18CS504

Hall Ticket Number:

III/IV B.Tech Regular DEGREE EXAMINATION

February, 2021 — **Computer Science & Engineering**

Fifth Semester — **Computer Networks**

Time: Three Hours — **Maximum :** 50 Marks

Answer Question No.1 compulsorily. (1X10 = 10 Marks)

Answer any four questions. (4X10=40 Marks)

1 Answer all questions (1X10=10 Marks)

a) Define Protocol.
b) What are the services provided by Data Link Layer?
c) What is Data Communication System?
d) What is store and forward switching?
e) What is the Purpose of flooding?
f) Define congestion.
g) Write the differences between IP address and port number.
h) What is the purpose of ICMP?
i) Differentiate TCP and UDP.
j) What is DNS?

UNIT I

2 a) Explain about the components of a Data Communication System? 5M
b) Write about Data Communication Tasks? 5M

(OR)

3 Explain in detail about the OSI Reference Model? 10M

UNIT II

4 What is Flow Control? Explain about Stop &Wait and Sliding Window Flow Control Mechanisms. 10M

(OR)

5 a) Discuss about Congestion Control in Virtual-Circuit Subnets. 5M
b) Explain about Hierarchal Routing? 5M

UNIT III

6 a) Explain about Leaky Bucket Algorithm? 5M
b) Explain about Token Bucket Algorithm? 5M

(OR)

7 a) Explain about IPV4 Header format. 5M
b) Explain about Internet Control Protocols. 5M

UNIT IV

8 Discuss in detailed about the TCP Segment Header? 10M

(OR)

9 a) Discuss about Name spaces in DNS? 5M
b) Discuss about Resource Records in DNS? 5M

1 Answer all questions (1X10=10 Marks)

a) Define Protocol.
A protocol is a set of rules and guidelines for communicating data.

b) What are the services provided by Data Link Layer?
Framing, Flow Control, Error Detection, Error Correction

c) What is Data Communication System?
For Data Communication to occur, the communicating devices must be a part of a communication system made up of some specific kind of hardware and software This type of a system is known as a "DATA COMMUNICATION SYSTEM".

d) What is store and forward switching?
Store and forward is a data communication technique in which a message transmitted from a source node is stored at an intermediary device before being forwarded to the destination node.

e) What is the purpose of flooding?
Flooding is a way to distribute routing information updates quickly to every node in a large network.

f) Define Congestion.
Too many packets present in the network causes packet delay and loss that degrades performance. This situation is called congestion.

g) Write the differences between IP address and port number.
An IP address identifies a particular computer on the Internet.
The port number identifies a particular program running on that computer.

h) What is the purpose of ICMP.
ICMP is a mechanism used by hosts & routers to send notification of datagram problems Back to sender.

i) Differentiate TCP and UDP.
TCP is connection oriented – once a connection is established, data can be sent bidirectional.UDP is a simpler, connectionless Internet protocol.

j) What is DNS?
The Domain Name System (aka DNS) is used to resolve human-readable hostnames like www.Dyn.com into machine-readable IP addresses like 204.13.248.115.

UNIT I

2 a) Explain about the components of a Data Communication System? 5M

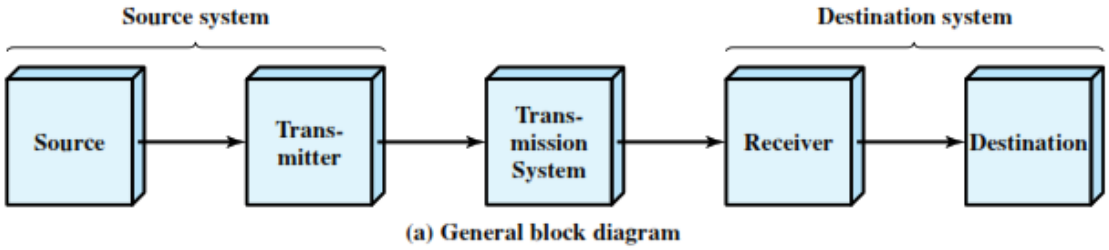
Source. This device generates the data to be transmitted; examples are telephones and personal computers.

Transmitter: Usually, the data generated by a source system are not transmitted directly in the form in which they were generated. Rather, a transmitter transforms and encodes the information in such a way as to produce electromagnetic signals that can be transmitted across some sort of transmission system. For example, a modem takes a digital bit stream from an attached device such as a personal computer and transforms that bit stream into an analog signal that can be handled by the telephone network.

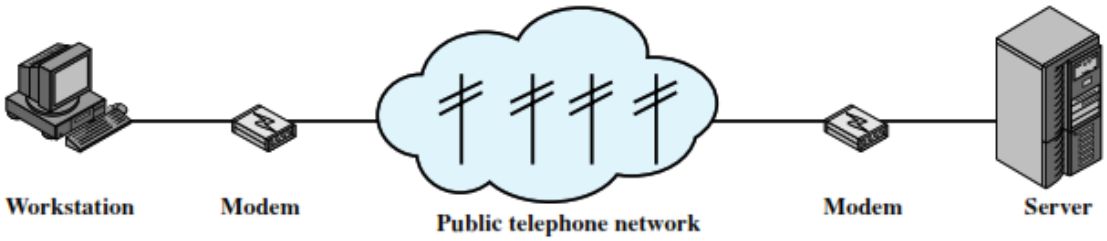
Transmission system: This can be a single transmission line or a complex network connecting source and destination.

Receiver: The receiver accepts the signal from the transmission system and converts it into a form that can be handled by the destination device. For example, a modem will accept an analog signal coming from a network or transmission line and convert it into a digital bit stream.

Destination: Takes the incoming data from receiver.



(a) General block diagram



(b) Example

b) Write about Data Communication Tasks? 5M

Transmission System Utilization :-Need to make efficient use of Transmission facilities that are shared among a no. of communicating devices.

Interfacing: Communication between the devices and transmission channel takes place with the help of Interface. Interface is the way; a computer presents information to users or receives information from users.

Signal Generation: After establishing an interface, the other job of communication system is to generate the signals. These signals can either be in analog or digital format and in the format that is easily understood by destination.

Synchronization :-The transmission and the reception should be properly synchronized. Synchronization means that the receiver must be able to determine, when to expect a new transmission and when to send acknowledgements. In other words transmitter and receiver should have an agreement on the nature as well as timing of the signals.

Exchange Management: - If the data needs to be exchanged in both directions over a period of time, both parties must cooperate as follows: Whether both devices must transmit simultaneously or take turns. Amount of Data to be sent at one time. Format of the Data. What to do when an Error Arises

Error Detection and Correction: -In all comm. Systems, there is a potential risk for errors and impairments. Signals are distorted to some extent before reaching their destination. Error Detection &Correction needs to be employed in Data Processing Systems where a change in say the contents of a file cannot be tolerated

Flow Control: - To make sure that source does not overwhelm destination by sending data faster than it can be handled and processed.

Addressing & Routing: -If TX facility is shared by two or more devices, source must specify the identity or the address of the destination system. Routing is a mechanism of choosing optimal path or shortest path through the network when different paths are available.

Recovery: -If a data transmission is interrupted due to a fault somewhere in the system, recovery techniques are needed. The objective is either to resume activity at the point of interruption and to restore the state of the system to what it was prior to the interruption

Message formatting: - sender and receiver must first agree on the format of data to be

exchanged which can either be i the form of signals or binary format.

Security:- is very important issue in a Data Communication System. The sender needs to be assured that Only the Intended receiver receives the data.

Network management: -Data communication facility is a complex system that cannot create or run itself. Network management capabilities are needed to configure the system, monitor its status, react to failures and overloads and plan intelligently.

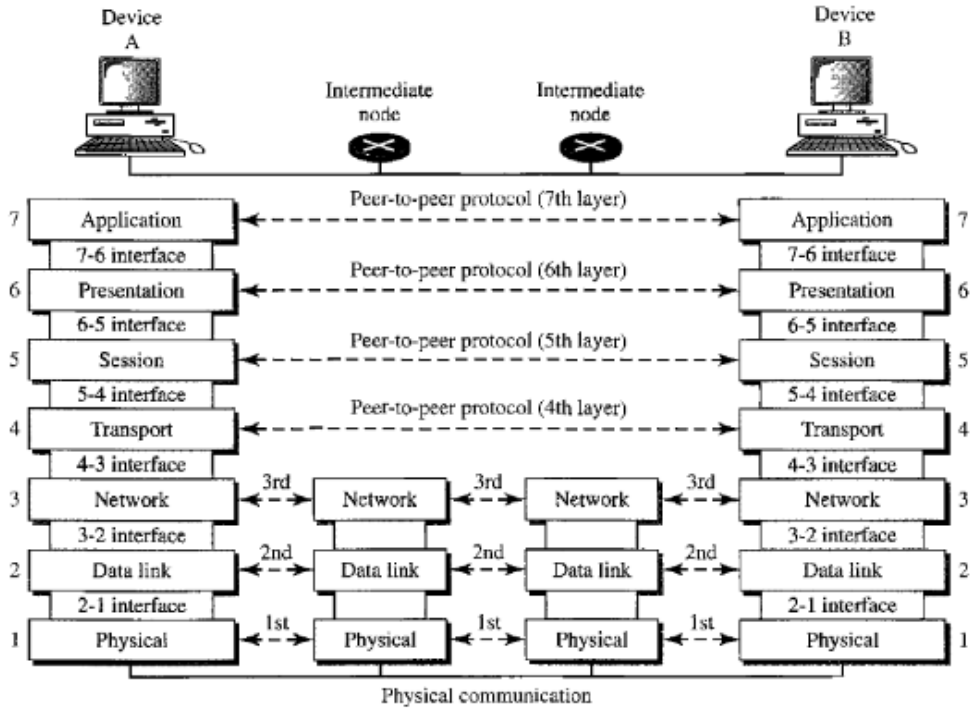
(OR)

3 Explain in detail about the OSI Reference Model? 10M

THE OSI MODEL: Established in 1947, the International Standards Organization (ISO) is a Multinational body dedicated to worldwide agreement on international standards. An ISO standard that covers all aspects of network communications is the Open Systems Interconnection (OSI) model. .

LAYERS IN THE OSI MODEL

- Physical Layer
- Data Link Layer
- Network Layer
- Transport Layer
- Session Layer
- Presentation Layer
- Application Layer



The physical layer: is responsible for movements of individual bits from one hop(node) to the next.

Duties of physical layer:

1. Physical characteristics of interfaces and medium:

It defines the characteristic of the interface between devices and media. It also defines the type of transmission media

2. Representation of bits: The bit stream must be encoded into signals. It defines the type of representation (how 0, 1 are changed to signal).
3. Data rate: It defines the number of bits sent per second and also the duration of bits.

Data link layer:-The data link layer is responsible for moving frames from one hop (node) to the next.

Duties of data link layer: -

1. Framing: Divide the stream of bits received from network layer into data units called frames.
2. Flow control: It imposes a flow control mechanism, if the data rate at the receiver is less than produced by sender the data link layer imposes a flow control to avoid overwhelming the receiver.
3. Access control: When two or more devices than one device are connected to the same link,

data link layer protocols are necessary to determine which device has control over the link at given time.

Network layer: The Network layer is responsible for the delivery of individual packets From source host to the destination host.

Duties of network layer:

1. Logical addressing: IP addresses: In contrast to physical addressing implemented by data link layer handling the addressing problem locally. Network layer adds unique identifier (IP or logical address) to the packet. These unique identifier (as tel. no, each tel. has unique number) enable special devices called router to make sure the packet get to correct system.
2. Routing:-Provide the routing mechanism for the router which route the packet to their final destination.

Transport layer: The transport layer is responsible for the delivery of a message from one process to another. Reliable process-to-process delivery of a message.

Duties of transport layer:-

1. Port addressing (Service-point addressing):Computer often run several process (running programs) at the same time, so the process to process delivery means delivery from a specific process on a computer to specific process to the other.
2. Segmentation and reassembly: A message is divided into small pieces (Segment), each segment containing sequence number. These number enable the transport layer to reassemble the message correctly at destination and to identify and replace segment that were lost in transmission.
3. Flow control: Like the data link layer, transport layer responsible for flow control. Flow control at this layer is performed end to end rather than across a signal link.

Session layer:- The session layer is responsible for dialog control and synchronization.

Duties of Session layer:

1. Dialog control: Allows two systems to enter into dialog. It allows communication between two processes in either half or full duplex.
2. Synchronization: Allow a process to add check points (Synchronization point) into a stream of data. So that if a failure of some sort occurs between checkpoints, the layer can retransmit all data since the last checkpoint.

Presentation layer:- The presentation layer is responsible for translation, compression, and encryption.

Duties of presentation layer:

1. Translation: At the sender it changes the information from its sender –dependent format

into common format. At receiving, changes the common format into its receiver dependent Format.

2. Encryption-Decryption: To ensure privacy and security

3. Compression: Data compression reduces the number of bits contained in the information. It is important in the transmission of multimedia such as audio or video.

Application layer: The application layer is responsible for providing services to the user. Specific services provided by the application layer include the following:

1. Network virtual terminal. A network virtual terminal is a software version of a physical terminal, and it allows a user to log on to a remote host. To do so, the application creates a software emulation of a terminal at the remote host. The user's computer talks to the software terminal which, in turn, talks to the host, and vice versa. The remote host believes it is communicating with one of its own terminals and allows the user to log on.

2. File transfer, access, and management. This application allows a user to access files in a remote host (to make changes or read data), to retrieve files from a remote computer for use in the local computer, and to manage or control files in a remote computer locally.

3. Mail services. This application provides the basis for e-mail forwarding and storage.

UNIT II

4 a) What is Flow Control? Explain about Stop&Wait and Sliding Window Flow Control. 10M

Flow Control: is a set of procedures that tells the sender how much data it can transmit before it must wait for an ACK from the receiver. The flow of data must not be allowed to overwhelm the receiver.

Stop and Wait: In this method, the sender waits for an ACK after every frame it sends**.** Only when an ACK has been received, is the next frame sent. This process of alternately sending and waiting repeats until the sender transmits an EOT frame.

Example: Officer giving dictation to the typist, He says a word, typist says OK, he says the next word, typist says OK and so on.

Advantages of Stop and Wait:

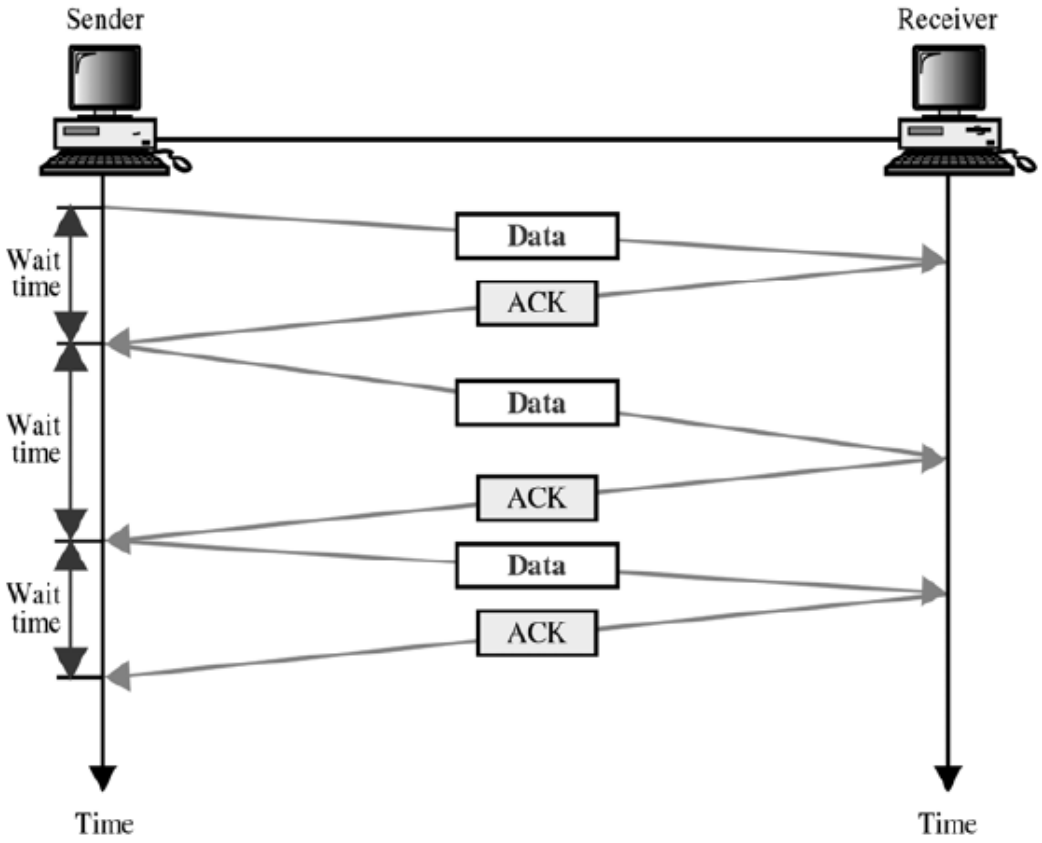
SIMPLICITY: Each frame is checked and acknowledged before the next frame is sent.

Disadvantages of Stop and Wait:

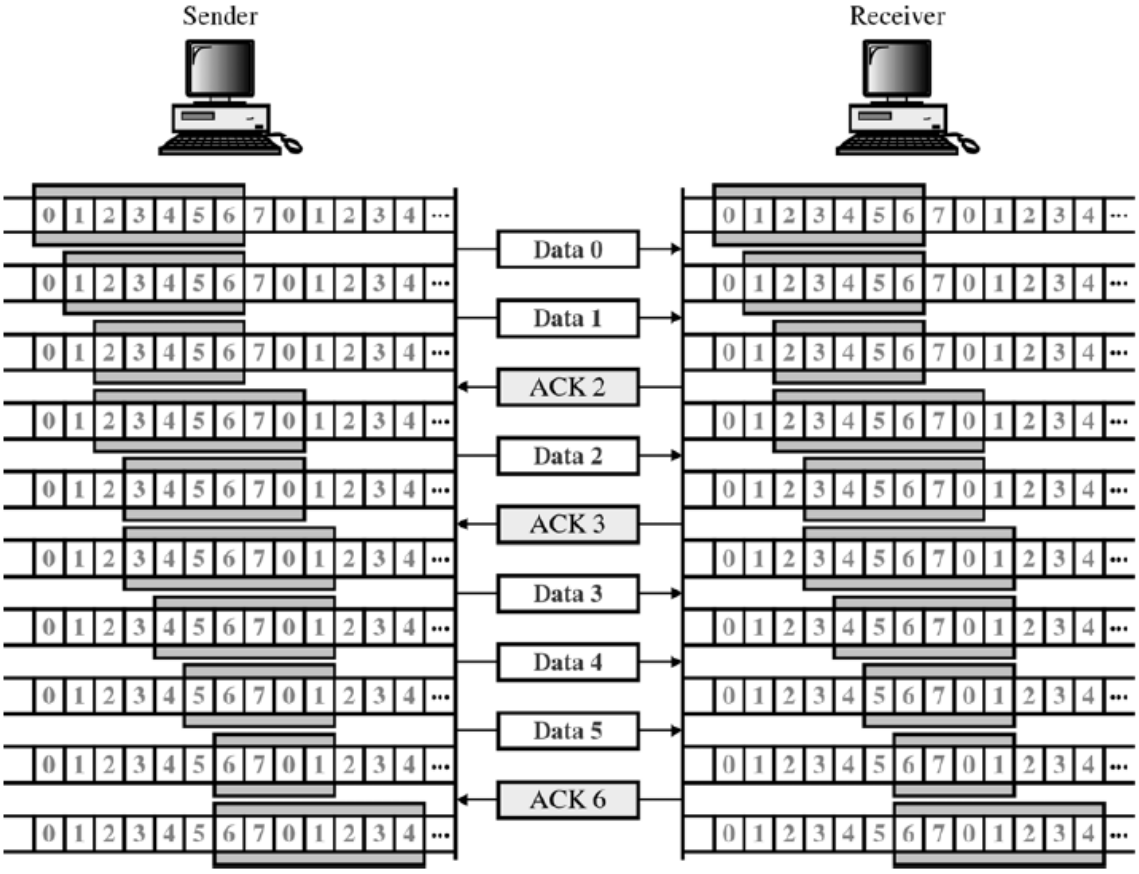
INEFFICIENT (Slow): Each frame must travel all the way to the receiver and an ACK must travel all the way back before the next frame can be sent. If the distance between devices is long, the time spent waiting for ACKs between each frame can be significantly long.

Sliding Window: In this method, sender can transmit several frames before needing an ACK. Frames can be sent one right after another meaning link can carry several frames at once and its capacity can be used efficiently. The receiver uses a single ACK to confirm the receipt of multiple data frames. Sliding Window refers to imaginary boxes at both the sender and the receiver upper limit. This window can hold frames at either end and provides upper limit on the no of frames that can be sent before requiring an Ack. Frames may be ACK at any point w/o waiting for the window to fill up and may be TX as long as the window is not yet Full o To keep track of which frames have been transmitted and which received, sliding window introduces an identification scheme based on the size of the window o The frames are numbered modulo-n means from 0 to n-1 o If n=8, frames are numbered 0,1,2,3,4,5,6,7,0,1,2,3,4,5,6,7,0,…. So on. When the receiver sends the ACK, it includes the number of the next frame it expects to receive.

Stop&wait example:



Sliding window example:



5 a) Discuss about Congestion Control in Virtual-Circuit Subnets. 6M

Congestion Control in Virtual-Circuit Subnets: Until now we were discussed about how to avoid the congestion from the occurring at first time. From now onwards we will discuss about how to handle the congestion after occurrence? Here we will describe some approaches to dynamically controlling congestion in virtual-circuit subnets.

1. Admission control
2. Careful establishment
3. Resource reservation

Admission control: It is the one of the technique that is used when the congestion occurs to keep the congestion not getting worse. The idea behind this is "once the congestion was identified in a network (by one of the close loop solution mechanisms) no new virtual circuits are set up until the problem was gone away". I.e. by allowing more things in getting matter more badly. It is easy to implement Example: In the telephone system when a switch gets overloaded, it also practices admission control by not giving dial tones.

Careful establishment: An alternative approach is to allow new virtual circuits but carefully route/establish all new virtual circuits around problem areas. The working of this approach like this

Step 1: find out the congested routers in the network by using open

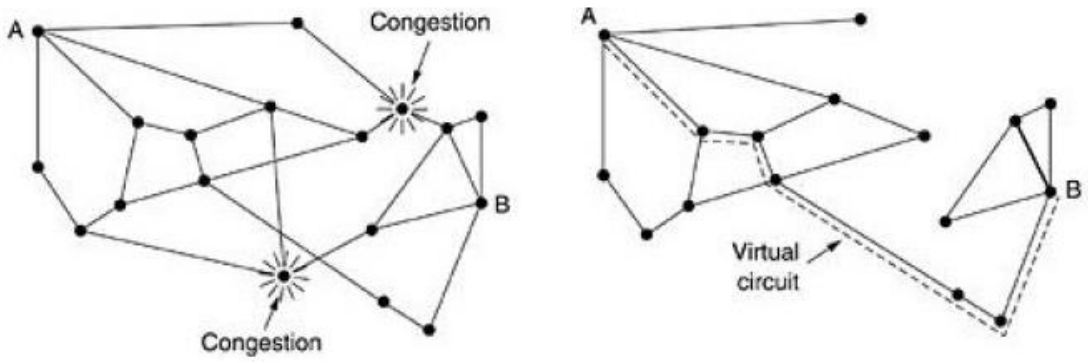
loop mechanisms.

Step 2: construct a new subnet by eliminate those congested routers

from the network.

Step 3: establish a new virtual connection.

EXAMPLE:



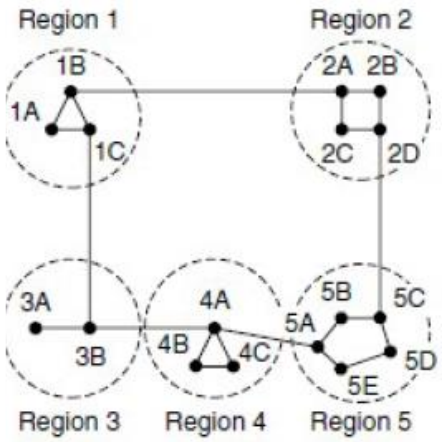
Resources reservation: Congestion can be controlled by allocating maximum resources at the time of establishing the virtual circuit. The details of this virtual circuit are stored in the buffer of routers at the time of establishing virtual circuit. In this way, congestion is unlikely to occur on the new virtual circuits because all the necessary resources are guaranteed to be available.

Disadvantage: waste of resources.

b) Explain about Hierarchal Routing? 5M

Hierarchal Routing:As networks grow in size, the router routing tables grow proportionally. Not only is router memory consumed by ever-increasing tables, but more CPU time is needed to scan them and more bandwidth is needed to send status reports about them. At a certain point, the network may grow to the point where it is no longer feasible for every router to have an entry for every other router, so the routing will have tobe done hierarchically, as it is in the telephone network. When hierarchical routing is used, the routers are divided into what we will call regions. Each router knows all the details about how to route packets to destinations within its own region but knows nothing about the internal structure of other regions. When different networks are interconnected, it is natural to regard each one as a separate region to free the routers in one network from having to know the topological structure of the other ones.For huge networks, a two-level hierarchy may be insufficient; it may be necessary to group the regions into clusters, the clusters into zones, the zones into groups, and so on, until we run out of names for aggregations.

Figure 5-14:



(a)

Full table for 1A

Dest.	Line	Hops
1A	–	–
1B	1B	1
1C	1C	1
2A	1B	2
2B	1B	3
2C	1B	3
2D	1B	4
3A	1C	3
3B	1C	2
4A	1C	3
4B	1C	4
4C	1C	4
5A	1C	4
5B	1C	5
5C	1B	5
5D	1C	6
5E	1C	5

(b)

Hierarchical table for 1A

Dest.	Line	Hops
1A	–	–
1B	1B	1
1C	1C	1
2	1B	2
3	1C	2
4	1C	3
5	1C	4

(c)

Figure 5-14. Hierarchical routing.

Figure 5-14 gives a quantitative example of routing in a two-level hierarchy with five regions. The full routing table for router 1A has 17 entries, as shown in Fig. 5-14(b). When routing is done hierarchically, as in Fig. 5-14(c), there are entries for all the local routers, as before, but all other regions are condensed into a single router, so all traffic for region 2 goes via the 1B-2A line, but the rest of the remote traffic goes via the 1C-3B line. Hierarchical routing has reduced the table from 17 to 7 entries. As the ratio of the number of regions to the number of routers per region grows, the savings in table space increase. Unfortunately, these gains in space are not free. There is a penalty to be paid: increased path length. For example, the best route from 1A to 5C is via region 2, but with hierarchical routing all traffic to region 5 goes via region 3, because that is better for most destinations in region 5.

UNIT III

6 a) Explain about Leaky bucket Algorithm? 5M

The Leaky Bucket Algorithm used to control rate in a network. It is implemented as a single-server queue with constant service time. It was proposed a 19th century networking engineer by **Turner**.

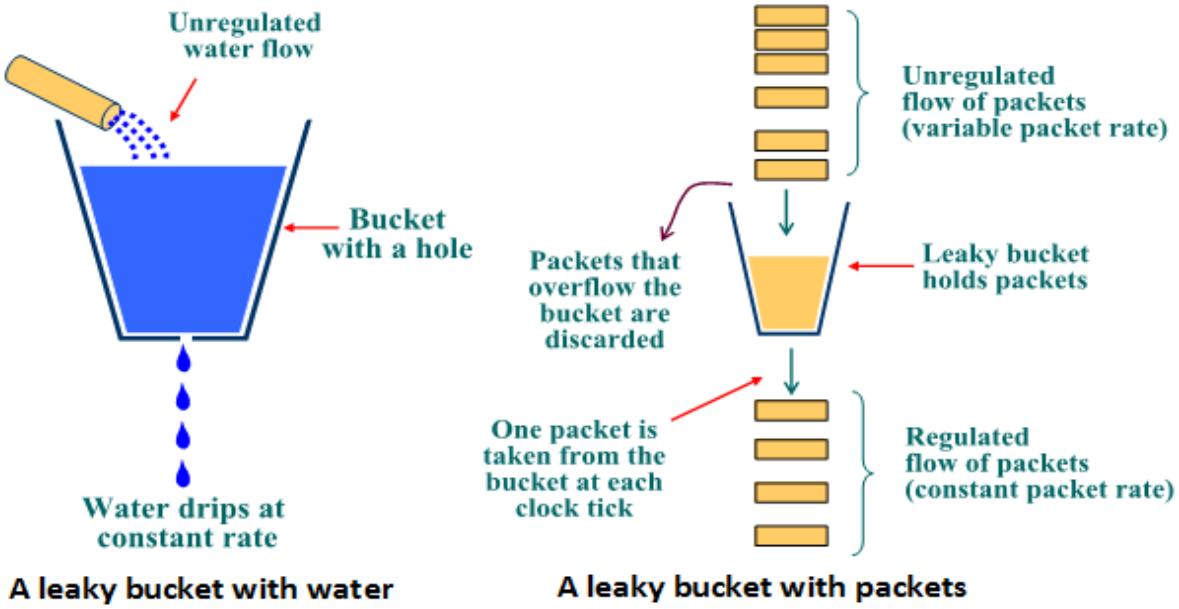
One day evening turner sit on his house balcony, his father is cleaning his motor cycle with a bucket of water and some cloth. That bucket has a hole on lower part of it. The water was leaking at a constant rate, after some time the bucket was empty because of leakage. And his mother fill that bucket with water by using other bucket (it has better storage capacity) at the end of filling process the water start spills over the sides of bucket.

From that situation he observe two important points

- The water was leaking at a constant rate
- Water start spills over the sides of bucket when the bucket is full.

By using those two points he implements a new algorithm.

Diagram:



Algorithm:

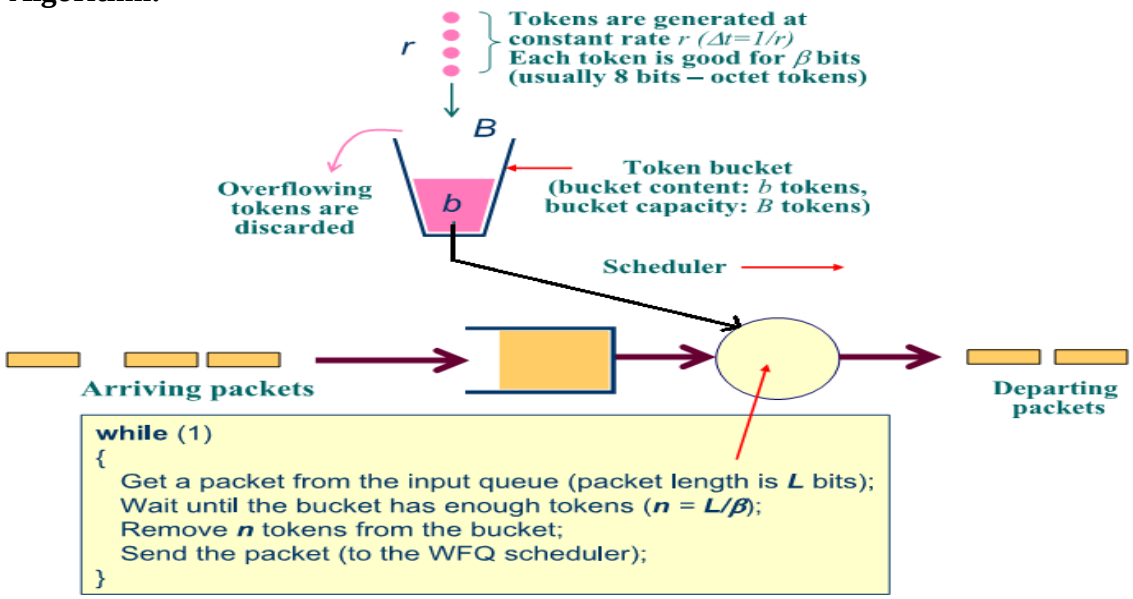
- **Step 1:** Does nothing when input is idle.
- **Step 2:** When a packet arrives, if buffer is full then discard packet. Else append to the buffer.
- **Step 3:** At every **clock tick**, one packet is transmitted (unless the queue is empty).

Advantages: control data rate in a network.
Disadvantage: If data sending too fast, data is dropped.

6 b) Explain about Token Bucket Algorithm 5M

Leaky bucket algorithm does not allow sending **burst of packets**, but only at a specified rate. If there is no traffic for a certain period of time, the amount of unused bandwidth cannot be used for later packets; this is achieved by using a token bucket algorithm.

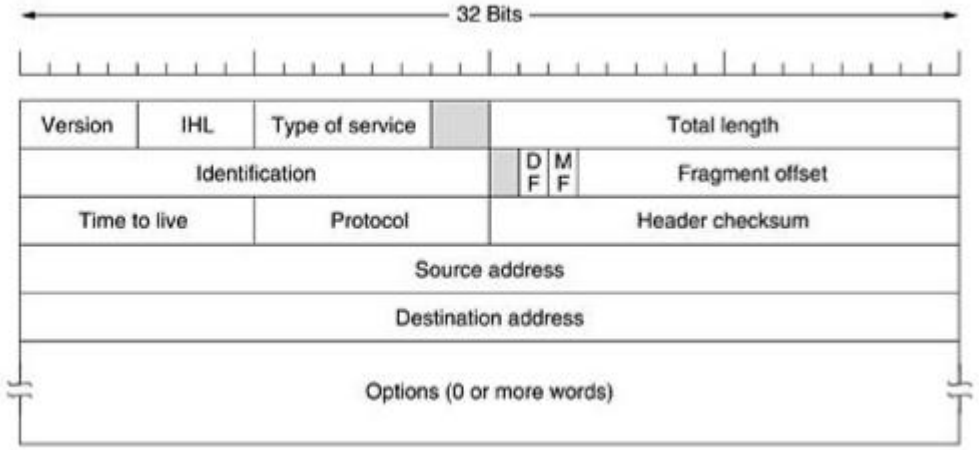
Algorithm:



(OR)

7 a) Explain about IPV4 Header format. 5M

• The Internet can be viewed as a collection of subnetworks or Autonomous Systems (AS).
• IP (Internet Protocol) hosts the whole Internet together.
• Communication in the Internet works as follows:
– The transport layer takes data streams and breaks them up into datagrams.
– Each datagram is transmitted through the Internet.
– When all the pieces finally get to the destination machine, they are reassembled by the network layer, which inserts it into the receiving process' input stream.
• IP addresses are the most common logical addresses. (Everyone on the Internet has one.)
• 32 - bit numbers (IP version 4)
• 32 - bits yields 2^{32} unique numbers
• 2^{32} = 4,294,967,296
– there are over 4 billion possible IPv4 addresses
– but many are "wasted" due to the allocation scheme



Version – The IP version number, 4.
• Header length – The length of the datagram header in 32-bit words.
• Type of service – Contains five subfields that specify the precedence(priority 0-7), delay, throughput, reliability, and cost desired for a packet.
• Total length – The length of the datagram in bytes including the header, options, and the appended transport protocol segment or packet. The maximum length is 65535 bytes.
• Identification – An integer that identifies the datagram.
• DF – Don't fragment
• MF – More Fragments. All fragments except the last one have this bit set.
• Fragment offset – The relative position of this fragment measured from the beginning of the original datagram in units of 8 bytes.
• Time to live – How many routers a datagram can pass through. Each router decrements this value by 1 until it reaches 0 when the datagram is discarded. This keeps misrouted datagrams from remaining on the Internet forever.
• Protocol – The high-level protocol type.
• Header checksum – A number that is computed to ensure the integrity of the header values.
• Source address – The 32-bit IPv4 address of the sending host.
• Destination address – The 32-bit IPv4 address of the receiving host.
• Options – A list of optional specifications for security restrictions, route recording, and source routing. Not every datagram specifies an options field.
• Padding – Null bytes which are added to make the header length an integral multiple of 32 bytes as required by the header length field.

b) Explain about Internet Control Protocols. 5M

ICMP is a transport level protocol within TCP/IP which communicates information about network connectivity issues back to the source of the compromised transmission. It

sends control messages such as *destination network unreachable*, *source route failed*, and *source quench*. It uses a data packet structure with an 8-byte header and variable-size data section.

ICMP is used by a device, like a router, to communicate with the source of a data packet about transmission issues. For example, if a datagram is not delivered, ICMP might report this back to the host with details to help discern where the transmission went wrong. It's a protocol that believes in direct communication in the workplace.

Ping is a utility which uses ICMP messages to report back information on network connectivity and the speed of data relay between a host and a destination computer. It's one of the few instances where a user can interact directly with ICMP, which typically only functions to allow networked computers to communicate with one another automatically.

ARP

In an IPv4 network keep an ARP cache. When the host requests a MAC address to send a packet to another host in the LAN, it checks its ARP cache to check that the MAC address translation already presents.

Let us understand this concept with an example:

· Host P resolves protocol address for host U for protocol messages from an application on P sent to U.
· P does not resolve a protocol address for host U
· By using the internet layer, host P delivers to host U by routing through T1 and T2.
· Host P resolves the T1 hardware address.
· Network layer on host P passes packet containing destination protocol address for U for delivery to T1
· T1 delivers the packet to T2 which in turn forwards the packet to Host U.

DHCP

Dynamic Host Configuration Protocol (DHCP) is a standardized network protocol used on Internet Protocol (IP) networks. The DHCP is controlled by a DHCP server that dynamically distributes network configuration parameters for interfaces and services. Networks ranging in size from small home networks to campus networks frequently use DHCP.

Based on the Bootstrap Protocol (BOOTP) released in 1985, DHCP differs from BOOTP in that it can dynamically allocate IP addresses from a pool and reclaim them when they are no longer in use.A DHCP server can manage TCP/IP settings for devices on a network by automatically, dynamically, or manually assigning them IP addresses.

Dynamic: a Network Admin reserves a set number of IP addresses and each DHCP client on the LAN is configured to request an IP address from the server during network initialization.

Automatic: Similar to Dynamic, but the DHCP server keeps a list of previous IP address assignments in order to assign a client the same IP addresses as in the past.

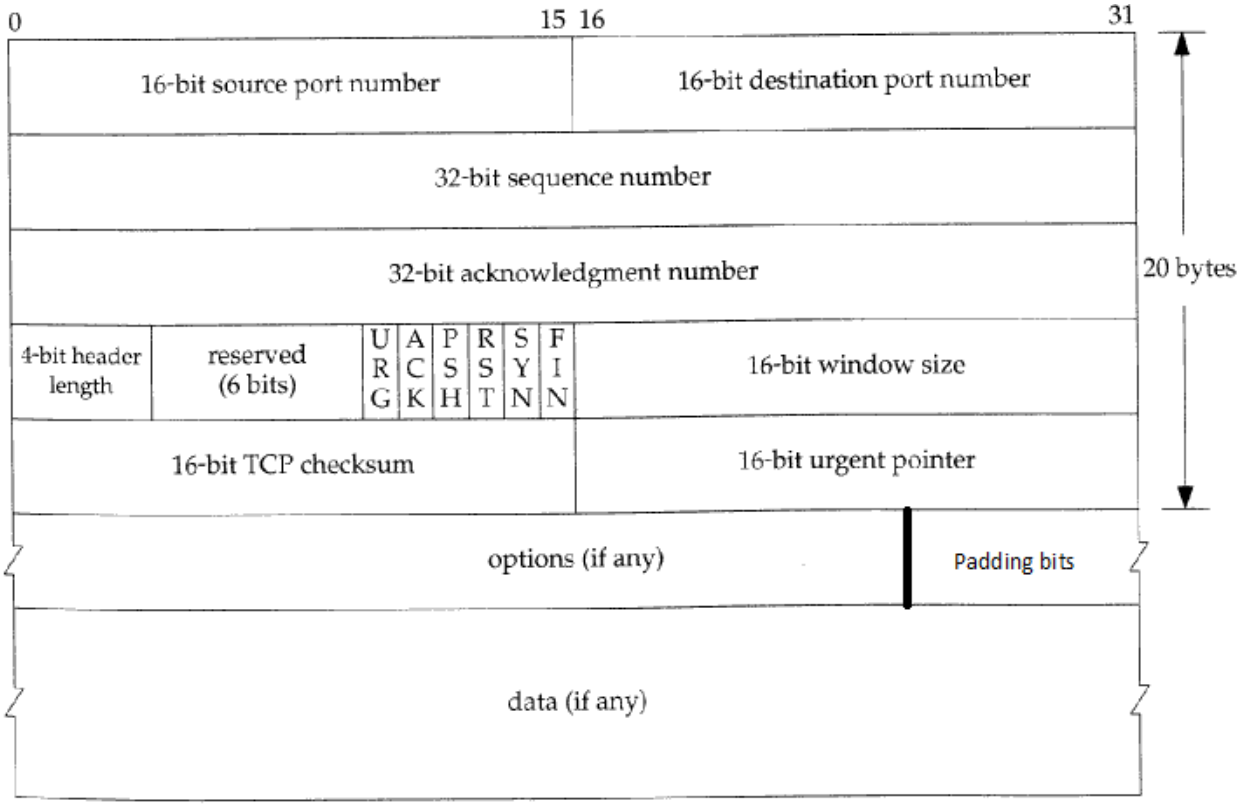
Manual: Based on parameters defined by the administrator, the DHCP server issues a private IP address dependent on each client's individual MAC address. If no match is found, the network can fall back on either Dynamic or Automatic protocol.

UNIT IV

8 Discuss in detailed about the TCP Segment Header? 10M

The TCP Segment Header:

Each and every TCP segment contains the **20 bytes fixed header** and variable length **options** followed by data. These details are used to send the TCP segment reliably to destination processes.



Fields:

Source & **destination port numbers:** these fields represents the source and destination process TSPA's.

Sequence number: Each transmitted byte of TCP payload data contains a 32 bit sequence number so that the TCP stream can be properly sequenced. The initial sequence number is effectively **random** it is negotiated during connection setup; it may be any value between 0 and 4,294,967,295. It was wrapping when they reach 2^{32}-1.

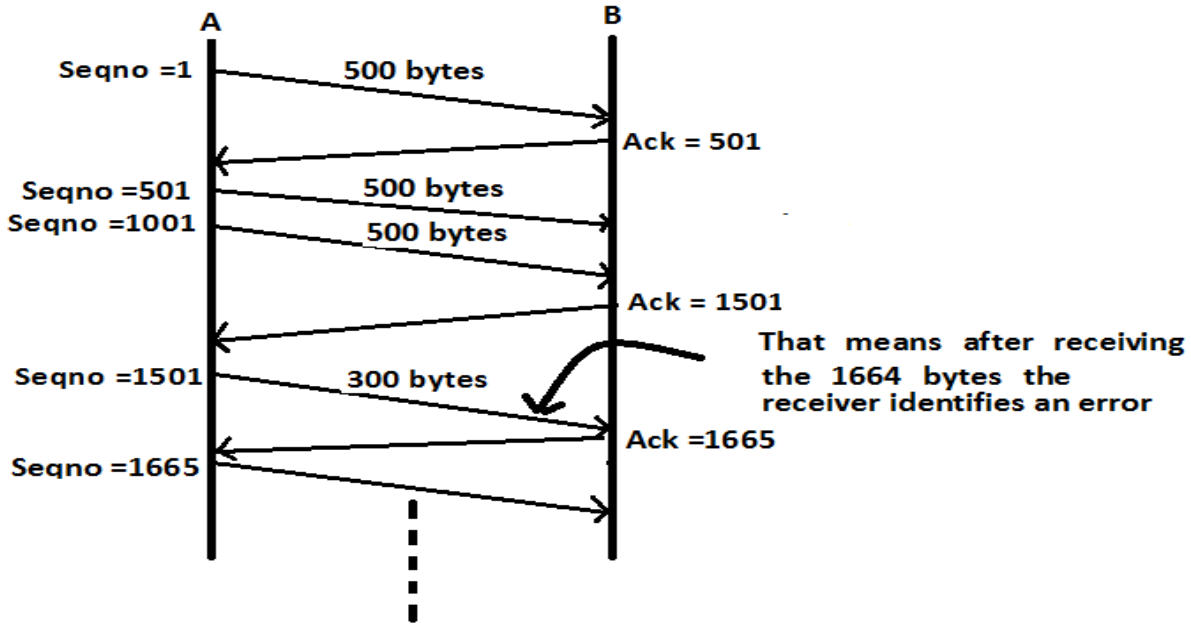
NOTE: Sequence number of first byte in payload is written in Sequence Number field and the following bytes are numbered consecutively.

Acknowledgment number: In TCP payload data each and every byte must be acknowledge. An acknowledgment is a confirmation of delivery of data. When a TCP receiver wants to acknowledge data, it writes a sequence number in the **Acknowledgement Number** field, and sets the **ACK flag**.

NOTE: The acknowledgment mechanism employed is **cumulative** so that an acknowledgment of sequence number X indicates that all octets up to but not including X have been received.

Example: Ackno=5 confirms delivery for 1,2,3,4 (but not 5).

Diagram:



Header length (4 bit): this field contains the size of the TCP header in the 32-bit **words.** It is also called data offset because it also indicates where the Data part of the packet actually starts. The minimum value of this field is 0101 (5). Even though header contains the options the header length is always multiples of 32, for that we add padding bits.

Reserved bits: 6 bits are reserved for future use.

Flag bits:

Urgent Pointer Field Significant (URG): When URG=1, indicates that the current segment contains urgent / high-priority data. And that the Urgent Pointer field value is valid.

Acknowledgment Field Significant (ACK): When ACK=1, indicates that the value contained in the Acknowledgment Number field is valid. This bit is usually set to 1, except during the first message during connection establishment.

Push Function (PSH): Used when the transmitting application wants to force TCP to immediately transmit the data that is currently buffered without waiting for the buffer to fill;

Reset Connection (RST): When RST=1, indicates that immediately terminates the TCP connection.

Synchronize Sequence Numbers (SYN): used to establish a connection, indicating that the segments carry the initial sequence number.

Finish (FIN): Set to request normal termination of the TCP connection in the direction this segment is traveling; completely closing the connection requires one FIN segment in each direction.

NOTE: SYN and ACK flags are used in connection established phase of different request and replay packets.

- for **request** SYN=1 and ACK=0
- for **replay** SYN=1 and ACK=1
- for **acknowledgement** SYN=0 and ACK=1
- for **data** SYN=0 and ACK=0

Window size (16 bit): it contains the value of the receiver window size. That tells the source how much data the destination host willing to accept by specifying its buffer size. **Maximum window size is 2^{16}-1= 65535 bytes.**

NOTE: The sequence number (32 bits), acknowledgement number (32 bits) and window (16 bits) fields are used to provide a reliable data transfer, using a window-based protocol.

Urgent pointer (16 bit): it specifies the end of the urgent data. It contains 0x00000000 when URG flag =0. The urgent data has been marked as high priority by the upper layer applications.

Options: this is used to specify the extra options that are not mention in TCP header. Especially used at connection establishment to negotiate verity of options. The most commonly used option is MSS (maximum segment size). It tells the source how much data the destination host is willing to receive (due to smaller buffer than source), by default the MSS is 536 bytes.

Data: contains PDU coming from the upper layers.

Checksum (16 bit): it is used for the error detection, Same as IP checksum, TCP checksum is also one's complement of the one's complement sum of all 16 bit words in the computation data.

(OR)

9 a) Discuss about Name spaces in DNS? 5M

The DNS Name Space:

Conceptually, the Internet is divided into over 200 top-level domains, where each domain covers many hosts. Each domain is partitioned into subdomains, and these are further partitioned, and so on. All these domains can be represented by a tree, as shown in Fig. a. The leaves of the tree represent domains that have no subdomains (but do contain machines, of course). A leaf domain may contain a single host, or it may represent a company and contain thousands of hosts. The top-level domains come in two flavors: generic and countries. The original generic domains were *com (commercial)*, *edu* (educational institutions), *gov* (the U.S. Federal Government), *int* (certain international organizations), *mil* (the U.S. armed forces), *net* (network providers), and *org* (nonprofit organizations).

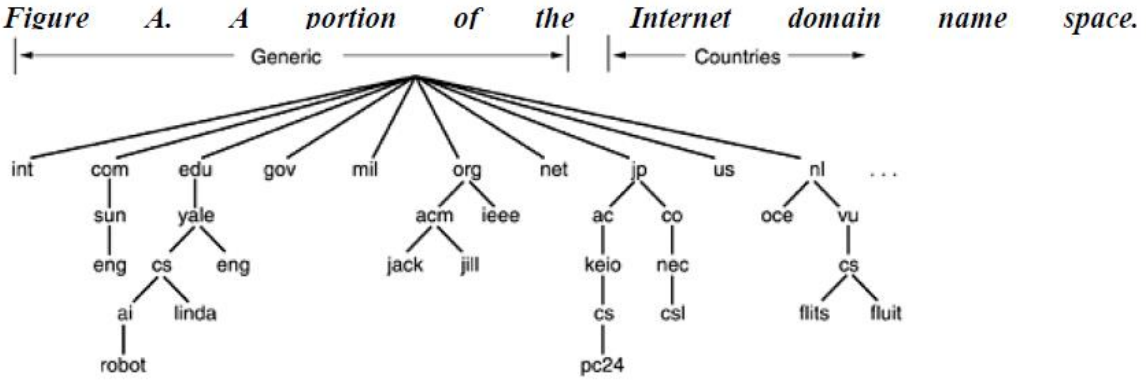


Figure A. A portion of the Internet domain name space.

b) Discuss about Resource Records in DNS? 5M

Resource Records: Every domain, whether it is a single host or a top-level domain, can have a set of resource records associated with it. For a single host, the most common resource record is just its IP address, but many other kinds of resource records also exist. When a resolver gives a domain name to DNS, what it gets back are the resource records associated with that name. Thus, the primary function of DNS is to map domain names onto resource records. A resource record is a five-tuple. Although they are encoded in binary for efficiency, in most expositions, resource records are presented as ASCII text, one line per resource record. The format we will use is as follows:

Domain_name Time_to_live Class Type Value .

The *Domain_name* tells the domain to which this record applies. Normally, many records

exist for each domain and each copy of the database holds information about multiple domains. This field is thus the primary search key used to satisfy queries. The order of the records in the database is not significant. The *Time_to_live* field gives an indication of how stable the record is. The third field of every resource record is the *Class*. The *Type* field tells what kind of record this is. The most important types are listed in fig b.

Figure B: The principal DNS resource record types for IPv4.

Type	Meaning	Value
SOA	Start of Authority	Parameters for this zone
A	IP address of a host	32-Bit integer
MX	Mail exchange	Priority, domain willing to accept e-mail
NS	Name Server	Name of a server for this domain
CNAME	Canonical name	Domain name
PTR	Pointer	Alias for an IP address
HINFO	Host description	CPU and OS in ASCII
TXT	Text	Uninterpreted ASCII text

An *SOA* record provides the name of the primary source of information about the name server's zone (described below), the e-mail address of its administrator, a unique serial number, and various flags and timeouts.

The most important record type is the *A* (Address) record. It holds a 32-bit IP address for some host. Every Internet host must have at least one IP address so that other machines can communicate with it.

The next most important record type is the *MX* record. It specifies the name of the host prepared to accept e-mail for the specified domain. It is used because not every machine is prepared to accept e-mail. The *NS* records specify name servers. *CNAME* records allow aliases to be created.