Name: Meraz Ahmed

ID: IT-18005

Class Test-01

Question no: 1

a) Define permutation. State the difference between fully qualified and partially qualified. 6

b) How is a secret key different from public key? 3

c) What are the advantages and disadvantages of public key encryption? 5

Question no: 2

a) What is the backbone network? Define node. 3

b) What is anonymous FTP? Describe NAT. 6

c) What is TCP/IP? Explain 5

Question no: 3

a) Discuss about the OSI and TCP/IP model with a proper figure. 7

b) Discuss client-server model with proper figure 7

Question no: 4

a) What is bandwidth? Write about VPN. 5

b) What are the main element of a protocol? 3

c) Describe about application layer? 6

Question no: 5

a) How to create a Network app? Briefly explain 5

b) Why is an application such as POP needed for electroning messaging? 4

c) Define socket with a figure. 5

Question no: 6

a) What is NIC? Define Firewall. 3

b) What is meant by 127.0.0.1 and localhost 5

c) What are the different types of a network? Explain each briefly. 6

Question no: 7

a) What is digital signature? Define substitution and transposition-encryption. 6

b) Define File-Sharing services and SMB protocol. 8

Question no: 8

a) Define primary zone. 3

b) Explain Authoritative Name server? 6

c) What is the nature of domain name disputes?

Ans to the question no:01 (a)

a) **Permutation:** Permutation is transposition in bit level.

* Straight permutation:

The number of bits in the input and output are preserved.

* Compressed permutation:

The no. of bits is reduced (some of the bits are dropped)

* Expanded permutation:

The no. of bits is increased (some bits are repeated)

Difference between fully qualified and partially qualified domain name:

Fully qualified	partially qualified
It gives the full location of the specific domain that bears it's name with the whole DNS name space.	It doesn't give full of the domain.

Fully qualified	partially qualified
Fully qualified domain names are called absolute domain names.	Partially qualified domain names are sometimes called domain names.

Ans to the question no: 01 (b)

In secret key, the same key is used by both patients. The sender uses this key and an encryption algorithm to encrypt data; the receiver uses the same key and the corresponding decryption algorithm to decrypt the data.

In public key, there are two keys; a private key and a public key. The private key is kept by the receiver. The public key is announced to the public.

Ans to the question no: 01(c)

Advantages:

1. Remove the restriction of a shared secret key between two entities. Here each entity can create a pair of keys, keep the private one and the publicly one.
2. The no. of keys needed is reduced tremendously. For one million users to communicate, only two million keys are needed.

Disadvantages:

If you use large numbers the method to be effective. Calculating the cipher text using the long keys takes a lot of time. So it is not recommended for large amount of text.

Ans to the question no: 02(a)

Backbone network: A backbone network is a centralized infrastructure that is designed to distribute different routes and data to various networks. It also handles the management of bandwidth and multiple channels.

Node: A node refers to a point or joint where a connection takes place. It can be a computer or device that is part of a network. Two or more nodes are needed to form a network connection.

Ans to the question no: 02(b)

Anonymous FTP: Anonymous FTP is a way of granting user access to files in public servers. Users that are allowed to data in these servers do not need to

identify themselves but instead log in an anonymous guest.

NAT is network address translation. This is a protocol that provides a way for multiple computers on a common network to share single connection to the internet.

Ans to the question no: 02(c)

~~TCP/IP:~~

TCP/IP: TCP/IP is a name given to the collection of networking protocol that have been used to construct the global internet. The protocols are also reffered to as the DOD or Arpanet protocol suite because their early development was fundoed by the Advanced Research projects Agency of the us department of Defence.

TCP/IP model is an implementation of OSI reference model.

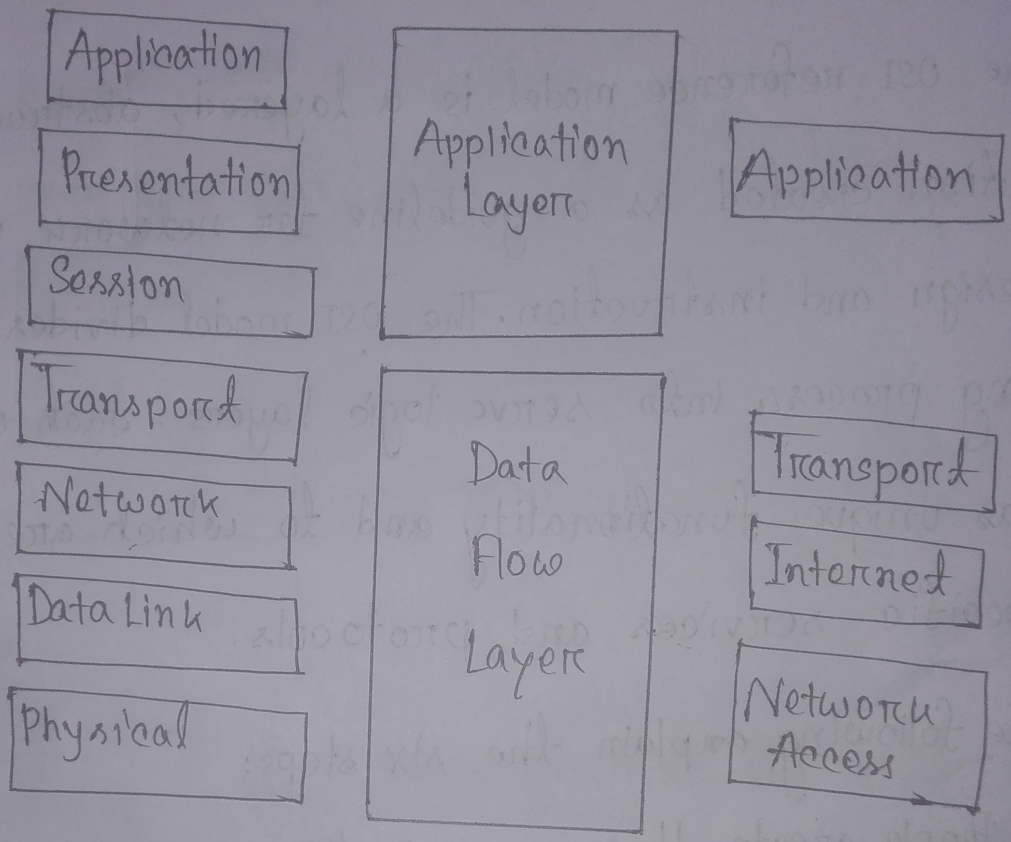
Ans to the question no: 03(a)

The OSI reference model is a layered, abstract representation created as a guideline for network protocol design and instruction. The OSI model divides the networking process into seven logic layers, each of which has unique functionality and to which are assigned specific services and protocols.

The following explain the six steps:

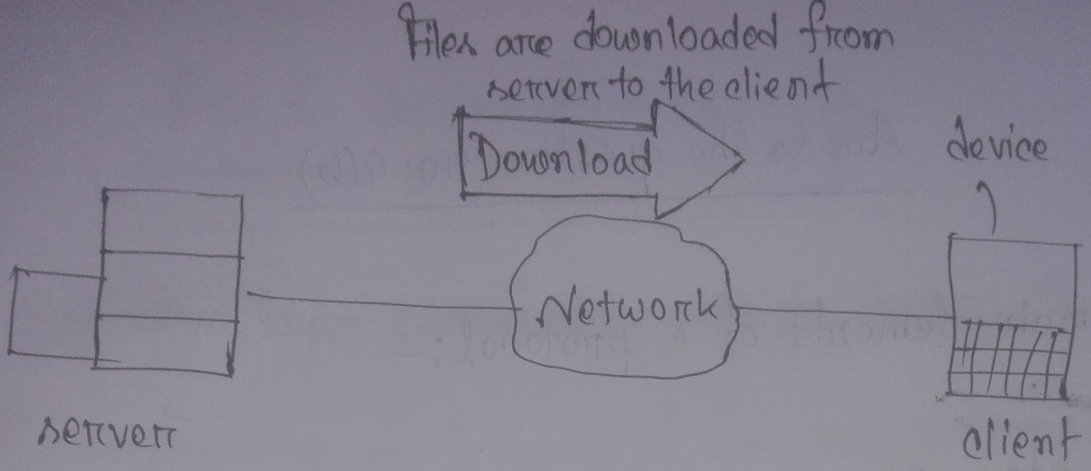
1. People create the communication
2. The application layer prepares human communities
3. Software and hardware convert communication to a digit format.
4. Application layer services initiate the data transfer
5. Each layer plays its node.

6. The application layer receives data from the network and prepares it for human use.



Ans to the question no: 3(b)

In the client/server model, the device requesting the information is called a client and the device responding to the request is called a server. Client and server processes are considered to be in the application layer. The client begins the exchange be requesting data from the server, which responds by sending one or more streams of data to the client. Application layer protocols describe the design of the requests and responses between client and servers. In additio to the actual data transfer, this exchange can require control information such as user authenti- cation and the identification of a data file to be transformed.



Ans to the question no: 4(a)

Bandwidth: Every signal has a limit of upper range frequency and lower range frequency. The range of limit of network its upper and lower frequency is called bandwidth.

VPN means virtual private networks, a technology that allows a secure tunnel to be created across a network such as the internet. For example VPNs allow you to establish a secure dial-up connection to a remote server.

Ans to the question no: 4(b)

The main elements of a protocol:-

Syntax: It specifies the structure or format of the data. It also specifies the order in which they are presented.

Semantics: It specifies the meaning of each section of bits.

Timing: Timing specifies two characteristics, when data should be sent and how fast it can be sent.

Ans to the question no: 4(c)

→ Application layer enables the user to access the network.

→ It is the top most layer of the OSI reference model

→ Application layer protocol are the file transfer protocol, simple mail transfer protocol, domain nam system etc.

→ The most widely used application protocol is HTTP. A user sends the request for the web page usin HTTP.

Ans to the question no: 5(a)

Creating a network app.

Writing programs that:

1. Run on (different) end systems.
2. Communicate over network
3. e.g. web server software communicates with browser software.
4. No need to write software for network core devices.

1. Network core devices don't ~~do~~ run user application.
2. Application on end systems allows for rapid app development propagation.

Ans to the question no: 5(b)

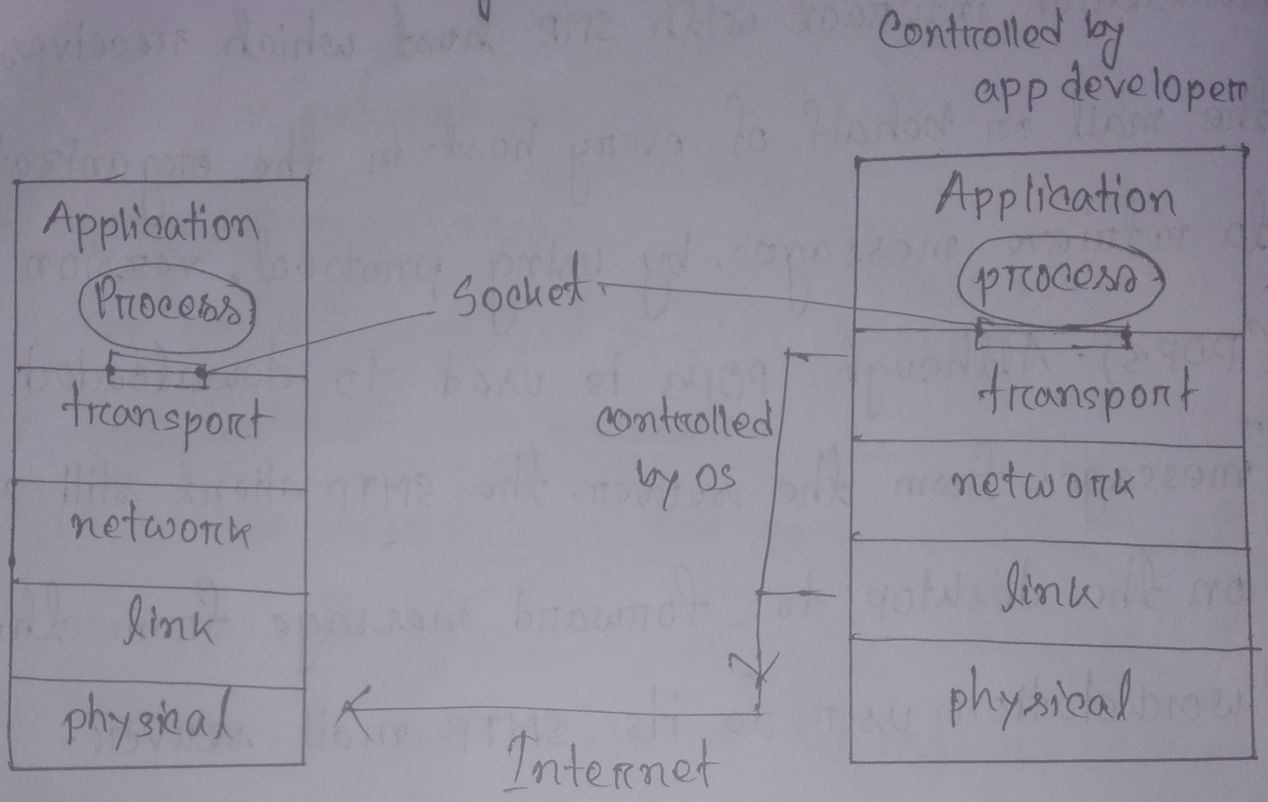
Workstation interact with SMP host which receives the mail on behalf of every host in the organizations to retrieve messages, by using protocol, version 3 (POP3). Although POP3 is used to downloaded messages from the server, the SMTP client still needed on the desktop to forward message from the workstation user to its SMTP mail server.

Ans to the question no: 5(c)

Sockets:

* Process sends/receives messages from to its socket
* Socket analogous to door:
  1. Sending process shove messages alarst door
  2. Sending process relies on transport instructur

on other side of door to delievery message to socket at receiving process.



Ans to the question no: 6(a)

NIC: NIC stands for network Interface card. It is also known as Network Adapter or Ethernet card. It is in the form of an add-in card

is installed on a computer so that the computer can be connected to a network.

Firewall is a network security system that is used to protect computers networks from unauthorized access. It prevents malicious access from outside to the computer network. A firewall can also be built to grant limited access to outside users.

Ans to the question no: 6(b)

IP address 127.0.0.1 is reserved for loop back or localhost connections. These networks are usually reserved for the biggest customers or some of the original members of the internet. To identify any connection issue, the initial step is to ping

used at home. It is a connection between the computers and another device such as mobile, printers, modem etc.

* Local Area Network (LAN): Lan is used in a small offices and internet cafes to connect a small group of computers to each other. Usually they are used to transfer a file or for playing the games in a network.

* Metropolitan Area Network (MAN): It is a powerful network type then LAN. The area covered by MAN is a small town, city etc. A huge server is used to covered such a large span of area the connection.

* Wide Area Network (WAN): It is more complex than LAN and covers a large span of the area typically a large physical distance. WAN is spread across the world.

Ans to the question no: 7(a)

Digital Signature: Digital signature is an electric signature that can be used to authenticate the identity of the sender of a message or document and possibly to ensure that the origin content sent is unchanged. Digital signature is easily transportable, can not be imitate by someone else, and can be automatically. The ability to ensure that the original signed

message. can not repudiate it later.

Substitution: A character level encryption in which the characters retain their painful but the position of the character changes.

Transposition: A character level encryption in which the character retain their plantext but the position of the character changes.

Ans to the question no: 7(b)

Server Message Block (SMB) is a client/server file sharing protocol. IBM developed SMB in the 1980s to describe the structure of shared network resources, such as directions, file printers. It is a request/response protocol. Unlike the file sharing

supported by FTP. clients establish a log-term connection to servers. After the connection is established. the use of the client can access the resources on the server as if the resource is local to the client host.

SMB file-sharing and print services have become the mainstay of Microsoft networking. With the introduction of the windows 2000 series of software, Microsoft changed the underlying structure for using SMB.

The linux and UNIX operating systems also provide a method of sharing resources with microsoft networks using a version of SMB called SAMBA.

Ans to the question no: 8(a)

Primary Zone: This is the read and writable copy of a zone file in the DNS namespace. This is the primary ~~squat~~ source for information about the zone and it stores the master copy of zone data in local life. or in ADDS. By default the primary zone file is named as zone-name dns in %windir% system32 DNS folder on the server.

Ans to the question no: 8(b)

An authoritative name server is a name server that gives answers that have been configured by an original source, for example the domain

administrator or by dynamic DNS method.

In contrast to answers that were obtained via a regular DNS query to another name server. An authoritative only name server only returns answer to queries about domain names that have been specifically configured by the administrator.

Ans to the question no: 8(c)

Domain name disputes enable the users to find the computers and people in an easy way.

→ Domain name has significance that has

acquired business demands and identifiers to identify the business and target only the busines existing.

→ These disputes rises due to the cyber solution this provides a way to pre-emptive the registration process for the trademarks by third parties and as a domain names.

→ Domain names are registered and targeted for the benefit of other person or company. It is being done by the cyber squatters.