APJ ABDUL KALAM TECHNOLOGICAL UNIVERSITY

STUDY MATERIALS

KTU ASSIST

a complete app for ktu students

Get it on Google Play

www.ktuassist.in

Module 4

QoS and Internetworking

CONGESTION CONTROL

Ques 1) What is congestion? What are the causes of congestion?

Or

Show the effect on congestion on throughput of a network using a diagram.

Ans: Congestion

Congestion occurs in a computer network when the resource demands exceed the capacity. Packets may be lost due to too much queuing in the network. During congestion, the network throughput may drop and the path delay may become very high. Congestion in a network may occur if users send data into the network at a rate greater than that allowed by network resources. **For example,** congestion may occur because the switches in a network have a limited buffer size to store arrived packets before processing.

Congestion in a frame relay network is a problem that must be avoided because it decreases throughput and increases delay.

A congestion control scheme helps the network to recover from the congestion state. A congestion avoidance scheme allows a network to operate in the region of low delay and high throughput. Such schemes prevent a network from entering the congested state.

Congestion avoidance is a prevention mechanism while congestion control is a recovery mechanism. Congestion control concerns controlling traffic entry into a telecommunications network, so as to avoid congestive collapse by attempting to avoid over-subscription of any of the processing or link capabilities of the intermediate nodes and networks and taking resource reducing steps, such as reducing the rate of sending packets. It should not be confused with flow control, which prevents the sender from overwhelming the receiver.

Causes of Congestion

The main causes of congestion over network are as below:

1) Unpredictable statistical fluctuation of traffic flows,
2) Fault conditions within the network, and
3) Slow processor speed. If the router's CPU speed is low and performing tasks like queuing buffers, table updating etc. queues are built up, even though the line capacity is not fully utilized.
4) Inefficient control policies (buffers not allocated fairly or correctly).
5) Bandwidth of the links is important in congestion. The links to be used must be of high bandwidth to avoid the congestion.

The **effect on congestion on throughput of a** network is shown in **figure 4.1**.

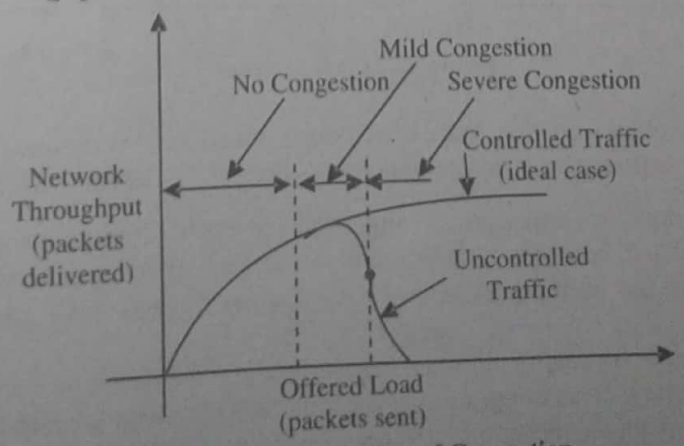


Figure 4.1: Effect of Congestion

DOWNLOADED FROM KTUASSIST.IN

Scanned by CamScanner

Ques 2) What are the different congestion control methods?

Or

What is open-loop and closed-loop congestion control?

Ans: Congestion Control Methods

The solutions to congestion problems can be divided into two categories or groups as:

1) **Open-Loop Congestion Control:** Open-loop congestion control algorithms which do not depend on any sort of direct feedback from the network. They can be implemented using a combination of CAC (Connection Admission Control) and UPC (Usage Parameter Control) procedures. The techniques used in open-loop congestion control are given below:
   i) **Retransmission Policy:** Retransmission is sometimes unavoidable. If the sender feels that a sent packet is lost or corrupted, the packet needs to be retransmitted. Retransmission in general may increase congestion in the network. However, a good retransmission policy can prevent congestion.
   ii) **Window Policy:** The type of window at the sender may also affect congestion. The Selective Repeat Window is better than the Go-Back-N window for congestion control. In the Go-Back-N window, when the timer for a packet times out, several packets may be resent, although some may have arrived safe and sound at the receiver.
   iii) **Acknowledgement Policy:** The acknowledgement policy imposed by the receiver may also affect congestion. If the receiver does not acknowledge every packet it receives, it may slow down the sender and help prevent congestion. Several approaches are used in this case. A receiver may send an acknowledgment only if it has a packet to be sent or a special timer expires.
   iv) **Discarding Policy:** A good discarding policy by the routers may prevent congestion and at the same time may not harm the integrity of the transmission.
   v) **Admission Policy:** An admission policy, which is a quality-of-service mechanism, can also prevent congestion in virtual-circuit networks. Switches in a flow check the resource requirement of a flow before admitting it to the network.

2) **Closed-Loop Congestion Control**: Closed loop congestion control algorithms adopt a method where the source recognizes network congestion by means of feedback information from the network. The source then limits the number of cells injected into the network by some appropriate method. The techniques used in closed-loop congestion control are given below:
   i) **Backpressure:** The technique of backpressure refers to a congestion control mechanism in which a congested node stops receiving data from the immediate upstream node or nodes. This may cause the upstream node to become congested and they, in turn, reject data from their upstream nodes or nodes.
   ii) **Choke Packet:** A choke packet is a packet sent by a node to the source to inform it of congestion. In backpressure, the warning is from one node to its upstream node, although the warning may eventually reach the source station. In the choke packet method, the warning is from the router, which has encountered congestion, to the source station directly. The intermediate nodes through which the packet has travelled are not warned.

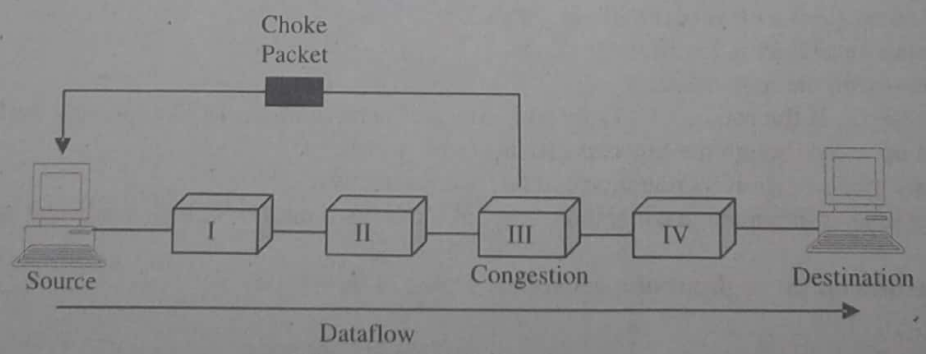


Figure 4.2: Choke Packet

   iii) **Implicit Signaling:** In implicit signaling, there is no communication between the congested node or nodes and the source. The source guesses that there is congestion somewhere in the network from other symptoms.
   iv) **Explicit Signaling:** The node that experiences congestion can explicitly send a signal to the source or destination. The explicit signaling method, however, is different from the choke packet method. In the choke packet method, a separate packet is used for this purpose; in the explicit signaling method, the signal is included in the packets that carry data. It is of two types:
      a) **Backward Signaling:** A bit can be set in a packet moving in the direction opposite to the congestion. This bit can warn the source that there is congestion and that it needs to slow down to avoid the discarding of packets.
      b) **Forward Signaling:** A bit can be set in a packet moving in the direction of the congestion. This bit can warn the destination that there is congestion. The receiver in this case can use policies, such as slowing down the acknowledgements, to alleviate the congestion

DOWNLOADED FROM KTUASSIST.IN

Scanned by CamScanner

Ques 3) **List and explain various congestion control algorithms.**

Or

Define leaky bucket and token bucket algorithm for congestion control.

Ans: Types of Congestion Control Algorithms

Congestion in a frame relay network is a problem that must be avoided because it decreases throughput and increases delay. Following are the two types of algorithm for congestion control:

1) **Leaky Bucket Algorithm:** If there is a hole at the bottom of a bucket, then no matter at what rate the bucket is filled up, the water leaks out drop by drop at a constant rate from the hole. Each host is connected by an interface that has finite queue acting like a "leaky bucket".

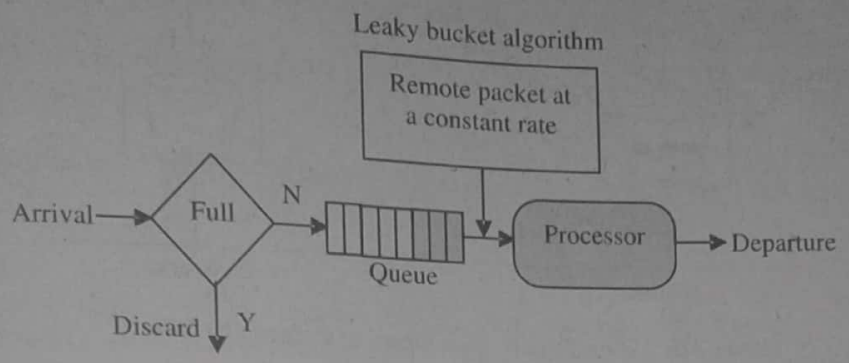


Figure 4.3: Leaky Bucket Implementation

When a packet comes to a host with the queue full, it is discarded. The host is allowed to put one packet per clock tick info the network. This can be enforced by the interface card or by the operating system. This converts an uneven flow of packets from the user process in an even flow of packers onto the network. Conceptually, each host is connected to the network by an interface containing a leaky bucket, that is, a finite internal queue. If a packet arrives at the queue when it is full, the packet is discarded.

In other words, if one or more processes within the host try to send a packet when the maximum number is already queued, the new packet is unceremoniously discarded. This arrangement can be built into the hardware interface or simulated by the host operating system. It was first proposed by Turner (1986) and is called the **leaky bucket algorithm**. In fact, it is nothing other than a single-server queuing system with constant service time. This mechanism turns an uneven flow of packets from the user processes inside the host into an even flow of packets onto the network, smoothing out bursts and greatly reducing the chances of congestion.

Implementing the original leaky bucket algorithm is easy. The leaky bucket consists of a finite queue. When a packet arrives, if there is room on the queue it is appended to the queue; otherwise, it is discarded. At every clock tick, one packet is transmitted (unless the queue is empty).

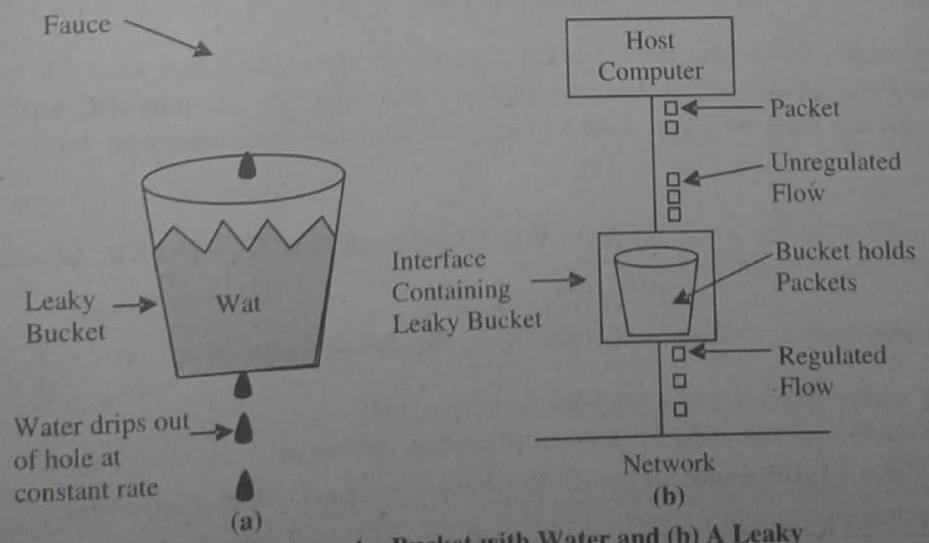


Figure 4.4: (a) A Leaky Bucket with Water and (b) A Leaky Bucket with Packets

Suppose data comes in 1-million-byte bursts, one 40-msec burst every second. To reduce the average rate to 2 MB/sec, we could use a leaky bucket with $\rho = 2$ MB/sec and a capacity, C, of 1 MB. This means that bursts of up to 1 MB can be handled without data loss, and that such bursts are spread out over 500 msec, no matter how fast they come in.

DOWNLOADED FROM KTUASSIST.IN

Scanned by CamScanner

2) **Token Bucket Algorithm:** The leaky bucket algorithm enforces a rigid output pattern at the average rate, no matter how burst the traffic is. For many applications, it is better to allow the output to speed up somewhat when large bursts arrive, so a more flexible algorithm is needed, preferably one that never loses data. One such algorithm is the **token bucket algorithm**. In this algorithm, the leaky bucket holds tokens, generated by a clock at the rate of one token every ΔT sec. For a packet to be transmitted, it must capture and destroy one token.

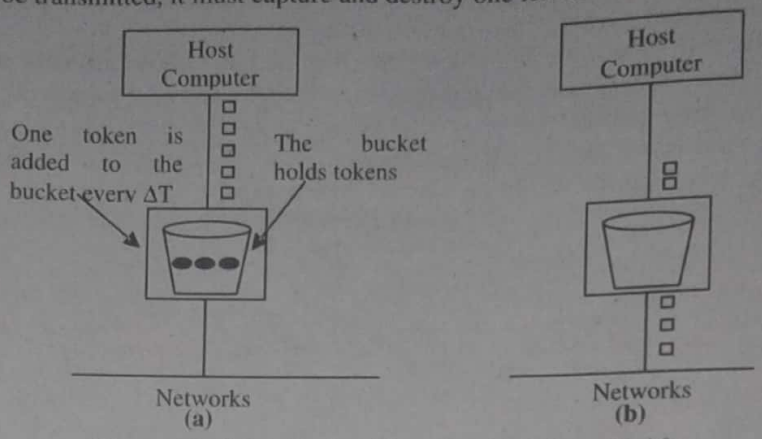


Figure 4.5: Token Bucket Algorithm (a) Before, (b) After

The leaky bucket algorithm does not allow idle hosts to save up permission to send large bursts later. The token bucket algorithm does allow saving, up to the maximum size of the bucket, n. This property means that bursts of up to n packets can be sent at once, allowing some burstiness in the output stream and giving faster response to sudden burst of input. Another difference between the two algorithms is that the token bucket algorithm throws away tokens when the bucket fills up but never discards packets. In contrast, the leaky bucket algorithm discards packets when the bucket fills up.

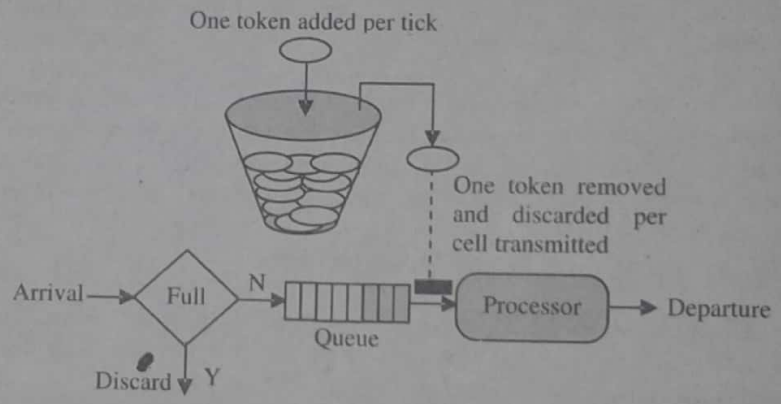


Figure 4.6: Token Bucket

If one call the burst length S sec, the token bucket capacity C bytes, the token arrival rate ρ bytes/sec, and the maximum output rate M bytes/sec, we see that an output burst contains a maximum of C + ρS bytes. We also know that the number of bytes in a maximum-speed burst of length S seconds in MS. Hence we have

$$C + \rho S = MS$$

We can solve this equation to get $S = C/(M - \rho)$. For our parameters of C = 250 KB, M = 25 MB/sec, and ρ = 2 MB/sec, we get a burst time of about 11 msec.

Ques 4) What is difference between Token-bucket and leaky-bucket algorithm?

Ans: Difference between Token-Bucket and Leaky-Bucket algorithm

The difference between token bucket and leaky bucket algorithm is given below:

Table 4.1: Difference between Token-Bucket and Leaky-Bucket Algorithm

Token Bucket Algorithm	Leaky Bucket Algorithm
Token dependent	Token independent
If bucket is full token are discarded, but not the packet.	If bucket is full packet or data is discarded.
Packets can only transmitted when there are enough token.	Packets are transmitted continuously.
It allows large bursts to be sent at faster rate after that constant rate.	It sends the packet at constant rate.
It saves token to send large bursts.	It does not save token.

DOWNLOADED FROM KTUASSIST.IN

Scanned by CamScanner

QUALITY OF SERVICE (QOS)

Ques 5) What is meant by term QoS? What are the different flow characteristics?

Ans: Quality of Service

Quality of service is defined as something a flow seeks to attain.

A stream of packets from a source to destination is called **flow**. In a connection–oriented network all packets belonging to a flow, follow the same route; in a connection-less service they may follow different routes.

The needs of each flow can be characterised by primary parameters *viz*, reliability, delay, jitter and bandwidth. Together these determine the QoS (Quality of Service) the flow requires.

QoS defines a set of attributes related to the performance of the connection. For each connection, the user can request a particular attribute.

Flow Characteristics

Traditionally, four types of characteristics are attributed to a flow which is given below:

1) **Reliability:** Reliability is a characteristic that a flow needs. Lack of reliability means losing a packet or acknowledgement, which entails retransmission. However, the sensitivity of application programs to reliability is not the same.

2) **Delay:** Source-to-destination delay is another flow characteristic. Again applications can tolerate delay in different degrees. In this case, telephony, audio conferencing, video conferencing and remote log-in need minimum delay, while delay in file transfer or e-mail is less important.

3) **Jitter:** Jitter is the variation in delay for packets belonging to the same flow. **For example,** if four packets depart at times 0, 1, 2 and 3 and arrive at 20, 21, 22 and 23, all have the same delay, 20 units of time.

   Jitter is defined as the variation in the packet delay. High jitter means the difference between delays is large; low jitter means the variation is small.

4) **Bandwidth:** Different applications need different bandwidths. **In video conferencing** one need to send millions of bits per second to refresh a colour screen while the total number of bits in an e-mail may not reach even a million.

Ques 6) What are the different QoS attributes?

Ans: QoS Attributes

The attributes can be classified into two major categories as below:

1) **User-Related Attributes:** These attributes are related to the end user in the sense that they define how fast a user wants to send/receive data.

   These attributes are negotiated and defined at the time of the contract between the user and the network service provider.

   Table 4.2 summarises user-related attributes:

Table 4.2: User-Related QoS Attributes

Attribute	Description
Sustained Cell Rate (SCR)	This is the average cell rate over a period of time, which could be more or less the actual transmission rates, as long as the average is maintained.
Peak Cell Rate (PCR)	This is the maximum transmission rate at a point of time.
Minimum Cell Rate (MCR)	This is the minimum cell rate that the network guarantees a user.
Cell Variation Delay Tolerance (CVDT)	This is a unit of measuring the changes in cell transmission times (i.e., what is the maximum and minimum delay between the delivery of any two cells).

2) **Network-Related Attributes:** These attributes define the characteristics of a network.

DOWNLOADED FROM KTUASSIST.IN

Scanned by CamScanner

Table 4.3 summarises network-related attributes:

Table 4.3: Network-Related QoS Attributes

Attribute	Description
Cell Loss Ratio (CLR)	This attribute defines the fraction of the cells lost/delivered too late during transmission.
Cell Transfer Delay (CTD)	This is the average time required for a cell to travel from the source to the destination.
Cell Delay Variation (CDV)	This is the difference between the maximum and minimum values of CTD.
Cell Error Ratio (CER)	This parameter defines the fraction of cells that contained errors.

INTERNETWORKING

Ques 7) What is internetworking?

Ans: Internetworking

As the computer got smaller, cheaper and yet more powerful, more and more organisations, companies and people began having their own private network, even internetworks in case of large organisations.

Most of them wanted to join the rest of the information world by further connecting to the internet. Some of organisations used internet as a vehicle of communication between their remotely located private networks/internetworks.

All of these developments saw the internetworking technology to evolve as an important technology. An internetwork is a collection of individual networks, connected by intermediate networking devices, that functions as a single large network. There are various types of networks like LAN, MAN, WAN.

An internetwork may also be defined as a network of computer communication networks every authorised member of which could communication with every other authorised member directly or indirectly.

When two or more networks are interconnected, such extended network is referred to as internetwork.

Figure 4.7 shows interconnection of two WANs and one LAN.

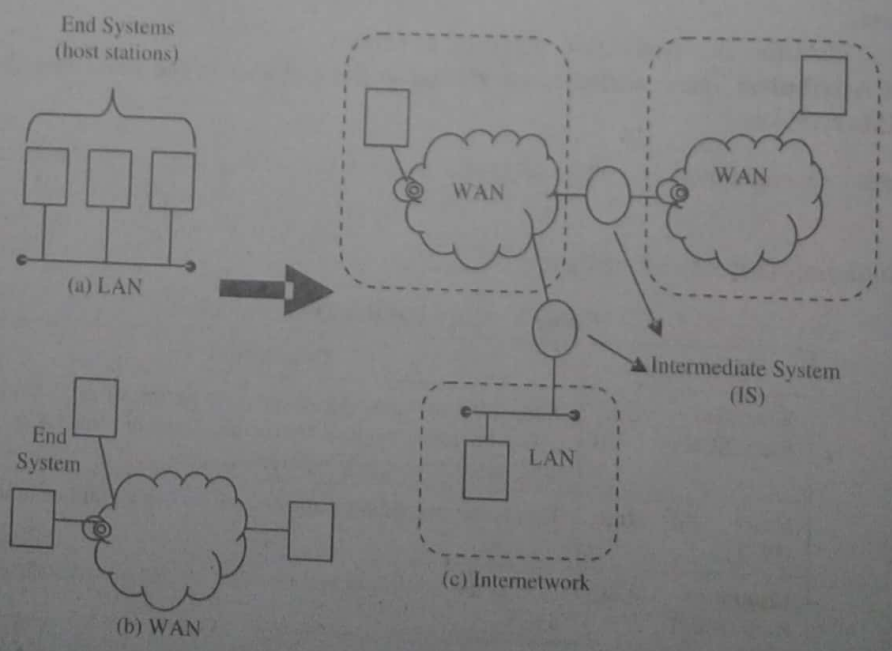


Figure 4.7: Internetworking

For example, consider **figure 4.8** which consists of a simple internetwork consisting of four routers. The routers are interconnected by point-to-point WAN links. The routers also connect to the local area networks.

DOWNLOADED FROM KTUASSIST.IN

Scanned by CamScanner

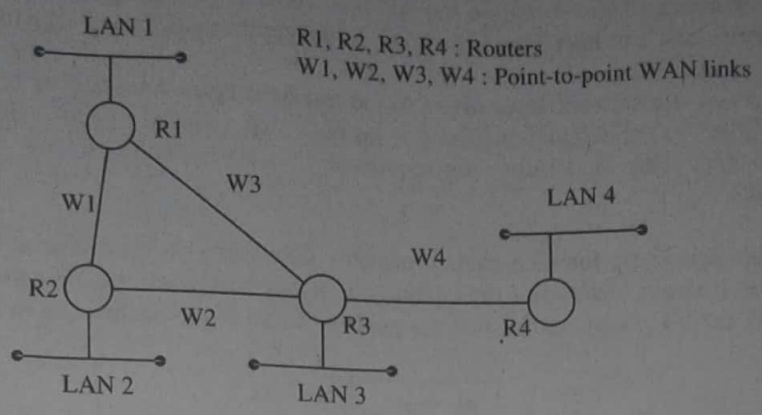


Figure 4.8: Internetwork

Ques 8) What are the different types of internetworking?

Or

Discuss about the concatenated virtual circuit and connectionless internetworking.

Or

What problem occures in connectionless internetworking?

Ans: Different Types of Internetworking

Two styles of internetworking are common:

1) **Concatenated Virtual Circuit:** In the concatenated virtual circuit model, shown in **figure 4.9** a connection to a host in a distant network is set up in a way similar to the way connections are normally established. The subnet sees that the destination is remote and builds a virtual circuit to the router nearest the destination network. Then it constructs a virtual circuit from that router to an external "gateway" (multiprotocol router). This gateway records the existence of the virtual circuit in its tables and proceeds to build another virtual circuit to a router in the next subnet. This process continues until the destination host has been reached.

   Once data packets begin flowing along the path, each gateway relays incoming packets, converting between packet formats and virtual circuit numbers as needed. Clearly, all data packets must traverse the same sequence of gateways, and thus arrive in order.

   Figure 4.9 shows the connection made with a full gateway; it could equally well be done with half-gateways.

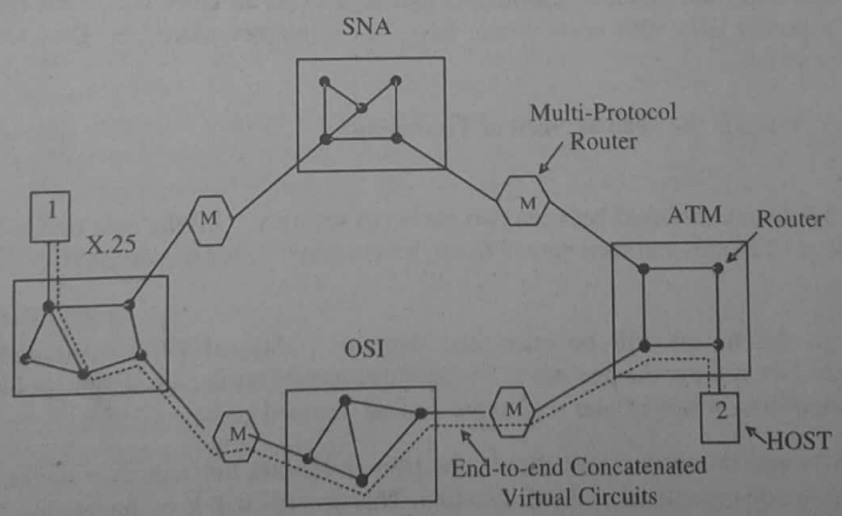


Figure 4.9: Internetworking using Concatenated Virtual Circuits

The **essential feature** of this approach is that a sequence of virtual circuits is set up from the source through one or more gateways to the destination. Each gateway maintains tables telling which virtual circuits pass through it, where they are to be routed, and what the new virtual circuit number is. Concatenated virtual circuits are also common in transport layer.

In particular it is possible to build a bit pipe using say, SNA which terminates in a gateway to the next gateway. Hence, end-to-end virtual circuit can be built spanning different networks and protocols.

DOWNLOADED FROM KTUASSIST.IN

Scanned by CamScanner

2) **Connectionless Internetworking:** The alternative internetwork model is the datagram model, shown in **figure 4.10**. In this figure datagrams from host 1 to host 2 are shown taking different routes through the internetwork.

In this model, the only service the network layer offers to the transport layer is the ability to inject datagrams into the subnet and hope for it will get to the destination. There is no notion of a virtual circuit at all in the network layer, let alone a concatenation of them. This model does not require all packets belonging to one connection to traverse the same sequence of gateways.

A routing decision is made separately for each packet, possibly depending on the traffic at the moment the packet is sent. This strategy can use multiple routes and thus achieve a higher bandwidth than the concatenated virtual circuit model. On the other hand, there is no guarantee that the packets arrive at the destination in order, assuming that they arrive at all.

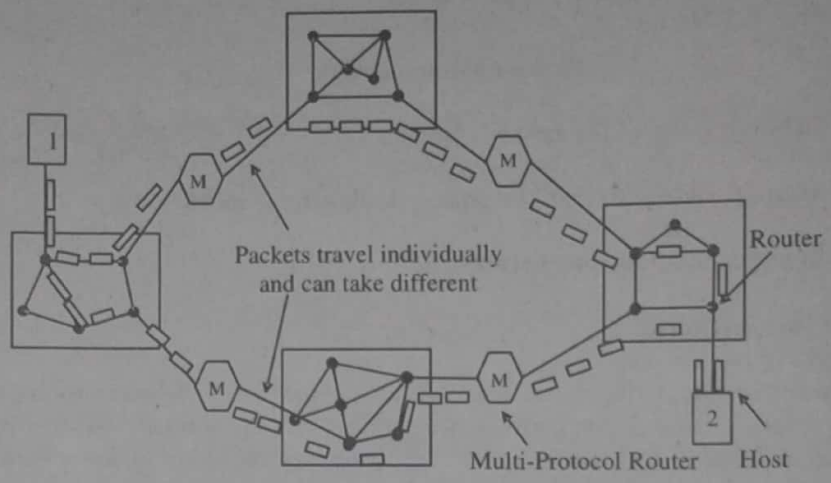


Figure 4.10: Connectionless Internet

Problems in Connectionless Internetworking

i) **Conversion:** If each network has its own network layer protocol, it is not possible for a packet from one network to transit another one. Multiprotocol routers tries to translate from one format to another, but such conversions will always be incomplete and often move to failure unless the two formats are close relatives with the same information fields,. For this reason, conversion is rarely attempted.

ii) **Addressing:** Imagine a simple case: a host on the Internet is trying to send an IP packet to a host on an adjoining OSI network. The OSI datagram protocol. Problem is that IP packets all carry the 32-bit Internet address of the destination host in a header field. OSI hosts do not have 32-bit Internet addresses. They use decimal addresses similar to telephone numbers.

Ques 9) What is tunneling? What is the need of Need of Tunneling?

Ans: Tunneling

"Tunneling is a way in which data is transferred between two networks securely." All the data that is being transferred are fragmented into smaller packets or frames and then passed through the tunnel. This process is different from a normal data transfer between nodes.

Every frame passing through the tunnel will be encrypted with an additional layer of tunneling encryption and encapsulation which is also used for routing the packets to the right direction. This encapsulation would then be reverted at the destination with decryption of data which is later sent to the desired destined node.

A tunnel is a logical path between the source and the destination endpoints between two networks. Every packet is encapsulated at the source will be de-capsulated at the destination. This process will keep happening as long as the logical tunnel is persistent between the two endpoints.

Need of Tunneling

Handling the general case of making two different networks inter work is exceedingly difficult. However, there is a common special case that is manageable. This case is where the source and destination hosts are on the same type of network, but there is a different network in between.

For example, consider International bank with a TCP/IP based Ethernet in Delhi, a TCP/IP based Ethernet in Mumbai, and a PTT WAN in between, as shown in **figure 4.11.**

DOWNLOADED FROM KTUASSIST.IN

Scanned by CamScanner

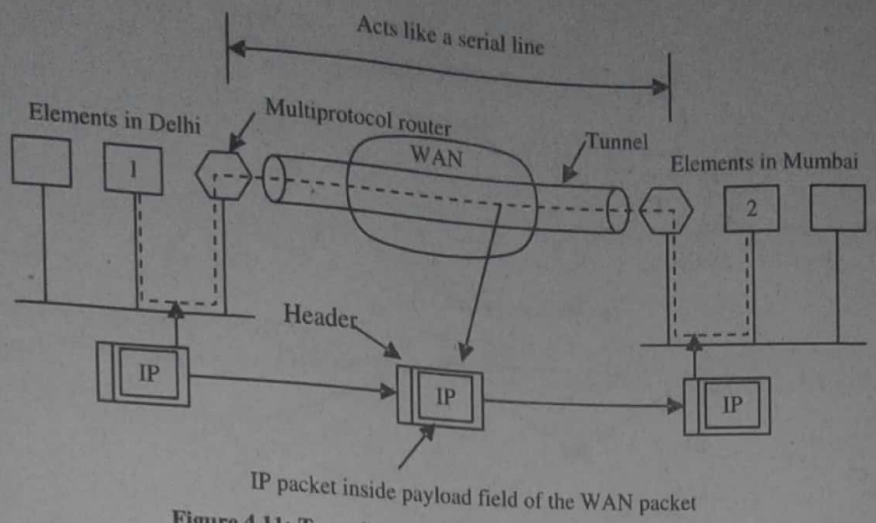


Figure 4.11: Tunneling a Packet from Delhi to Mumbai

The solution to this problem is a technique called **tunneling**. To send an IP packet to host 2, host 1 constructs the packet containing the IP address of host 2, inserts it into an Ethernet frame addressed to the Delhi multi-protocol router, and puts it on the Ethernet. When the multi-protocol router gets the frame, it removes the IP packet, inserts it in the payload field of the WAN network layer packet, and addresses the latter to the WAN address of the Mumbai multi-protocol router. When it gets there, the Mumbai router removes the IP packet and sends it to host 2 inside an Ethernet frame.

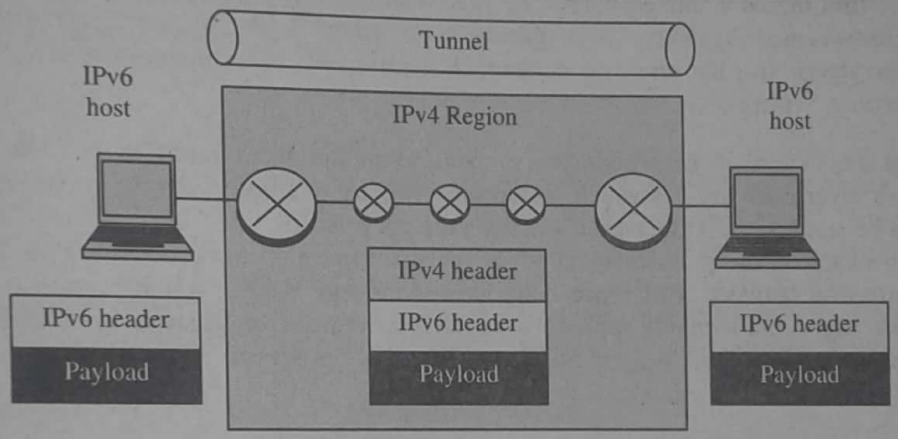


Figure 4.12: Tunneling

Tunneling is a strategy used when two computers using IPv6 want to communicate with each other when the packet must pass through a region that uses IPv4. To pass through this region, die packet must have an IPv4 address. So, the IPv6 packet is encapsulated in an IPv4 packet when it enters die region, and the IPv6 packet leaves its capsule when it exits die region. It seems as if die IPv6 packet enters a tunnel at one end and emerges at the other end. To make it clear that the IPv4 packet is carrying an IPv6 packet as data, the protocol value is set to 41. (**Figure 4.12**)

Ques 10) What are the advantages of tunneling?

Ans: Advantages of Tunneling

1) Uses IP for multiprotocol encapsulation.
2) Supports additional applications without having to change firewall.
3) Allows network-based authentication.
4) Supports compression for improved throughput.

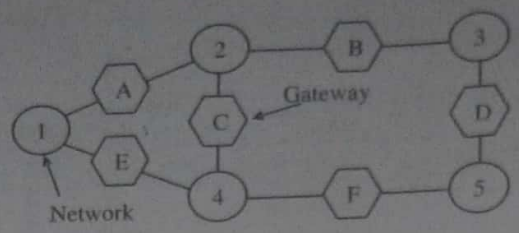
Ques 11) What is internetwork routing?

Ans: Internetwork Routing

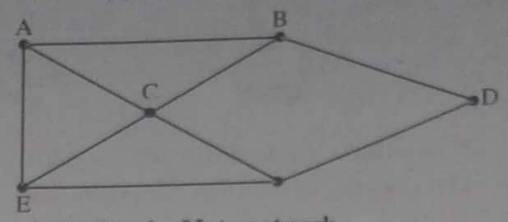
Routing through an internetwork is called internetwork routing. Routing through an internetwork is similar to routing within a single subnet, but with some added complications.

For example, the internetwork of **figure 4.13(a)** in which five networks are connected by six multiprotocol routers. Making a graph model of this situation is complicated by the fact that every multiprotocol router can directly access (i.e., send packets to) every other router connected to any network to which it is connected. B in **figure 4.13(a)** can directly access A and C via network 2 and also D *via* network 3. This leads to the graph of **figure 4.13(b).**

DOWNLOADED FROM KTUASSIST.IN
Scanned by CamScanner



(a) Internetwork



(b) Graph of Internetwork

Figure 4.13:

Once the graph has been constructed, known routing algorithms, such as the distance vector and link state algorithms, can be applied to the set of multiprotocol routers. This gives a **two-level routing algorithm.**

Two-level routing algorithm means within each network an interior gateway protocol is used, but between the networks, an exterior gateway protocol is used ("gateway" is an older term for "router"). In fact, since each network is independent, they may all use different algorithms. Because each network in an internetwork is independent of all the others, it is often referred to as an Autonomous System (AS).

A typical internet packet starts out on its LAN addressed to the local multiprotocol router (in the MAC layer header). After it gets there, the network layer code decides which multiprotocol router to forward the packet to, using its own routing tables. If that router can be reached using the packet's native network protocol, it is forwarded there directly. Otherwise it is tunneled there, encapsulated in the protocol required by the intervening network. This process is repeated until the packet reaches the destination network. Difference between interior and exterior routing is the cost. Within a single network, a single charging algorithm normally applies. However, different networks may be under different managements, and one route may be less expensive than another. Similarly, the quality of service offered by different networks may be different, and this may be a reason to choose one route over another.

Ques 12) What is fragmentation?

Or

What are the different fragmentation strategies?

Ans: Fragmentation

Fragmentation literally means the breaking up of data into smaller packets. The maximum packet size is dependent on various factors like:

1) Width of TDM slot
2) Protocols used
3) Types of operating system
4) International standards
5) Efforts to reduce retransmission
6) Desire to avoid the same packet occupy the channel for too long.

When a large packet wants to travel in the network for long but its maximum packet size is too small then there is a problem. The solution to this problem is **fragmentation**. In this technique gateways break packets up into fragments, and sending each fragment as a separate internet packet. However, converting a large object into small fragments is considerable easier than the other way round. Packet-switching networks also face trouble in putting the fragments back together again.

Strategies of Fragmentation

There are strategies that recombine the fragments back into the original packet.

1) **Transparent Fragmentation Strategy** is to make fragmentation caused by a "small packet" network transparent to any subsequent networks through which the packet passes on its way to the final destination. This is shown in **Figure 4.14**. When an oversized packet comes at a gateway, the gateway breaks it up into fragments. Each fragment is addressed to the same exit gateway, where the pieces are reassembled. In this way passage through the small packet network is made transparent. Subsequent networks are not even aware of fragmentation.

DOWNLOADED FROM KTUASSIST.IN

Scanned by CamScanner

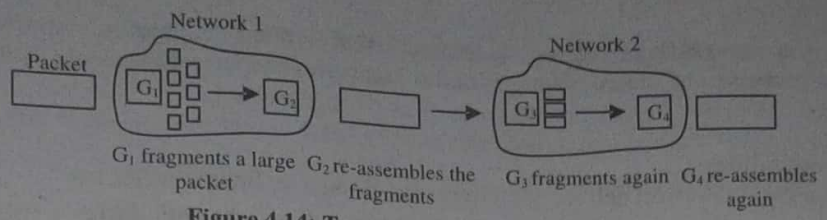


Figure 4.14: Transparent Fragmentation

2) **Non-Transparent Fragmentation strategy** is – Once a packet has been fragmented to treat each fragment an original packet. All fragments are then passed through the exit gateway, as shown in **Figure 4.15**. Reassembly takes place only at the destination host.

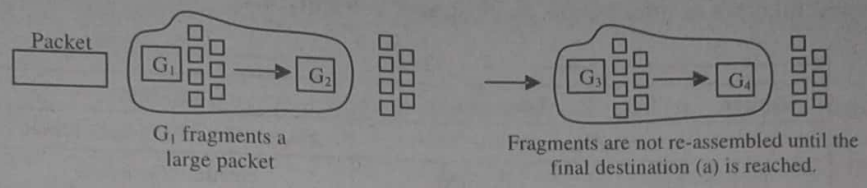


Figure 4.15: Non-Transparent Fragmentation

NETWORK LAYER IN INTERNET

Ques 13) Give the introduction of TCP/IP protocol?

Ans: TCP/IP Protocol Suite

The transmission Control Protocol/Internet Protocol (TCP/IP) was originally developed by the Department of Defense (DoD) for communications between computers. It is built into the UNIX system and has become the de facto standard for data transmission over networks, including the Internet. The TCP/IP protocols were originally designed for a large network that served as a classified DoD project designed to maintain open communications even during war time periods. This classified project was undertaken by a branch of the DoD known as Advanced Research Projects Agency (ARPA). This project became known as ARPANet. With the advent of Unix and the advancement of client/server networking architecture, ARPANet was declassified in the 80s and it is now known as the Internet. The TCP\IP holds the Internet together is the network layer protocol. The TCP/IP protocol suite, also known as the internet Protocols, is a suite of industry-standard protocols and can handle just about any task for the user.

The **Internet Protocol (IP)** provides all of the Internet's data transport services. Every other Internet protocol is ultimately either layered a top Internet Protocol, or used to support Internet Protocol from below.

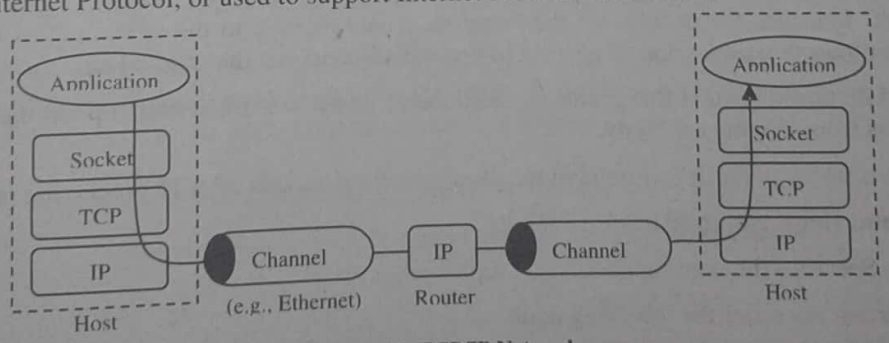


Figure 4.16: TCP/IP Network

The popularity of TCP/IP emanates from the fact that it is not proprietary to any company, it is suitable with any network software or equipment, and one can connect multiple LANs into a large Internet work.

Ques 14) What is internet protocol (IP)? Also give the frame format of IP?

Ans: Internet Protocol (IP)

Internet Protocol (IP) is a datagram-oriented protocol, treating each packet independently. Also Internet Protocol makes no attempt to determine if packets reach their destination or to take corrective action if they do not. Internet Protocol provides the following functions:

1) Addressing
2) Fragmentation
3) Packet timeouts

DOWNLOADED FROM KTUASSIST.IN

Scanned by CamScanner

Internet Protocol (IP) is a network-layer (Layer 3) protocol that contains addressing information and some control information that enables packets to be routed. Along with the Transmission Control Protocol (TCP), IP represents the heart of the Internet protocols.

IP has two primary responsibilities:
1) Providing connectionless, best-effort delivery of datagrams through an internetwork; and
2) Providing fragmentation and reassembly of datagrams to support data links with different maximum-transmission unit (MTU) sizes.

IP Packet Format
An IP packet contains several types of information, as illustrated in **Figure 4.17**.

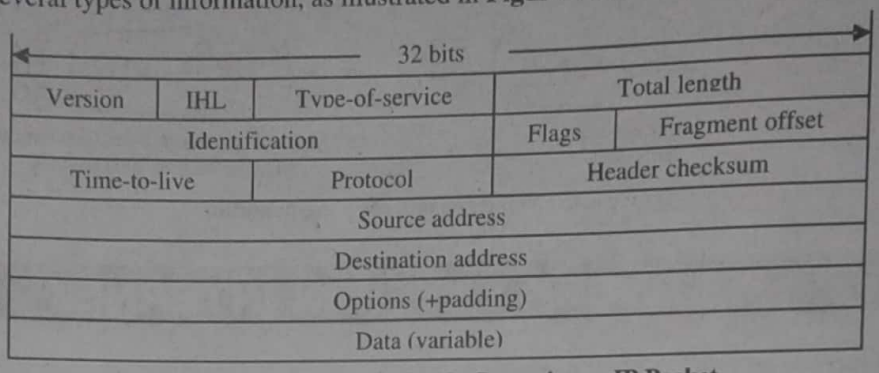


Figure 4.17: Fourteen Fields Comprise an IP Packet

1) **Version:** Indicates the version of IP currently used.
2) **IP Header Length (IHL):** Indicates the datagram header length in 32-bit words.
3) **Type-of-Service:** Specifies how an upper-layer protocol would like a current datagram to be handled, and assigns datagram various levels of importance.
4) **Total Length:** Specifies the length, in bytes, of the entire IP packet, including the data and header.
5) **Identification:** Contains an integer that identifies the current datagram. This field is used to help piece together datagram fragments.
6) **Flags:** Consists of a 3-bit field of which the two low-order (least-significant) bits control fragmentation. The low-order bit specifies whether the packet can be fragmented. The middle bit specifies whether the packet is the last fragment in a series of fragmented packets. The third or high-order bit is not used.
7) **Fragment Offset:** Indicates the position of the fragment's data relative to the beginning of the data in the original datagram, which allows the destination IP process to properly reconstruct the original datagram.
8) **Time-to-Live:** Maintains a counter that gradually decrements down to zero, at which point the datagram is discarded. This keeps packets from looping endlessly.
9) **Protocol:** Indicates which upper-layer protocol receives incoming packets after IP processing is complete.
10) **Header Checksum:** Helps ensure IP header integrity.
11) **Source Address:** Specifies the sending node.
12) **Destination Address:** Specifies the receiving node.
13) **Options:** Allows IP to support various options, such as security.
14) **Data:** Contains upper-layer information.

Ques 15) What is IP Addressing? Discuss its type.
Or
What is classful and classless addressing?
Or
Explain the IP frame format and IP address classes in detail.

Ans: IP Addressing
As with any other network-layer protocol, the IP addressing scheme is integral to the process of routing IP datagrams through an internetwork. Each IP address has specific components and follows a basic format. These IP addresses can be subdivided and used to create addresses for sub networks.

DOWNLOADED FROM KTUASSIST.IN
Scanned by CamScanner

Each host on a TCP/IP network is assigned a unique 32-bit logical address that is divided into two main parts:

1) **Network Number:** The network number identifies a network and must be assigned by the Internet Network Information Center (InterNIC) if the network is to be part of the Internet. An Internet Service Provider (ISP) can obtain blocks of network addresses from the InterNIC and can itself assign address space as necessary.
2) **Host Number:** The host number identifies a host on a network and is assigned by the local network administrator.

Types of IP Addressing

IP addressing can be two types:

1) **Classful Addressing:** In the classful addressing system all the IP addresses that are available are divided into the five classes A,B,C,D and E, in which class A,B and C address are frequently used because class D is for Multicast and is rarely used and class E is reserved and is not currently used. Each of the IP address belongs to a particular class that's why they are classful addresses.

   Earlier this addressing system did not have any name, but when classless addressing system came into existence then it is named as Classful addressing system. The main disadvantage of classful addressing is that it limited the flexibility and number of addresses that can be assigned to any device. One of the major **disadvantages of classful addressing** is that it does not send subnet information but it will send the complete network address. The router will supply its own subnet mask based on its locally configured subnets.

IP Address Format

The 32 bits IP address is divided into four octets and each octet is written in eight bit decimal numbers. These four octets are separated by dots and ranges from 0 to 255. The binary weights of each bit in the octet is 128, 64, 32, 16, 8, 4, 2, 1. The format of the 32-bit IP address is illustrated in the **figure 4.18**.

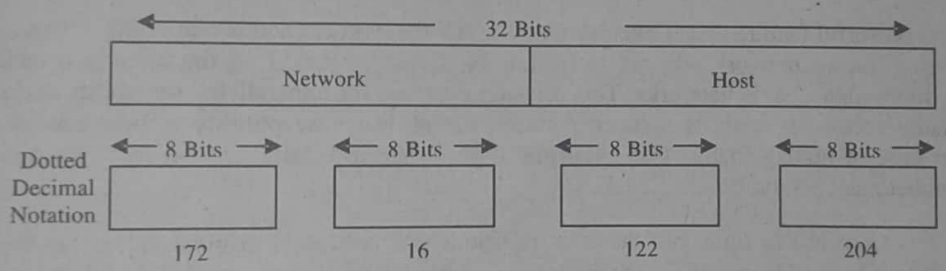


Figure 4.18: IP Address Format

IP Address Classes

A class is used to recognise the part of 'network address' and 'node address' given in an IP address. There are five classes associated with IP addresses: A, B, C, D and E where only A, B and C are used for commercial purpose.

The network class can be determined by examining the left most bits of the network address. The First octet from left of IP address constitute the network address of class A address, where First two octets from the network address of class B address and First 3 octets from the left constitute the network address of class C address.

The reference information of the five address classes are defined in the following **table 4.4**.

Table 4.4: Reference Information about Five IP Address Classes

IP Address Class	Format	Objective	High order Bit(s)	Address Range	No. of Bits Network/Host	Maximum Hosts
A	N.H.H.H	Few large organization	0	1.0.0.0. to 127.0.0.0	7/24	16,777, 216 (2^{24}-2)
B	N.N.H.H	Medium-size organization	1,0	128.1.0.0 to 191.254.0.0	14/16	65,536 (2^{16}-2)
C	N.N.N.H	Relatively small organization	1, 1, 0	192.0.1.0 to 223.255.254.0	22/8	256 (2^{8}-2)
D	N/A	Multicast groups (RFC 1112)	1, 1, 1, 0	224.0.0.0 to 239.255.255.255	N/A (not for commercial use)	N/A
E	N/A	Experimental	1, 1, 1, 1	240.0.0.0 to 240.255.255.255	N/A	N/A

Where, N = Network number, H = Host number.

For recognising the class of IP address examine the first octet of address and match it with already fixed range of the class. The following **table** illustrates the range of the various classes:

DOWNLOADED FROM KTUASSIST.IN

Scanned by CamScanner

Address Class	First Octet in Decimal	High-Order Bits
Class A	1 – 126	0
Class B	128 – 191	10
Class C	192 – 223	110

For example, consider an IP address 172.31.1.2. Its first octet is 172, so, it belongs to class B.

2) **Classless Addressing:** There were certain problems with classful addressing such as address depletion and less organisation access to Internet. To overcome these problems, classful addressing is replaced with classless addressing. As the name of the addressing scheme implies, the addresses are not divided into classes; however, they are divided into blocks and the size of blocks varies according to the size of entity to which the addresses are to be allocated. For example, only a few addresses may be allocated to a very small organisation while a larger organisation may obtain thousands of addresses IPv6 addressing is a classless addressing.

The Internet authorities have enforced certain limitations on classless address blocks to make the handling of addresses easier. These **limitations** are as follows:

i) The addresses of a block must be contiguous.
ii) Each block must have a power of 2(that is, 1, 2, 4, 8…) number of addresses.
iii) The first address in a block must be evenly divisible by the total number of addresses in that block.

Ques 16) What is Subnetting?
Or
What is subnet mask?

Ans: Subnetting
Subnetting is a unique and powerful feature that is exclusive to the TCP/IP protocol and is one of the reasons TCP/IP offers great scalability. Subnetting allows network address to be further divided, apart from the already established classful boundaries, into smaller, more manageable networks. This division provides for unparalleled scalability and hierarchy, and gives a network administrator benefits such as reduced network traffic, less susceptibility to broadcast traffic, network optimisation, and greater ease of management. **For example,** if you were to borrow one bit from the host portion of a Class B network, your subnet mask would be 255.255.128.0.

Remember, you borrow bits from left to right, but those bit positions still hold their original values, so the rightmost bit would be valued at 128. If you wanted to create four subnets, your subnet mask would read 255.255.192 because you have now borrowed two bits, one valued at 128 and another valued at 64. So, 128 + 64 = 192.

Subnet Mask
There are two parts to the IP address, the network portion and the host portion. Node assigned that IP address as well as other nodes that must communicate with it have no idea of the location of the line between host and network portions of the address. The subnet mask provides the answer to this dilemma. The subnet mask follows the IP address and details the line indicating where the network portion of the address ends and the host portion begin. Like the IP address, the subnet mask is in a 4-octet, 32-byte format.

An **example** of a subnet mask is 255.0.0.0. a value of 255 means match all. Each of the three configurable IP address classes has a default subnet mask:

1) Class A 255.0.0.0
2) Class B 255.255.0.0
3) Class C 255.255.255.0

Ques 17) Find the class of each address:
1) 4.23.145.90
2) 227.34.78.7
3) 246.7.3.8
4) 29.6.8.4
5) 198.76.9.23

Ans: The first byte defines the class.
1) Class A
2) Class D
3) Class E
4) Class B
5) Class C

DOWNLOADED FROM KTUASSIST.IN

Scanned by CamScanner

Ques 18) IP address 172. 31. 192. 166 and subnet mask 255. 255. 255. 248, which subnet does the IP address belong.

Ans:
Host id is .248
i.e. it uses 5 bit
i.e. host = $2^5 = 32$
i.e.

Ist	subnet network address	172. 31. 192. 0
IInd	subnet network address	172. 31. 192. 32
IIIrd	subnet network address	172. 31. 192. 64
IVth	subnet network address	172. 31. 192. 96
Vth	subnet network address	172. 31. 192. 128
VIth	subnet network address	172. 31. 192. 160
VIIth	subnet network address	172. 31. 192. 192
VIIIth	subnet network address	172. 31. 192. 224

So the IP address 172.31.192.166 lies in the VIth subnet network then the subnet network is 172.31.192.160

Ques 19) Explain IPv4 with its datagram format?

Ans: IPv4 (Internet Protocol Version 4)
The Internet Protocol version 4 (IPv4) is the delivery mechanism used by the TCP/IP protocols. **Figure 4.19** shows the position of IPv4 in the suite.

IPv4 is an unreliable and connectionless datagram protocol – a best-effort delivery service. The term best-effort means that IPv4 provides no error control or flow control (except for error detection on the header). IPv4 assumes the unreliability of the underlying layers and does its best to get a transmission through to its destination, but with no guarantees.

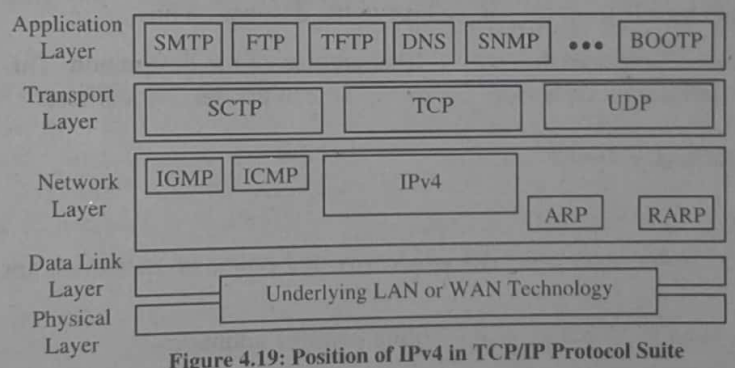


Figure 4.19: Position of IPv4 in TCP/IP Protocol Suite

IPv4 Datagram Format
Packets in the IPv4 layer are called datagrams. **Figure 4.20** shows the IPv4 datagram format.

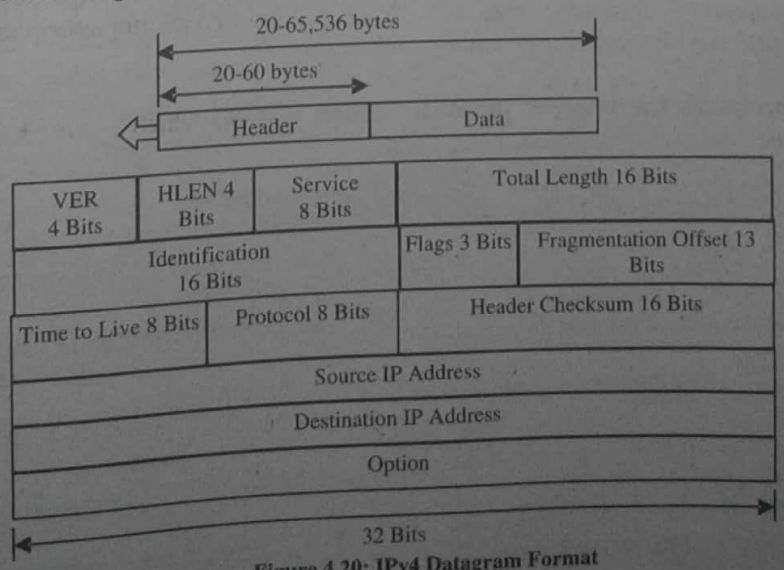


Figure 4.20: IPv4 Datagram Format

DOWNLOADED FROM KTUASSIST.IN

Scanned by CamScanner

A datagram is a variable-length packet consisting of two parts: header and data. The header is 20 to 60 bytes in length and contains information essential to routing and delivery. It is customary in TCP/IP to show the header in 4-byte sections. A brief description of each field is in order:

1) **Version (VER):** This 4-bit field defines the version of the IPv4 protocol. Currently the version is 4. However, version 6 (or IPng) may totally replace version 4 in the future.

2) **Header Length (HLEN):** This 4-bit field defines the total length of the datagram header in 4-byte words. This field is needed because the length of the header is variable (between 20 and 60 bytes).

3) **Services:** IETF has changed the interpretation and name of this 8-bit field. This field, previously called service type, is now called differentiated services.

4) **Total Length:** This is a 16-bit field that defines the total length (header plus data) of the IPv4 datagram in bytes. The header length can be found by multiplying the value in the HLEN field by 4.

   Length of Data = Total Length – Header Length

5) **Identification:** This field is used in fragmentation.

6) **Flags:** This field is used in fragmentation.

7) **Fragmentation Offset:** This field is used in fragmentation.

8) **Time to Live:** This field was originally designed to hold a timestamp, which was decremented by each visited router.

9) **Protocol:** This 8-bit field defines the higher-level protocol that uses the services of the IPv4 layer. An IPv4 datagram can encapsulate data from several higher-level protocols such as TCP, UDP, ICMP and IGMP. This field specifies the final destination protocol to which the IPv4 datagram is delivered.

10) **Checksum:** The checksum in the IPv4 packet covers only to header and not data.

11) **Source Address:** This 32-bit field defines the IPv4 address of the source. This field must remain unchanged during the time the IPv4 datagram travels from the source host to the destination host.

12) **Destination Address:** This 32-bit field defines the IPv4 address of the destination. This field must remain unchanged during the time the IPv4 datagram travels from the source host to the destination host.

Ques 20) What are the limitations of Ipv4?

Ans: Limitations of Ipv4

1) The IP address relies on network layer addresses to identify end-points on networks, and each networked device has a unique IP address.

2) Uses a 32-bit addressing scheme, which gives it 4 billion possible addresses.

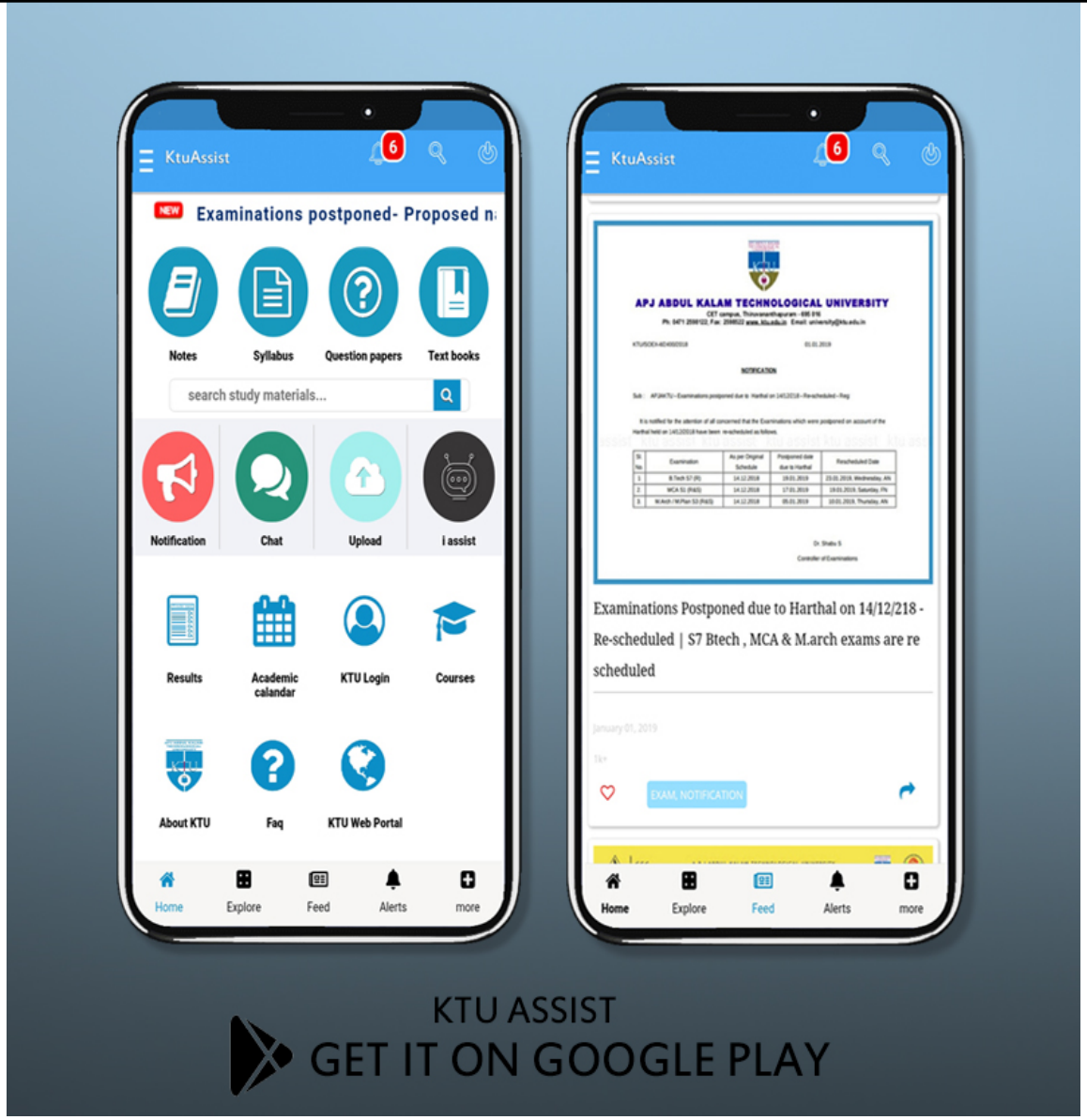
3) If a network has slightly more number of hosts than a particular class, then it needs either two IP addresses of that class or the next class of IP address.

4) Identified limitations of the Ipv4 protocol are: Complex host and router configuration, non-hierarchical addressing, difficulty in re-numbering addresses, large routing tables, non-trivial implementations in proving security, QoS (Quality of Services), mobility and multi-homing, multicasting etc.

To **overcome these problems the internet protocol version 6(Ipv6)** which is also known as internet protocol, next generation was proposed.

DOWNLOADED FROM KTUASSIST.IN

Scanned by CamScanner



END

facebook.com/ktuassist

instagram.com/ktu_assist