UNIT 1 INTRODUCTION TO LAYER FUNCTIONALITY AND DESIGN ISSUES

Structure Nos. **Page**

1.0 INTRODUCTION

In the previous blocks of this course, we have learned the basic functions of physical layer and data link layer in networking. Now, in this chapter, we will go through the functions of the network layer.

The network layer is at level three in OSI model. It responds to service requests from the transport layer and issues service requests to the data link layer. It is responsible for end-to-end (source to destination) packet delivery, whereas the data link layer is responsible for node-to-node (hop-to-hop) packet delivery. Three important functions of the network layers are:

- **Path Determination:** It determines the route taken by the packets from the source to the destination.
- **Forwarding:** It forwards packets from the router's input to the appropriate router output.
- **Call Setup:** Some network architectures require router call setup along the path before the data flows. To perform these functions, the network layer must be aware of the topology of the communication subnet (i.e., set of routers, communication lines).

For end-to-end delivery, the network provides two type of services i.e., **connection oriented service** and **connection less service** to the transport layer. The network layer services meet the following entries [*ref.1]*.

- Transport layer should not be aware of the topology of the network (subnet).
- Services should be independent of the router technology.

In this unit, we will first go through the basic concepts of these services and will then differentiate between these two. Then, we will introduce some other concepts like routing and congestion.

1.1 OBJECTIVES

After going through this unit, you should be able to:

- define basic functions of the network layer;
- differentiate between connection oriented and connection less services;
- define the concept of addressing in networking;
- define congestion in the network layer;
- explain the concept of routing;
- explain the concept of pocket switching, and
- define packet switching network.

1.2 CONNECTION ORIENTED Vs. CONNECTION- LESS SERVICES

In computer networks, delivery between source and destination can be accomplished in either of the two ways:

- Connection-oriented services
- Connection-less services.

1.2.1 Connection-oriented Services

Connection-oriented services define a way of transmitting data between a sender and a receiver, in which an end-to-end connection is established before sending any data. After establishing a connection, a sequence of packets, (from the source to destination), can be sent one after another. All the packets belonging to a message are sent from the same connection. When all packets of a message have been delivered, the connection is terminated.

In connection-oriented services, the devices at both the endpoints use a protocol to establish an end-to-end connection before sending any data.

Connection-oriented service usually has the following **characteristics**:

i) The network guarantees that all packets will be delivered in order without loss or duplication of data.

ii) Only a single path is established for the call, and all the data follows that path.

iii) The network guarantees a minimal amount of bandwidth and this bandwidth is reserved for the duration of the call.

iv) If the network is over utilised, future call requests are refused.

Connection-oriented service is sometimes called a "**reliable"** network service because:

- It guarantees that data will arrive in the proper sequence.
- Single connection for entire message facilitates acknowledgement process and retransmission of damaged and lost frames.

Connection-oriented transmission has three **stages**. These are:

(i) Connection establishment: In connection oriented services, before transmitting data, the sending device must first determine the availability of the other to exchange data and a connection must be established by which data can be sent. Connection establishment requires three steps. These are:

a) First the sender computer requests the connection by sending a connection request packet to the intended receiver.
(b) Then the receiver computer returns a confirmation packet to the requesting computer.
(c) Finally, the sender computer returns a packet acknowledging the confirmation.

(ii) Data transfer: After the connection gets established, the sender starts sending data packets to the receiver.

(iii) Connection termination: After all the data gets transferred, the connection has to be terminated. Connection termination also requires a three-way handshake i.e.,

(a) First, the sender computer requests disconnection by sending a disconnection request packet.
(b) Then, the receiver computer confirms the disconnection request.
(c) Finally, the sender computer returns a packet acknowledging the confirmation.

Transmission Control Protocol (TCP) is a connection-oriented protocol.

1.2.2 Connection-less Services

Connection-less services define a way of communication between two network end points in which, a message can be sent from one end point to another without prior arrangement. The sender simply starts sending packets, addressed to the intended recipient.

Connectionless service is a service that allows the transfer of information among subscribers without the need for end-to-end connection establishment procedures.

Connection-less service is sometimes known as "**unreliable"** network service. Connection-less protocols are usually described as stateless because the endpoints have no protocol-defined way of remembering where they are in a "conversation" of message exchange.

The **Internet Protocol (IP)** and **User Datagram Protocol (UDP)** are connectionless protocols, but TCP/IP (the most common use of IP) is connection-orientated.

1.3 IMPLEMENTATION OF THE NETWORK LAYER SERVICES

In this section, we will examine how the network layer services are implemented. Two different services are taken into consideration depending on the type of service being offered. These two schemes are known as virtual circuit subnet (VC subnet) for connection-oriented service and datagram subnet for **connection-less** services. A VC subnet may be compared to the physical circuit required in a telephone setup. In a connection-oriented service, a route from the source to the destination must be established. In a datagram subnet, no advance set up is needed. In this case, packets are routed independently. But, before we take up the implementation issues let us,

revisit the packet switching concepts once again. The services are implement through a packet switched network.

1.3.1 Packet Switching

In the fourth unit of Block 1, we introduced the concept of packet switching. We further elaborate in this section, in the context of the network layer. The network layer operates in the packet switched network (or subnet) environment which comprises several routers linked with transmission lines (leased or dial up) besides user's machines as shown in *Figure 1*.

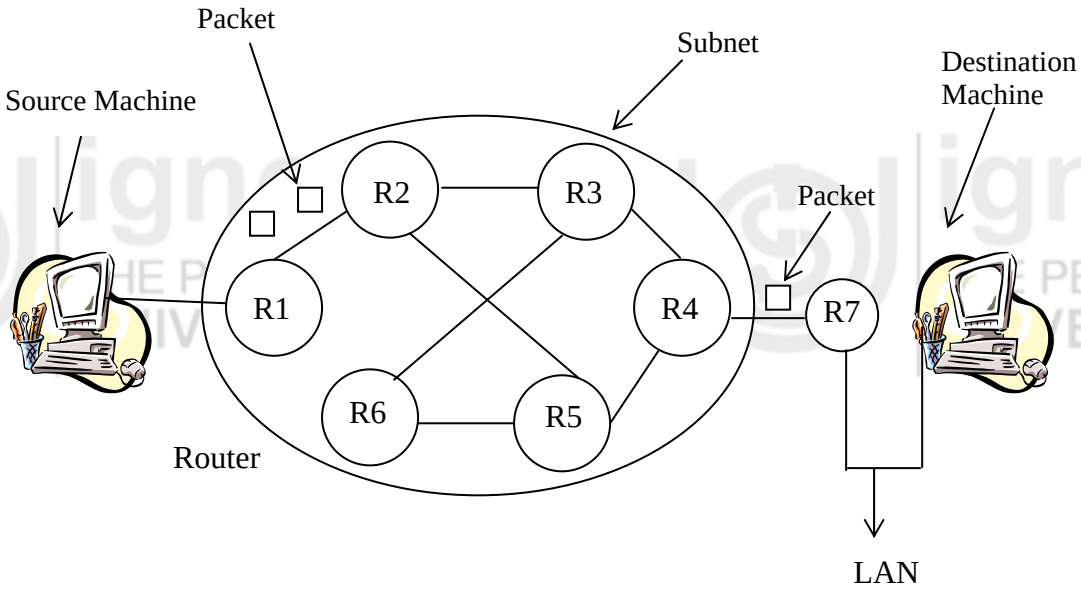


Figure 1: A Packet switched network

This subnet works in the following manner. Whenever user wants to send a packet to another users, s/he transmits the packet to the nearest router either on its own LAN or over a point-to-point link to the carrier. The packet is stored for verification and then transmitted further to the next router along the way until it reaches the final destination machine. This mechanism is called packet switching.

But, why packet switching? Why not circuit switching? Now, let us discuss these issues.

Circuit switching was not designed for packet transmission. It was primarily designed for voice communication. It creates temporary (dialed) or permanent (leased) dedicated links that are well suited to this type of communication *[Ref. 2]*.

(i) Data transmission tend to be bursty, which means that packets arrive in spurts with gaps in between. In such cases, transmission lines will be mostly idle leading to wastage of resources if we use circuit switching for data transmission.

(ii) **Single Data Rate:** In circuit switching mechanism there is a single data rate for the two end devices which limits flexibility and usefulness of circuit switched connection for networks interconnection of a variety of digital devices.

(iii) **No priority to transmission:** Circuit switching treats all transmissions as equal. But often, with data transmission we may be required to send a certain packet on a high priority basis, which may not be implemented with the circuit switching approach.

1.3.2 Implementation of Connection-oriented Services

To implement connection-oriented services, we need to form a **virtual-circuit** subnet. This idea behind the creation of a VC is so that, a new route for every packet sent.
In virtual circuits:

- First, a connection needs to be established.
- After establishing a connection, a route from the source machine to the destination machine is chosen as part of the connection setup and stored in tables inside the routers. This route is used for all traffic flowing over the connection.
- After transmitting all the data packets, the connection is released. When the connection is released, the virtual circuit is also terminated.

In a connection-oriented service, each packet carries an identifier that identifies the virtual circuit it belongs to.

Now, let us take an example, consider the situation of a subnet in *Figure 2*. In this figure, H1,H2 and H3 represent host machines and R1, R2, R3, R4, R5 and R6 represent routers. Processes are running on different hosts.

Here, host HI has established connection 1 with host H2. It is remembered as the first entry in each of the routing tables as shown in *Table 1*. The first line of R1's table says that, if a packet bearing connection identifier 1 comes in from HI, it is to be sent to router R3, and given connection identifier 1. Similarly, the first entry at R3 routes the packet to R5, also with connection identifier 1.

Now, let us consider a situation in which, H3 also wants to establish a connection with H2. It chooses connection identifier 1 (because it is initiating the connection and this is its only connection) and informs the subnet to setup the virtual circuit. This leads to the second row in the table. Note, that we have a conflict here because although R1 can easily distinguish connection 1 packets from HI and connection 1 packets from H3, R3 cannot do this. For this reason, R1 assigns a different connection identifier to the outgoing traffic for the second connection (No.2). In order to avoiding conflicts of this nature, it is important that routers have the ability to replace connection identifiers in outgoing packets. In some contexts, this is called **label switching**.

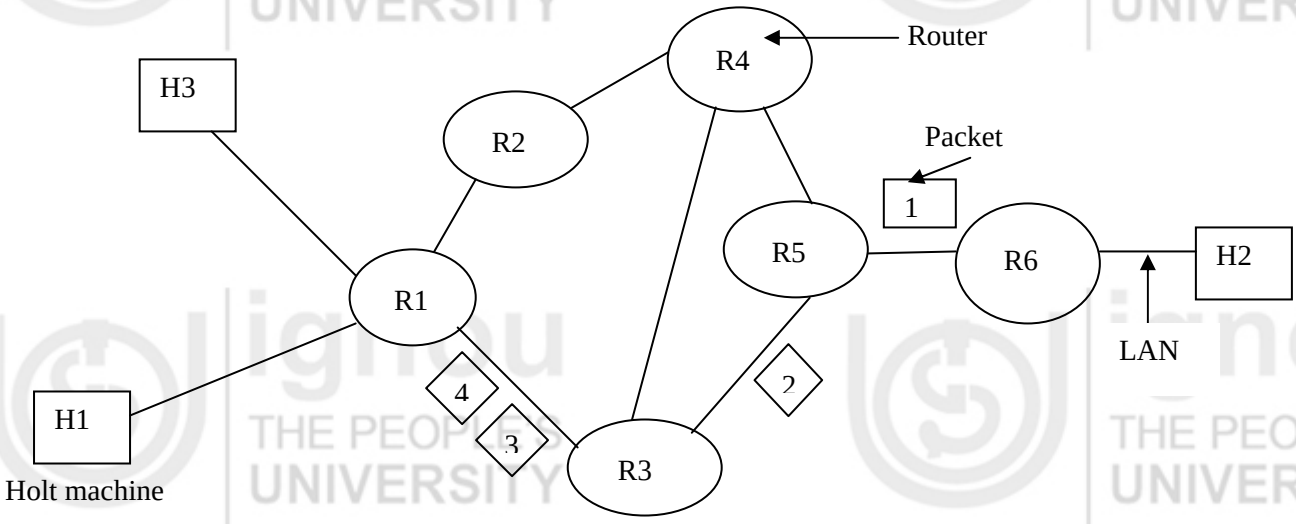


Figure 2: Routing in a virtual circuit subnet

Table 1: Routing table for VC subnet

R1's Table

in		out	
H1	1	R3	1
H3	1	R3	2

R3's Table

R1	1
R1	1

in

R5	1
R5	2

out

R5's Table

R3	1
R3	1

in

R6	1
R6	1

out

1.3.3 Implementation of Connection-less Services

In this section, we shall discuss the implementation of these services i.e., how connection-less services are implemented in real networks. To implement connection-less services, we need a datagram subnet.

In these services, packets are individually injected into the subnet and their routing decisions are not dependent on each other (packets). Therefore, in connectionless services, no advance setup is needed. In this context, the packets are frequently called **datagrams** and the subnet is called a **datagram subnet**.

Now, let us take an example to learn how a datagram subnet works. Consider the situation of *Figure 3*. In this *Figure*, H1 and H2 represent host machines and R1, R2, R3, R4, R5 and R6 represent routers. Suppose, that the process running at host H1 has a long message to be transmited to a process running at H2 machine. To do so, it transfers the message to the transport layer with appropriate instructions to deliver it to the process running at H2. Where is the transfer layer process running, can you figure out? Well, it may also be running on H1 but within the operating system. The transport layer process adds a transport header to the front of the message and transfers the message (also called TPDU) to the network layer, The network layer too, might be running as another procedure within the operating system.

Let us assume, that the message is five times longer than the maximum packet size, therefore, the network layer has to break it into five packets, 1,2, 3, 4 and 5 and send each of them in turn to router R1 (because it is linked to R1) using some point-to-point protocol. After this, the carrier (supported by ISP) takes over. Every router has an internal table telling it where to send packets for each possible destination. Each table entry is a pair consisting of a destination and the outgoing line to use for that destination. Only directly-connected lines can be used. For example, in *Figure 3*, R1 has only two outgoing lines-to R2 and R3. So every incoming packet must be sent to one of these routers.

As the packets arrive at R1 from H1, packets 1, 2, and 3 were stored briefly (to verify their checksums). Then, each packet was forwarded to R3 according to R1's table (table not shown here). Packet 1 was then forwarded to R5 and from R5 to R6. When it got to R6, it was encapsulated in a data link layer frame and sent to H2. Packets 2 and 3 follow the same route.

However, something different happened to packet 4 and 5. When it got to R1 it was sent to router R2, even though it has the same destination. Due to some reason (for ex. congestion), R1 decided to send packet 4 and 5 via a different route than that of the first three.

The algorithm that manages the tables and makes the routing decisions is known as the **routing algorithm**. In next unit, we shall study routing algorithms. Students are

requested to refer to [Ref. 1] for further study on the implementation of connection oriented and connection less services. You should focus on connecting routing tables.

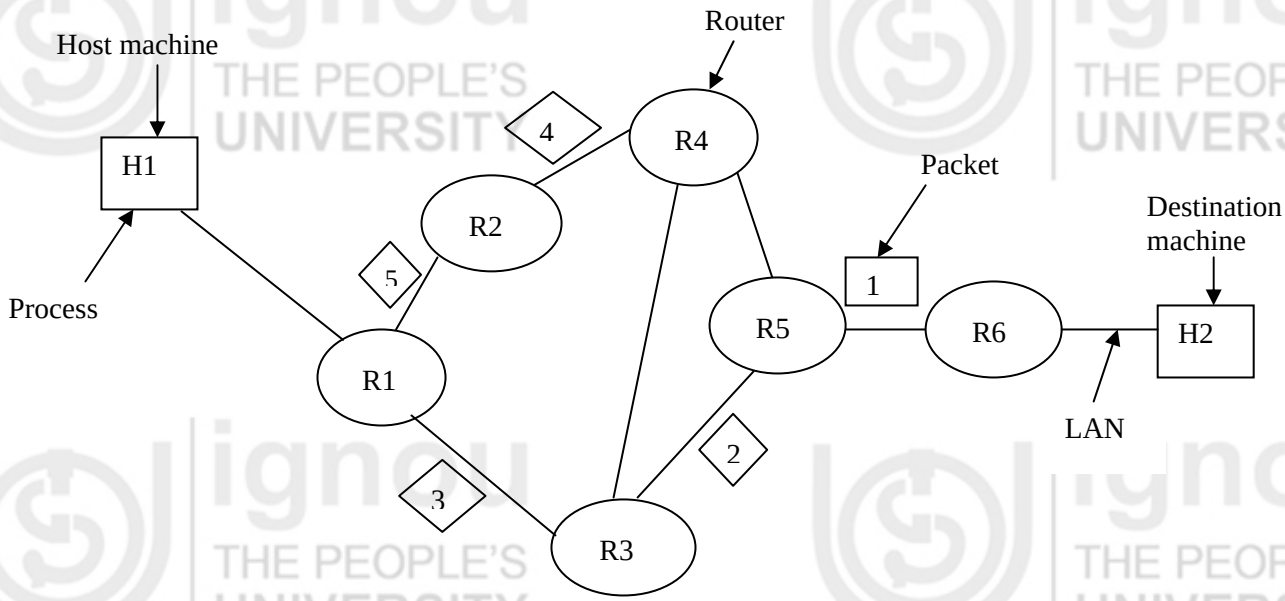


Figure 3: Routing in a datagram subnet

1.4 COMPARISON BETWEEN VIRTUAL CIRCUIT AND DATAGRAM SUBNET

Both virtual circuits and datagrams have their pros and cons. We shall compare them on the basis of different parameters. These various parameters are:

- **Router memory space and bandwidth**

Virtual circuits allow packets to contain circuit numbers instead of full destination addresses. A full destination address in every packet may represent a significant amount of overhead, and hence waste bandwidth.

- **Setup time vs. address parsing time**

Using virtual circuits requires a setup phase, which takes time and consumes memory resources. However, figuring out what to do with a data packet in a virtual-circuit subnet is easy: the router simply uses the circuit number to index into a table to find out where the packet goes. In a datagram subnet, a more complicated lookup procedure is required to locate the entry for the destination.

- **Amount of table space required in router memory**

A datagram subnet needs to have an entry for every possible destination, whereas a virtual-Circuit subnet just needs an entry for each virtual circuit.

- **Quality of service**

Virtual circuits have some advantages in guaranteeing quality of service and avoiding congestion within the subnet because resources (e.g., buffers, bandwidth, and CPU cycles) can be reserved in advance, when the connection is established. Once the packets start arriving, the necessary bandwidth and router capacity will be there. With a datagram subnet, congestion avoidance is more difficult.

- **Vulnerability**

Virtual circuits also have a vulnerability problem. If, a router crashes and loses its memory, even if it comes back a second later, all the virtual circuits passing through it will have to be aborted. In contrast, if a datagram router goes down, only those users whose packets were queued in the router at the time will suffer, and maybe not even all those, depending upon whether they have already been acknowledged. The loss of a communication line is fatal to virtual circuits using it but can be easily compensated for if datagrams are used.

- **Traffic balance**

Datagrams also allow the routers to balance the traffic throughout the subnet, since routes can be changed partway through a long sequence of packet transmissions. A brief comparison between a virtual circuit subnet and a datagram subnet is given in *Table 2.* Students should refer to Reference 1 for further discussion.

Table 2: Comparison between Virtual Circuit and Datagram Subnets *(Source: Ref. [1])*

Issue	Datagram subnet	Virtual-circuit subnet
Addressing machine	Each datagram contains the full source and destination address	Each datagram contains a Small VC number
Referencing of Circuit setup	Not needed	Required
State information by a router	Routers do not hold state information about connections.	Each VC requires router table space per connection.
Routing procedure	Each datagram is routed independently.	Route is selected when VC is set up and all the packets follow all routes.
Effect of router failures	None, except the datagram lost during the crash	All VCs that passed through the failed router are terminated and the new virtual circuit is established
Quality of service	Difficult	Easy
Congestion control mechanism	Difficult	Easy

☞ Check Your Progress 1

Give right choice for the following:

1) Connection-oriented service is sometimes called a ……network service.
   (a) Reliable
   (b) Unreliable.

2) ……is a connection-oriented protocol.
   (a) UDP
   (b) TCP
   (c) IP

3) Why are connection oriented services known as reliable services? Explain brifly.

……

……

……

……

1.5 ADDRESSING

Network addresses identify devices separately or as members of a group. Addressing is performed on various layers of the OSI model. Thus, schemes used for addressing vary on the basis of the protocol used and the OSI layer. On this basis, internetwork addresses can be categorised into three types. These are:

(a) Data link layer addresses

(b) Media Access Control (MAC) addresses

(c) Network layer addresses.

a) Data Link Layer Addresses

Data-link layer addresses sometimes are referred to as *physical* or *hardware addresses*, uniquely identify each physical network connection of a network device. Usually data-link addresses have a pre-established and fixed relationship to a specific device.

End systems generally have only one physical network connection and thus, have only one data-link address. Routers and other internetworking devices typically have multiple physical network connections and therefore, have multiple data-link addresses.

b) Media Access Control (MAC) Addresses

Media Access Control (MAC) addresses are used to identify network entities in LANs that implement the IEEE MAC addresses of the data link layer. These addresses are 48 bits in length and are expressed as 12 hexadecimal digits.

MAC addresses are unique for each LAN interface. These addresses consist of a subset of data link layer addresses. *Figure 4* illustrates the relationship between MAC addresses, data-link addresses, and the IEEE sub-layers of the data link layer.

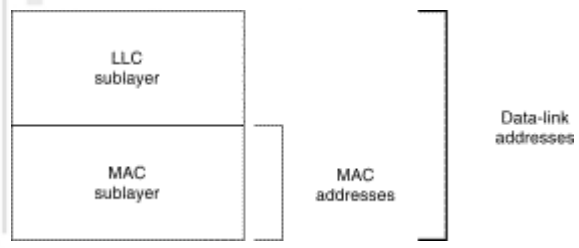


Figure 4: MAC addresses, data-link addresses, and the IEEE Sub-layers of the data link layer are all related

c) Network Layer Addresses

Network addresses are sometimes called virtual or logical addresses. These addresses are used to identify an entity at the network layer of the OSI model. Network addresses are usually hierarchical addresses.

1.5.1 Hierarchical vs. Flat Address

Usually Internetwork addresses are of two types:

(i) **Hierarchical address**

Hierarchical addresses are organised into a number of subgroups, each successively narrowing an address until it points to a single device as a house address.

(ii) **Flat address**

A flat address space is organised into a single group, such as, your enrolment no. Hierarchical addressing offers certain advantages over flat-addressing schemes. In hierarchical addressing, address sorting and recalling is simplified using the comparison operation. For example, “India” in a street address eliminates any other country as a possible location. *Figure 5* illustrates the difference between hierarchical and flat address spaces.

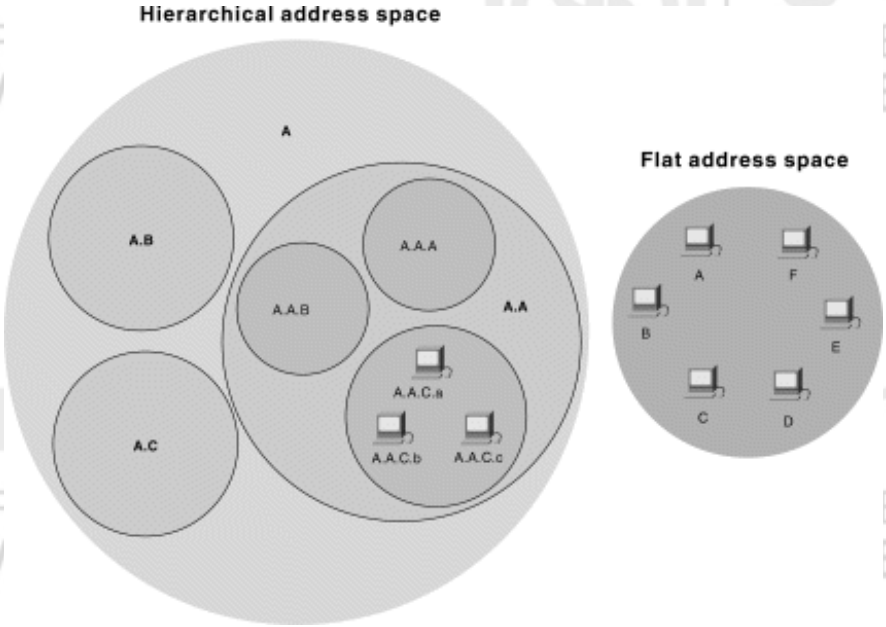


Figure 5: Hierarchical and flat address spaces differ in comparison operations

1.5.2 Static vs. Dynamic Address

In networking, the address to a device can be assigned in either of these two ways:

(i) **Static address assignment:** Static addresses are assigned by a network administrator according to a preconceived internetwork addressing plan. A static address does not change until the network administrator changes it manually.

(ii) **Dynamic addresses:** Dynamic addresses are obtained by devices when they are attached to a network, by means of some protocol-specific process. A device using dynamic address often has a different address each time it connects to the network.

1.5.3 IP Address

IP address is a unique address i.e., no two machines on the Internet can have same IP address. It encodes it’s network number and host number. Every host and router, in a internetwork has an IP address.

The format of an IP address is a 32-bit numeric address written as four numbers separated by periods. Each number can be zero to 255. For example, 1.160.10.240 could be an IP address. These numbers defines three fields:

(i) **Class type:** Indicate the IP class, to which the packet belongs:

(ii) **Network identifier (netid):** Indicates the network (a group of computers). Networks with different identifiers can be interconnected with routers.

(iii) **Host identifier (hostid):** Indicates a specific computer on the network.

Class type	Netid	Hostid

Figure 6: IP address

You will read more details on IP address in unit 4.

☞ Check Your Progress 2

1) What are three types of internetwork addresses? Explain in brief.

……

……

……

……

2) Differrentiate between following:

(i) Hierarchical address and Flat address

(ii) Static and Dynamic address.

……

……

……

……

1.6 CONCEPT OF CONGESTION

In the network layer, when the number of packets sent to the network is greater than the number of packets the network can handle (capacity of network), a problem occurs that is known as congestion. This is just like congestion on a road due to heavy traffic. In networking, congestion occurs on shared networks when, multiple users contend for access to the same resources (bandwidth, buffers, and queues).

When the number of packet sent into the network is within the limits, almost all packets are delivered, however, the traffic load increases beyond the network capacity. As a result the system starts discarding packets.

Figure 7 shows congestion in a network due to too much traffic**.**

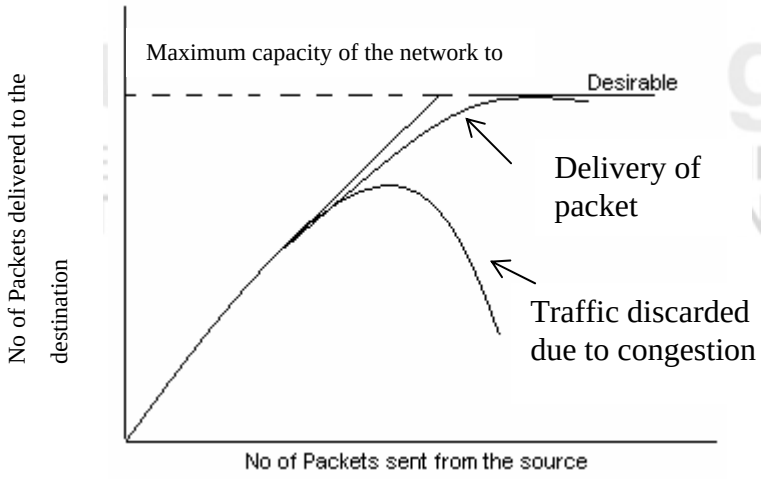


Figure 7: Congestion

Because routers receive packets faster than they can forward them, one of these two things may happen in case of congestion:

- The subnet may prevent additional packets from entering the congested region until those already present can be processed, or
- The congested routers can discard queued packets to make room for those that are arriving currently.

Congestion Control

Congestion control refers to the network mechanism and techniques used to control congestion and keep the load below the networks capacity.

Congestion handling can be divided into the following:

- **Congestion recovery:** Restore the operating state of the network when demand exceeds capacity.
- **Congestion avoidance:** Anticipate congestion and avoid it so that congestion never occurs.

By storing content closer to users i.e., caching can be the best congestion control scheme. In this manner, majority of the traffic could be obtained locally rather than being obtained from distant servers along routed paths that may experience congestion.
Some basic techniques to manage congestion are:

1) **End-system flow control:** This is not a congestion control scheme. It is a way of preventing the sender from overrunning the buffers of the receiver.

2) **Network congestion control:** In this scheme, end systems throttle back in order to avoid congesting the network. The mechanism is similar to end-to-end flow controls, but the intention is to reduce congestion in the network, not at the receiver's end.

3) **Network-based congestion avoidance:** In this scheme, a router detects that congestion may occur and attempts to slow down senders before queues become full.

4) **Resource allocation:** This technique involves scheduling the use of physical circuits or other resources, perhaps for a specific period of time. A virtual circuit, built across a series of switches with a guaranteed bandwidth is a form

of resource allocation. This technique is difficult, but can eliminate network congestion by blocking traffic that is in excess of the network capacity.

1.7 ROUTING CONCEPT

Suppose, you need to go from location (A) to another location (B) in your city and more than one routes are available for going from location A to location B. In this case, first you decide the best route for going from location A to B. This decision may be based on a number of factors such as distance (route with minimum traffic distance), time (route with minimum traffic jam), cost etc. After deciding the best route you start moving on that route. The same principle is at work here, in computer networks also. While transferring data packets in a packet switched network the same principle is applied, and this is known as routing. Now, we can say that *routing is the act of moving data packets in packet-switched network, from a source to a destination*. Along the way, several intermediate nodes typically are encountered.

Routing occurs at Layer 3 (the network layer) in OSI reference model. It involves two basic activities:

- Determining optimal routing paths.
- Forwarding packets through a subnet. In this section, we will look at several issues related to routing.

1.7.1 Main Issues in Routing

Routing in a network typically involves a rather complex collection of algorithms that work more or less independently mainly due to the environment in which it works and yet support each other by exchanging services or information. The complex is due to a number of reasons. First, routing requires coordination between all the nodes of the subnet rather than just a pair of modules as, for example, in data link and transport layer protocols. Second, the routing system must cope with transmission link and router failures, requiring redirection of traffic resetting up of new VC and an update of the routing tables databases maintained by the system. Third, to achieve high performance, the routing algorithm may need to modify its routes when some areas within the network become congested.

There are two main performance measures that are substantially affected by the routing algorithm – throughput (quantity of service) and latency (average packet delay when quality of service is required). The parameter **throughput** refers to the number of packets delivered in the subnet. Routing interacts with **flow control** in determining these performance measures by means of a feedback mechanism shows in *Figure 8* When the traffic load offered by the external resources to the subnet is within the limits of the carrying capacity of the subnet, it will be fully accepted into the network, that is,

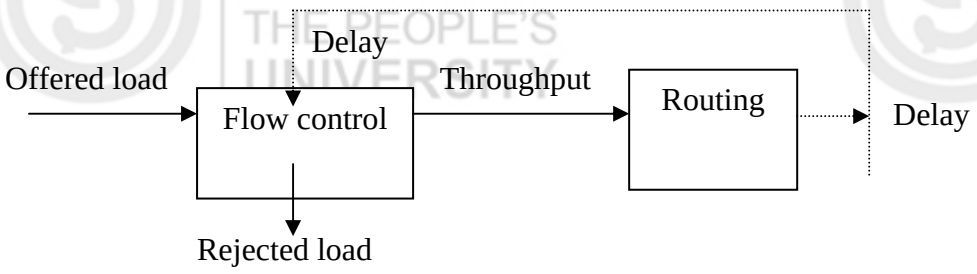


Figure 8: Interaction of routing and flow control

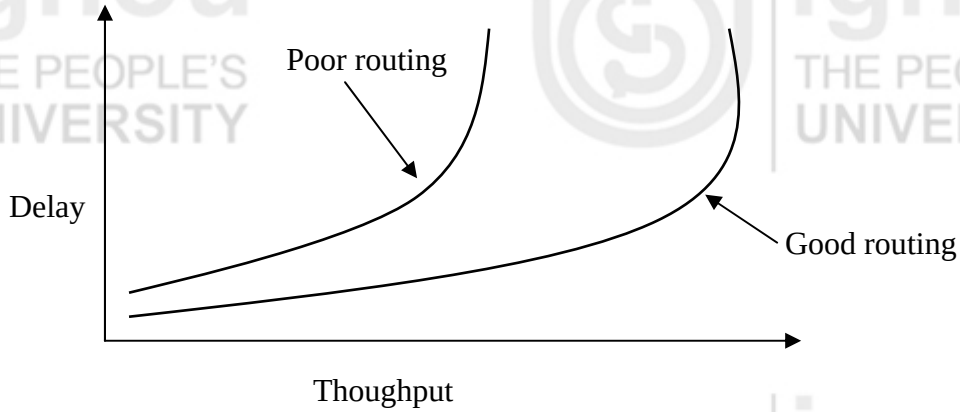
Network throughput = offered packets

But, when the offered load exceeds the limit, the packet will be rejected by the flow control algorithm and

Network Throughput = offered packets – rejected packets

The traffic accepted into the network will experience an average delay per packet that will depend on the routes chosen by the routing algorithm.

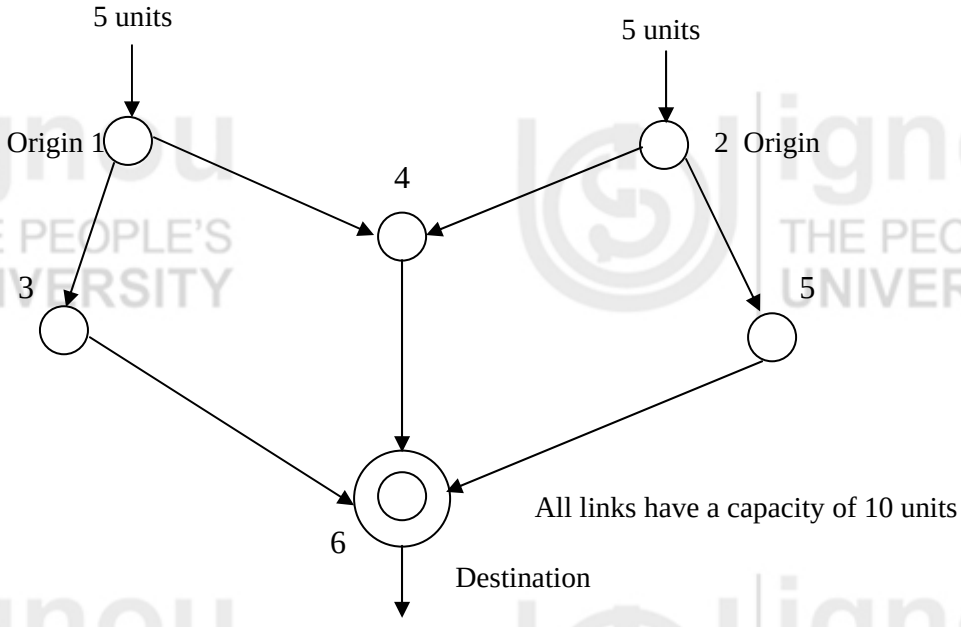
However, throughput will also be greatly affected (if only indirectly) by the routing algorithm because typical flow control schemes operate on the basis of striking a balance between throughput and delay. Therefore, as the routing algorithm is more successful in keeping delay low, the flow control algorithm allows more traffic into the network, while the precise balance between delay and throughput will be determined by flow control, the effect of good routing under high offered load conditions is to realise a more favourable delay-throughput curve along which flow control operates, as shown in *Figure 9.*



(Source: Ref.[2])

Figure 9: Throughput vs. delay graph

Let us take an example to understand the intencacy. In the network of *Figure 10*, all links have a capacity of 10 units. There is a single destination (R6) and two origins (R1 and R2). The offered pockets from each of R1 and R2 to R5 and R6 is 5 units. Here, the offered load is light and can easily be accommodated with a short delay by routing along the leftmost and rightmost paths, 1-3-6 and 2-5-6, respectively. If instead, however, the routes 1-4-6 and 2-4-6 are used, the flow on link (4,6) with equal capacity, resulting in very large delays.



(Source ref. [2])

Figure 10: Example a sub network

Observe *Figure 10* once again. All links have a capacity of 10 units. If, all traffic is routed through the middle link (R4,R6), congestion occurs. If, instead, paths (R1-R3-R6) and (R2-R5-R6) are used , the average delay is shorter/lesses.

In conclusion, the effect of good routing is to increase throughput for the same value of average delay per packet under high offered load conditions and decrease average delay per packet under low and moderate offered load conditions. Furthermore, it is evident as low as possible for any given level of offered load. While this is easier said than done, analytically. Students are requested to refer to *(Ref. 2)* for further discussion. You are requested to further enhance your knowledge by reading *[Ref. 2]*.

1.7.2 Classification of Routing Algorithm

Routing can be classified into the following types:

(i) Adaptive Routing

In adaptive routing; routing decisions are taken for each packet separately i.e., for the packets belonging to the same destination, the router may select a new route for each packet. In it, routing decisions are based on condition or the topology of the network.

(ii) Non-adaptive Routing

In non-adaptive routing; routing decisions are not taken again and again i.e., once the router decides a route for the destination, it sends all packets for that destination on that same route. In it routing decisions are not based on condition or the topology of the network.

☞ Check Your Progress 3

1) What is congestion in the network? Explain in brief.

……

……

……

……

2) Explain various congestion control schemes.

……

……

……

……

3) What is routing? What are various activities performed by a router?

……

……

……

……

4) Differentiate between adaptive and non-adaptive routing.

……

……

……

……

1.8 SUMMARY

In this unit, we looked at the two types of end-to-end delivery services in computer networks i.e., connection oriented service and connection less service. Connection-oriented service is a reliable network service, while connection-less service is unreliable network service. Then we studied the concept of addressing. A network addresses identifies devices separately or as members of a group. Internetwork addresses can be categorised into three types i.e., data link layer addresses, media access control (MAC) addresses and network layer addresses. After this, we studied a problem that occurs at the network layer level i.e., congestion. It is a problem that occurs due to overload on the network. Then, we discussed routing. It is the act of moving data packets in packet-switched network, from a source to a destination. We also examined the relationship between routing and flow control through an example and digrams.

1.9 SOLUTIONS/ANSWERS

Check Your Progress 1

1) a

2) b

3) Connection-oriented service is sometimes called a "reliable" network service because:
   - It guarantees that data will arrive in the proper sequence.
   - Single connection for entire message facilitates acknowledgement process and retransmission of damaged and lost frames.

Check Your Progress 2

1) Three types of internetwork addresses are:

(i) Data link layer addresses:
Data-link layer addresses sometimes are referred to as *physical* or *hardware addresses*, because they uniquely identifies each physical network connection of a network device.

(ii) Media Access Control (MAC) addresses:
Media Access Control (MAC) addresses are used to identify network entities in LANs that implement the IEEE MAC addresses of the data link layer.

(iii) Network layer addresses:
Network addresses are sometimes called virtual or logical addresses. These addresses are used to identify an entity at the network layer of the OSI model.

2) (a) *Hierarchical addresses* are organised into a number of subgroups, each successively narrowing an address until it points to a single device as an house address.

A *flat address* space is organised into a single group, such as, your enrolment no.

(b) *Static addresses* are assigned by a network administrator according to a preconceived internetwork addressing plan. A static address does not change until the network administrator manually changes it.

Dynamic addresses are obtained by devices when they are attached to a network, by means of some protocol-specific process. A device using dynamic address often has a different address each time that it connects to the network.

Check Your Progress 3

1) In the network layer, when the number of packets sent to the network is greater then the number of packets the network can handle (capacity of network), a problem occurs that is known as congestion.

2) Congestion handling can be broadly divided into the following:

Congestion recovery: Restores the operating state of the network when demand exceeds capacity.

Congestion avoidance: Anticipates congestion and avoids it so that congestion never occurs.

Some basic techniques to manage congestion are:

(a) End-system flow control: This is not a congestion control scheme. It is a way of preventing the sender from overrunning the buffers of the receiver.

(b) Network congestion control: In this scheme, end systems throttle back in order to avoid congesting the network. The mechanism is similar to end-to-end flow controls, but the intention is to reduce congestion in the network, not at the receiver's end.

(c) Network-based congestion avoidance: In this scheme, a router detects that congestion may occur and attempts to slow down senders before queues become full.

(d) Resource allocation: This technique involves scheduling the use of physical circuits or other resources, perhaps for a specific period of a time. A virtual circuit, built across a series of switches with a guaranteed bandwidth is a form of resource allocation. This technique is difficult, but can eliminate network congestion by blocking traffic that is in excess of the network capacity.

3) Routing is the act of moving data packets in packet-switched network, from a source to a destination.

A Router is a device used to handle the job of routing. It identifies the addresses on data passing through it, determines which route the transmission should take and collects data in packets which are then sent to their destinations.

4) In *adaptive routing*, routing decisions are taken on each packet separately i.e., for the packets belonging to the same destination, the router may select a new route for each packet.

In *non-adaptive routing*, routing decisions are not taken again and again i.e., once the router decides a route to the destination, it sends all packets for that destination on the same route.

1.10 FURTHER READINGS

1) *Computer Network*, A. S. Tarenbaum, 4th edition, Prentice Hall of India, New Delhi, 2002.

2) *Data Network*, Drnitri Berteskas and Robert Galleger, Second edition, Prentice Hall of India, 1997, New Delhi.