NAME : RADHIKA PATWARI
ROLL NO. : 18CS10062

DATE : 30/1/2021

==========

1.

IF using same port address, tcp will not be able to differentiate as the destination port address is a part of the response and request.

http://80:www.mypages.ac.in/index.html
http://8080:www.mypages.ac.in/index.html

2. HTTP GET requests required = 3. They are :

GET http://www.mynetworkcourse.org/mypage.html HTTP/1.1
GET /network.gif HTTP/1.1
GET /images/cs31006.gif HTTP/1.1

3. SMTP is a push protocol so the sending mail server pushes the file to the receiving mail server. So, when the user wants to retrieve his emails from MTA,it is basically a pull type request and can be established using protocols like HTTP, POP3 and IMAP which support the get method.But SMTP does not provide such request functionality and hence cannot be used.

For the given scenario in the question,
For SMTP to push the email from MTA to client mailbox at User agent, first a TCP connection needs to be established between MTA and UA. It may happen that the client UA is behind a firewall and hence the TCP connection request gets ignored. Thus the mail will never be sent to the user and he will never be informed that a mail has come for him.
The SMTP at MTA does not know the port address of the client mailbox at UA because it may happen that the UA is set on a local PC of the user and hence all available ports have value > 1023 and cannot be just guessed. Hence the default port for SMTP i.e., 25 cannot be used in this case.

Presently IMAP protocol is used which provides user extra facilities of creating folders in MTA and rearranging the mails. Also the user can opt to download just the header or a small part of the mail instead of the entire mail. These facilities will not be there if SMTP is modified to push mails from MTA to UA.

4. FTP uses two parallel TCP connections to transfer a file, a control connection and a data connection. The control connection is used for sending control information between the two hosts—information such as user identification, password, commands to change remote directory, and commands to “put” and “get” files. The data connection is used to actually send a file. Because FTP uses a separate control connection, FTP is said to send its control information out-of-band. HTTP sends request and response header lines into the same TCP connection that carries the transferred file itself.It is thus said to send its control information in-band.Hence in FTP, while the connection is established at the control end, large files can be easily transferred through the data connection, thus reducing traffic. In passive mode, this feature enables the server to satisfy the request of many clients through FTP else the server may get blocked till the entire file is transferred/received to/from the client.

5. The command channel is used to send control information between the FTP client and server. This involves information such as user identification, password, commands to change remote directory, and commands to “put” and “get” files.
The data connection is used to actually transfer the file from server to client and to receive the file from client at server end.
Using two separate channels ensures that the file transfer takes place through a separate channel without any traffic. Also if the file transfer is taking time, in the meantime FTP can break the control connection with this client and the server can accept the connection request from a new client.

Especially in ‘passive’ mode, after the client initiates a control connection with FTP server at port 21, the server passes a randomly available port through ‘PASV’ command and then the FTP client initiates a connection to this random port for file transfer. In one data connection,only one file can be transferred either from server side or client side. Thus in passive mode, the client can initiate multiple data connections at various ports of server and enable sharing of multiple large files simultaneously.

This is not possible in ‘active’ mode as the port 20 of server is reserved for file transfer.

6.
There are 2 transactions between client computer and local DNS - one request and one response. But on local dns side, there are 6 more transactions - between local dns and root server,between local dns and top level domain server,between local dns and authoritative server - one request and one response each.
Thus for a query , there are a total of 8 transactions.

Yes if many clients are connected to the same local dns, there can be traffic and congestion of network.However, local dns uses cache feature but for millions of clients even that may not suffice.

7.

- cse.iitkgp.ac.in is the Domain name to which the DNS record applies
- 86400 is the Time to live in seconds.This implies that the record is valid for 86400 seconds.After this it will expire and will not be valid.
- IN implies that the DNS record is based on internet resources.
- A means it is a A type record which returns a 32-bit ipv4 address of the host whose ip is asked in the DNS query.
- 203.110.245.250 is the ipv4 address of the host ‘cse.iitkgp.ac.in’

8.

(a)False, devices like L2 switch supports physical and data link layer, router supports physical,data link and network layer only; hence it is not necessary that all devices have to support all 5 layers in a network.
(b) False, as we move down in the protocol stack from application layer, tcp header at transport layer, IP header at networks layer, MAC header at data link layer and physical header and trailer at physical layer are added.. Thus length of pdu increases as we move down in the network protocol stack.
(c)False, DNS uses normal UDP and after sending numerous requests to dns server, if no reply is received, the connection is aborted and a error is received at client side.
(d) True, as more than one http get request can be sent from client side without waiting for the response of previous requests from http server.