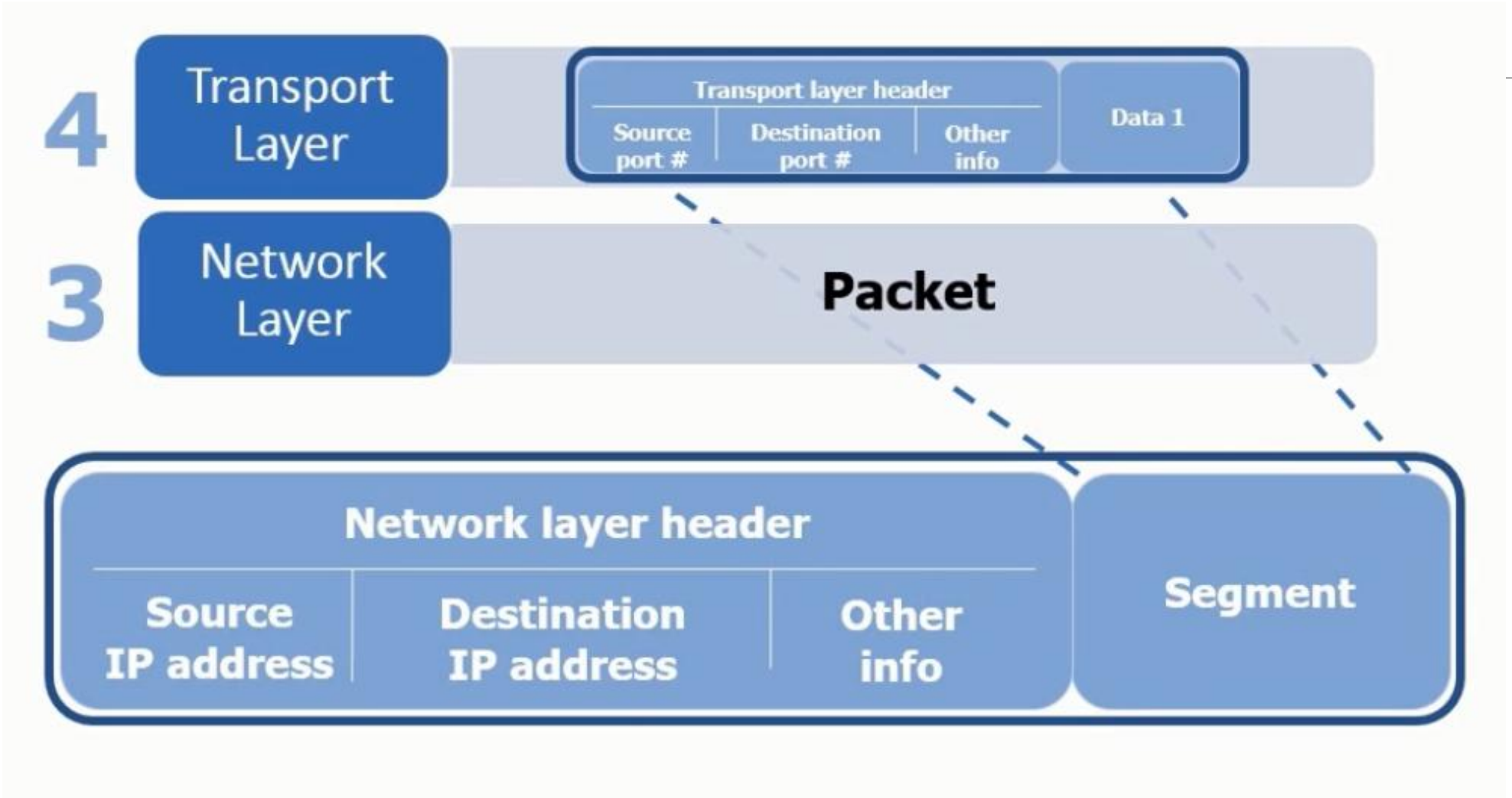
OSI Model & Encapsulation : Application Layer



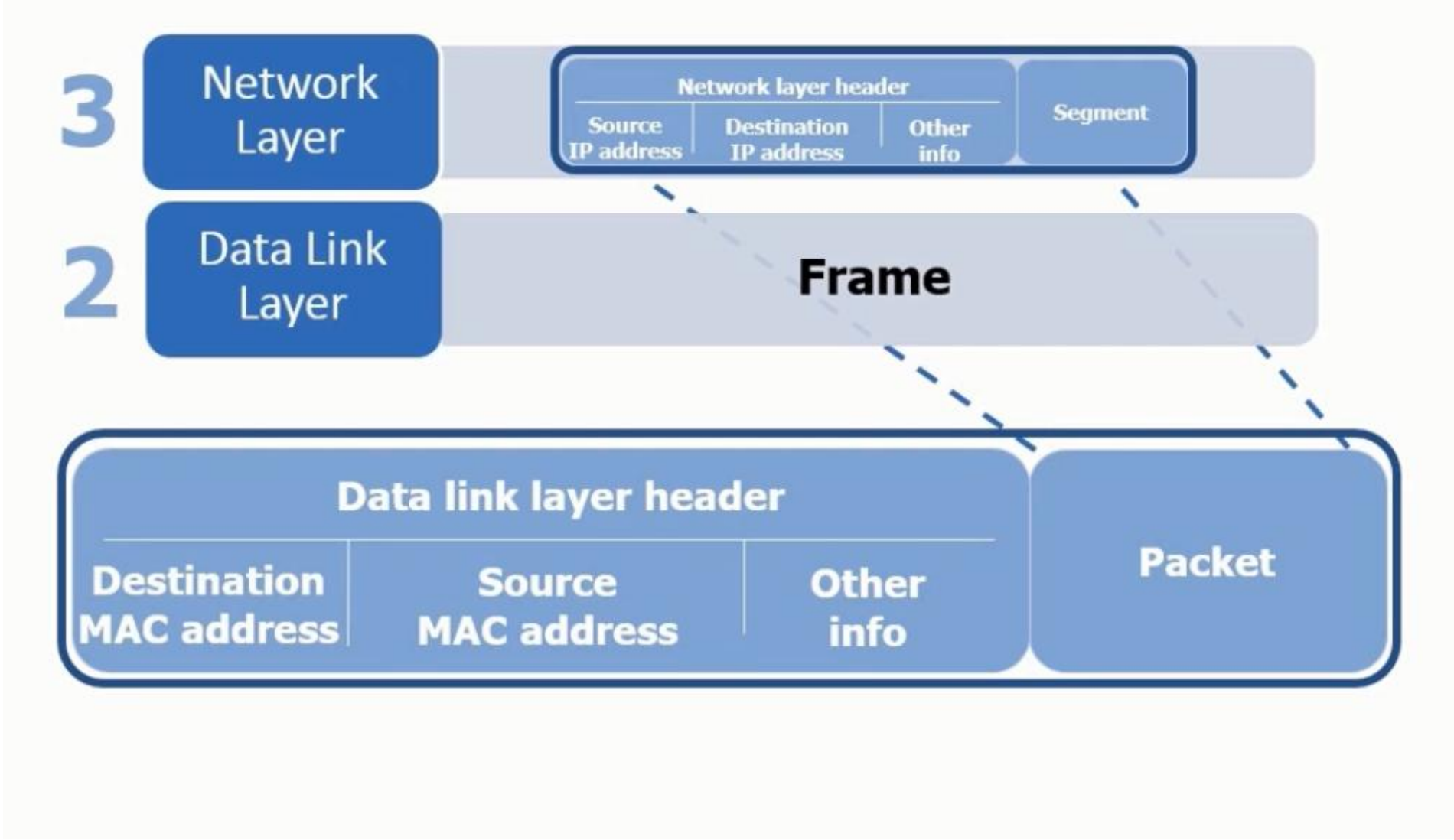
OSI Model & Encapsulation : Transport Layer



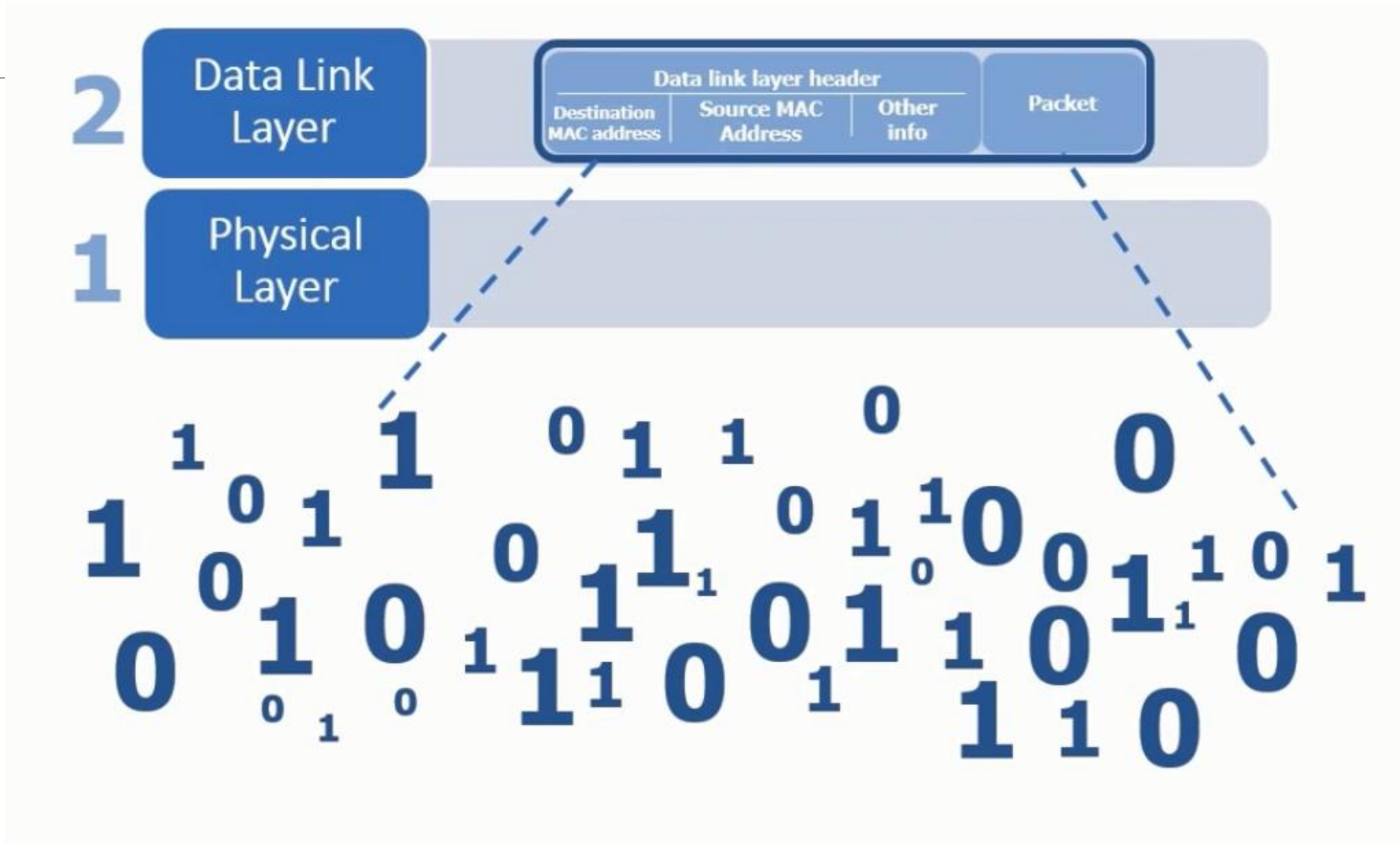
OSI Model & Encapsulation : Network Layer



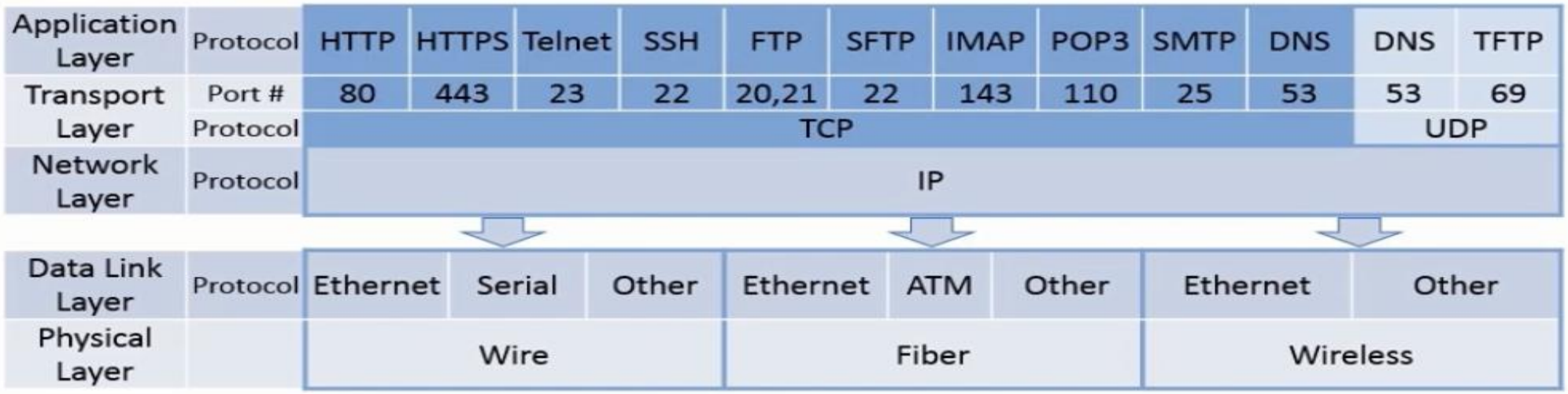
OSI Model & Encapsulation : Datalink Layer



OSI Model & Encapsulation : Physical Layer



OSI Model and Protocol at each layer



Internetworking

- Until now, we have implicitly assumed that there is a single homogeneous network, with each machine using the same protocol in each layer.
- Many different networks exist, including PANs, LANs, MANs, and WANs. We have described Ethernet, Internet over cable, the fixed and mobile telephone networks, 802.11, 802.16, and more.
- Various issues arise when two or more networks are connected to form an internetwork, or more simply an internet

Internetworking

- Let us explore how interconnection with a common network layer can be used to interconnect dissimilar networks. An internet comprised of 802.11, MPLS, and Ethernet networks is shown in Fig. 5-39(a)

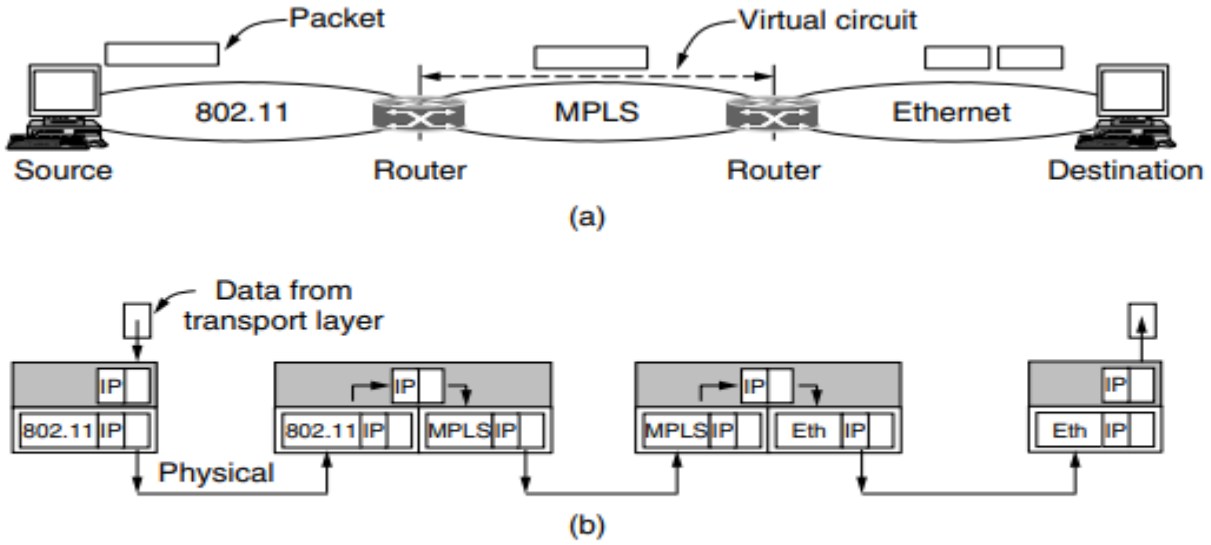


Figure 5-39. (a) A packet crossing different networks. (b) Network and link layer protocol processing.

Internetworking

- The source accepts data from the transport layer and generates a packet with the common network layer header, with ultimate destination address, which is used to determine that the packet should be sent via the first router.
- So the packet is encapsulated in an 802.11 frame whose destination is the first router and transmitted. At the router, the packet is removed from the frame's data field and the 802.11 frame header is discarded. The router now examines the IP address in the packet and looks up this address in its routing table.
- Based on this address, it decides to send the packet to the second router next. For this part of the path, an MPLS virtual circuit must be established to the second router and the packet must be encapsulated with MPLS headers that travel this circuit.
- Since the packet is too long to be sent over Ethernet, it is split into two portions. Each of these portions is put into the data field of an Ethernet frame and sent to the Ethernet address of the destination. At the destination, the Ethernet header is stripped from each of the frames, and the contents are reassembled. The packet has finally reached its destination.

Tunneling

What Is Tunneling?

- Tunneling is a protocol that allows for the secure movement of data from one network to another
- Tunneling involves allowing private network communications to be sent across a public network, such as the Internet
- In tunneling, the data are broken into smaller pieces called packets as they move along the tunnel for transport
- As the packets move through the tunnel, they are encrypted and encapsulated

Tunneling

Consider an international bank with an IPv6 network in Paris, an IPv6 network in London and connectivity between the offices via the IPv4 Internet. This situation is shown in Fig. 5-40.

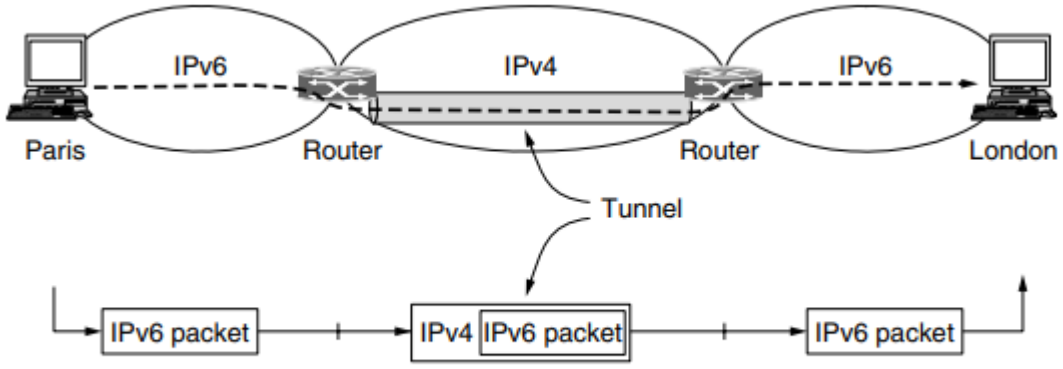


Figure 5-40. Tunneling a packet from Paris to London.

Tunneling

- To send an IP packet to a host in the London office, a host in the Paris office constructs the packet containing an IPv6 address in London and sends it to the multiprotocol router that connects the Paris IPv6 network to the IPv4 Internet.
- When this router gets the IPv6 packet, it encapsulates the packet with an IPv4 header addressed to the IPv4 side of the multiprotocol router that connects to the London IPv6 network. That is, the router puts a (IPv6) packet inside a (IPv4) packet.
- When this wrapped packet arrives, the London router removes the original IPv6 packet and sends it onward to the destination host.
- The path through the IPv4 Internet can be seen as a big tunnel extending from one multiprotocol router to the other. The IPv6 packet just travels from one end of the tunnel to the other, snug in its nice box.

Tunneling

- Tunneling is widely used to connect isolated hosts and networks using other networks. The network that results is called an overlay since it has effectively been overlaid on the base network.
- Example: VPNs (Virtual Private Networks). A VPN is simply an overlay that is used to provide a measure of security.

Congestion Control

- Too many packets present in (a part of) the network causes packet delay and loss that degrades performance. This situation is called congestion.
- The network and transport layers share the responsibility for handling congestion.
- Figure 5-21 depicts the onset of congestion

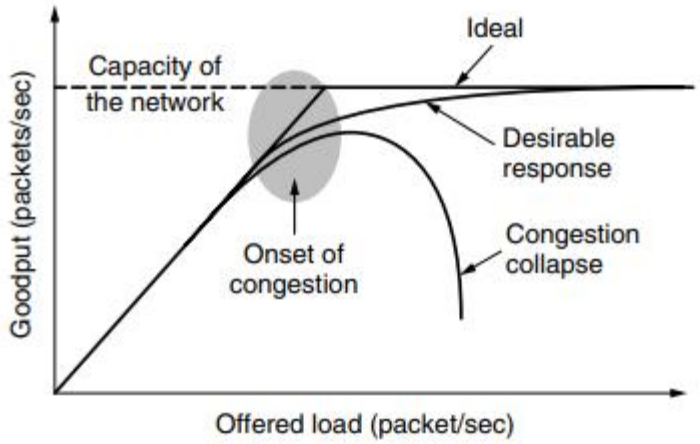


Figure 5-21. With too much traffic, performance drops sharply.

Congestion Control

- When the number of packets hosts send into the network is well within its carrying capacity, the number delivered is proportional to the number sent. If twice as many are sent, twice as many are delivered.
- However, as the offered load approaches the carrying capacity, bursts of traffic occasionally fill up the buffers inside routers and some packets are lost. These lost packets consume some of the capacity, so the number of delivered packets falls below the ideal curve. The network is now congested.
- Unless the network is well designed, it may experience a congestion collapse, in which performance plummets as the offered load increases beyond the capacity.
- Goodput is the rate at which useful packets are delivered by the network.

Causes of Congestion

- Congestion occurs when a router receives data faster than it can send it
  - Insufficient bandwidth
  - Slow hosts
  - Data simultaneously arriving from multiple lines destined for the same outgoing line.
- The system is not balanced
  - Correcting the problem at one router will probably just move the bottleneck to another router.

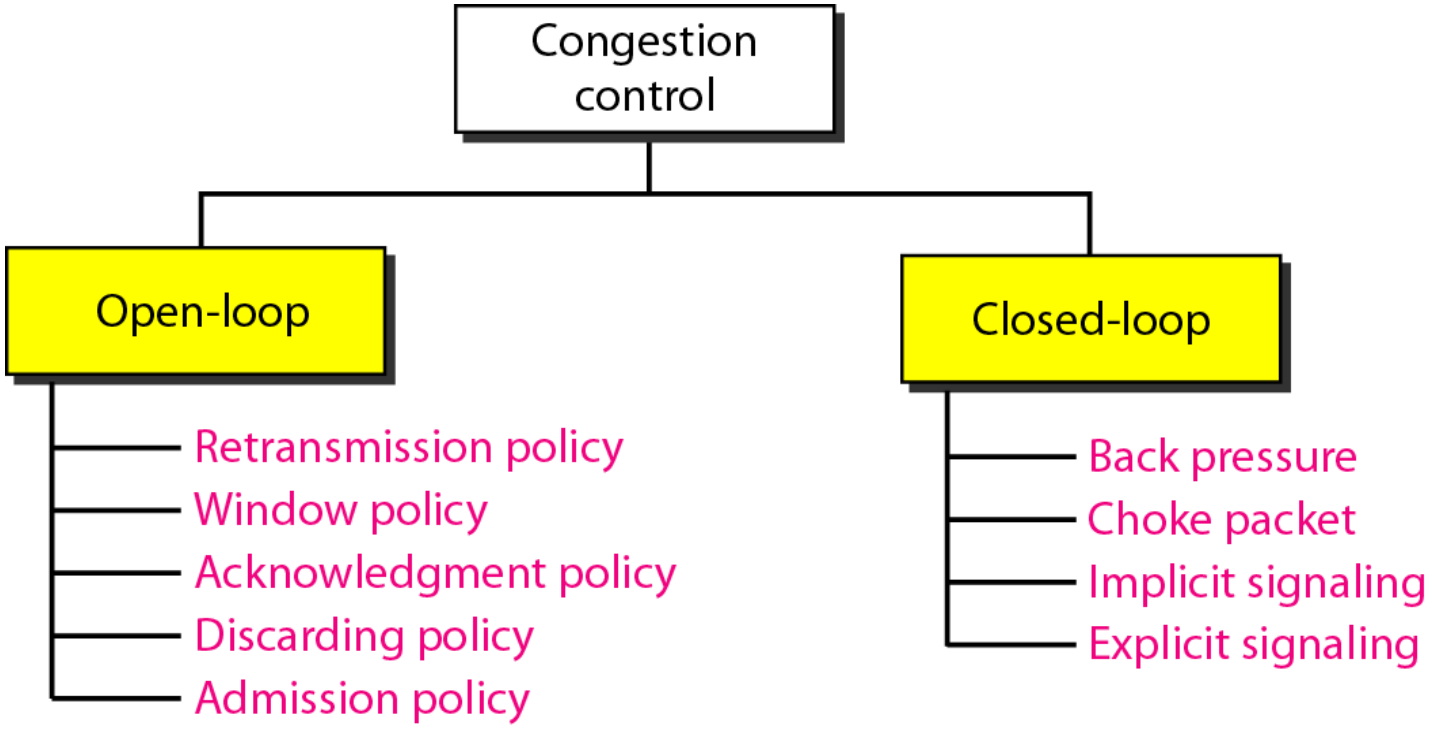
Congestion Control

Congestion control refers to techniques and mechanisms that can either prevent congestion, before it happens, or remove congestion, after it has happened. In general, we can divide congestion control mechanisms into two broad categories:

- Open-loop congestion control:
  - Attempt to prevent problems rather than correct them
  - Does not utilize runtime feedback from the system

- Closed-loop congestion control
  - Uses feedback (measurements of system performance) to make corrections at runtime.

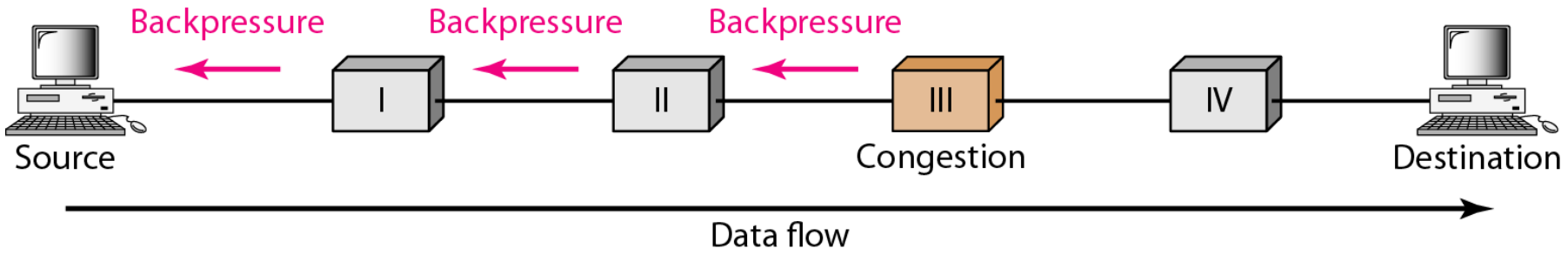
Figure 24.5 *Congestion control categories*



Warning Bit/ Backpressure

- A special bit in the packet header is set by the router to warn the source when congestion is detected.
- The bit is copied and piggy-backed on the ACK and sent to the sender.
- The sender monitors the number of ACK packets it receives with the warning bit set and adjusts its transmission rate accordingly.

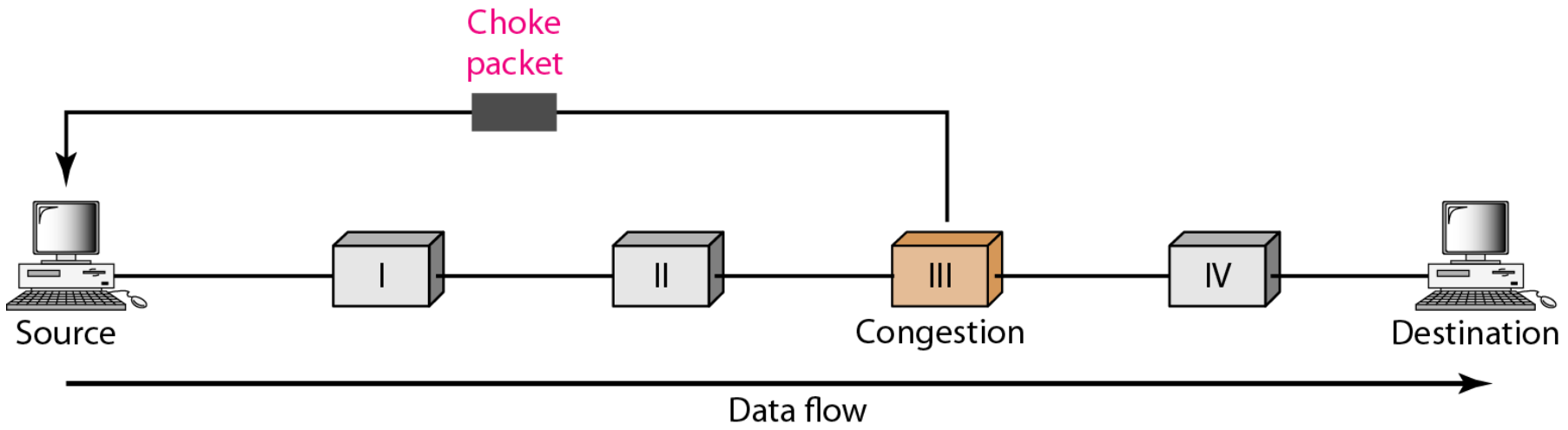
Figure 24.6 *Backpressure method for alleviating congestion*



Choke Packets

- A more direct way of telling the source to slow down.
- A choke packet is a control packet generated at a congested node and transmitted to restrict traffic flow.
- The source, on receiving the choke packet must reduce its transmission rate by a certain percentage.
- An example of a choke packet is the ICMP Source Quench Packet.

Figure 24.7 *Choke packet*



Other Approaches to Congestion Control

Provisioning:

- The most basic way to avoid congestion is to build a network that is well matched to the traffic that it carries.
- Resources can be added dynamically when there is serious congestion, by turning on spare routers or enabling lines that are normally used only as backups or purchasing bandwidth on the open market.

Traffic-aware routing:

- Routes can be tailored to traffic patterns that change during the day as network users wake and sleep in different time zones.
- For example, routes may be changed to shift traffic away from heavily used paths by changing the shortest path weights
- Splitting traffic across multiple paths is also helpful

Admission control:

- Sometimes it is not possible to increase capacity. The only way then to beat back the congestion is to decrease the load.

Finally, when all else fails, the network is forced to discard packets that it cannot deliver. The general name for this is load shedding.

NAT

Before starting the explanation of Network Address Translation let’s recall some key points. That will help you to understand the explanation and working of NAT.

Key Points

We generally have two types of IP address, which are as follows −

- Private IP address
- Public IP address

NAT

- Private IP address normally used in the LAN (Local area network) side of the Network.
- Public IP address provided by the ISP is configured in the WAN side of the network.
- Public IP addresses are always paid, while the private IP address is free.

Private IP addresses range as follows −

- 192.168.0.0 - 192.168.255.255 (65,536 IP addresses)
- 172.16.0.0 - 172.31.255.255 (1,048,576 IP addresses)
- 10.0.0.0 - 10.255.255.255 (16,777,216 IP addresses)

NAT

Now let us try to understand what Network Address Translation (NAT) is.

Step 1 − Consider you have internet provided by Internet Service Provider ABC.

Step 2 − So, they will give you connection to your Modem. That connection we used to call WAN.

Step 3 − This connection is always configured with a Public IP address.

Step 4 − Then, your LAN side of the MODEM is configured with a Private IP address.

NAT

Now let us try to understand what Network Address Translation (NAT) is.

Step 5 − That means your computer or laptop connected to the network receives a Private IP address.

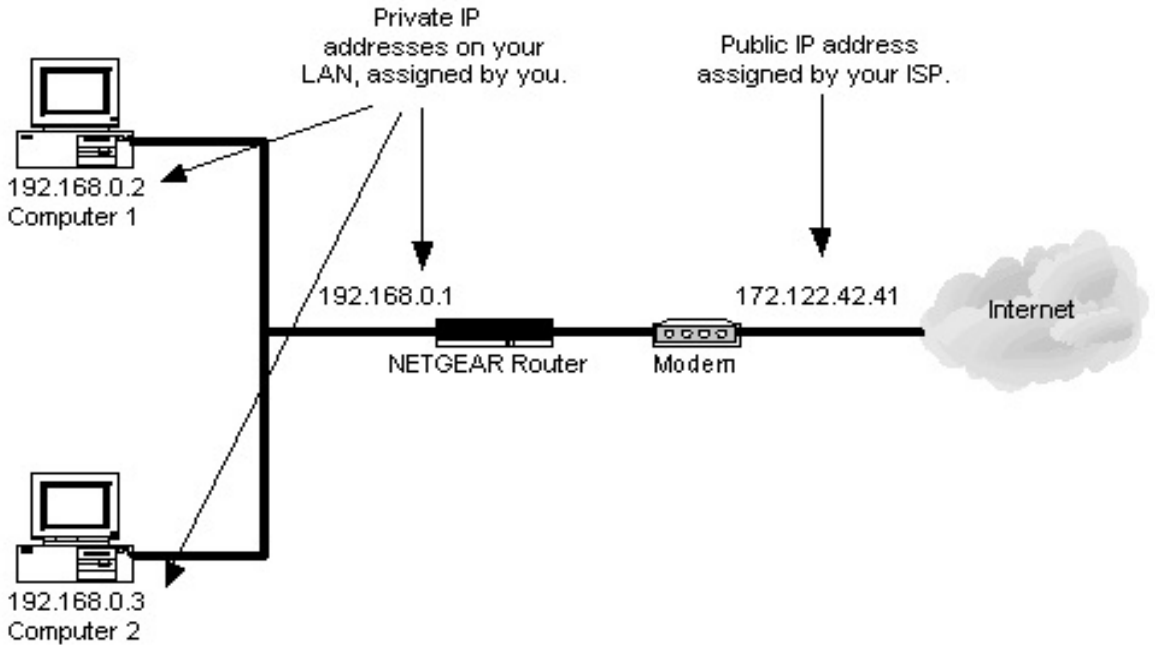
Step 6 − As per the standard Private IP will not communicate with Public IP address at any Point of time.

Step 7 − To achieve this, Private IP addresses need to be translated to Public IP addresses with help of NAT.

Step 8 − In simple words, Network Address translation is used to translate Private IP address to Public IP address to communicate LAN side of the Device to Global Network. Network address translation can be processed in Router or Firewall.

NAT

Given below is the diagram of the NAT −



NAT

Working of NAT

- Usually we used gateway router / Border devices used for NAT configuration.
- One of the interfaces for that device is connected to the local Area network (INSIDE) and one of the interfaces for this device connected to the outside network (OUTSIDE).
- When we have received a request from our local machine it will hit the configuration pool then that Private IP will convert it into Public IP address and vice versa.

NAT

Working of NAT

- **Inside worldwide location** − IP address that speaks to at least one inside nearby IP delivers to the rest of the world. This is within have as observed from the external organization.

- **Outside residential area** − This is the genuine IP address of the objective host in the nearby organization after interpretation.

- **Outside worldwide location** − This is the external host as observed to structure the external organization. It is the IP address of the external objective host before interpretation.

NAT

How Does NAT Work?

- Let’s say that there is a laptop connected to a home network using NAT. That network eventually connects to a router that addresses the internet.

- Suppose that someone uses that laptop to search for directions to their favorite restaurant. The laptop is using NAT.

- So, it sends this request in an IP packet to the router, which passes that request along to the internet and the search service you’re using.

- But before your request leaves your home network, the router first changes the internal IP address from a private local IP address to a public IP address.

NAT

How Does NAT Work?

- Your router effectively translates the private address you're using to one that can be used on the internet, and then back again. Now you know that your humble little cable modem or DSL router has a little, automated translator working inside of it.

- If the packet keeps a private address, the receiving server won't know where to send the information back to. This is because a private IP address cannot be routed onto the internet.

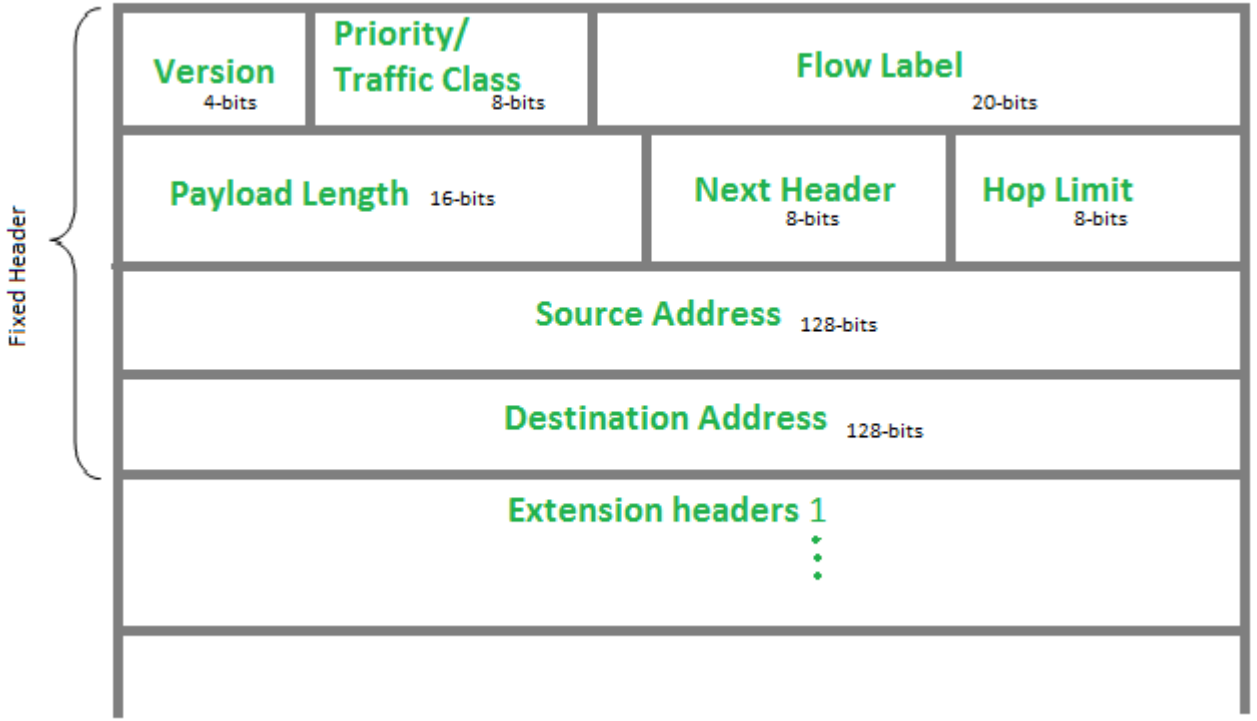
- If your router were to try doing this, all internet routers are programmed to automatically drop private IP addresses. The nice thing is, though, that all routers sold today for home offices and small offices can readily translate back and forth between private IP address and publicly-routed IP addresses.

IPv6: Frame Formats

IP version 6 is the new version of Internet Protocol, which is way better than IP version 4 in terms of complexity and efficiency. Let’s look at the header of IP version 6 and understand how it is different from the IPv4 header.

The wonder of IPv6 lies in its header. An IPv6 address is 4 times larger than IPv4, but surprisingly, the header of an IPv6 address is only 2 times larger than that of IPv4. IPv6 headers have one Fixed Header and zero or more Optional (Extension) Headers. All the necessary information that is essential for a router is kept in the Fixed Header. The Extension Header contains optional information that helps routers to understand how to handle a packet/flow.

IPv6: Frame Formats



IPv6: Frame Formats

IPv6 fixed header is 40 bytes long and contains the following information.

Version (4-bits): It represents the version of Internet Protocol, i.e. 0110.

Traffic Class (8-bits): These 8 bits are divided into two parts. The most significant 6 bits are used for Type of Service to let the Router Known what services should be provided to this packet. The least significant 2 bits are used for Explicit Congestion Notification (ECN).

IPv6: Frame Formats

Flow Label (20-bits): This label is used to maintain the sequential flow of the packets belonging to a communication. The source labels the sequence to help the router identify that a particular packet belongs to a specific flow of information. This field helps avoid re-ordering of data packets. It is designed for streaming/real-time media.

Payload Length (16-bits): This field is used to tell the routers how much information a particular packet contains in its payload. Payload is composed of Extension Headers and Upper Layer data. With 16 bits, up to 65535 bytes can be indicated; but if the Extension Headers contain Hop-by-Hop Extension Header, then the payload may exceed 65535 bytes and this field is set to 0.

IPv6: Frame Formats

Next Header (8-bits): This field is used to indicate either the type of Extension Header, or if the Extension Header is not present then it indicates the Upper Layer PDU. The values for the type of Upper Layer PDU are same as IPv4's.

Hop Limit (8-bits): This field is used to stop packet to loop in the network infinitely. This is same as TTL in IPv4. The value of Hop Limit field is decremented by 1 as it passes a link (router/hop). When the field reaches 0 the packet is discarded.

Source Address (128-bits): This field indicates the address of originator of the packet.

Destination Address (128-bits): This field provides the address of intended recipient of the packet.

IPv6: Frame Formats

Extension Headers: In order to rectify the limitations of the IPv4 Option Field, Extension Headers are introduced in IP version 6. The extension header mechanism is a very important part of the IPv6 architecture. The next Header field of IPv6 fixed header points to the first Extension Header and this first extension header points to the second extension header and so on.