CONGESTION

occur 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 allowed by network resources. for example, Congestion may occur because the switched in a network have a limited buffer size to store arrived packets before processing

Causes of Congestion

1: Unpredictable statistical fluctuation of traffic flows

2: faults conditions within the network

3: Slow processor speed. if the router's CPU speed is very low and performing tasks like queuing buffer, tables updating etc. queries are built up, even though the line capacity is not fully utilized

4: Inefficient control policies

5: Bandwidth of the links is important in Congestion. The links to be used must be of high Bandwidth to avoid Congestion

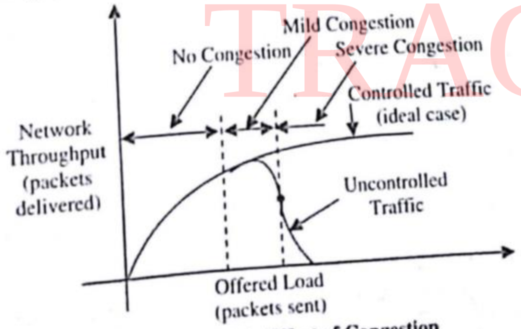


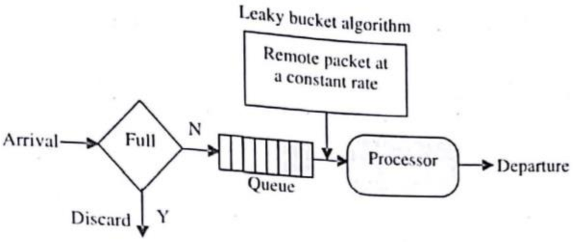
Figure 4.1: Effect of Congestion

TYPES OF CONGESTION CONTROL ALGORITHMS

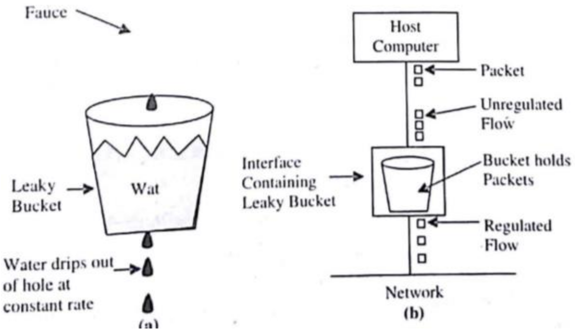
Congestion in a frame relay network is a problem that must be avoided because it decreases throughput and increases delay

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 leaky Bucket.

When a packet comes to a host with the queue full, it is discarded. The host 1s allowed to put one packet per clock tick info the network. This can he 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 word, 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 4ueue it is appended to the queue otherwise, it is discarded. At every clock tick, one packet is transmitted (unless the queue is empty).

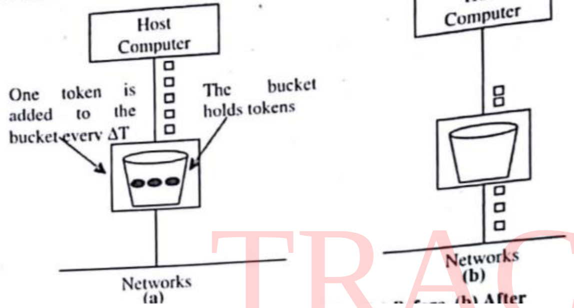
This arrangement can be simulated in the operating system or can be built into the hardware. Implementation of this algorithm is easy and consists of a finite queue. Whenever a packet arrives, if there is room in the queue it is queued up and if there is no room then the packet is discarded

2: Token Bucket Algorithm

This algorithm allows bursts for short transmission while making sure that no data is lost. In contrast to the Leaky Bucket algorithm, not the data that is to be send but tokens are queued in a time-depended queue. One token is needed to send a single portion of data Implementations contain a token counter that is incremented on every time interval, so that the counter grows over time up until a maximum counter value is reached. The token counter is decremented by one for every data portion sent. When the token counter is zero no data can be transmitted.

For many applications it is better to allow the output to speed up somewhat when a larger burst arrives than to lose the data. Token Bucket algorithm provides such a solution.

be transmitted, it must capture and destroy one



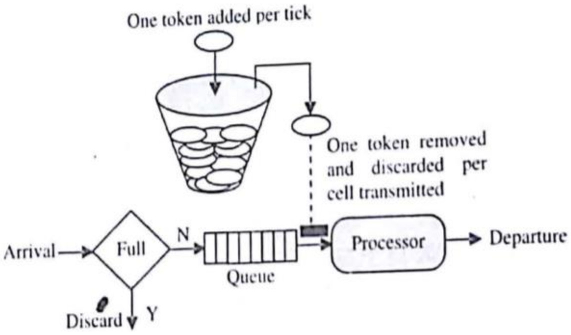
Main steps of this algorithm can be described as follows:

* In regular intervals tokens are thrown into the bucket.

* The bucket has a maximum capacity.

* If there is a ready packet, a token is removed from the bucket, and the packet is send.

* If there is no token in the bucket, the packet cannot be send.



Token Bucket Algorithm

*Token dependent

*If bucket is full token are discarded, but not the packet.

*Packets can only transmitted when there are enough token.

*It allows large bursts to he sent at faster rate after that constant rate.

*It saves token to send large bursts.

Leaky Bucket Algorithm

*Token independent

*If bucket is full packet or data is discarded.

*Packets are transmitted continuously.

*It sends the packet at constant rate.

*It does not save token.

QUALITY OF SERVICE

is defined as something 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 vi, 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 attributes.

flow Characteristics

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

2: Delay: Source-to-destination delay is another characteristic Again application can tolerate delay in different degree. In this case, telephony, audio conferencing, video conferencing and remote login 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.

QoS Attributes

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

The Attributes are negotiated and defined at the time of the contact between the user and the network service provider

*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 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 guarantee a user

*Cell Variation Delay Tolerance(CVDT): This is a unit of measuring the changes in cell transmission times

2: Network Related Attributes: These Attributes defines the chara of a network

*Cell Loss Ratio(CLR): This Attribute define the fraction of cells lost/delivered too late during transmission

*Cell Transfer Delay(CTD): This is the average time required for a cell travel from the source to destination

*Cell Delay Variation(CDV): This is the difference between maximum and minimum values of CTD

*Cell Error Ratio(CER): This parameter defines the ratio of cells that contain errors

INTERNETWORKING

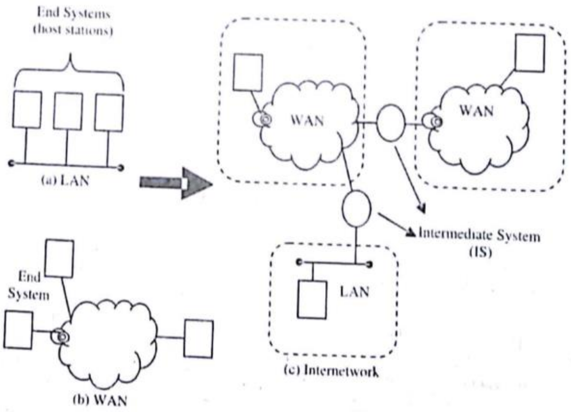
As the computer got smaller, cheaper and yet more powerful. more and more organisation, companies and people began having their own private network, even Internetworks in case of large organisations

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

All of these development saw the Internetworking technology to evolve as an important technology. an Internetworking is a collection of individual networks, connected by intermediate networking devices, that function as a single large network. there are various types of networks like LAN,WAN,MAN

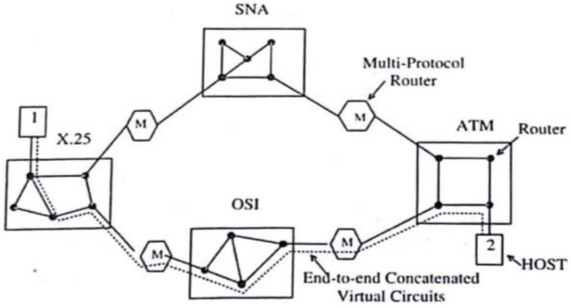
An Internetwork may also be defined as a network of computer communication network every authorised member of which could communication with every other authorised member directly or indirectly

Shows Interconnection Of 2 WAN and 1 LAN



Types or Internetworking

1: Concatenated Virtual Circuit: In the concatenated virtual circuit model, shown in figure 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

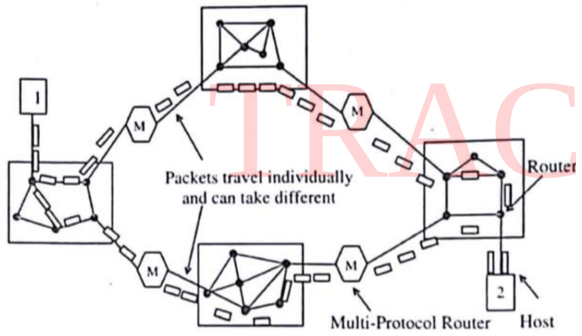


The essential feature of this approach is that a sequence of virtual circuits is set up from the source through one or more gateways to the destination. Each gateway maintains tables telling which virtual circuits pass through it.

2: Connectionless internetworking: The alternative internetwork model is a the datagram model, in this figure datagram from host 1 to host 2 are shown taking different routes through the internetwork

In this model, the only service t11e network layer offers to the transport layer is the ability to inject datagram into the subnet and hope for it will get to the destination. There is no notion of 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 or 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



Problems in Connectionless Internetworking

1: 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.

2: 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

INTERNET PROTOCOL (IP)

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

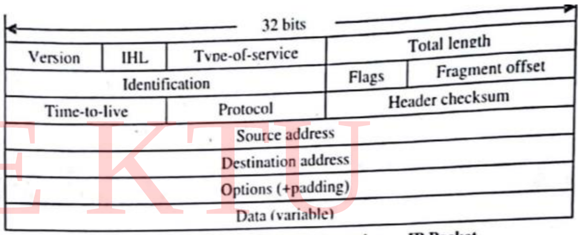
Internet Protocol (IP) is a network layer (Layer 3) protocol chat contains addressing information and some control information that enables packets to be routed. Along with the transmission Control Protocol(TCP), IP represents the heart of the Internet protocols.

IP has two primary responsibilities

1: Providing Connectionless, best effort delivery of datagram through an internetwork

2: Providing fragmentation and reassembly of datagram to support data links with different maximum transmission unit(MTU) sizes

IP Packet Format



Version	IHL	Type-of-service	Total length
Identification		Flags	Fragment offset
Time-to-live	Protocol	Header checksum	
Source address			
Destination address			
Options (+padding)			
Data (variable)			

Figure 4.17: Fourteen Fields Comprise an IP Packet

1: Version: Indicates the version of IP currently used.

2: IP Header Length (1HL): 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 tow-order (least-significant) bits control fragmentation.

7: Fragment Offset: Indicates the position of the fragment's data relative to the beginning of the data in the original datagram

8: Time-to-Live: Maintains a counter that gradually decrements down to zero, at which point the datagram is discarded.
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 1he 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.

IP ADDRESSING

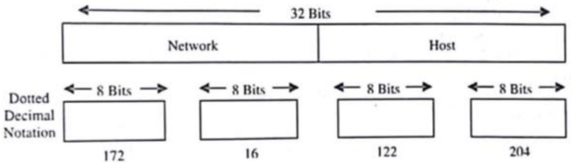
As with any other network-layer protocol, the IP addressing scheme is integral to the process of routing IP datagram through internetwork. Each IP address has specific components and follows a basic format These IP addresses can be subdivided and used to create addresses for sub networks.
1: Network Number: It identifies a network and must be assigned by the internet network information centre(InterNIC) if the network is to be part of internet. an ISP can obtain block of network addresses from InterNIC and can itself assign address space as necessary
2: Host Number: It identifies a host on a network and assigned by the local network administrator

TYPES OF IP ADDRESSING

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

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 octet are separated by dots and ranges from O 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



IP Address Classes
A class is used to recognise the part of network address and node address given in an IP address. There are 5 classes associated with IP addresses. A,B,C,D,E where A,B,C are used for commercial purpose

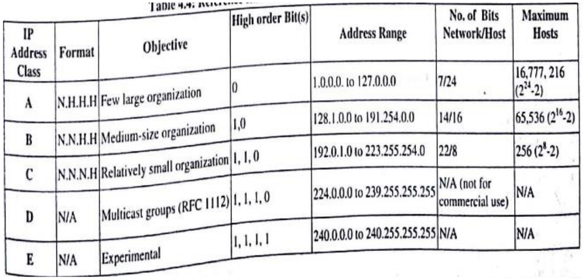
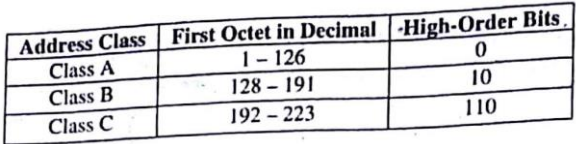


Table 4.4:

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



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

2: Classless Addressing: There were certain problems with classful addressing such as address depletion and less organization access to internet. to overcome these problems, classful addressing is replaced with Classless addressing. as the name of Addressing schemes implies, the address 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. IPv6 is classless addressing
The Internet authorities have enforced certain limitations on classing 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.

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

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

IPv4 (INTERNET PROTOCOL VERSION 4)

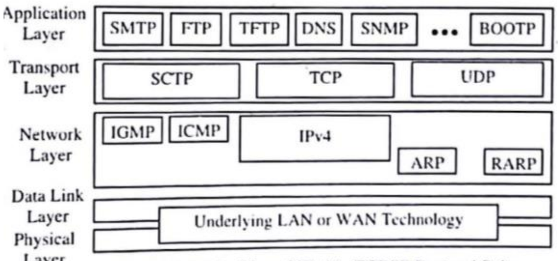
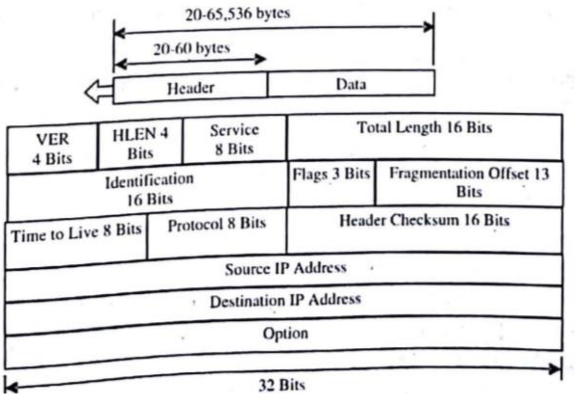


Figure 4.19: Position of IPv4 in TCP/IP Protocol Suite

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.

IPv4 Datagram Format



Limitation of IPv4

1: The IP address relies on network layer address 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 host 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 renumbering address large routing tables, non-trivial implementations in providing security. QoS (Quality of Services) mobility and multi-homing, multicasting etc.