Shakhera Khanom
ID : IT-18033
CT NO :- 03

Question Set

01.

a. What is transport layer? what does transport layer do? 4

b. what are functions of a transport layer in networking? 4

c. Why are transport layer services called end-to-end? How does end-to-end communication work? 6

02.

a. What is Transmission Control Protocol used for? What are the features of TCP? 5

b. Do port addresses need to be unique? why or why not? why are port addresses shorter than IP addresses? 4

c. How does TCP work? what is the TCP packet format? 5

03.

a. What is User Datagram Protocol in networking? Write the features of UDP. 5

b. Write down the application of UDP. Is UDP better than TCP? Explain your answer. 4

c. Compare the TCP header and the UDP header. List the fields in the TCP header that are missing from UDP header. Give the reason for their absence. 5

04.

a. What is application layer? Why is the application layer important? 4

b. What is the difference between a primary server and secondary server 4

c. How the client-server model works? Write the advantage and disadvantage of client-server model. 6

05.

a. What is Remote Procedure call? How does Remote procedure call work ? 5

b. What are the two main categories of DNS message? Write the answer with block diagram. 4

e. DNS uses UDP instead of TCP. If a DNS packet is lost, there is no automatic recovery. How is this problem handled? 5

06.

a. What is DNS? What are the three domains of domain name space in internet? Explain with details. 6

b. Describe the addressing system used by SMTP. How does SMTP work? 5

c. What is the difference between SMTP and SNMP? 3

07.

a. What is FTP? How does FTP work? 5

b. Write the advantage and disadvantage of FTP. 4

c. What is POP3 and which are are default POP3 ports.? 3

d. Is a Gmail a POP3 or IMAP? 2

08.

a. What is HTTP? Write the features of HTTP. 5

b. What is the difference between HTTP and FTP? 3

c. What is node-to-node, host-to-host and process-to-process delivery? 3

d. Write the difference types of network services. Write the feature of communication services. 3

Shakhera Khanom Shifa

Question and Answer

Ans: to the que: no:- 1(a)

Ques: what is transport layer? what does transport layer do?

Answer:

The transport layer is the fourth layer in the open system interconnection (OSI) model, and is responsible for end-to-end communication over a network. This layer enables the host-to send and receive error corrected data, packets or messages over a network and is the network component that allows multiplexing.

Transport layer provides transparent transfer of data between end users, providing reliable data transfer services to the upper layers. The transport layer controls the reliability of a given link through flow control, segmentation and

desegmentation, and error control. Some protocols are state and connection oriented. This means that the transport layer can keep track of the segments and retransmit those that fail. The transport layer also provides the acknowledgement of the successful data transmission and sends the next data if no errors occurred. Typically examples of layer 4 are the Transmission Control Protocol (TCP) and user Datagram Protocol (UDP).

Ans: to the que: no:- 1 (b)

Ques: What are the functions of a transport layer in networking?

Answer:

The transport layer is the fourth layer in the OSI layered architecture. The transport layer is responsible for reliable data delivery. The upper

layer protocols depends heavily on the transport layer protocol. A high level of error recovery is also provided in this layer. This layer ensures, that packets are delivered error-free, in sequence and with no losses or duplications.

Some functions of transport layer are as follows:

1. This layer is the first one which breaks the information data, supplied by Application layer in to smaller units called segments. It numbers every byte in the segment and maintains their accounting.
2. This layer ensures that data must be received in the same sequence in which it was sent
3. This layer provides end-to-end delivery of data between b hosts which may or may not belong to the same subnet
4. All server processes intend to communicate over the network are equipped with well-known Transport Service Access Points (TSAPs) also

known as port numbers.

Ans: to the que: no: - 1(c)

Ques: Why are transport layer services called end-to-end? How does end-to-end communication work?

Answer: That because some transport layer protocols, for example TCP, but not UDP, provide end-to-end reliable communication.
Also you should have a proper knowledge about the Network Layer where it does the routing part and Transport Layer does the end to end communication. The transport layer is also responsible for the management of error correction, providing quality and reliablility to the end user. This layer enables the host to send and receive error correction data, packets or messages over a network and is the network component that allows

multiplexing.
Simply this layerc doesn't involve with the routing mechanism in the network, just the end to end communication.

How does end to end communication works: The end-to-end principle is a network design method in which application-specific features are kept at communication end points.

The principle is in contrast to features existing on intermediate points between the client and end points, like gateways and routers. In this method, intermediate nodes pass data randomly. The lack of discrimination makes it possible to replace any intermediate node with any other one without failure of functions, since functions exist in end points.

The end to end principle removes critical components from intermediary communications nodes in order to increase routing options, improve data delivery

rates and make sure applications only fail if the end point fails. The principle was developed to address the need for reliable communications in inherently unstable environments and has long been employed in most networking models. Net neutrality is conceptually based on the end-to-end principle. In the same way that data passes through any intermediate nodes neutrality requires that Internet service providers (ISP) refrain from discriminating between data on their network.

Ans: to the que: no:- 2(a)

Ques: What is Transmission Control Protocol used for? What are the features of TCP?

Answer:

Transmission control Protocol accepts data from a data stream, divides it into chunks, and add a TCP header creating a TCP segment. The TCP segment is then encapsulated into an Internet Protocol (IP) datagram, and exchanged with peers.

Features:

- TCP is reliable protocol. That is, the receiver always sends either positive or negative acknowledgement about the data packet to the sender, so that the sender always has bright clue about ~~whetever~~ whether the data packet is reched the destination or it needs to resent it.
- TCP ensures that the data reaches intended the destination ~~or it~~ in the same order it was sent.

- TCP is connection oriented. TCP requires that connection between two remote points be established before sending actual data.
- TCP provides error-checking and recovery mechanism
- TCP provides end-to-end communication
- TCP provides flow control and quality of service.
- TCP operates in client/server point-to-point mode.
- TCP provides full duplex server, i.e. it can perform roles of both receiver and sender

Answer: to the que: no:-2(b)

Ques: Do port addresses need to be unique? Why or why not? Why are port addresses shorter than IP addresses?

Answer:

Port addresses do not need to be universally unique as long as each IP address.

Port address pair uniquely identify a particular

process running on a particular host. A good example would be a network consisting of 50 hosts, each running echo server software. Each server uses the well known port number 7, but the IP address together with the port number of 7, uniquely identify a particular server program on a particular host. Port addresses are shorter than IP addresses, ~~all systems on~~ because their domain, a single system, is smaller than the domain of IP addresses, all systems on the Internet.

Ans: to the que: no:- 2 (c)

Ques: How does TCP work? What is the TCP packet format?

Answer:

TCP uses a three-way handshake to establish a connection between client and server. It uses SYN,

ACK and FIN flags (1 bit) for connecting two end-points. After the establishment of the connection, data is transferred sequentially. If there is any loss of packet, it retransmits data

The TCP packet format consists of these fields:

Source port and Destination Port fields (16 bits each); Sequence Number field (32 bits); Acknowledgement Nember field (32 bits), Data offset (a.k.a. Header length) field (variable length); Reserved field (6 bits); Flags field (6 bits) contains the various flags:

URG, ACK, PSH, RST, SYN, FIN; Window field (16 bits); checksum field (16 bits); Urgent pointer field (16 bits); Options field (variable length) & Data field (variable length).

Source Port			Destination Port
Sequence Number			
Acknowledgement Number			
Data Offset	Reserved	Flags	Window Size
Checksum			Urgent
Options			

Ans: to the que: no:- 3(a)

Q: What is User Datagram Protocol in networking? Write the features of UDP.

Answer:

The User Datagram Protocol (UDP) is simplest Transport Layer communication protocol available of the TCP/IP protocol suite. It involves minimum amount of communication mechanism. UDP is said to be an unreliable transport protocol but it uses IP services which provides bet of effort delivery

mechanism.

In UDP, the receiver does not generate an acknowledgement of packet received and in turn, the sender does not wait for any acknowledgement of packet sent. This shortcoming makes this protocol unreliable as well as easier on processing.

Features:

UDP is used when acknowledgement of data does not hold any significance.
UDP is good protocol for data flowing in on direction
UDP is simple and suitable for query and based communications
UDP is not connection oriented
UDP does not provide congestion control mechanism
UDP does not guarantee ordered delivery of data
UDP is stateless.

UDP is suitable protocol for streaming applications such as VoIP, multimedia streaming.

Ans: to the que: no:- 3 (b)

Q: Write down the application of UDP. Is UDP better than TCP? Explain your answer.

Answer:

Here are few applications where UDP is used to transmit data:

Domain Name Services
Simple Network Management Protocol
Trivial File Transfer Protocol
Routing Information Protocol
Kerberos.

Both protocols are used for different purposes. If the user wants error-free and guarantees to deliver data, TCP is the choice. If the user

wants fast transmission of data and little loss of data is not a problem, UDP is the choice.

Ans: to the ques no: 3(c)

Q: Compare the TCP header and the UDP header. List the fields in the TCP header that are missing from UDP header. Give the reason for their absence.

Answer:

Fields in UDP	Fields in TCP	Explanation
Source Port Address	Source Post Address	
Destination Port Address	Destination Post Address	
Total Length		There is no need for total length.
checksum	checksum	
	Sequence Numbers	UDP has no flow and error control

	Acknowledgement Numbers	UDP has no flow and error control.
	Header Length	UDP has no flow and error control.
	Reserved	UDP has no flow and error control.
	Control	UDP has no flow and error control
	Window Size	UDP has no flow and error control
	Urgent Pointer	UDP cannot handle urgent data.
	Options and Padding	UDP uses no options.

Ans: to the que: no:- 4(a)

Q: What is application layer? why is the application layer important?

Answer:

The application layer is the top-most layer in the OSI model and is used for establishing process-to-process communication and user services in a network. It's the interface between user applications and the underlying network. whether you open a web page in a browser or read an email, you are interacting with the application layer of the network. In short, it's a layer which involves human interaction with applications and software to connect users together across the globe.

A protocol is a set of rules used to communicate between systems in a network. Although the

application layer is the medium through which you are able to communicate with other users, a set of protocols are required to assist with this communication.

For example, if you have to open a web page, you need the HTTP or HTTPS protocols. Similarly, you would require POP3 or IMAP and SMTP for sending and receiving emails.

Application layer importance: The application layer is the highest abstraction layer of the TCP/IP model that provides the interfaces and protocols needed by the users. It combines the functionalities of the session layer, the presentation layer and application layer of the OSI model.

The functions of the application layer are.

- It facilitates the user to use the services of the network.
- It is used to develop network-based application.

It provides user services like user login, naming network devices, formatting message, and e-mails, transfer of files etc.

It is also concerned with error handling and recovery of the message as a whole.

Ans: to the que: no:- 4 (b)

Q: What is the difference between a primary Servers and secondary server?

Answer:

A primary server is a Servers that stores a file about the zone for which it is an authority.	A secondary server is a Servers that transfers the complete information about a zone from another Server.

It is responsible for, creating, maintaining and updating the zone file.	The secondary servers neither creats nor updates the zone files. If updating is required, it must be done by the primary server.
It stores the zone file on a local disk.	It store the file on it's local disk.
It is the ~~ke~~ read/write copy of the DNS database.	It is the read only copy of the DNS records.
Sends information to the secondary servers	Receives data from the primary servers automatically
One DNS servers can have only one primary DNS Server.	There are can be up to 255 Secondary DNS servers.

Ans: to the que: no:- 4(c)

Q: How the client-servers model works? Write the advantage and disadvantage of client-servers model

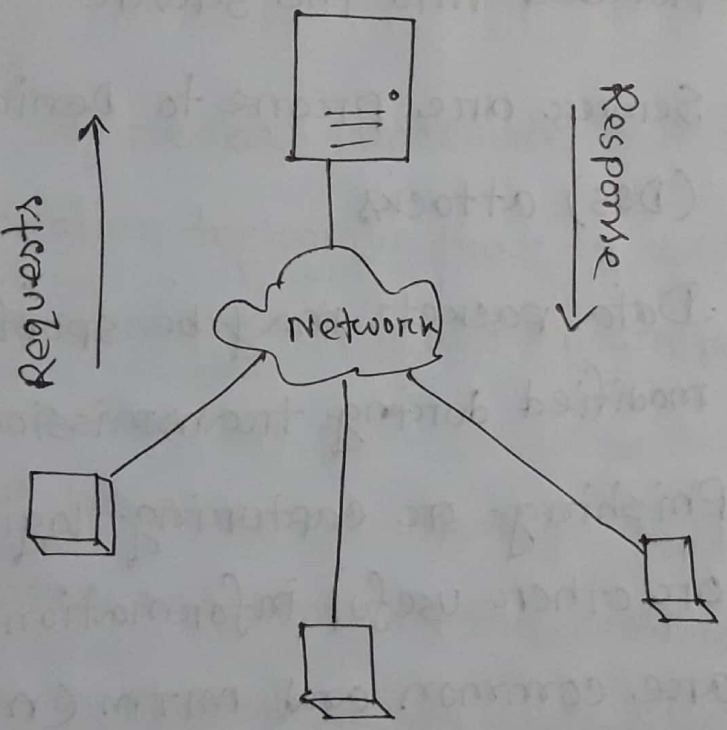
Answer:

In this article we are going to take

a dive into the client-servers model and have a look at how the Internet works via, web browsers. This article will help us in having a solid foundation of the WEB and help in working with WEB technologies with ease.

- Client: when we talk the word client, it mean to talk of a person or an organization using a particular service.
  Similarly in the digital world a client is a computers (Host) i.e. capable of receiving information or using a particular service from the service providers (servers).
- Servers: when we talk the word servers, it mean a person or medium that serves something. Similarly in this digital world a Server is a remote computers which provides information (data) or access to particular services.

So, it basically the client requesting something and the servers serving it as long as it present in the database.



Advantage of client-servers model :

Centralized system will all data in a single place
Cost efficient requires less maintenance cost and Data recovery is possible.
The capacity of the client and servers can be changed separately.

Disadvantages of client-server model:

clients are prone to viruses, Trojans and worms if present in the server or uploaded into the server

Servers are prone to Denial of service (DOS) attacks

Data packets may be spoofed or modified during transmission.

Phishing or capturing login credentials or other useful information of the user are common and MITM (Man in the middle) attacks are common.

Ans: to the que: no:- 5 (a)

Q: What is Remote ~~Rt~~ Procedure Call? How does remote procedure call work?

Answer:

A remote procedure call is an interprocess communication technique that is used for client-server based applications. It is also known as a subroutine call or a function call.

A client has a request message that the RPC translates and sends to the server. This request may be a procedure or a function call to a remote server. When the server receives the request, it sent the required response back to the client. The client is blocked while the server is processing the call and only resumed execution after the server is finished.

This is the mechanism where one process interacts

with another by means of procedure calls. One process (client) calls the procedure lying on remote host. The process on remote host is said to be Server. Both processes are allocated stubs. This communication happens in the following ways:

- The client process calls the client stub. It passes all the parameters pertaining to program local to it.
- All parameters are then packed (marshalled) and a system call is made to send them to other side of the network.
- Kernel sends the data over the network and the other end receives it.
- The remote host passes data to the server stub where it is unmarshalled
- The parameters are passed to the procedure and the procedure is then executed.

- The result is sent back to the client in the same manner.

Ans: to the que: no:- 5 (b)

Q: What are the two main categories of DNS message? Write the answer with ~~diagr~~ block diagram

Answer:

DNS have two types of message :-

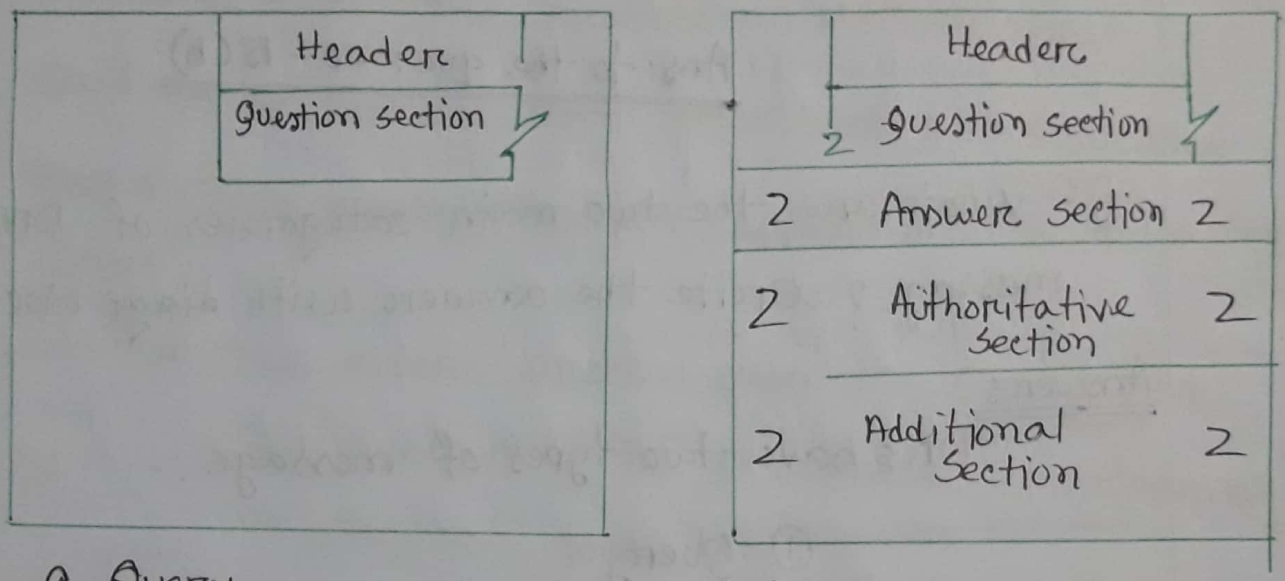
1. Query
2. Response

Both type have ~~f~~ same format

1. Query :- The query message consists of a
   - Header and
   - Question records
2. Response :- The response message consists of a
   - Header
   - Question records
   - Answer records
   - Authoritative records

- Additional records.

Figure



a. Query

b. Response

Header:

- Both query and Response message have the save header format with some fields set to zero for the query menages.
- The header is 12 bytes.

Question section:

- This is a section consisting of one or more question records
- It is present on both query and response message.

Answer Section:

- This is a section consisting of one or more response records.
- It is present only on response message.
- Includes the answer from the server to the client.

Authoritative section:

- This is a section consisting of one or more ~~Present~~ resource records.
- It is present only on response message.
- Gives information about one or more authoritative servers.

Additional Information section:

- This is the section consisting of one ~~one~~ or more resource records.
- It is present only on response message.
- Provides the additional information that may help the resolver.

Ans: to the que: no:- 5 (c)

Q: DNS uses UDP instead of TCP. If a DNS packet is lost, there is no auto automatic recovery. How is this problem handled?

Answer:

Yes, when DNS packets are lost, or a DNS servers is unable to respond, this can cause problems with applications. DNS handles the resolution of host names to IP address. Without this information, an application cannot initiate a connection with the appropriate host on the network or Internet. For example, when you a type in www.yahoa.com into a web browser, then DNS resolves the address to 66.94.230.38, and the browser attempts an http connection to this IP address. When you see problems with DNS, you see the browser "wait"

for a response; or in the case of Explorer, it will eventually come back and tell you it couldn't find a particular domain.

There are a couple of ways to minimize the impact of a DNS problem. First is to configure your computers to use multiple DNS servers. In this case, if the primary DNS server fails, the backup servers will be used to try to resolve the data. On a windows machine this can be configured within the Internet Protocol (TCP/IP) Properties window associated with a given Network connection.

A second, but not very graceful, way around this with critical applications is to not use hostnames at all, but to use the fixed IP address in the configuration. This circumvents the DNS process completely. Unfortunately, this is not very scalable and does not allow for graceful IP address changes.

Ans: to the que: no:-6(a)

Q: What is DNS? What are the three domains of domain name space in internet? Explain with details.

Answer:

The Domain Name System (DNS) is the phonebook of the Internet. ~~Humas~~ Humans access information online through domain names, like nytimes.com or espn.com. Web browsers interact through Internet Protocol (IP) addresses. DNS translates domain names to IP addresses so browsers can load Internet resources.

Each device connected to the Internet has a unique IP address which other machines use to find the device. DNS servers eliminate the need for ~~humas~~ humans to memorize IP addresses such as 192.168.1.1 (in IPv4), or more complex newer alphanumeric IP addresses such as 2400:cb00:2048:1::c629:d7a2 (in IPv6).

There are three domains of domain name space are:

① Generic domain
② Country domain
③ Inverse Domain

→ It defines the registered hosts according to their generic behavior.

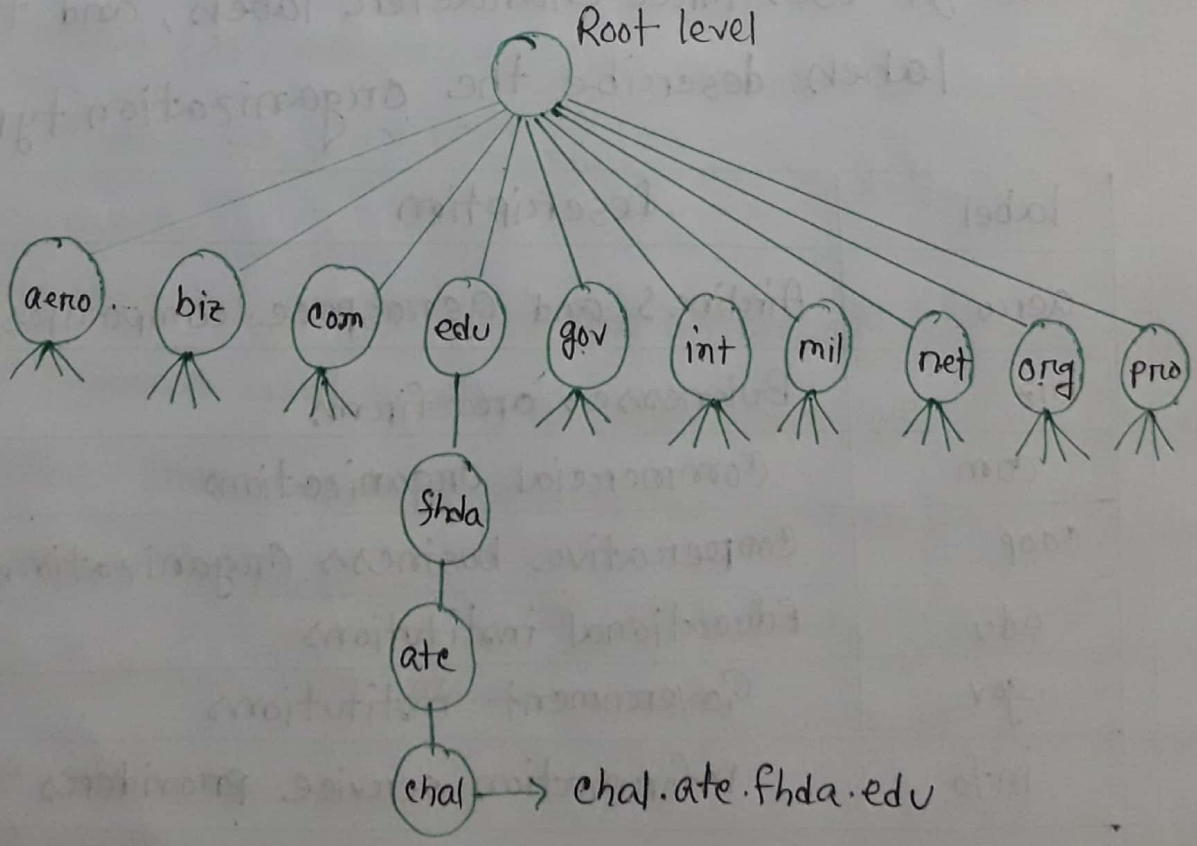
→ Each node in a tree defines the domain name, which is an index to the DNS database.

→ It uses three-character labels, and these labels describe the organization type.

label	Description
aero	Airlines and aerospace companies
biz	Businesses or firms
com	Commercial organizations
coop	Cooperative business organizations
edu	Educational institutions
gov	Government institutions
info	Information service providers

int	International Organizations
mil	military groups
museum	Museum & other nonprofit organizations
name	Personal names
net	Network support centers
org	Nonprofit Organizations
pro	Professional individual Organizations

Figure of generic domains:

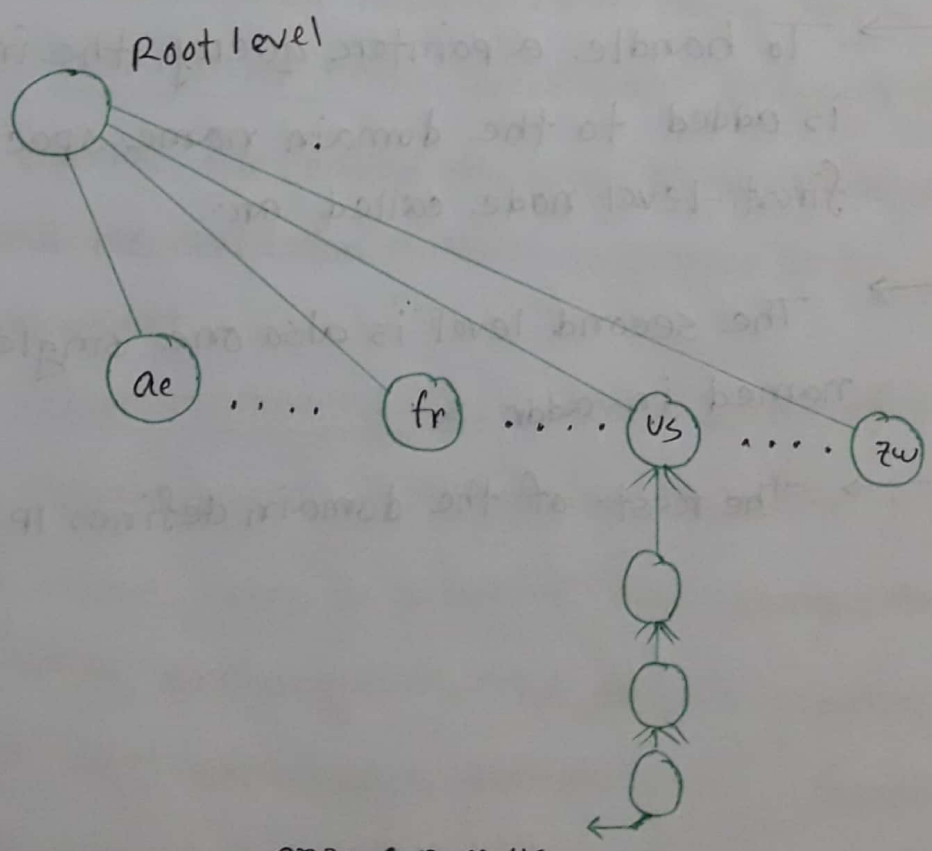


② Country domain :-

→ The country domain sections uses two character country abbreviation.

→ Second labels can be organizational or they can be more specific national designations

→ The address anza.cup.ca.us can be translated to De Anza college in Cupertino, ~~calfo~~ california, in the United states.



③ Inverse domain:

→ The inverse domain is used to map an address to name

→ This may happen, for example, when a server has received a request from a client to do a task. Although the server has a file that contains a list of authorized clients only the IP address of the client in listed

→ To handle a pointer query, the inverse domain is added to the domain name space with the first-level node called arc.

→ The second level is also one single node named in-addr

→ the rest of the domain defines IP address.

Ans: to the que: no:- 6(b)

Q: Describe the addressing system used by SMTP. How does SMTP work?

Answer:

The addressing system used by SMTP consists of two parts: a local part and a domain name, separated by an @ sign. The domain name refers to a host ~~hat~~ that receives and sends mail.

Local Part: The local part defines the name of a special file, called the user mailbox, where all the mail received for a user is stored to be used by the user agent.

Domain name: The second part of the address is the domain name. An organization usually selects one or more hosts to receive and send; they are called mail exchangers. The domain name assigned to each mail exchanger either comes from the DNS database or is a logical name.

Working of an SMTP: The functioning of a SMTP servers can be broken down into two steps. The first step includes verification of the computers configuration through which an email is sent and granting permission for the process. In the second step, it sends out the message and follows the successful delivery of the mail. If due to some reason, the mail fails to be delivered, it is returned to the sender.

The SMTP servers understands simple text commands. The most common commands are as follows:

HELO: Introduce yourself

EHLO: Introduce yourself and request extended mode

MAIL FROM: Specify the sender

RCPT TO: Specify the recipient

DATA: Specify the body of the mail.

Ans: to the que: no:- 6 (c)

Q: What is the difference between SMTP and SNMP?

Answer:

SMTP: SMTP is simple mail Transfer Protocol. This protocol is used in computer networks for email purposes. the mail servers listens on tcp port number 25 while clients send their queries on tcp port number 587. These ports can be changed. These are the default port numbers.

SNMP: SNMP is simple Network management Protocol. This network protocol is used to monitor the health status, disk utilisation, temprature, no of cpu's and other parameters of a network device. These network device can be a routers, switch, load-balancers, servers, etc. For SNMP there has to be a Servers which listens on UDP port 514. A client has to be configured to sent the above mentioned parameters to the SNMP server.

Ans: to the que: no:- 7(a)

Q: What is FTP? How does FTP work?

Answer:

File Transfer Protocol (FTP) is a client/server protocol used for transferring files to or from a host computer. FTP may be authenticated with user names and passwords.

The end-users machine is typically called the local host machine, which is connected via the internet to the remote host - which is the second machine running the FTP software.

Anonymous FTP is a type of FTP that allows users to access files and other data without needing an ID or ~~pass~~ password. Some websites will allow visitors to use a guest ID or password - anonymous FTP allows this.

How FTP works: FTP is a client-server protocol that relies on two communications channels between client and server: a command channel for controlling the conversation and a data channel for transmitting file content. Clients initiate conversations with servers by requesting to download a file. Using FTP a client can upload, download, delete, rename, move, and copy files on a server. A user typically needs to log on to the FTP server, although some servers make some or all of their content available without login, known as ~~anof~~ anonymous FTP.

FTP sessions work in passive or active modes. In active mode, after client initiates a session via a command channel request, the server initiates a data connection back to the client and begins transferring data. In passive mode, the server instead uses the command channel to send the

client the information it needs to open a data channel. Because passive mode has the client initiating all connections, it works well across firewalls and Network Address-Translation (NAT) gateways.

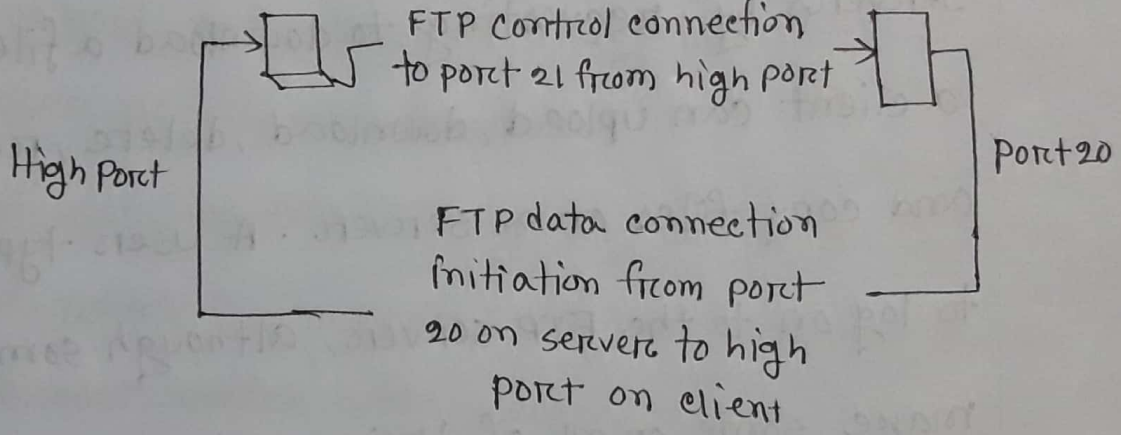


fig: Active FTP

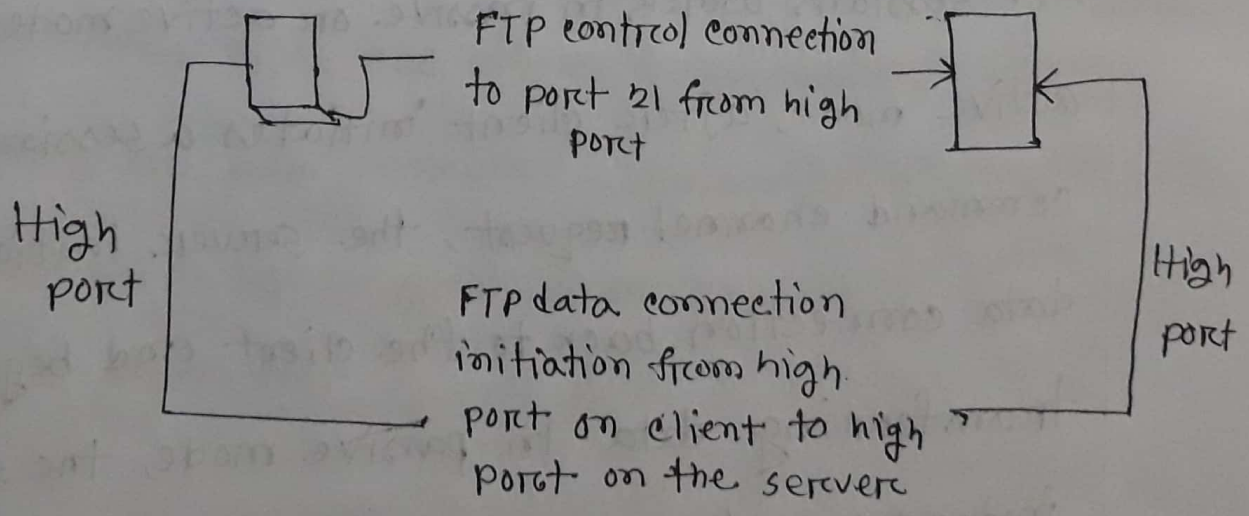


fig: Passive FTP

Users can work with FTP via a simple command line interface (for example, from a console or terminal window in Microsoft Windows, Apple OS X or Linux) or with a dedicated graphical user interface (GUI). Web browsers can also serve as FTP clients.

Ans: to the que: no:- 7 (b)

Q: Write the advantage and ~~dist~~ disadvantages of FTP.

Answer:

Advantages of FTP:

- **Speed:** one of the biggest advantages of FTP is speed. The FTP is one of the fastest way to transfer the files from one computer to another computer.
- **Efficient:** It is more efficient as we do not need to complete all the operations to get the entire file.
- **Security:** To access the FTP server, we need to

login with the username and password. Therefore, we can say that FTP is more secure.

- Back & forth movement: FTP allows us to transfer the files back and forth. Suppose you are a manager of the company, you send some information to all the employees, and they all send information back on the same server.

Disadvantages of FTP:

- The standard requirement of the industry is that all the FTP transmissions should be encrypted. However, not all the FTP providers are equal and not all the provider offers encryption. So, we will have to look out for the FTP providers that provides encryption.
- FTP serves two operations, i.e, to send and receive large files on a network. However,

the size limit of the files in 2GB that can be sent. It also doesn't allow you to run simultaneous transfers to multiple receivers.

- Passwords and file contents are sent in clear text that allows unwanted eavesdropping. So, it is quite possible that attackers can carry out the brute force attack by trying to guess the FTP password.
- It is not compatible with every system.

Ans: to the que: no:- 7(c)

Q: What is POP3 and which are the default POP3 ports.

Answer:

Post office Protocol version 3 (POP3) is a standard mail protocol used to receive emails from a remote server to a local email client. POP3 allows you to download email message on your local

computer and ~~read~~ read them even when you are offline. Note, that when you use pop3 to connect to your email account, messages are downloaded locally and removed from the email server. This means that if you access your account from multiple locations, that may not be the best option for you. On the other hand, if you use pop3, your messages are stored on your local computer, which reduces the server your mail account uses on your web server.

By default, the pop3 protocol works on two ports

- Port 110 – this is the default pop3 non-encrypted port.
- Port 995 - this is the port you need to use if you want to connect using pop3 securely.

Ans: to the que: no:- 7 (d)

Q: Is Gmail a pop 3 or IMAP ?

Answer: Gmail allows access to its IMAP and pop mail servers so you can set up the email software on your computer or mobile device to work with the service. Most premium and some free email applications offer both IMAP and pop email compatibility, while other free email programs may offer only the pop email service.

Ans: to the que: no:- 8 (a)

Q: What is Hypertext Transfer Protocol (HTTP)? Write the features of HTTP.

Answer:

The Hypertext Transfer Protocol (HTTP) is an application-level protocol for distributed, collaborative, hypermedia information systems. This is the foundation

for data communication for the World Wide Web. HTTP is a generic and stateless protocol which can be used for other purposes as well using extensions of its request methods, error codes, and headers. Basically, HTTP is a TCP/IP based communication protocol, that is used to deliver data (HTML files, image files, query results, etc) on the World Wide Web. The default port is TCP 80, but other ports can be used as well. It provides a standardized way for computers to communicate with each other. HTTP specification specifies how clients' request data will be constructed and sent to the server, and how the servers response to these requests.

Features of HTTP:

There are three basic feature that make HTTP a simple but Powerful protocol:

HTTP is connectionless: The HTTP client, i.e., a browser initiates an HTTP request and after

a request is made, the client waits for the response. The server processes the request and sends a response back after which client disconnect the connection. So client and server knows about each other during current request and response only. Further requests are made on new connection like client and server are new to each other.

- HTTP is media independent: It means, any type of data can be sent by HTTP as long as both the client and the servers know how to handle the data content. It is required for the client as well as the servers to specify the content type using appropriate MIME-type.

- HTTP is stateless: As mentioned above, HTTP is connectionless and it is a direct result of HTTP being a stateless protocol. The servers and client are aware of each other only during a current request.
Afterwards, both of them forget about each

other. Due to this nature of the protocol, neither the client nor the browser can retain information between different requests across the web pages.

Ans: to the que: no:- 8(b)

Q: What is the difference between HTTP and FTP?

Answer:

~~Basis~~	HTTP	FTP
Basic	HTTP is used to access websites.	FTP transfers file from one one host to another
connection	HTTP establishes data connection only.	FTP establishes two connection one for data and one for the control connection.
TCP port	HTTP uses TCP's port number 80	FTP uses TCP's port number 20 and 21
URL	If you are using HTTP, http will appear in URL.	If you are using FTP, ftp will appear in URL

Efficient	HTTP is efficient in transferring smaller files like web pages.	FTP is efficient in transferring large files.
Authentication	HTTP does not require authentication.	FTP requires a password.
	The content transferred to a device using HTTP is not saved to the memory of that device.	The file transferred to the host device using FTP is saved in the memory of that host device.

Ans: to the que: no:- 8(c)

Q: What is node-to-node, host-to-host and process-to-process delivery?

Answer:

Node-to-node delivery: The data link layer is responsible for delivery of frames between two neighboring nodes over a link. This is called note-to-node delivery.

Host-to-host delivery: The network layer is responsible for delivery of datagrams between two hosts. This is called host-to-host delivery.

Process-to process delivery: Communication on the internet is not defined as the exchange of data between two nodes or between two hosts. Real communication takes place between two process. So that we need process-to-process delivery.

The transport layer is responsible for process-to-process delivery. The delivery of a packet. part of a message, from one process to another.

Answer: to the que: no:- 8(d)

Q: Write the different types of Network Services? And write the feature of communication services?

Answer:

There are four types of network services

① Directory Services

② File Services

③ Communication Services

④ Application Services

Communication Services:

- **Email:** Electronic mail is a communication method and something a computer user cannot work without.
- **Social Networking:** Recent technologies have made technical life social. The computer savvy peoples, can find other known peoples or fiends, can connect with them, and can share throughts, pictures and videos.
- **Internet Chat:** Internet chat provides instant text transfer services between two hosts. Two or more people can communicate with other using text based Internet Relay chat Services
- **Discussion Boards:** Discussion boards provide a mechanism to connect multiple peoples with same interests.