# UNIT 1 INTRODUCTION TO LAYER FUNCTIONALITY AND DESIGN ISSUES



## 1.0 INTRODUCTION

This chapter discusses about the network layer, which is the third layer of the OSI model. Job of this layer is to send the packets from a source to destination. This layer responds to the service requests of the transport layer and takes the services from the data link layer. This chapter starts with an overview of the services of the network layer. Switching is the backbone of network architecture. This important concept of packet switching is elaborated with diagrams in section 1.3. How the address will be assigned to a host and the different concepts of addressing are discussed in further section. This is followed by congestion and routing concepts. Delay is an important concept in packet switched networks. The various types of delay have been discussed. The delay computation in different scenarios is illustrated with various examples in further section.

## 1.1 OBJECTIVES

After completing this unit, a student will be able to

- Explain the basic concepts and services of network layer.
- define the concepts of packet switching
- Differentiate between virtual circuit and datagram approach.
- Elaborate and utilize the concepts of addressing
- define congestion and policies to overcome the congestion in the network layer

- explain the concept of routing;
- calculate the delay in a given network scenario

## 1.2 SERVICES OF THE NETWORK LAYER

The third layer of the protocol stack is the network Layer. This layer is responsible for delivering the data from source machine to the destination machine that is end to end communication. At the source machine, it takes the services from the transport layer. Whereas on the destination side, the network layer provides the services to the upper layer that is transport layer. The important services provided by the network layer are

a) **Routing** – As discussed above, this layer is responsible for machine to machine communication. Thus, this layer decides the route that a packet has to follow from source to destination. There could be various possible paths from a source to a destination. Based on the chosen metric like delay, number of hops, a particular path would be selected as the best route.

b) **Packetization**–At the source machine, network layer receives the segment from the transport layer and send further to the data link layer. The received segment needs to be divided further into small packets or send as a whole packet, this decision is to be taken by the network layer by visualizing the maximum transmission unit of the data link layer. Control information i.e. header is to be added at the sending side so at the receiving side, packet is to be reassembled or decapsulated correctly.

c) **Forwarding** – when a packet is send from a source to a destination, this packet pass through a number of routers along the path. A router has a number of interfaces. Which interface is to be selected for the packet is decided by the network layer.

Let us understand the clear distinction between routing and forwarding with an example. We are planning a drive from JIIT, Noida to IGNOU. There are various possible paths like one is via GT road, another is via Indirapuram and so- on. Which path is the best one as per the time taken or road conditions? This decision process is routing and here our metric to decide the best route could be any one like traffic conditions on the road, infrastructure of the road, etc. Suppose the selected route is via Indirapuram, and the person started the journey. At one of the intermediate junctions, there are various directions. Which direction to be chosen at the junction is the forwarding decision taken by the router.

## 1.3 Packet Switching

There are two switching mechanisms that work in the backbone of the network, circuit switching and packet switching. In today's Internet, packet switching is utilized where telephone networks is an example which best describes the concept of circuit switching. In circuit switching, the resources are reserved for a user where as in packet switching, the resources are shared among different users on demand basis.

Network layer utilizes the packet switching as packet is the basic data unit used at this layer.

Let us understand the concept of packet switching more clearly with the following scenario. Consider two banks where bank 1 requirement is book an appointment before coming to the bank. If you reach directly, you would not be entertained.If already booked an appointment, your waiting time is negligible. There is no such requirement for 2nd bank. As soon as you reach to the bank, you will be entertained based on the number of people already waiting. The services will be provided to you without any hassle, if no one is there. If already a large number of people are waiting, then your waiting time would be large or in some situations, bank will say it's already full, kindly come on next day. But on the other hand, there is no hassle of calling before leaving from home. The scenario of 2nd bank describes how packets will be handled during packet switching.

Network layer receives the data from the transport layer and divide into manageable units known as packets. Based on different forwarding mechanisms used by connected devices to forward the packets from a given source to a particular destination, packet switched networksare further divided into two categories: virtual circuit approach and datagram approach.

## 1.3.1 Virtual Circuit Approach (Connection-oriented Service)

Before going into the detail of virtual circuit approach, first let us understand the meaning of **connection oriented service**. Connection oriented service in which an end to end logical connection would be established between the source machine and destination machine. All the data between a source destination pair would be sent through the same connection. After sending the data, connection would be terminated. A connection oriented service has the following properties

a) All data would be sent in order and without any error to the destination machine.
b) All the received data would be acknowledged by the destination machine.
c) The underlying service guarantees the in-order delivery of packets without any loss or duplication of packets.
d) There is a retransmission policy which will handle the lost packets.

Due to all these properties, connection oriented service is also known as **reliable** service. A connection oriented service is a three step process which are described as follows

a) **Connection establishment:** This is a handshaking process which needs to be executed before any data exchange among two entities. Suppose, person A wants to talk to other unknown person B. Before any informal or formal talk, they will exchange formal hello messages. Similarly, here in connection oriented service, source machine will send the connection request message (control message) to the intended destination machine. In receipt of this, destination machine will send an acknowledgement message to the source machine. Source machine will send a confirmation of the received

acknowledgment message. Purpose of this 3 step control messages exchange is to prepare both the entities for handling the data transfer further.

b) **Data transfer:**Once the connection gets establishment, data could be transferred among the two entities.

c) **Connection termination:** Once the data transfer is over, a connection termination request will be send by the source machine to the destination machine. Connection termination is also a three step process similar to the connection establishment phase. Source machine will send the connection termination request to the destination machine. Destination machine will send the ACK of termination request and its own termination request. In the last step, sender sends the confirmation of received acknowledgement and termination packet.

**Transmission Control Protocol (TCP)** is an example of connection oriented protocol which works at the transport layer. Connection oriented service is provided at the transport layer as well as the network layer. However, there are some subtle differences. At the transport layer, only two end systems are involved in connection establishment and setting of parameters, where as in the network layer, along with end systems, connecting devices i.e. routers along the path are also involved in setup process. Connection oriented service at the transport layer is implemented in the two end systems where as in the network layer it is implemented in all the routers in the chosen path along with the end systems.

In virtual circuit approach, a virtual connection would be established from source to destination on which all packets among this source destination pair would be sent. Therefore, it is also known as connection oriented service.

A network layer packetcontains the source and destination address as a part of header information because it provides logical communication among the machines.In virtual circuit approach, along with the source and destination addresses, packet contains a VC-ID. It is necessary to mention VC-ID in the packet as all packets has to follow the same virtual connection. When packet reaches to a router it will consult the forwarding table on the basis of VC-ID mentioned in the packet and decide the output port.

A virtual circuit approach involves three phases. The phases are a) setup phase b) data transfer and then connection termination. All are explained as follows:

a) **Setup phase:** Establishing a virtual circuit implies the following needs to be done.
   i. Deciding the path between a source and destination
   ii. Assigning a virtual circuit identifier (VC-ID) to each link along the path
   iii. Change in the forwarding table of all intermediate routers along the path with respect to virtual circuit

Let us understand this process with the figure 1.

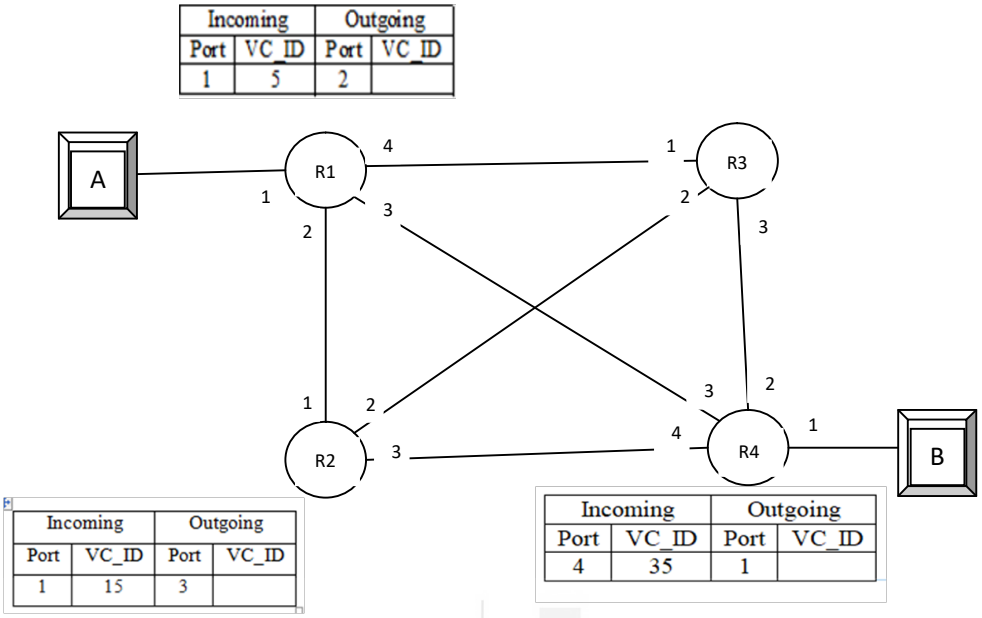


**Figure 1: Sending of Request packet in virtual connection establishment process**

As shown in figure 1, machine A wants to send the data to machine B. Let us chosen path between machine A and B is A-R1-R2-R4-B. Thus, a virtual connection needs to be established among A and B by involving all the intermediate routers. The process is as follows

1) Machine A will chose a VC-ID from its available list of VC-ID's and send the request packet to R1. As shown in figure 1, chosen VC-ID by A is 5.
2) As soon as Router R1 will receive this request packet, it will create an entry for this virtual circuit in its forwarding table as shown in figure 1. In this entry, Router R1 notes that the packet is coming from incoming port 1 and incoming VC-ID 5. Outgoing port is 2 and leave blank in place of outgoing VC-ID.
3) Now, R1 will forward this request packet to R2. In the similar manner, R2 will create an entry of this virtual circuit request in its forwarding table. Suppose, the chosen VC-ID by R1 is 15, thus the values of incoming port, incoming VC-ID, outgoing port and outgoing VC-ID are 1, 15, 3 and blank respectively.
4) R2 will forward the packet to R4. R4 complete the three entries of its forwarding table in the similar manner as shown in figure 1.
5) R4 sends the packet further to machine B. Machine B will chose a VC-ID and let this value is 60. In future communications, the VC-ID 60 is an indication for B that this packet comes from machine A.

All these five steps show the forwarding of request packet for setting the virtual connection from source machine A to destination machine B. But this forwarding completes the only three entries in the forwarding table. To complete the 4$^{th}$ entry of forwarding table, B will send an acknowledgment packet back to A via same path that is B-R4-R2-R1-A. The process can be visualized in figure 2 and explained as follows.

1) Destination machine B sends an acknowledgement packet carrying VC-ID 60 to R4. By knowing this value, Router R4 will complete the 4th column i.e. outgoing VC-ID of its forwarding table as shown in figure 2.
2) Router R4 will forwardthis acknowledgement packet to router R2. This packet contains the incoming VC-ID 35 which will be copied at the place of outgoing VC-ID in the table of R2.
3) Similar process will happen at R1. Router R1 receives the incoming VC-ID 15 from the R2 table. It will be copied at the place of outgoing VC-ID in the table of R1.
4) Finally, R1 forwards the acknowledgement packet to machine A which carries incoming VC-ID as 5. This VC-ID is chosen by A only in the initial process. Machine A knows that this VC-ID is to be used for communication to B.

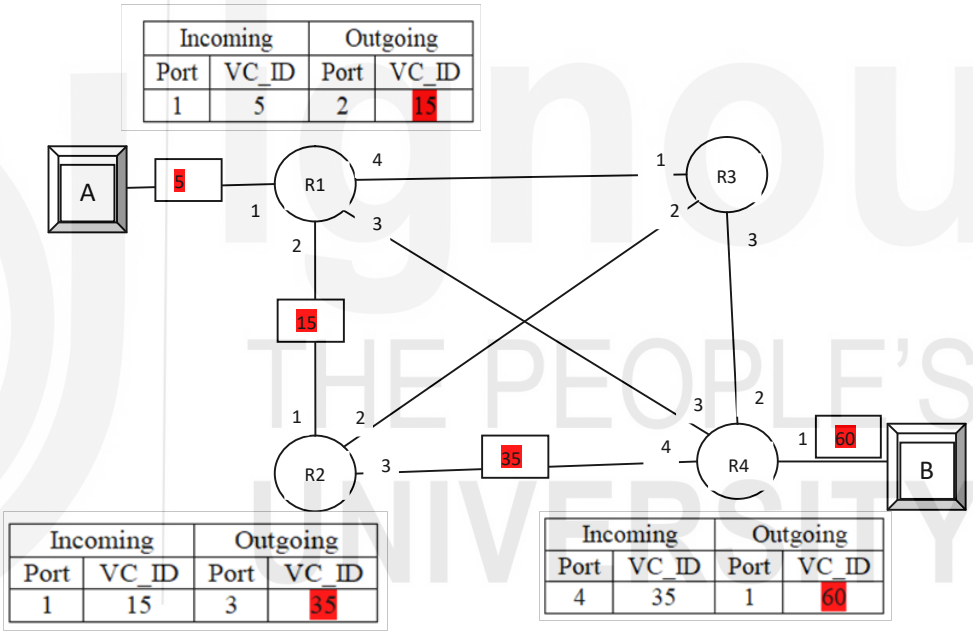


**Figure 2: Sending of Acknowledgment packet in virtual connection establishment process**

As discussed initially in the setup phase the virtual circuit establishment implies three works (deciding the path, assignment of VC-ID to each link, change in forwarding table) to be done. So, as explained in figure 1 and 2, all three mentioned works has been completed.

b) **Data transfer:**All the packets between A and B will be sent through the same established virtual circuit between them. As a result, thus all reach to the destination in order. Each intermediate router changes the value of VC-ID by seeing the forwarding table as shown in figure 3. As soon as the packet is reached to a router, it will see the VC_ID of this packet. In this

example it is 5. Thus, R1 will see its forwarding table for the VC_ID 5 and incoming port 1. It can be visualized from figure 3, for these values as an index; the outgoing port is 2 and VC_ID is 15. R1 will change the VC_ID value in the packet and forward it further. Similar process will be followed at the other routers as well and finally the packet will be delivered to the destination machine B via established virtual connection. The figure3 shows the process for one packet. The same process would be followed by all the packets.

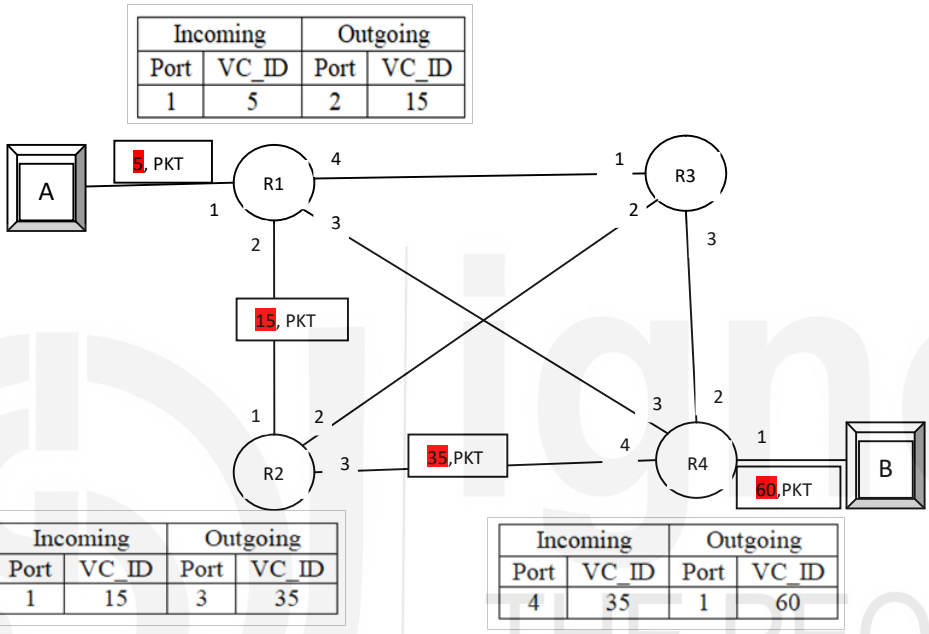


**Figure 3: Packet transfer over an established virtual connection**

c) **Connection termination:** Once A has sent all the packets to B, machine A will send a termination request packet to B and in return, B will send an acknowledgment of the same. As a result, all the routers delete the entry from the routing table.

## 1.3.2 Datagram Approach (Connection-less Service)

Datagram approach is used in today's Internet scenario. This approach follows the concepts of connection-less service. So, let us first understand the basic concepts of connection less service.

**Connection less service**, as its name implies no virtual connection would be made between source and destination. Both the entities does not do any handshaking. When a machine wants to send the packet to another machine, it simply starts sending. The message is divided into manageable units called packets where each packet is treated individually. Each packet can follow same or different paths, thus they may reach out of order or can be lost in between. Sender machine does not have any clue regarding

the loss of packets as there is no provision of acknowledgement of packets. Due to all these properties, connection less service is an unreliable service.

Although this service is unreliable but it is required in some situations like where we want immediate transfer of data or where loss of some packets does not affect the overall quality of message or the situation where less overhead is required. The overhead of handshaking or sending acknowledgements is not present in connection less service.**User Datagram protocol (UDP)** and **Internet protocol (IP)** are the examples of connection less protocols which works at the transport layer and network layer respectively.

As **datagram approach** is a connection less service, thus all packets either belonging to same source destination pair or different, are treated individually. Here, packet is called as a datagram. Datagram contains the source and destination address. Forwarding decision is taken individually for each packet on the basis of destination address. Each router looks into the forwarding table for the mentioned destination address in the datagram. It returns the output interface based on matching on which the datagram will be forwarded further. If more than one entry are matched then based on the principle of longest prefix matching, the output interface would be selected.

In datagram approach, routing tables were modified by the routing algorithms. Routing algorithms is an important aspect of network layer which will be discussed later.

Destination address follows hierarchical addressing structure. How the destination address is actually extracted and processed to decide the path, let us understand it more clearly with an analogy. Suppose we want to go to a particular location 116-A, H Block, Vikaspuri, New Delhi. We started our journey from Noida and at the first junction if we ask for 116-A, H Block, Vikaspuri, New Delhi. Nobody will be able to tell the exact location or if somebody tried to do so, he or she will tell you only the road going towards Delhi. After reaching to Delhi, if u ask now for Vikaspuri, someone can instruct you by taking this path, you can reach to the desired location. Again the same situation, when you enter into Vikaspuri and you ask for 116-A, H Block , the person can tell you only about the path directions to reach H-block, not exactly 116-A. In the similar manner, part of destination address will be extracted and used to decide the output interface.

## 1.3.3 Comparison of Virtual Circuit and Datagram Approach

Both the approaches havetheir own advantages and disadvantages. Both the approaches can be compared on the basis of following points.

a) **Setup time:** Connection is to be setup in case of virtual circuit approach where as in datagram approach, no setup phase is required. Due to setup phase in virtual circuit approach, the sequencing of packets can be easily maintained. On the other hand, in datagram approach there is no setup overhead so sending of packets can be started immediately.

b) **Routing decision:**As the virtual circuit has been established between a specified source and destination, so no routing decision has to be taken for individual

packets. Thus, packets can be forwarded more quickly in virtual circuit approach whereas in datagram approach, for every packet, the routing decision is to be made. In virtual circuit approach, output port is decided by looking into the VC_ID of a packet where as in datagram approach, output port is decided by looking into the destination address.

c) **Reliability:**In virtual circuit approach, if a router gets failed, all the connection passing through that router or whose state information is maintained in this routergets lost. However, in datagram approach only the packets waiting in the queue of that router gets lost.

d) **Routing tables:** While establishing a virtual circuit, state of a connection needs to be updated in all the intermediate routers. Routing table is indexed by VC_ID where as in datagram approach, routing table is indexed by destination address and routing algorithms update the routing tables.

e) **Load balancing:** In datagram approach, packets may travel different paths. Thus traffic can be balanced over multiple routes.

f) **Reservation of resources:** In virtual circuit approach, resources are reserved so delivery can be guaranteed. If there are packets then allocated resources (like buffers, bandwidth, etc.) would be directly used. Whereas in datagram approach, the resources are shared on the demand basis. If everyone is trying to use the resources and resources are limited, then it may lead to congestion or packet loss. Congestion can be easily avoided in virtual circuit approach.

Table 1 provides a brief overview about the difference in virtual circuit and datagram approach.

Table 1: Comparison of virtual circuit and datagram approach

| **Virtual Circuit Approach** | **Datagram approach** |
|---|---|
| Route is decided for all packets of a conversation between S and D | Route is decided for each packet |
| Overload may block connection setup and increase packet delay | Overload increase packet delay |
| Connection set up delay along with packet transmission delay | Only packet transmission delay |
| Forwarding decision based on VC_ID | Forwarding decision based on destination address |
| Congestion avoidance is easy | Congestion avoidance is difficult |

## 1.3.4 A view of some Network Service models

Till now, we had discussed the overview of network layer services. This section discusses some of the network architectures to get an idea about their services.

Internet is most widely used network architecture. Internet's network layer provides best effort service. Best effort service implies it will try but does not guarantee anything. Therefore, it can be visualized from table 2, Internet network service model

does not guarantee on any issue like ordering of packets, packet loss, bandwidth etc. It does not even preserve the timings difference among packets when the packets reach at the receiver side. But, there are other network architectures which provide more than best effort service. Table 2 compares three network service architectures on the basis of their services. For more details please refer [1]

Table 2: Comparison of Network Service models

| | **Internet** | **ATM** | **ATM** |
|---|---|---|---|
| **Service model** | Best effort | CBR | ABR |
| **Guaranteed Bandwidth** | No | Constant rate Guarantee | Minimum Guarantee |
| **Delay Guarantee** | No | Yes | No |
| **Sequencing of packets** | Any order | In order | In order |
| **Packet Loss Guarantee** | No | Yes | No |
| **Congestion indication** | No | No chances of congestion | Provides congestion indication |

ATM CBR (constant bit rate) works on the principle of a virtual pipe between source and destination. Thus, it is able to provide some of the services like ordering of packets, guaranteed bandwidth to each user, etc. No packet would be lost and there are no chances of congestion as the resources are reserved while establishing the connection. ATM ABR (available bit rate) provides a minimum amount of bandwidth guarantee and delivers packets in order. But it does not provide any guarantee about the loss of packets and jitter among packets. Thus, ATM ABR is a little bit better than best effort service model of Internet.

### ➢ Check Your Progress 1

Choose the correct option.

Q1. _____ Approach takes the forwarding decision based on destination address.

a) Virtual circuit
b) Datagram

Q2. _____ is a connection less protocol used at the transport layer.

a) IP
b) TCP
c) UDP

Q3. _____ is an example of packet switched datagram networks.

a) Internet
b) Telephone networks

Q4. Compare Virtual circuit approach with the datagram approach. Provide at least two differences.

.....

.....

.....

## 1.4 NETWORK ADDRESSING

Network layer provides end to end communication i.e. it delivers the packets from source machine to the destination machine. This communication could be at a global level, thus, a unique identifier for every machine is required. This identifier is the logical address of machine, also known as Internet address or IP address. In actual terms, this address is not associated to the machine; it is associated to the interface. The portion between machine and the link is called as an interface. Generally, a host is connected to a single network through a link so it has one interface thus one IP address. On the other hand, a router is connected to many networks or hosts so it has multiple interfaces and each interface will have an IP address.

### 1.4.1 IP address

IP address is a 32 bit address. Along with the property of uniqueness, IP address should be universally acceptable also, that is who so ever wants to communicate, follow a common format. As the IP address is of 32 bits, thus $2^{32}$ unique addresses are possible. This much amount of address space impliesat an instant of time, approximately 4 billion machines with unique addresses could be connected.

IP address is generally written in dotted decimal notation (base 256). The other two notations are binary (base 2) and hexadecimal (base 16). As shown in figure 4, binary notation is just writing of all 32 bits in binary form. However, to increase its readability, the bits are written in a group of 8 bits that is a byte and some space will be provided between each byte. If we write decimal value of each byte and put a dot to separate the group is referred as dotted decimal notation. This is most commonly used notation. If we write hexadecimal value with respect to a group of 4 bits, then that notation is called as hexadecimal notation.

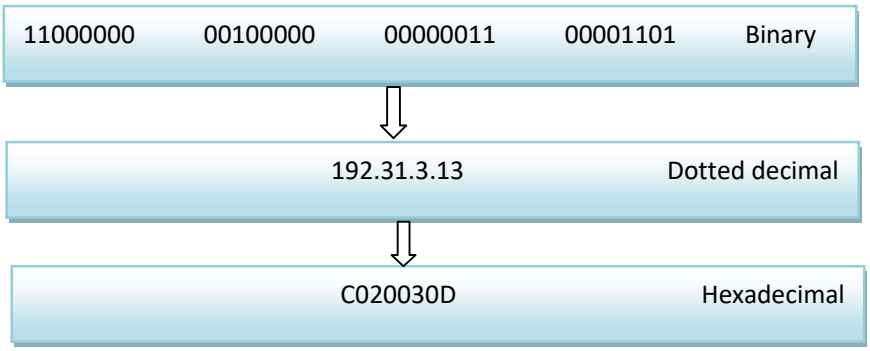


**Figure 4: IP Address notations**

### 1.4.2 Hierarchy in addressing

Network addressing follows hierarchical structure. The hierarchical structure can be easily visualized in our daily life examples like postal service, telephone networks. In postal service, posts have been distributed on the basis of written postal address. Postal address is extracted on the basis of country, state, district, city, street, building and house number. The address is always extracted in the reverse order. First, all the posts have been separated on the basis of country then state will be looked upon and so on. Similarly, the telephone networks also follow the hierarchy in telephone number. First few digits signify the country code which is followed by the area code and then the connection number itself.

In the similar manner, IP address is divided into two parts where first part signifies the network portion and second part is the host address. Network portion can be fixed or variable. If the network portion is fixed, it refers to **classful addressing** which is widely used in earlier days. But nowadays people switch onto the concepts of variable network portion which refers to **classless addressing**. The next chapter discusses the concept of classful and classless addressing in complete detail. Suppose $b$ bits are used to denote network address, then the remaining $(32 - b)$ bits would be used to denote host address.

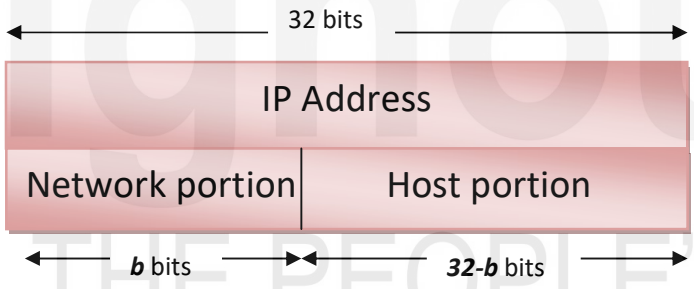


**Figure 5: Parts of IP address**

## 1.4.3 Getting an IP address

An IP address can be assigned to a host in two ways either manually or dynamically.

a) **Manual Assignment:** Network administrator allocates an IP address to the host from the available block of addresses. It would not be changed until the administrator himself changes it. This is also called static assignment.

b) **Dynamic Assignment:** When a host machine joins the network, an IP address would be automatically assigned by some protocol like Dynamic Host Configuration Protocol (DHCP). DHCP works like a plug and play protocol in the sense that as soon as someone joins the network, an address would be allocated and free the address when the host machine leaves the network. This is a dynamic assignment in the sense that every time a host joins a network, it will get a new address.

➢ **Check Your Progress 2**

Choose the correct option.

Q1. The _____ protocol is used to assign dynamic IP address.

a) Internet protocol
b) Transmission Control Protocol
c) Dynamic Host Configuration Protocol

Q2. If a host portion is of 8 bits then how many bits denote the network portion?

a) 32 bits
b) 24 bits
c) 16 bits

Q3. IP address is generally written in _____ notation.

a) Dotted decimal
b) Binary
c) Hexadecimal

Q4. How a host gets an IP address?

.....

.....

.....

## 1.5 CONGESTION

If the packets are coming at a faster rate than the handling capacity of the network, this leads to a situation known as congestion. Initially, when the packet arrival rate starts getting higher than the packet processing rate, queue starts filling up. As a result, packet delivery time gets increased. If the same situation continues, queue becomes full and packet drop starts.In this situation, source does not receive any acknowledgement and for a large number of the packets, the timer is up; which leads to unnecessary retransmissions. Sometimes the situation becomes worse and reaches to a deadlock point and whole system gets collapsed.

To understand the situation of congestion, let us see the behaviour of two important performance metrics i.e. delay and throughput with respect to the capacity of the network. Figure 6 shows the delay and throughput as a function of load.

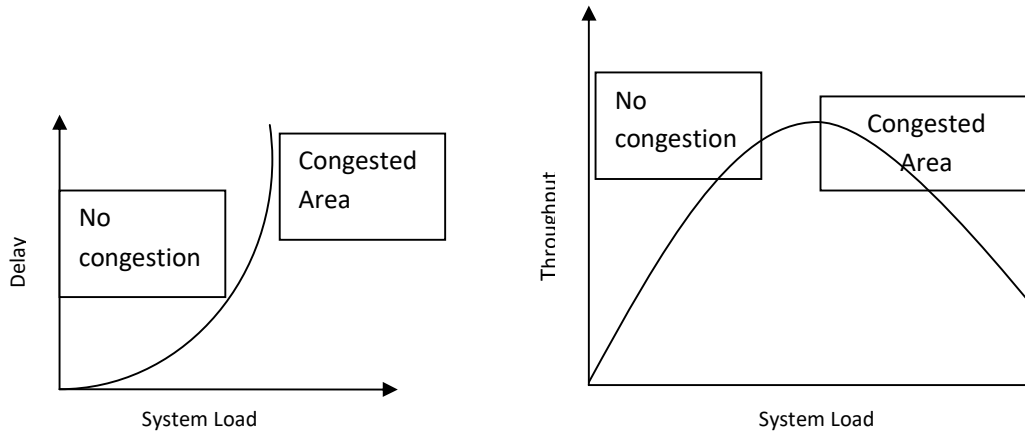


**Figure 6: Delay and Throughput vs Load**

Initially, when the less number of packets, they would be delivered without any delay and throughput is good. As the system load increases, packets experience queuing delay which in turn affects throughput as well. When the system load reaches the capacity, queue becomes full and some packets get discarded. As a result, delay approaches towards infinite value and throughput starts decreasing.

The issue of congestion is not only handled at the network layer; it is also handledat the transport layer. The main idea behind congestion is try to avoid the situation i.e. take preventive measures before reaching to a threshold and if the situation happens, try to come out of that situation. First one is known as congestion avoidance phase and second one is congestion removal. The policies used for congestion avoidance phase is called as open loop congestion control policies. Closed loop congestion control policies are for congestion removal phase.

Some of the **open loop congestion control policies** are as follows

a) Admission policy: A router can visualize the possibility of congestion and if there are chances of congestion then the new virtual connection request can be rejected.

b) Retransmission policy: When the sender does not receive any acknowledgement of the sent packet, it does the retransmission. For how long the sender has to wait or after how many lost packets, the packet needs to be retransmitted, all these kinds of retransmission policies should be designed in such a way that it will not add more congestion in the network.

c) Acknowledgement policy: Receiver's acknowledgement policy can also control the congestion at some level. For example, if receiver sends the acknowledgement packet after receiving some packets, it will slow the sender as well as not add a burden of sending acknowledgement packets.

d) Discard policy: If a router implements the good discarding policy then it can also prevent congestion at some level. The good discarding policy which does

not impact the overall quality of transmission. For example, in a multimedia transmission, some less priority packets gets discarded at the time of chances of congestion then it will not impact the overall quality of transmission.

Sometimes, even after taking all the preventive measures, congestion occurred. In this situation, **closed loop congestion control policies** to be used to avoid stucking into deadlock. These policies are

a) Sending of Choke packet: A choke packet is a control packet sent by the router to the source node. This packet informs the sender about congestion occurrence. This method is implemented by protocols like ICMP, etc.

b) Signaling: In this method a signal would be sent by the congested node to inform the sender about congestion. Rather than sending an explicit packet like choke packet, here, a signal will be sent in the existing packets carrying data.

c) Implicit signaling: In this method, no specific information is sent to the source rather sender itself guesses about congestion. For example, if the sender does not receive any acknowledgements of several packets with in timeout period is a signal for the sender that there is congestion in the network.

## 1.6 ROUTING

Job of the network layer is to send the datagram from a source end system to destination end system. Data may travel through different paths or through multiple hops to reach to the destination. The process of deciding about the path to reach to the destination is known as **routing**. There are routing protocols or which helps in constructing the forwarding table. The forwarding table or routing table is stored at every end system and router. Whenever a router receives a packet, router consults its routing table to decide the output interface. Looking into the routing table and choosing the output interface, this process is known as **forwarding**. Filling up of routing tables, their maintenance and regular updation is done at continuous intervals by **routing protocols or routing algorithms.**Routing algorithms is a part of network layer software.

There are various desirable properties ofa routing algorithm. These are as follows

1) Routing protocols decide the best route from a source S to destination D. This best route can be best in terms of any of the metrics like delay, throughput, packet loss, etc. This is similar to the analogy when we decide our travelling route from one city to another. There are various paths as well as various modes of transportation. We chose the one on the basis of cost,

comfort, time etc. Similarly, here in communication networks, the path is decided by looking into various metrics.

2) Other than the metrics, paths should be decided or updated in between by looking into the conditions of congestion into the network.
3) Routing is successful only when all the nodes are cooperative with each other. So, cooperation among the nodes is must.
4) Suppose, a link gets down or a router become fail, then all the routing tables to be quickly updated. This knowledge should be reflected in all the routing tables, so that packet loss will be minimal. Quick convergence and stability is very important in a routing algorithm.

To solve the routing problems, network isrepresented in terms of graphs. While formulations as a graph, routers are represented as nodes and the links connecting the routers are represented as edges. A graph G is represented as (V, E). Where, V is a set of nodes and E is a set of edges connecting those nodes. Each edge is labeled with a value representing its cost. This cost could be directly or indirectly related to the link type or metric value. For example, cost could be directly proportional to the congestion or inversely proportional to the bandwidth. Higher bandwidth link or less congested link gives a low cost value of that link. If the nodes are connected by an edge then the cost is associated with that edge else it is infinity. Undirected graphs are considered for formulation. Thus, the cost associated with edge (a, b) is same as edge (b, a). A path is a sequence of edges traversed from chosen starting node to chosen destination node. The cost of a path is sum of all the edges cost of that path. Let us understand this formation more clearly with the figure 7.

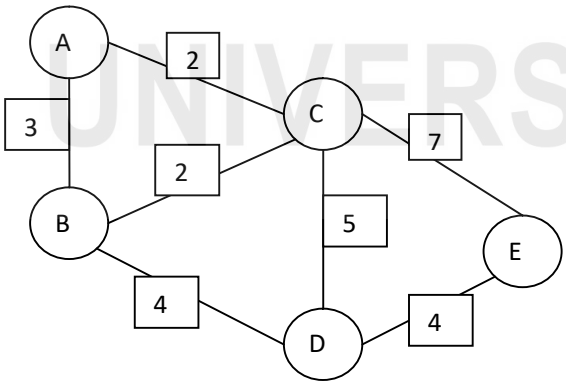


**Figure 7: Graph representation of a network**

It can be visualized from the figure 7, set V consist of routers {A, B, C, D, E} and set E consist of edges such as (A,B), (A,C), (D, E), etc. Each edge is labeled with a value known as cost. Let us calculate the path from node A to node E. It can be visualized from the figure there are multiple paths from A to E. Some of the paths and associated costs are as follows

| Path | Cost |
|---|---|
| A-C-E | 2+7=9 |

| | |
|---|---|
| A-B-C-E | 3+2+7=12 |
| A-B-D-E | 3+4+4 = 11 |

The cost of a path is sum of the costs of all traversed edges from A to E. On the basis of low cost, routing algorithm chose the path A-C-E. Suppose, all the edges have same unit cost, then the path with less number of hops is chosen. For this scenario, again path A-C-E would be selected because it has less number of hops in comparison to other paths.

Now, revise all this scenario of finding the paths in your mind and tell me, how you have chosen the path. Have you tried all the combinations? I think no, you have tried just 2-3 paths and convinced yourself that this is the least cost path. All this work of your mind is done actually by a routing algorithm but to do this job, routing algorithm shouldknow the complete knowledge about the network.

## 1.6.1 Classification of Routing Algorithms

Routing algorithms can be classified into different types like centralized or decentralized based on how the routes would be computed. Another categorization is adaptive or non-adaptive routing algorithms which are based on strategy of updation of routes. All these different types are discussed as follows

a) **Global Routing Algorithm**: These routing algorithms compute the best path (least cost one or shortest one) by gathering the complete knowledge about the network. It is also known as centralized routing algorithm. It can be run at one central location or a replica to be run at multiple locations. All the information about the nodes and links to be collected at the central algorithm and then this algorithm computes the routes. The computed routing tables would be distributed to all nodes. In this way, global optimal routes will be computed and distributed to all. It will reduce the burden on each node. **Link state algorithms** are a kind of global routing algorithms.

b) **Decentralized Routing Algorithm:** These routingalgorithms works in an iterative, asynchronous and distributive manner. Complete network knowledge is not available at a single location rather each node interacts with its neighbors about the cost and their knowledge. Now, these neighbors interact further with their neighbors and this process goes on. In this way, the path to one or more destinations would be computed. **Distance vector routing algorithm** is an example of decentralized routing algorithm.

**c)** **Adaptive Routing Algorithm:**These routing algorithms reflect the change in the routing tables whenever there is a change in topology. That's why these algorithms are also known as **Dynamic routing algorithms.** These algorithms also update the paths with respect to network traffic conditions.

d) **Non-adaptive Routing Algorithm:** These routing algorithms do not update the routing table periodically or at the instance of change in topology. Manually, the routes would be computed and stored. These routing algorithms do not respond to failures automatically, that's why these algorithms are also known as **Static algorithms**.

## ➢ Check Your Progress 3

Choose the correct option.

Q1._____ process creates and maintains the routing table.

Q2. Which routing algorithm works in an iterative, asynchronous and distributive manner?

a) Link state routing algorithm
b) Distance Vector routing algorithm
c) Static algorithm

Q3. Define congestion.

.....

.....

Q4. What are the various policies that can be used to avoid congestion?

.....

.....

.....

# 1.7 DELAY IN PACKET SWITCHED NETWORKS

The packet transmission process starts from a source and ends at a desired destination. In this transmission process, packet travels through a number of intermediate routers and paths. Thus, a packet will not reach immediately to the destination. Rather it experiences a number of delays.

## 1.7.1 Types of delay

A packet experience four types of delays which are explained as follows:

a) **Transmissiondelay**: A source machine transmits a packet means that source machine put one by one bit of that packet on the link. A packet has certain length thus, it can't be put on the link in one go. Total time experienced by the source machine in this process is known as transmission delay. If a packet length is denoted as L and transmission rate is denoted by R, then transmission delay is calculated as $L/R$ .

b) **Propagation delay:**As soon asthe bit is put on the link, this bit has to travel through a number of intermediate links. For a single intermediate link, propagation delay is calculated as distance of this link divided by the speed of the link. Speed of the link depends on the physical type of link. Generally, speed is considered as $3*10^8$ m/s, which is propagation speed of the vacuum.

c) **Processing delay:** This is the amount of time taken by a router or destination machine to process a packet. Packet content would be checked for error detection. Packet would be processed to the upper layer protocol if it is a destination machine. If it is a router, it would be processed to the selected outgoing port. Generally, the value of processing delay depends on the speed of the router.

d) **Queuing delay:**As its name suggests, this is the amount of time a packet waits for its turn to get to be transmitted. Each router has an input queue for incoming port and an output queue for outgoing port. Summation of both the waiting times is known as queuing delay. Queuing delay mainly depends on the packets already waiting for their turn. If there is no packet in the queue, queuing delay is zero.

## 1.7.2 Computation of delay

Total delay is the summation of all the above types of delays defined in above subsection. The following notations represent four delays.

- $d_t - Transmission\ delay$
- $d_p - Propagation\ delay$
- $d_{proc} - Processing\ delay$
- $d_q - Queuing\ delay$

To compute the total delay experienced by a packet from source to destination, it has to been how many links and routers in between. If there are $k$ links in the path from source to destination, it implies there are $k-1$ routers in between. For all the $k$ links, transmission, propagation and processing delays to be computed but queuing delay is to be computed at router only. Total delay is computed as follows

$$Total\ delay = k\left(d_T + d_P + d_{proc}\right) + (k-1)d_q$$

## 1.7.3 Numerical

**Q1.** Suppose two hosts Y and Z are directly connected by a link. Length of this link is 10,000 Km and this link transmission rate is 1Mbps. The propagation speed of the link is $2.5*10^8$ m/s. Based on this information answer the following parts

a) Y sends a file of 400K bits to Z. How long does it take to send the file assuming it is sent continuously?
b) Suppose now the file is broken up into 10 packets with each packet containing 40K bits. Z sends an ACK for each packet and Y cannot

send a packet until the preceding one is acknowledged. Transmission time of an ACK packet is negligible. How long does it take to send the file?

**Answer:**

a) File size = 400,000 bits , Transmission rate = 1 Mbps

Thus, transmission delay is

$$= \frac{file\ size}{trans\ rate} = \frac{400000}{10^6} = 400\ msec$$

Distance = 10,000 Km, Speed = 2.5 *$10^8$m/s

Thus, propagation delay is

$$= \frac{distance}{speed} = \frac{10 * 10^6}{2.5 * 10^8} = 40\ msec$$

In this scenario, there is no processing delay or queuing delay. Therefore, total delay is

Total delay = Trans delay + Propagation delay = 400 + 40 = **440 msec.**

b) Packet size = 40,000 bits , Transmission rate = 1 Mbps

Thus, transmission delay for one packet is

$$= \frac{file\ size}{trans\ rate} = \frac{40000}{10^6} = 40\ msec$$

Distance = 10,000 Km, Speed = 2.5 *$10^8$m/s

Thus, propagation delay is

$$= \frac{distance}{speed} = \frac{10 * 10^6}{2.5 * 10^8} = 40\ msec$$

There are two important points to be note down

i. Second packet is sent only when Y receives the acknowledgement of first packet, thus twice of propagation delay is used.
ii. Acknowledgement can be sent only when the first packet is received completely at the receiver end. Thus, twice of transmission delay is used.

Therefore, for one packet total delay is = 2*Trans delay + 2*Propagation delay

And the total delay for all 10 packets is = 10*(2*Trans. delay + 2*Propagation delay)

= 10*(2*40 + 2*40) =**1600 msec.**

**Q2.** Compute the end to end delay for circuit switching and packet switching for a network. This network is having 5 hops to switch a message of 1200 bits

where all the links have a data rate of 4800bps. Size of the packet is 1024 bits along with a header of 32 bits. In case of circuit switching, consider 0.5sec as a call setup time. Hop to hop delay is .02 sec. Assume zero processing delay.

**Answer:** This answer is divided into two parts a) Computation of delay in circuit switching scenario b) Computation of delay in packet switching scenario

a) Computation of delay in circuit switching scenario

Call set up time is = 0.5 sec
Propagation delay is = .02 sec
Transmission delay is = $\frac{1200}{4800} = 0.25$ sec
Total delay = call set up time + message delivery time
= 0.5 + 5*(propagation delay) + transmission delay
=0.5+ 5*(0.02) + 0.25 = **0.85 sec**

b) Computation of delay in packet switching scenario

The given packet size is 1024 bits. It implies 32 bits of header and the leftover 992 bits are data bits. Thus, to send the total message of 1200 bits, two packets are required.

- First packet is of 1024 bits (992 bits of data and 32 bits of header).
- Second packet is of 240 bits (1200 – 992= 208 bits of data and 32 bits of header).

Propagation delay is = 5*0.02 = 0.1 sec
Transmission delay at first hop = $\frac{1024}{4800} + \frac{240}{4800} = 0.213 + 0.05 = 0.263$ sec
Transmission delay at rest of the hops is $= 4 * \frac{1024}{4800} = 4 * 0.213 = 0.852$ sec. because at the rest of the hops there is no transmission delay for 2nd packet or any other number of packets.

The total delay is $0.1 + 0.263 + 0.852 = \mathbf{1.215}$ **sec.**

## ➢ Check Your Progress 4

Choose the correct option.

Q1. If there is no buffer at the router, each incoming packet directly forwarded further onto the outgoing port. In this situation which kind of delay is negligible?

a) Processing delay
b) Queuing delay
c) Transmission delay
d) Propagation delay

Q2. Host X is connected to Y via switch S. The link bandwidth is 10Mbps and propagation delay on each link is 20μs. S is a store and forward switch, it begins retransmitting a received packet 35μs after it has finished receiving it. Calculate the total time required to transmit 10,000 bits from X to Y.

a) As a single packet
b) As two 5,000 bit packets sent on right after the other

.....

.....

.....

.....

## 1.8 SUMMARY

In this unit, we understood the concepts of packet switching. Network layer follows the concept of packet switching as packet is the basic data unit used at this layer. There are two types of packet switching techniques, virtual circuit and datagram approach. In virtual circuit approach, before sending any data between a source destination pair, end to end logical connection needs to be established between them. Datagram approach is a connection less service. There is no handshaking between source and destination and each packet follows its own route.

Each machine is identified by a logical address, known as IP address. It is a 32 bit address which is unique for an individual. Due to overload of the network, network layer faces a problem which is known as congestion. Open loop congestion control policies for avoiding the congestion and Closed loop congestion control policies for congestion removal phase has been studied. A very important job of network layer is route the packets, thus concepts of routing has been discussed. It is followed by the computation of delay metric which is a very important in network layer as packet travels through a number of paths and routers.

## 1.9 SOLUTIONS

**Check your progress 1**

1) b

2) c

3) a

4) Virtual circuit approach decides the output port on the basis of VC_ID of a packet whereas datagram approach decides the output port on the basis of destination address mentioned in the packet. If a router gets failed, only the

packets waiting in the queue of that router gets lost in datagram approach. However, in virtual circuit approach, all the connection passing through that router or whose state information is maintained in this router gets lost.

## Check your progress 2

1) c

2) b

3) a

4) A host gets an IP address either manually which is assigned by a network administrator or dynamically assigned by the DHCP protocol. Manual assignment is also known as static assignment as the allocated address can't be changed until the administrator himself wants to change the same. In manual assignment, network administrator allocates an IP address to the host from the available block of addresses.
During dynamic assignment, Dynamic Host Configuration Protocol assigns the IP address to the machine as soon as the host joins the network and frees the address when the host machine leaves the network. Therefore, whenever host joins the network, it will get a new IP address.

## Check your progress 3

1) Routing

2) b

3) Network Layer faces this problem of congestion when the number of packets sent to the network is greater than the capacity of the network. Network is not able to handle the packets as packets are coming at a faster rate. Then, packet loss starts and sometimes it leads to a deadlock situation and the whole system gets collapsed.

4) There are policies used to avoid the congestion known as open loop congestion control policies. But if congestion occurred, then some of the policies are used to remove the congestion.

The following **open loop congestion control policies** can be used to avoid congestion. Receiver's acknowledgement policy can control the congestion at some level. For example, if receiver sends the acknowledgement packet after receiving some packets, it will slow the sender as well as not add a burden of sending acknowledgement packets. Another policy implemented by router that the router can visualize the possibility of congestion and if there are chances of congestion then the new virtual connection request can be rejected. Sender can implement the retransmission policy to avoid the problem of congestion. For how long the sender has to wait or after how many lost packets, the packet needs to

be retransmitted, all these kinds of retransmission policies should be designed in such a way that it will not add more congestion in the network. Sometimes, even after taking all the preventive measures, congestion occurred. In this situation, **closed loop congestion control policies** to be used to avoid stucking into deadlock.

These policies are mainly about informing all about the situation of congestion. One of the policy is sending a choke packet. A choke packet is a control packet sent by the router to the source node. This packet informs the sender about congestion occurrence. Another is signaling in which a signal would be sent by the congested node to inform the sender about congestion. Rather than sending an explicit packet like choke packet, here, a signal will be sent in the existing packets carrying data.

### Check your progress 4

1) b

2) Propagation delay =20μs
   Transmission delay $=\frac{L}{R}=\frac{10,000}{10*10^6}=1000\mu s$

   a) Total time (as a single packet) =20+1000+35+20+1000=2075μs
   b) Transmission delay $=\frac{L}{R}=\frac{5,000}{10*10^6}=500\mu s$
   Total time for first packet = 20+500+35+20+500=1075μs
   Total time for second packet = 500μs

   Thus, total delay = 1075+500 = 1575μs

## 1.10 FURTHER READINGS

[1] Kurose, J. F., & Ross, K. W. (2012). "Computer networking: A top-down approach featuring the Internet", Boston: Addison-Wesley.

[2] Forouzan, B.A., & Mosharraf, F. (2012), "Computer Networks: A top-down approach", McGraw Hill.