Advanced Computer Networks

Packet switched Networks

- Basic definition in Networks
- Communication network has became essential media for home and business network.
- The design of modern computer and communication networks must meet all the requirements for new communication applications.
- Communication services must available any ware and any time.
- The broadband network is required to support the exchange of multiple types of information such as a voice, and data among multiple types of users.

- Packet switched network are the building blocks of computer communication systems in which data units known as packets flow across networks.
- The goal of packet switched network is to provide flexible communication in handling all kinds of connection for wide rage of applications such as telephone calls, data transfer,teleconferencing,video broadcasting.

- Network Core
- Packet Switching
- In a network application, end systems exchange **messages** with each other.
- Messages can contain anything the application designer wants.
- Messages may perform a control function (for example, the “Hi” messages in our handshaking example in Figure 1.2) or can contain data, such as an email message, a JPEG image, or an MP3 audio file

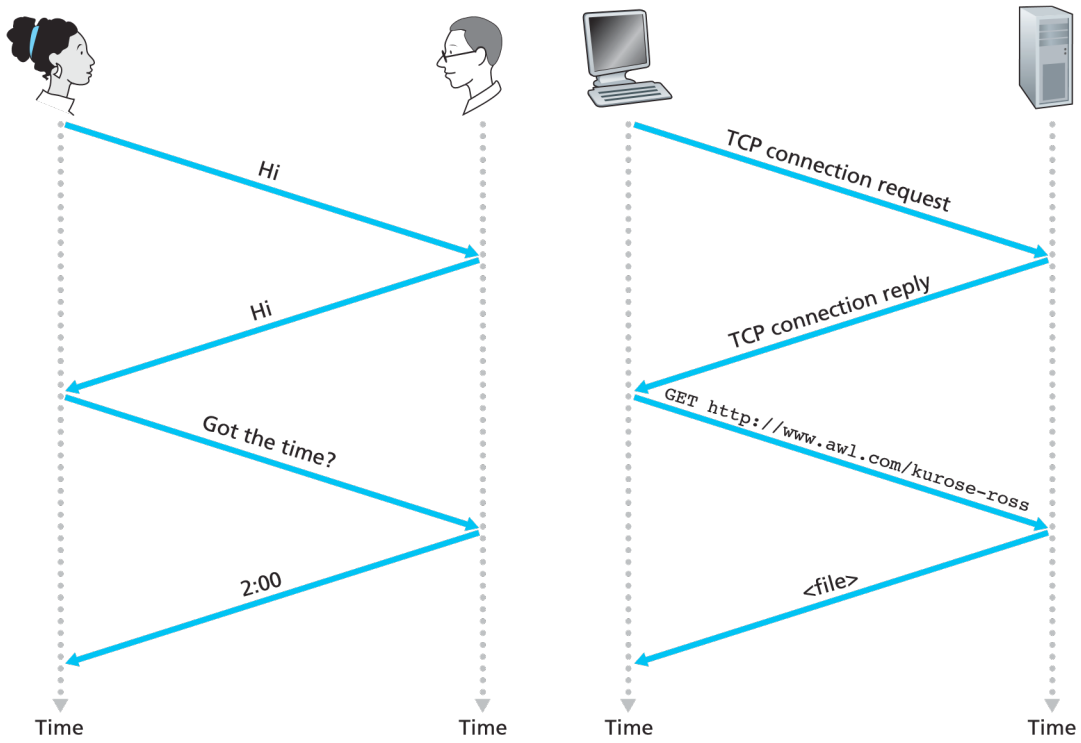


Figure 1.2 A human protocol and a computer network protocol

- To send a message from a source end system to a destination end system, the source breaks long messages into smaller chunks of data known as **packets**.
- Between source and destination, each packet travels through communication links and **packet switches** (for which there are two predominant types, **routers** and **linklayer switches**).
- Packets are transmitted over each communication link at a rate equal to the *full* transmission rate of the link. So, if a source end system or a packet switch is sending a packet of *L* bits over a link with transmission rate *R* bits/sec, then the time to transmit the packet is *L/R* seconds.

- **Store-and-Forward Transmission**
- Most packet switches use **store-and-forward transmission** at the inputs to the links. Store-and-forward transmission means that the packet switch must receive the entire packet before it can begin to transmit the first bit of the packet onto the outbound link
- To explore store-and-forward transmission in more detail, consider a simple network consisting of two end systems connected by a single router, as shown in Figure 1.11

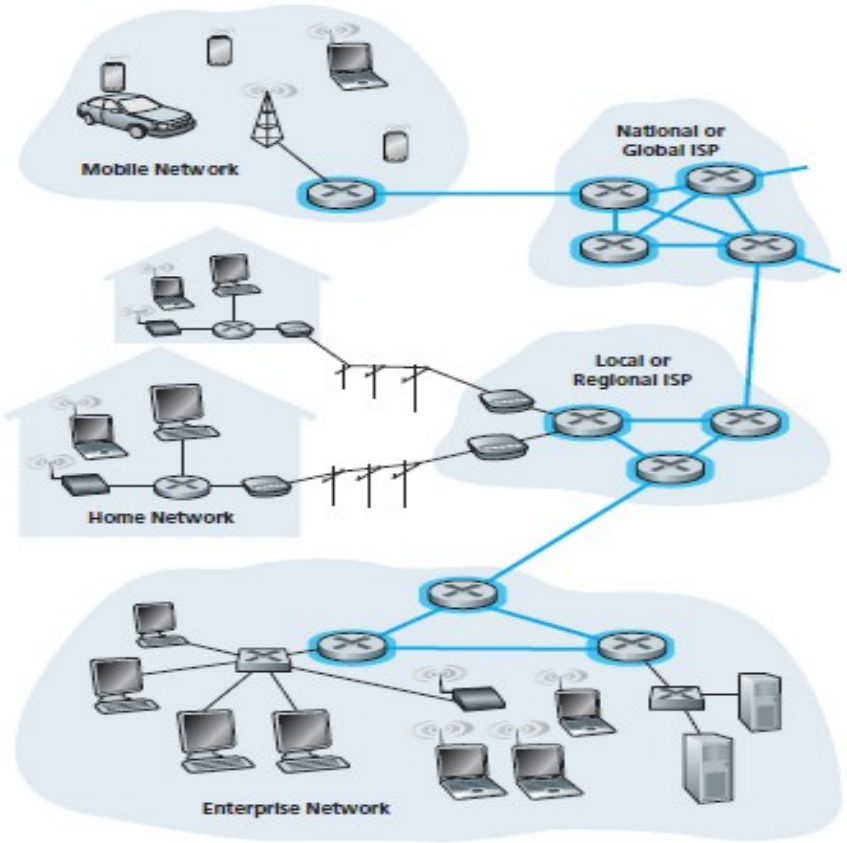


Figure 1.10 ♦ The network core

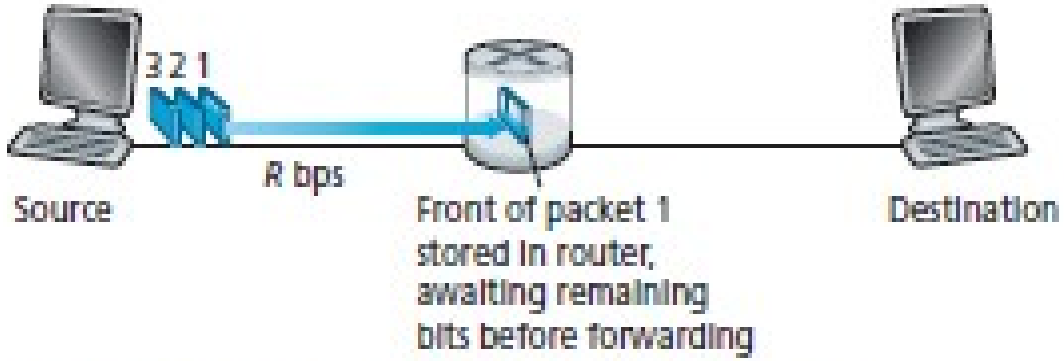


Figure 1.11 ♦ Store-and-forward packet switching

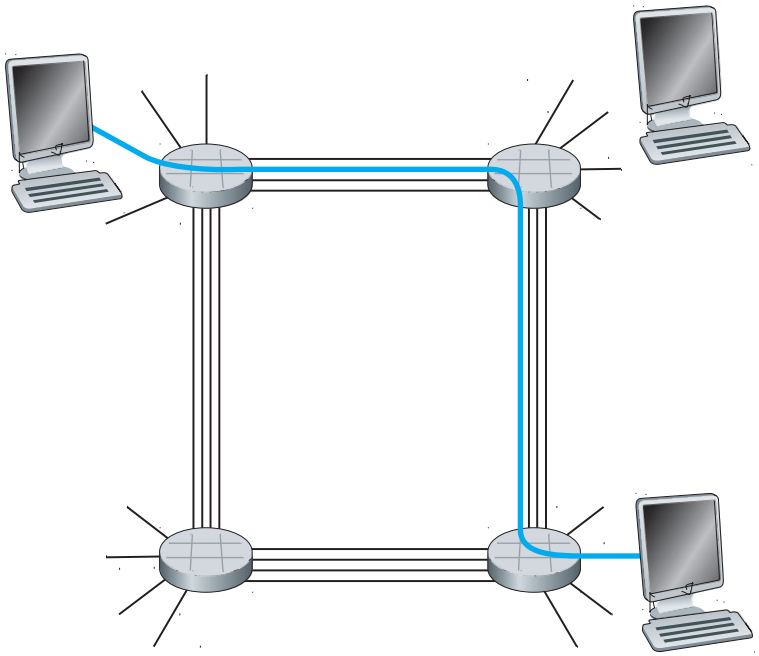
- **2 Circuit Switching**
- There are two fundamental approaches to moving data through a network of links and switches: **circuit switching** and **packet switching**. Having covered packet switched networks in the previous subsection, we now turn our attention to circuits switched networks.
- In circuit-switched networks, the resources needed along a path (buffers, link transmission rate) to provide for communication between the end systems are *reserved* for the duration of the communication session between the end systems

- Traditional telephone networks are examples of circuit-switched networks.
- Consider what happens when one person wants to send information (voice or facsimile) to another over a telephone network.
- Before the sender can send the information, the network must establish a connection between the sender and the receiver.
- This is a *bona fide* connection for which the switches on the path between the sender and receiver maintain connection state for that connection

- In the jargon of telephony, this connection is called a **circuit**.
- When the network establishes the circuit, it also reserves a constant transmission rate in the network's links for the duration of the connection.
- Since a given transmission rate has been reserved for this sender-to-receiver connection, the sender can transfer the data to the receiver at the *guaranteed* constant rate.

- Figure 1.13 illustrates a circuit-switched network. In this network, the four circuit switches are interconnected by four links.
- Each of these links has four circuits, so that each link can support four simultaneous connections.
- The hosts (for example, PCs and workstations) are each directly connected to one of the switches.
- When two hosts want to communicate, the network establishes a dedicated **end-to-end connection** between the two hosts.
- Thus, in order for Host A to communicate with Host B, the network must first reserve one circuit on each of two links.

- **Figure 1.13** A simple circuit-switched network consisting of four switches and four links



- Message, packets and frames
- A packet switched network is organized as a multilevel hierarchy,
- In such networks digital messages are fragmented into one or more smaller units of messages, each appended with a header to specify control information, such as SA and DA.
- This new unit of formatted message is called a packet as shown in fig 1.1.packets are forwarded to a data network to be delivered to their destinations

- In some circumstances ,packets are also required to be attached together or further fragmented ,forming a new packet known as a frame.
- Some times a frames may be required to have multiple headers to carry out multiple tasks in multiple layers of a networks as shown in fig 1.2
- Two packets A and B are being forwarded from one side of a network to other side.
- A single packet can be split into multiple packets before transmission .this technique is called packet fragmentation.
- The primary purpose of network is to direct the flow of data among the users.

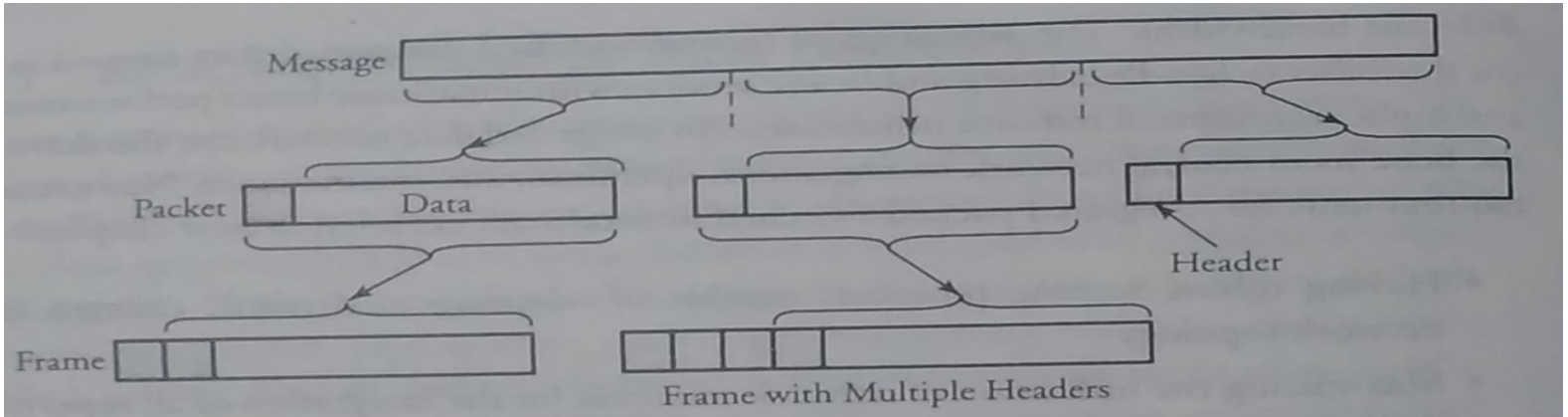


Figure 1.1 Creating packets and frames out of a raw digital message

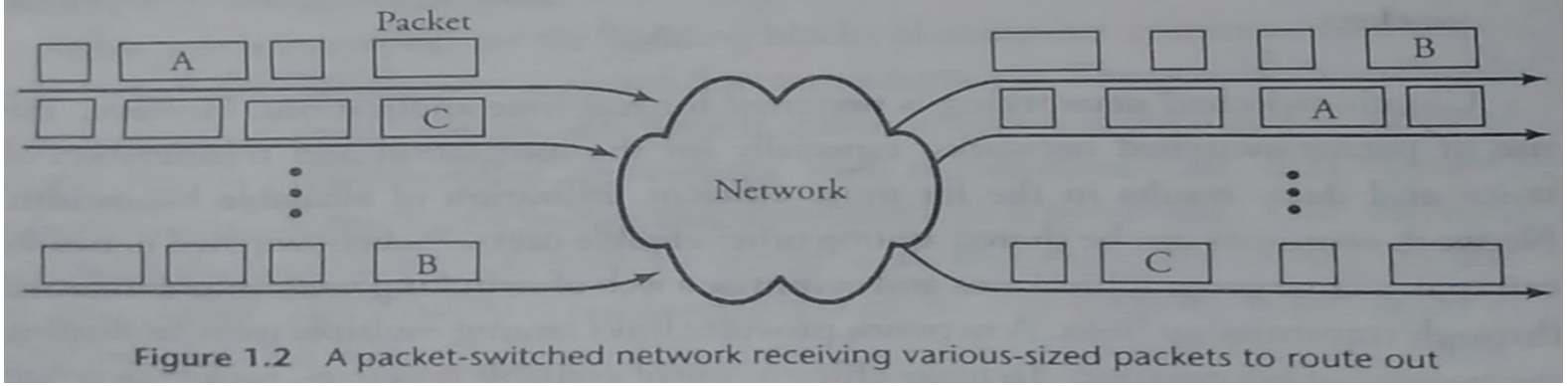


Figure 1.2 A packet-switched network receiving various-sized packets to route out

- The Internet
- The internet is a collection of hardware and software components that make up our global communication networks.
- The internet is collection of inter connected communicating devices that are all connected together to provide services to all distributed applications.
- To connect to the internet , users need the services of Internet service providers(ISP)

- Each country has international or national service providers, regional service providers, and local service providers.
- At the top of the hierarchy the national service providers connect nations.
- The traffic between the each two national ISPs is very heavy.
- Two ISPs are connected together through complex switching stations called network access points(NAS).Each NAP has its own Network administrator.

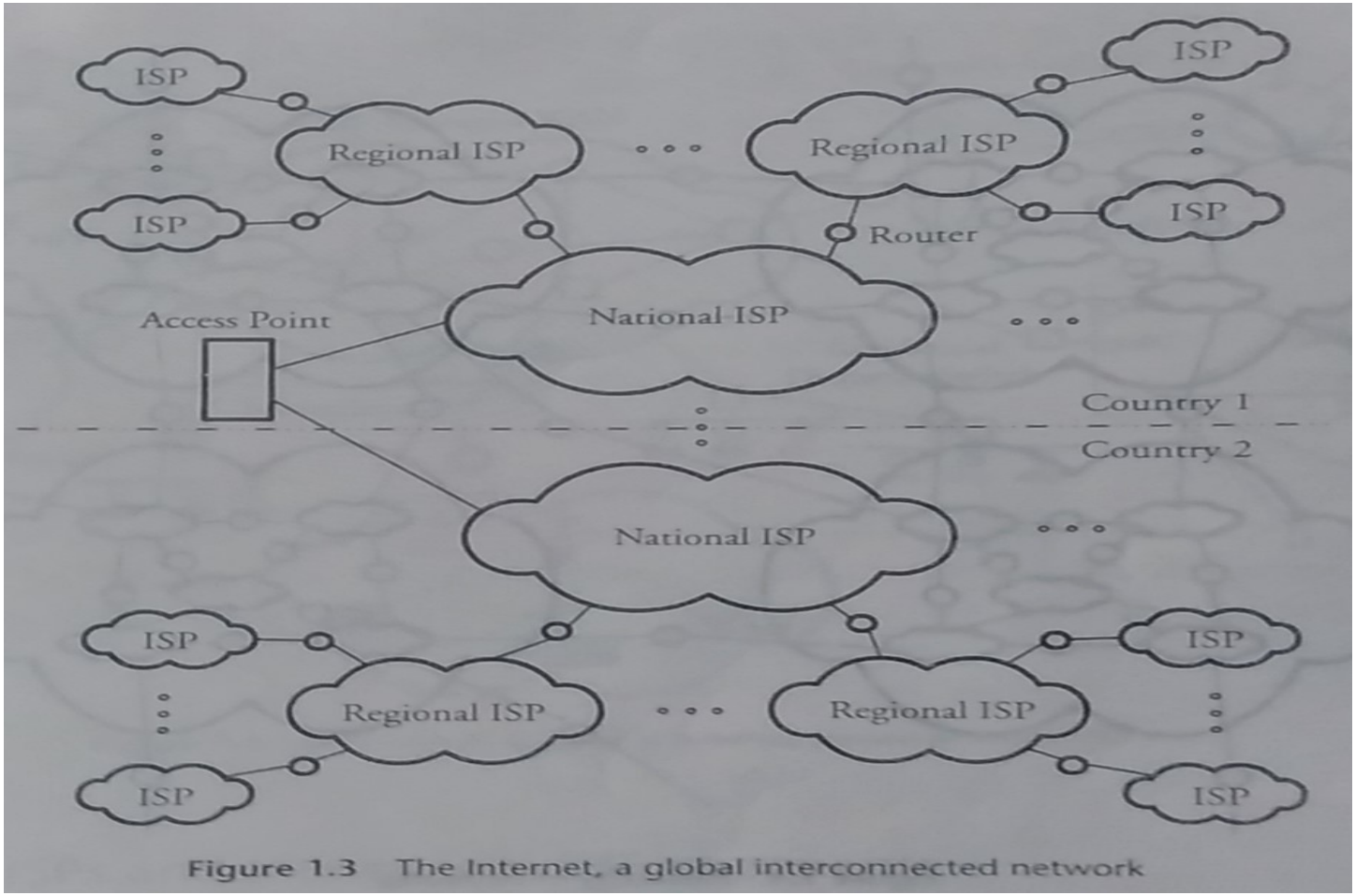


Figure 1.3 The Internet, a global interconnected network

- Each regional ISP can give services to a city
- The lowest networking entity of the Internet is a local internet service provider.
- A local ISP is connected to a regional ISP or directly to a national ISP and provides a direct services to the end users called hosts.
- End-users and systems are connected together by communication links.

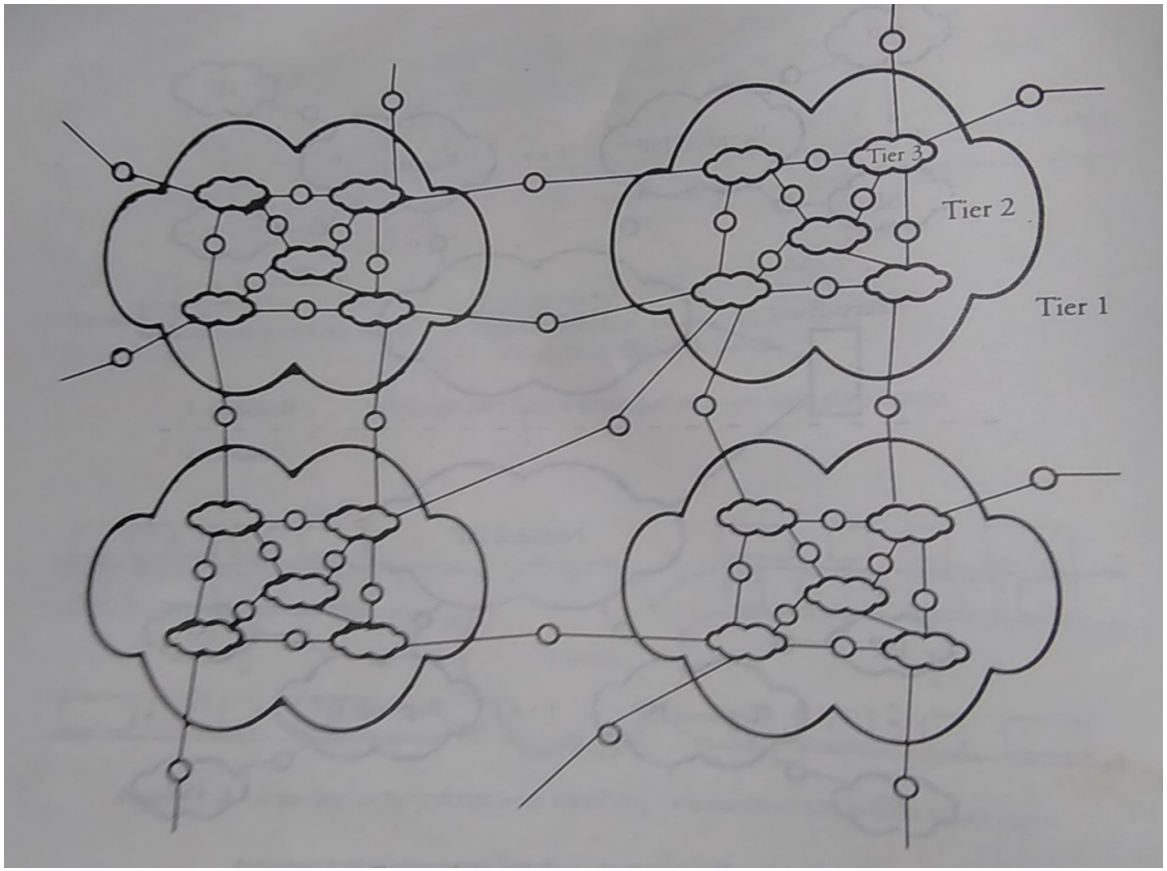


Fig 1.4 Hierarchy of networks

- Fig 1.4 illustrates a different perspective of the global interconnected networks.
- Image a global interconnected networks in a hierarchical structure.
- Each ISP of certain hierarchy or tier manages a number of other domains at its lower hierarchy.
- Tier1,tier 2,tier 3 represents a national ISP,reginal ISP,local ISP.

- 1.4 ISPs and Internetwork components
- Fig 1.5 shows an ISP. Network can be classified into two main categories.
- WAN
- LAN
- A WAN can be as large as the entire infrastructure of the data network access system known as the internet.
- Fig 1.5 shows several networks including LAN and WANs.

- End systems are indirectly conneted to each other through intermediate switching nodes known as routers.
- Switching devices are key components that allow the flow of information to be switched over other links.
- Multiple users accessing a single transmission medium at the same time are connected not only by switching nodes and interconnection links but also access multiplexer
- The mutiplexer combines traffic from several nodes into a cumulative flow

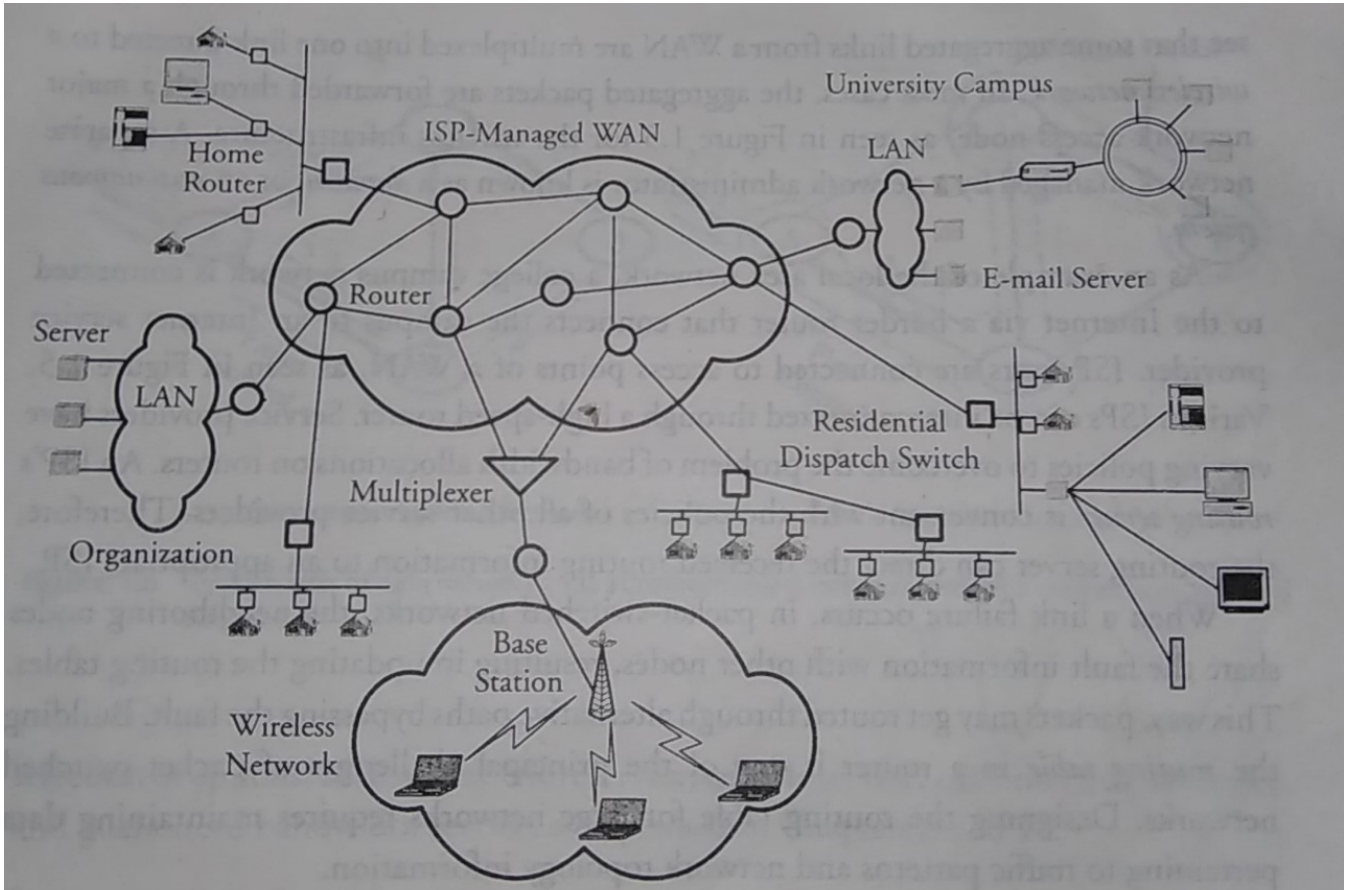
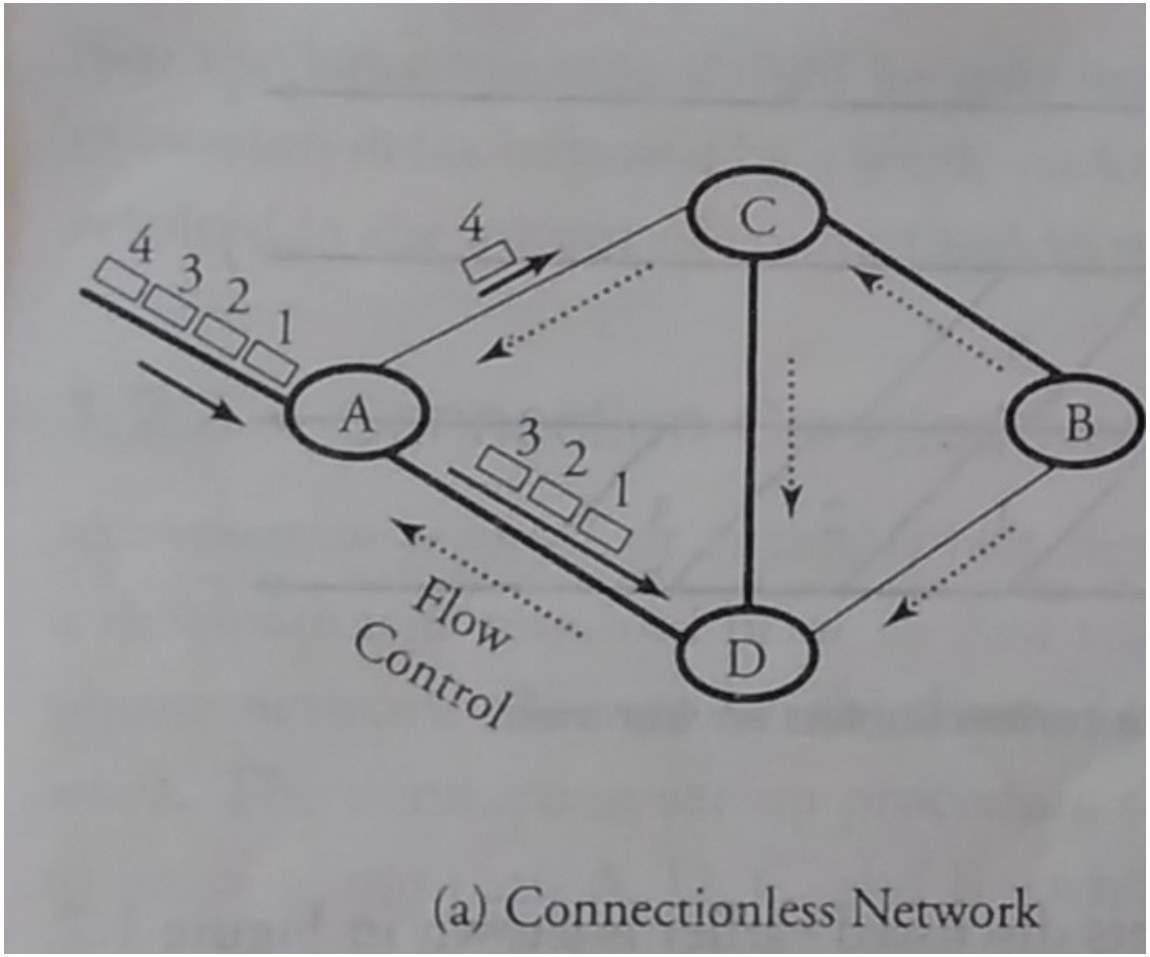


Figure 1.5 Overview of a regional Internet service provider (ISP)

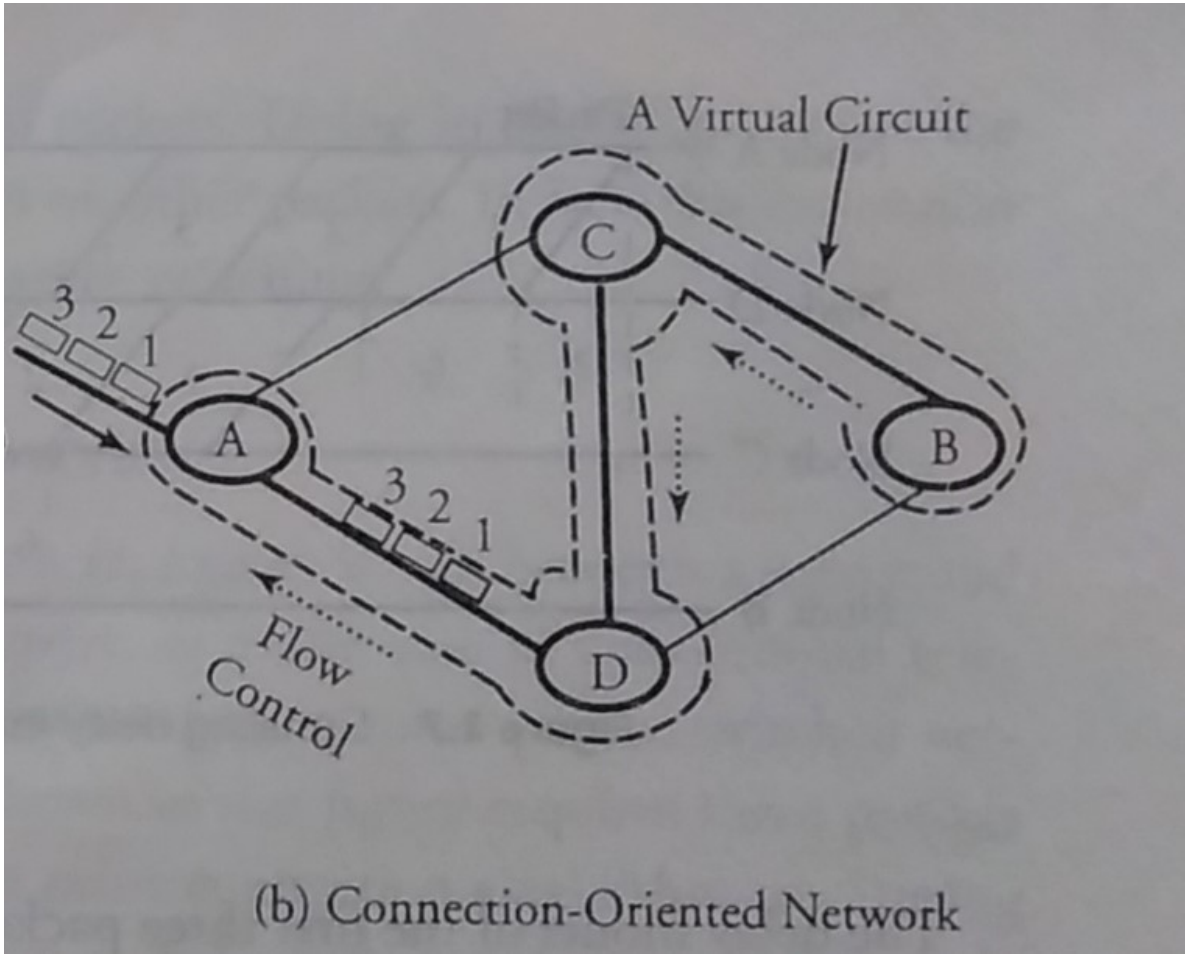
- This technique improves the bandwidth utilization efficiently.
- Types of packet switched networks
- packet switched networks are classified into
- 1.datagram or connectionless networks
- 2.virtualcircuit or connection oriented
- The simplest form of a network service is based on the connectionless protocol.
- In this type of a network, a user can transmit a packet at any time, without notifying the network layer.

- Packets are encapsulated into a certain ‘formatted header resulting in the basic internet transmission unit of data or datagram.
- A datagram is then sent over the network, with each router receiving the datagram forwarding it to the best route known until it reaches destination.
- In this scheme packets may be routed independently over different paths.
- However packet may arrive out of order.in this case certain network function takes care of the error control,flowcontrol resequencing packets



(a) Connectionless Network

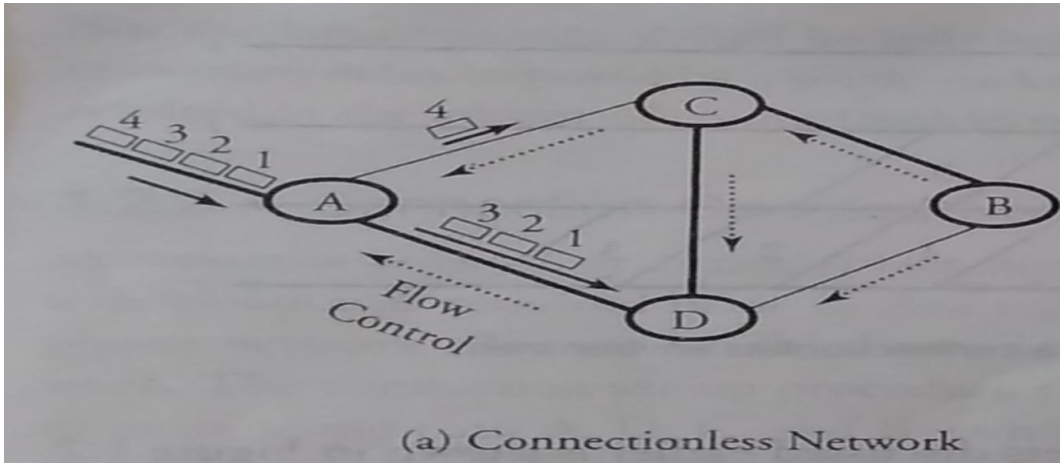
- In connection oriented service packets are transferred through an established virtual circuit between a source and a destination.
- When a connection is initially setup ,network resources are reserved for the call duration.
- after the communication is finished, the connection is terminated using connection termination procedures.
- In connection oriented the network can offer best-effort services, reliable services,guaranted delay services and guaranteed bandwidth services



(b) Connection-Oriented Network

- Connection less networks
- Connection less packet switching achieves high throughput.
- In this large packets are fragment into smaller packets.
- Packets from source are routed independently of one another.
- The connectionless-switching approach does not require a call setup to transfer a packets.

- The main advantage of this scheme is its capability to route packets through an alternative path in case a fault is present on the desired transmission link.
- Fig (a) shows the routing of four packets in a connectionless networks from point A to point B .
- The packet travel through intermediate notes in a store- and forward mechanism.



(a) Connectionless Network

- The first three packets are moving along the path A,D,C and B , where as the fourth packet moves on a separate path

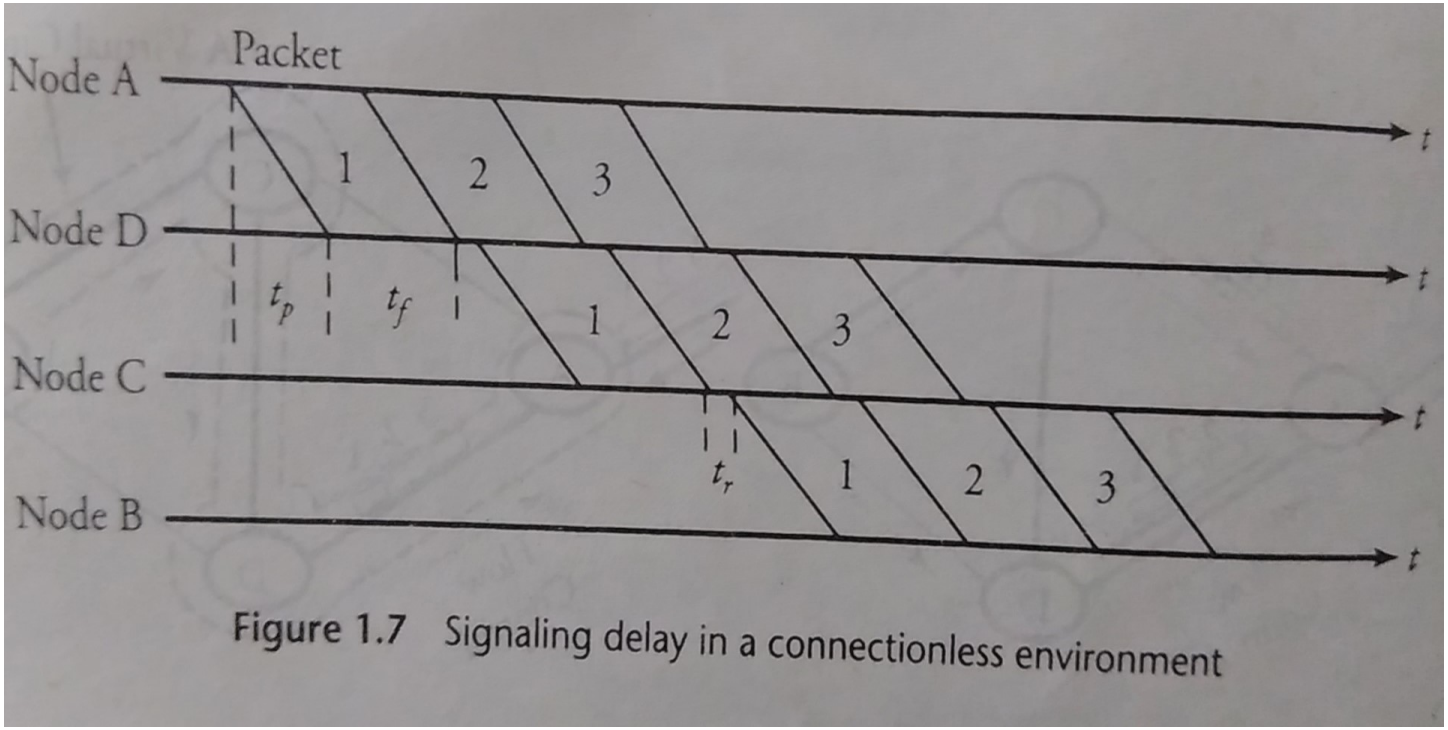


Figure 1.7 Signaling delay in a connectionless environment

- The delay model of the three packets discussed earlier is shown in fig 1.7
- The total transmission delay for a message three packets long traversing from the source node A to the destination node B can be approximately determined .
- Let t_p be propagation delay between each two node,
- And let t_f be the packet transfer time from one node to next node
- A packet is processed once it is received at a node with a processing time t_r
- The total transmission delay
- $$D_p = [n_p+(n_h-2)]t_f+(n_h-1)t_p+n_ht_r$$

Example. Figure 1.7 shows a timing diagram for the transmission of three packets on path A, D, C, B in Figure 1.6. Determine the total delay for transferring these three packets from node A to node B.

Solution. Assume that the first packet is transmitted from the source, node A, to the next hop, node D. The total delay for this transfer is $t_p + t_f + t_r$. Next, the packet is similarly transferred from node D to the next node to ultimately reach node B. The delay for each of these jumps is also $t_p + t_f + t_r$. However, when all three packets are released from node A, multiple and simultaneous transmissions of packets become possible. Thus, the total delay for all three packets to traverse the source and destination via two intermediate nodes is $D_p = 3t_p + 5t_f + 4t_r$.

connection oriented or virtual circuit networks

- In connection oriented or virtual circuit networks , a route set up between a source and destination is required prior to data transfer.
- Fig 1.6b shows a CO packet switched networks.
- The connection set-up procedure shown in the fig requires three packets to move along path A,D,C and B with a prior connection establishment.
- During the connection set-up process , a virtual path is dedicated and forwarding routing tables are updated at each node in the route.

- VC packet switching typically reserves the network resources such as the buffer capacity and the link bandwidth to provide guaranteed quality of service and delay.
- The main disadvantage in CO packet switched networks is that in case of link failure ,the call set-up process has to be repeated for all the affected routes.
- Also each switch needs to store information about all the flows routed through the switch.

- The total delay in transmitting a packet in connection oriented packet switching is the sum of the connection set-up time and the data transfer time.
- The estimation of the total delay time D_t to transmit n_p packets is similar to the one presented for connectionless networks.
- For connection oriented Networks the total time consists of two components D_p which represents the time to transmit packets and D_C, which represents the time for the control packets

$$D_t = D_{p+} D_C$$

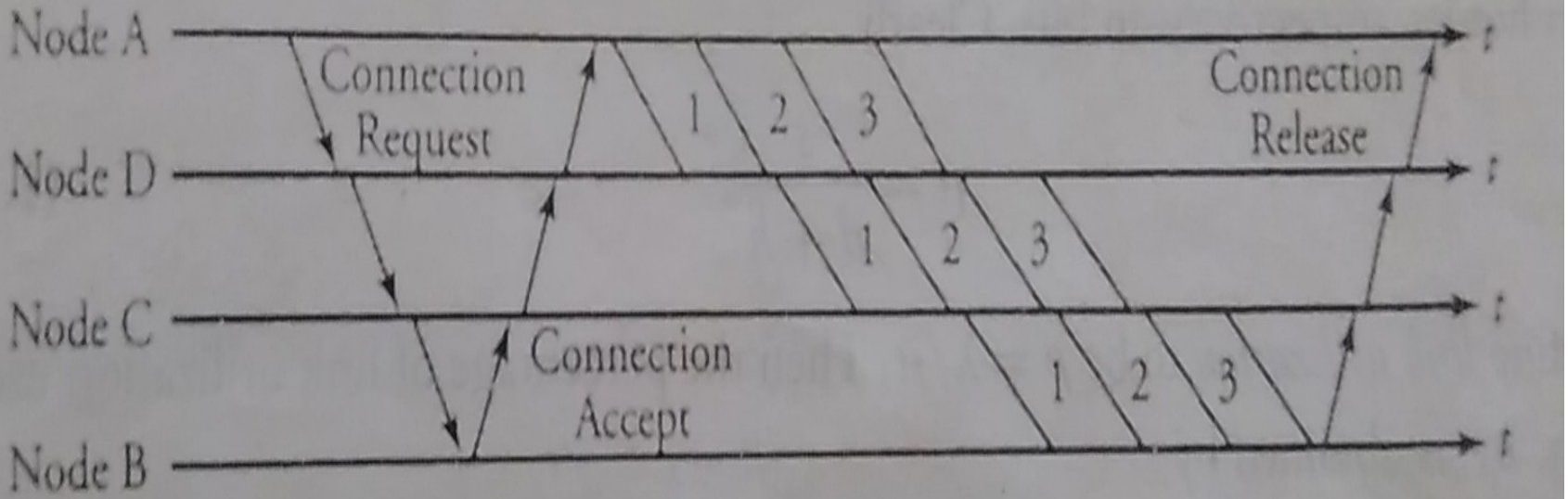


Figure 1.8 Signaling delay in a connection-oriented packet-switched environment

- Internet Protocol and Addressing
- The third layer of the communication protocol is Network layer. Which specifies the networking aspects of a communication transaction.
- This IP layer handles networking aspects and establishes routers for packets.
- The network layer handles the method of assigning address to packet transmission and determines how they should be forwarded from one point to another

- The protocol used in the network layer is IP.
- IP header contains the IP address of Source machine and destination machine.
- An IP packet can be encapsulated in the layers 2 frame when the packet enters in LAN.
- IP provides internet connectivity. This layer is based on connection less service or datagram service.

- The advantage of this kind of service
- Flexibility to allow inter connection between dissimilar networks
- Robustness to node failure
- The IP layer fragments packets to MTU and perform reassembly of packet fragments at destination

2.3.1 IP Packet

The packet format of IP version 4 (IPv4) is shown in Figure 2.3. Each packet comprises the header and data. The size of the header is variable, with 20 bytes of fixed-length header and an *options* field whose size is variable up to 40 bytes. A brief description of the fields follows.

- *Version* specifies the IP version.
- *Header length* (HL) specifies the length of the header.

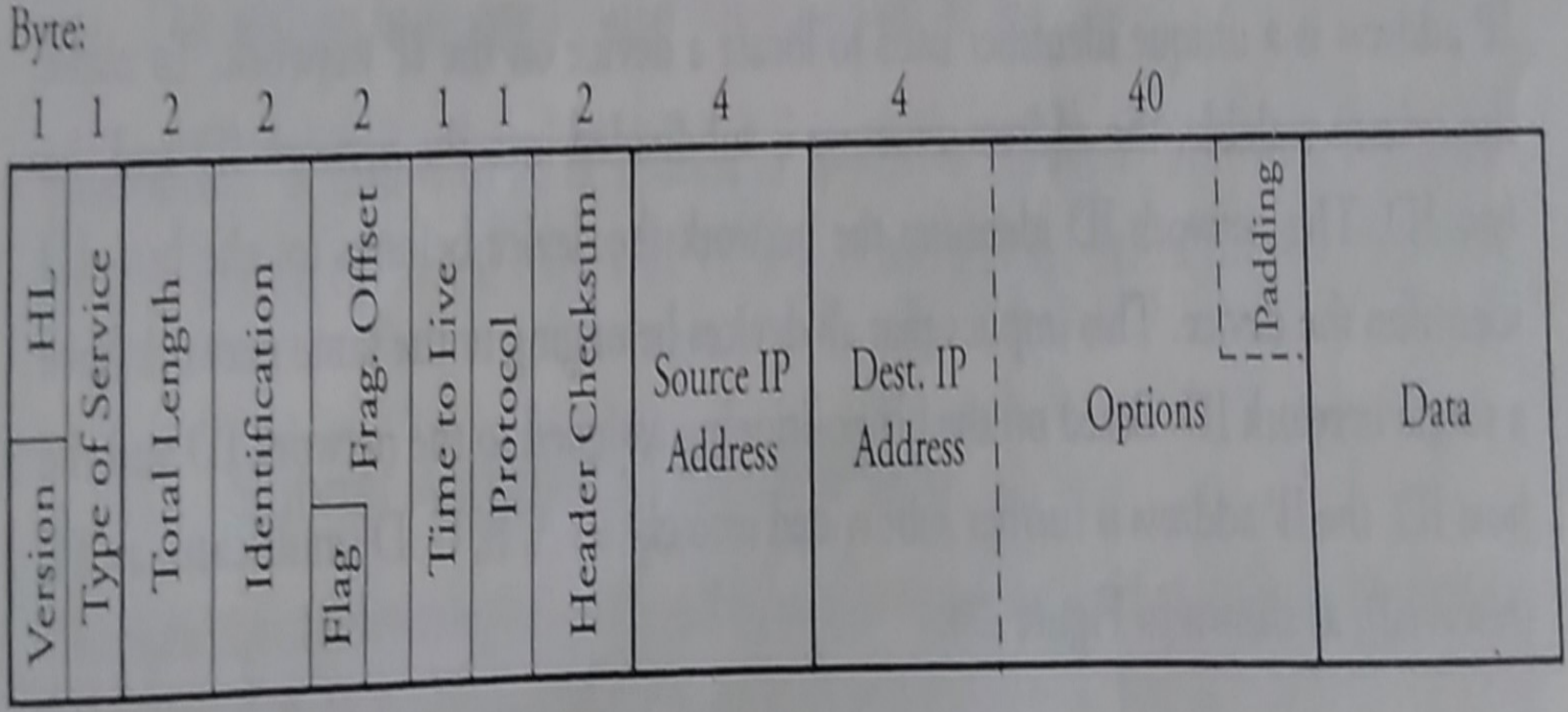


Figure 2.3 IP packet format

- *Type of service* specifies the quality-of-service (QoS) requirements of the packet, such as priority level, delay, reliability, throughput, and cost.
- *Total length* specifies the total length of the packet in bytes, including the header and data. A total of 16 bits are assigned to this field.
- *Identification*, *flags*, and *fragment offset* are used for packet fragmentation and reassembly.
- *Time to live* specifies the maximum number of hops after which a packet must be discarded.

- *Protocol* specifies the protocol used at the destination.
- *Header checksum* is a method of error detection and is described in Chapter 4.
- *Source address* and *destination address* are 32-bit fields specifying the source address and the destination address, respectively.
- *Options* is a rarely used variable-length field to specify security level, timestamp, and type of route.

2.3.2 IP Addressing Scheme

The IP header has 32 bits assigned for addressing a desired device in the network. An IP address is a unique identifier used to locate a device on the IP network. To make the system scalable, the address structure is subdivided into the *network* ID and the *host* ID. The network ID identifies the network the device belongs to; the host ID identifies the device. This implies that all devices belonging to the same network have a single network ID. Based on the bit positioning assigned to the network ID and the host ID, the IP address is further subdivided into classes A, B, C, D (multicast), and E (reserved), as shown in Figure 2.4.

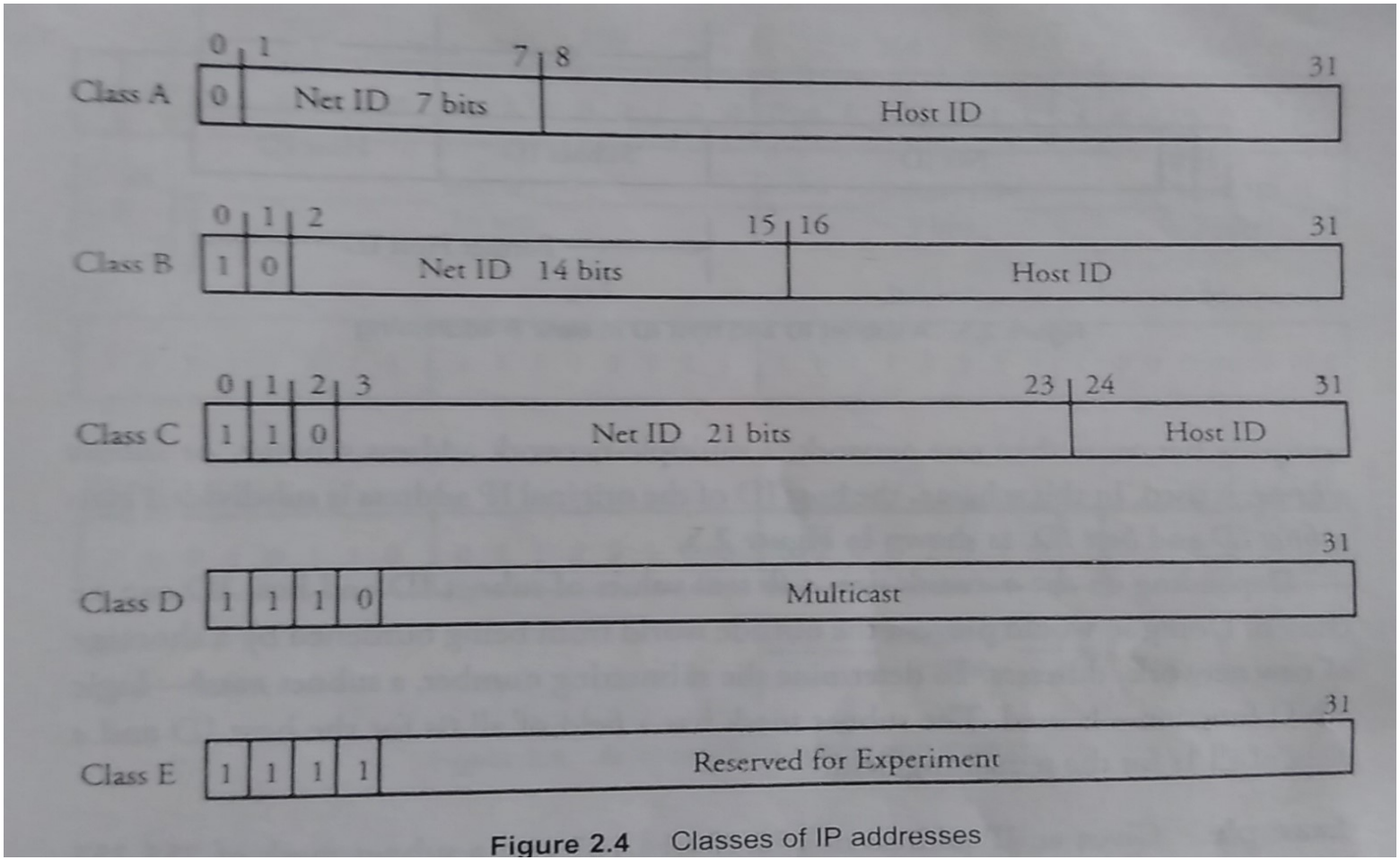
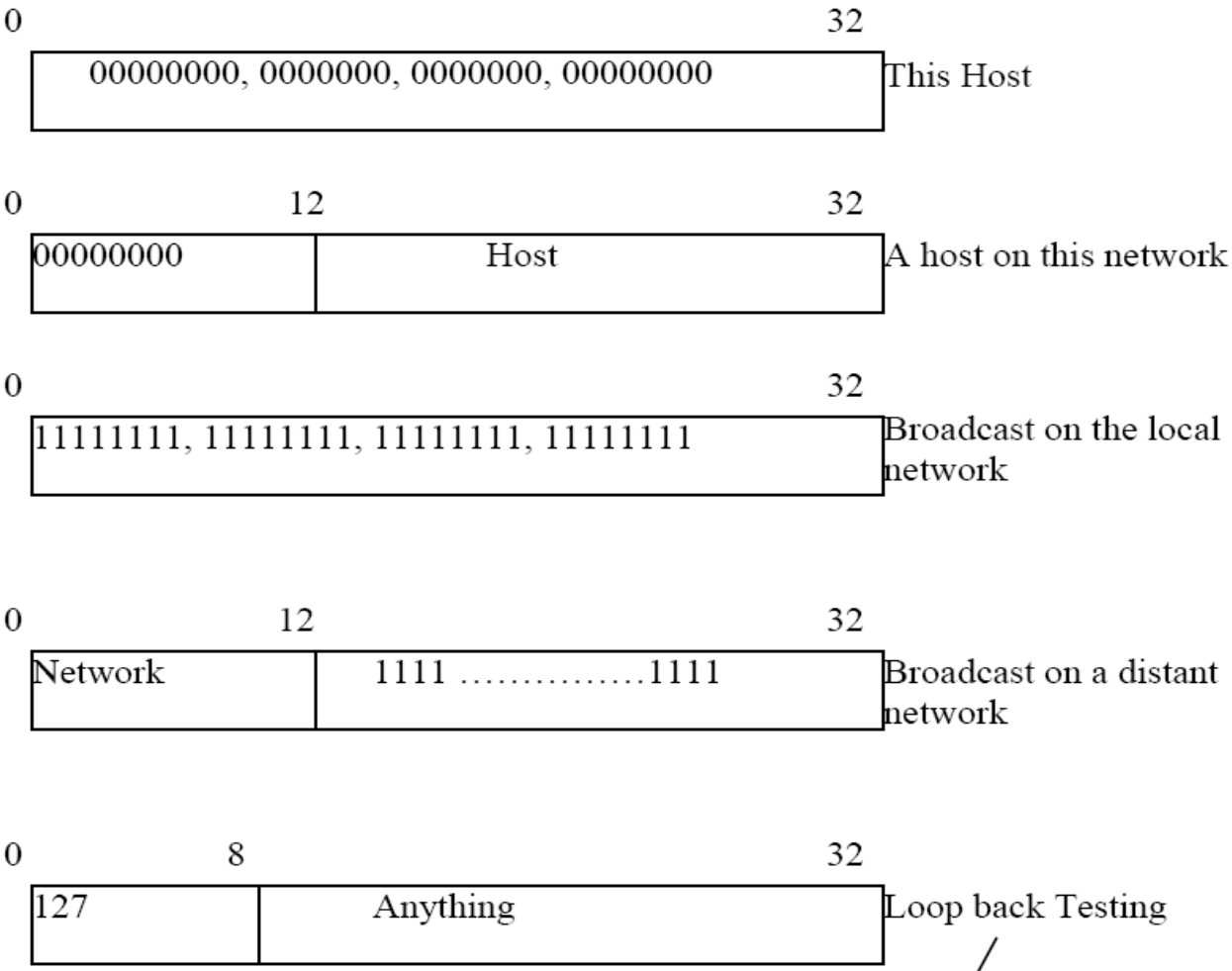


Figure 2.4 Classes of IP addresses

- Network addresses, which are 32-bit numbers, are usually written in dotted decimal notation. In this format, each of the 4 bytes is written in decimal, from 0 to 255.
- The lowest IP address is 0.0.0.0 and the highest is 255.255.255.255
- The values 0 and 1 (all 1s) have special meanings
- 0 -> means **This Network** or **this host**
- 1 -> Used as a broadcast address to mean all hosts on the indicated network

Example:


0
32
00000000, 0000000, 0000000, 00000000
This Host
0
12
32
00000000
Host
A host on this network
0
32
11111111, 11111111, 11111111, 11111111
Broadcast on the local network
0
12
32
Network
1111 ……1111
Broadcast on a distant network
0
8
32
127
Anything
Loop back Testing
[Packet send to this address are not put out on to the wire they are treated as incoming packet and processed locally]

2.3.3 Subnet Addressing and Masking

The concept of subnetting was introduced to overcome the shortcomings of IP addressing. Managing the large number of hosts is an enormous task. For example, a company that uses a class B addressing scheme supports 65,535 hosts on one network. If the

- Sub network or subnets:
- It is a logically visible subdivision of an ip network.
- Subnet ting is dividing the network into two or more networks is called subnet ting.
- Benefit of Subnets:

- Reduces the network traffic.
- Security
- Performance
- Troubleshooting - it is easier to find a problem in a smaller network than a large one.

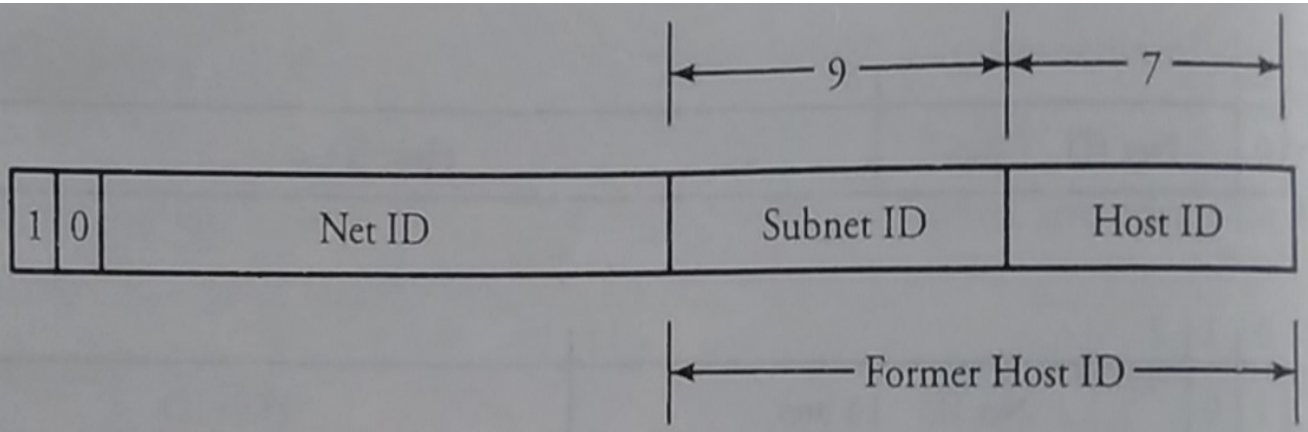
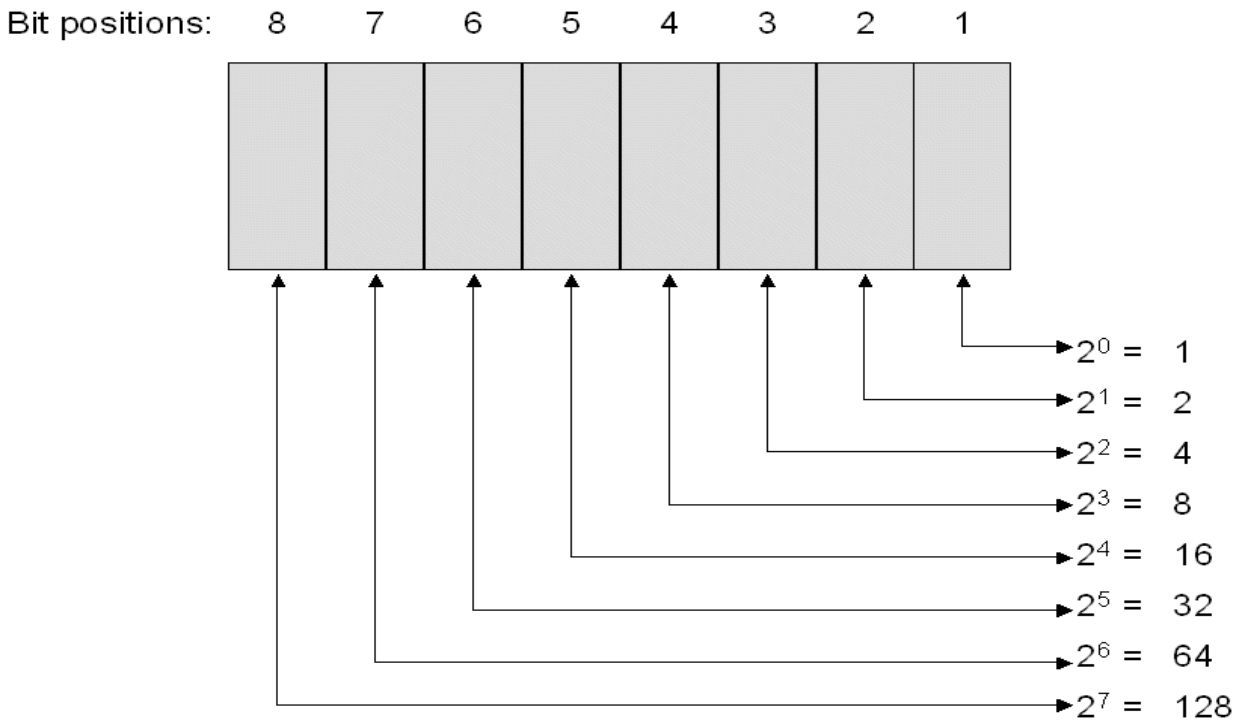


Figure 2.5 A subnet ID and host ID in class *B* addressing

company has more than one network, a multiple-network address scheme, or *subnet scheme*, is used. In this scheme, the host ID of the original IP address is subdivided into *subnet ID* and *host ID*, as shown in Figure 2.5.

subnetting(cont..)

- An IP address has two components, the network address and the host address
- Subnetting further divides the host part of an IP address into a subnet and host address (<network><subnet><host>).
- A Subnet mask is a 32-bit number that masks an IP address, and divides the IP address into network address and host address
- Subnet Mask is made by setting network bits to all "1"s and setting host bits to all "0"s.
- Within a given network, two host addresses are reserved for special purpose. The "0" address is assigned a network address and "255" is assigned to a broadcast address



	128	64	32	16	8	4	2	1
8 bit binary digit	1	0	1	1	0	0	0	1
	128 + 32 + 16 + 1 = 177							

1 Translating Binary to Decimal

Both IP addresses and subnet masks are composed of 32 bits divided into 4 octets of 8 bits each. Here is how a single octet translates from binary to decimal. Consider an octet of all ones: 11111111.

```
128    64    32    16    8    4    2    1
---    --    --    --    -    -    -    -
 1      1     1     1    1    1    1    1
128 + 64 + 32 + 16 + 8 + 4 + 2 + 1 = 255
```

Here's another: 10111001

```
128    64    32    16    8    4    2    1
---    --    --    --    -    -    -    -
 1      0     1     1    1    0    0    1
128 +  0 + 32  +16 + 8 + 0 + 0 + 1 = 185
```

and 00000000

```
128    64    32    16    8    4    2    1
---    --    --    --    -    -    -    -
 0      0     0     0    0    0    0    0
 0   +  0 +  0 +  0 + 0 + 0 + 0 + 0 = 0
```

2 Converting Decimal to Binary

Converting decimal to binary is similar. Consider 175:

```
128    64    32    16    8    4    2    1
---    --    --    --    -    -    -    -
 1      0     1     0    1    1    1    1
128 +  0 + 32 +  0 + 8 + 4 + 2 + 1 = 175
```

Tink –pair –share (group activity)

- Example : A network on the internet has subnet mask of 255.255.240.0 . What is the max number of hosts it can handle?

Example. Given an IP address of 150.100.14.163 and a subnet mask of 255.255.255.128, determine the maximum number of hosts per subnet.

Solution. Figure 2.6 shows the details of the solution. Masking 255.255.255.128 on the IP address results in 150.100.14.128. Clearly, the IP address 150.100.14.163 is a class B address. In a class B address, the lower 16 bits are assigned to the subnet and host fields. Applying the mask, we see that the maximum number of hosts is $2^7 = 128$.

subnetting(cont..)

- The default subnet mask for
- class A is 255.0.0.0
- class B is 255.255.0.0
- class C is 255.255.255.0

Bits Available for Creating Subnets

Address Class	Host Bits	Bits Available for Subnet
A	24	22
B	16	14
C	8	6

Calculating Subnets

There are two simple formulas to calculate these numbers:

Number of hosts per subnet = ($2^{\text{number of bits used for host}}$) - 2

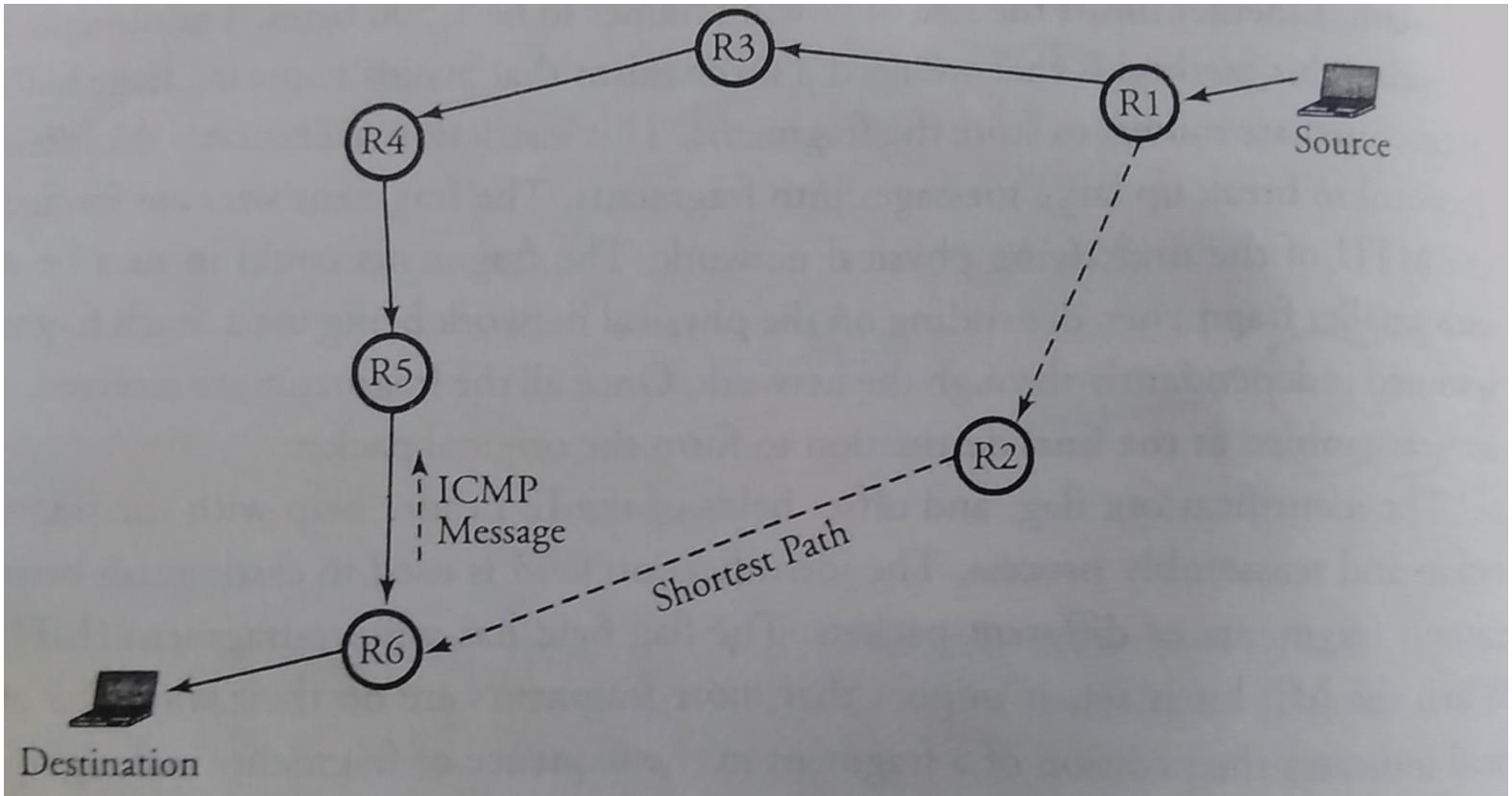
Number of subnets = ($2^{\text{number of bits used for subnets}}$) - 2

- Example : A network on the internet has subnet mask of 255.255.240.0 . What is the max number of hosts it can handle?
- Example : Given an IP address of 150.100.14.163 and a subnet mask of 255.255.255.128,determine the max no of hosts per subnets

- Packet fragmentation and Reassembly
- The physical capacity of networks enforces an upper bound on size of a packet.
- The maximum transferable unit(MTU) represents this restriction.
- For example, as a LAN standard, Ethernet limits the size of flowing frames to be 1500 bytes.
- The internet protocol to break up large messages into fragmnets.
- The fragment sizes are limited to the MTU of the network.

- Each fragment peace's are routed independently through the networks.
- Once all fragments are received ,they are reassembled at the final destination to form a original packet.
- The identification ,flag and offset fields of the IP header helps with the fragmentation and reassembly.
- The identification field is used to distinguish between various fragments of different packets.

- **Internet Control Protocols:**
- **ICMP [Internet Control Message Protocol]**
- Used to **test** the internet
- Routers continuously monitor the operation of the internet
- When something **unexpected occurs**, the event is reported by ICMP
- Different types of ICMP messages are defined and each ICMP message type is encapsulated in an IP packet



e 2.8 With ICMP, a redirect message cannot be sent to R1, since R6 does not know the address of R1.

Some of the message types are listed below:

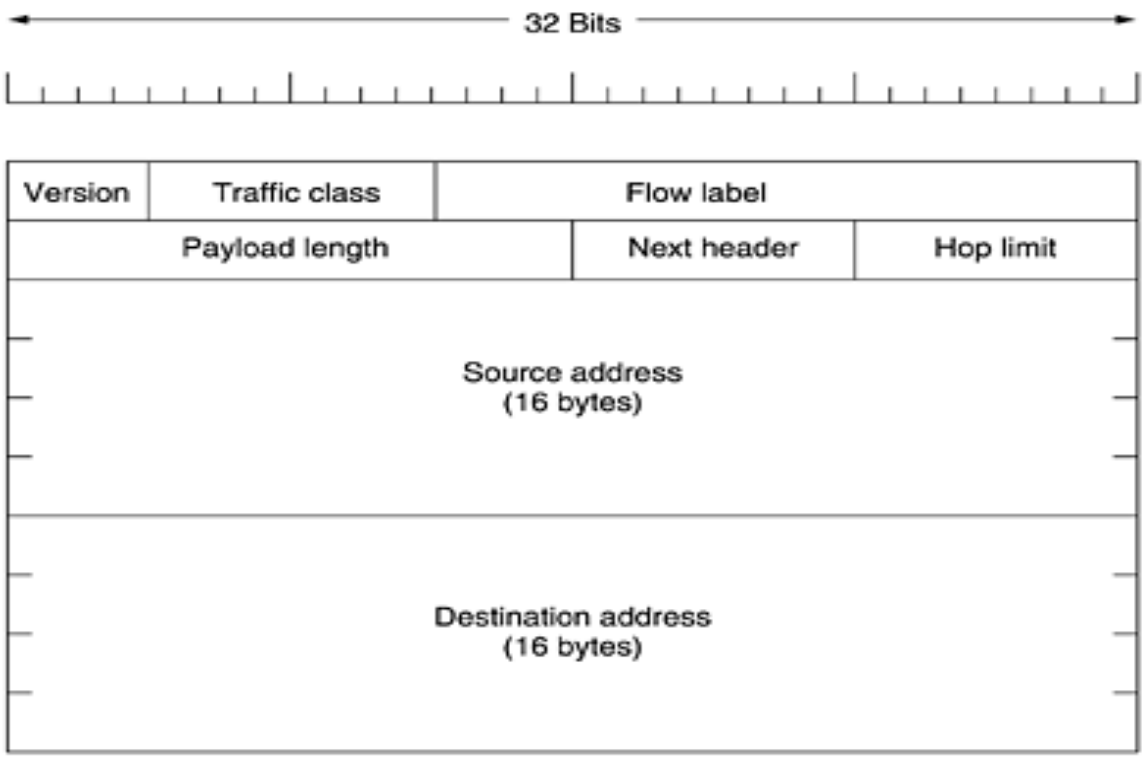
Message Type	Description
Destination Unreachable	Packet could not be delivered
Time exceeded	Time to live field hit zero
Parameter problem	Invalid header field
Source Quench	Choke packet
Echo request	Ask a machine if it is alive
Echo Reply	Yes I am alive
Time stamp request	Same as Echo, but with time stamp
Time stamp reply	Same as Echo, but with time stamp

- **IPv6** (**Internet Protocol version 6**) is the latest revision of the Internet Protocol (IP), the primary communications protocol upon which the entire Internet is built.
- IPv6 is intended to replace the older IPv4,
- IPv6 was developed by the Internet Engineering Task Force (IETF) to deal with the long-anticipated problem of IPv4 running out of addresses

- Each device on the Internet, such as a computer or mobile telephone, must be assigned an IP address in order to communicate with other devices.
- With the ever-increasing number of new devices being connected to the Internet, there is a need for more addresses than IPv4 can accommodate.
- IPv6 uses 128-bit addresses, allowing for 2^{128}, or approximately -340,282,366,920,938,463,463,374,607,431,768,211,456 3.4×10^{38} addresses — more than 7.9×10^{28} times as many as IPv4, which uses 32-bit addresses.

- **IPV6 was developed to meet the following goals:**
- (1) Supports billions of hosts,
- (2) Reduce the size of the routing table
- (3) Simplify the protocols, to allow routers to process packets faster
- (4) Provide better security [authorization and privacy] than current IP
- (5) Pay more attention to type of service, particularly for real time data
- (7) Make it possible for a host to roam without changing its address
- (8) Allow protocols to evolve in the future
- For IPv6, the 128-bit address is divided along 16-bit boundaries, each 16-bit block is converted to a 4-digit hexadecimal number and adjacent 16-bit blocks are separated by colons. The resulting representation is known as colon-hexadecimal.

- **Main Features:**
- IPV6 has **larger address** than IPV4. They are **16 bytes long** which provide an effectively unlimited supply of Internet address
- IPV6 is the simplification of the header. It contains only **7 fields**. This allows routers to **process packets faster** and thus **improve throughput**
- This process **speeds up packet processing time**


32 Bits
Version
Traffic class
Flow label
Payload length
Next header
Hop limit
Source address
(16 bytes)
Destination address
(16 bytes)

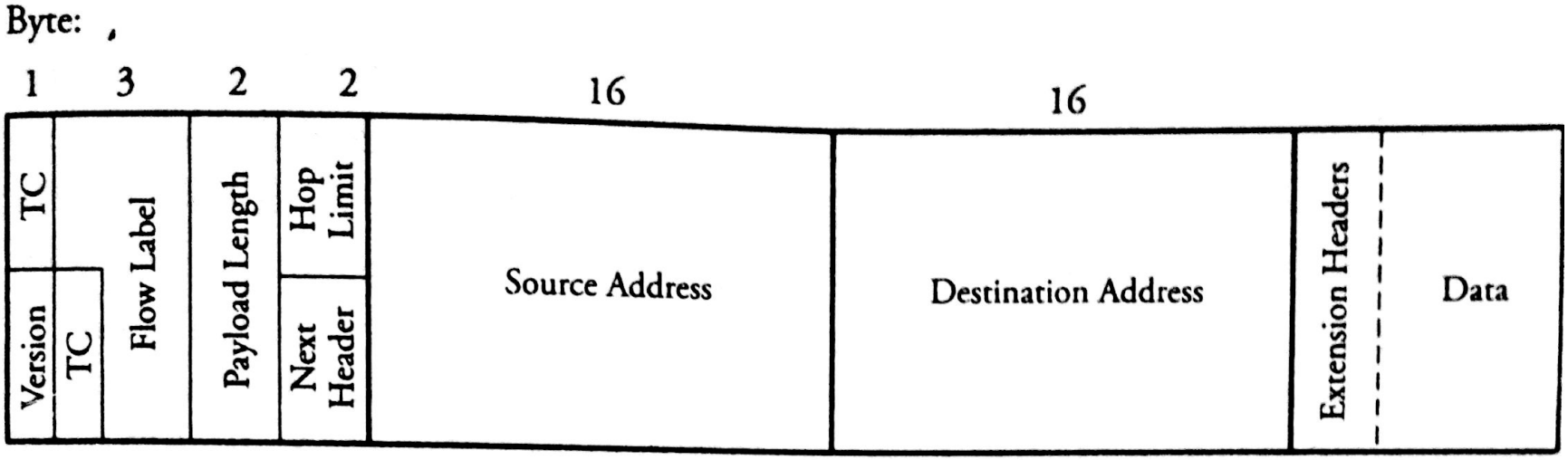


Figure 2.9 An IPv6 packet format

- **Version:** The Version field is always 6 for IPv6 (and 4 for IPv4).,
- **Traffic class :** specifies the priority level assigned to a packet.

  Flow Label : indicates the delay period within which application packets, such as real-time video, must be delivered..
- **Payload Length Field**: is the 16 bit specification of the length of the data, excluding the header
- **Next header field**: It tells the type of the next header (eg: TCP,UDP or extension headers)
- **Hop limit:** It is same as time to live field in IPV4, [i.e. a field that is decremented on each hop]
- **Source and destination Address:** IPV6 uses a fixed length 16 byte address