CSE421
Lab 02 Home Task
Summer 2022
ID-1910159
Sec-08

Write answers to the following questions.

1. How would a proxy server check to see if its data is up to date with the most updated data in the Origin Server?
   The proxy server acts as a gateway between the client pc and the internet. Proxy servers improve efficiency by using a local cache to provide documents rather than getting them from the origin server. If a document is out-of-date, the Proxy Server can inspect it and then refresh the cached copy. It tries to reroute the requests to check if the data is up-to-date or not. If the response from the web server is successful the proxy server ascertains that the data is up-to-date, if not, it gets the most updated one from the original server.

2. The HTTP protocol is implemented in the Physical layer. Is this statement true or false?
   Given that HTTP is an application layer protocol, the statement is false.

3. Can you receive mail using SMTP, why or why not?
   No, we cannot receive emails using SMTP protocol mainly because POP and IMAP are used to receive mail. Simple Mail Transfer Protocol (SMTP), as its acronym suggests, is a protocol used to send and transfer emails. Using an outbound SMTP server is essential because otherwise, the email message cannot be delivered to the recipient.

4. Briefly explain how SMTP and POP3 protocol works using a scenario.

   <SMTP SCENARIO>
   S: 220 coolbeans.edu
   C: HELO nuggets.fr
   S: 250 Hello crepes.fr, nice to meet you
   C: MAIL FROM: <jenny@nuggets.fr>
   S: 250 jenny@nuggets.fr... Sender ok
   C: RCPT TO: <james@coolbeans.edu>
   S: 250 james@ coolbeans.edu ... Recipient ok

C: DATA
S: 354 Enter mail, end with "." on a line by itself
C: Do you like Barbie?
C: How about Ken?
C: .
S: 250 Message accepted for delivery
C: QUIT
S: 221 coolbeans.edu closing connection

<POP Scenario>
S: +OK POP3 server ready
C: user Kenny
S: +OK
C: pass hungry
S: +OK user successfully logged on
C: list
S: 1 498
S: 2 912
S: .
C: retr 1
S: <message 1 contents>
S: .
C: dele 1
C: retr 2
S: <message 1 contents>
S: .
C: dele 2
C: quit
S: +OK POP3 server signing off

5. Why does root DNS servers maintain a hierarchical structure rather than a centralized structure?
   The DNS servers maintain a hierarchical structure to decrease the load on the root server. Since almost all the queries access the DNS server for DNS lookup, it would be impossible for a centralized server to take this many requests. The response time

would be too much and the response might be faulty. Hence, a hierarchical, decentralized structure is used for prompt request handling.

6. Suppose, you have a quiz which will take place at bux but your local DNS server does not know the IP address of "bux.bracu.ac.bd". Will you be able to attend your quiz? Please, provide a brief explanation.
   The website cannot be located or loaded if the DNS server cannot identify the right IP address that belongs to the hostname entered. So, without knowing the IP address of bux.bracu.ac.bd, the site cannot be accessed and I won't be able to attend the quiz. The authoritative name server or TLD name server will be returned if the DNS server doesn't have the IP address. This iterative process will be carried out by the requester until it receives a response or runs out of time. To solve this problem, I will have to manually type the IP address or else the site can't be loaded.
7. Suppose, you recently changed your ISP and the new ISP forgot to set the DNS server's IP address when configuring your internet connection. Can you now browse the internet properly?
   We can browse the internet using third party DNS server IP addresses but that won't be efficient and safe since it will take much more time to fetch the IP and load the sites. This might result in a 'time-out'. Since the hierarchical form of DNS is there so that our requests can be processed by the closest DNS server for the fastest response, the DNS set by the ISP is necessary. We can also manually paste and type IP addresses of websites but that seems like a very cumbersome process.

8. What is the size of an ARP request or reply packet (in bytes)?
   28 bytes
9. What happens to an ARP request packet when it is received by a host that does not match the target IP address of the request?
   Since ARP request packets are broadcasted to all the hosts, the ones receiving the unmatched IP addresses will drop or reject the packet.

10. What is the value of the 'operation' field in an ARP reply packet?
    This field in an ARP response has a value of 2 bytes.

11. What flags are used during a TCP connection establishment and TCP connection termination process.
    SYN and FIN flags respectively.

12. A web server sends a TCP packet to a client with sequence number=0 and acknowledgement number =1. Which stage of the 3 way handshake is this and what does the sequence and acknowledgement number mean?
    This is the second stage of the three-way handshake where sequence number=0 and acknowledgement number =1 means that the server device is acknowledging that the client is ready for receiving data.
13. In an outbound PDU packet, what does source port: 80 and destination port: 1027 means?
    Source port 80 indicates that a server is sending data to a receiver client. The destination port 1027, which was arbitrarily chosen for temporary use, is where this data is being received. Typically, HTTP activities run on port 80, whereas IPv6 uses port 1027.