**CSE421**

**Lab 02 Hometask**

**Summer 2023**

**Niamotullah Ratul – 19301151  
Section: 5**

1. How would a proxy server check to see if it’s data is up to date with the most updated data in the Origin Server?

Answer:

No matter if a client request a thing from proxy server, the proxy server always sends a Header request to the origin server. And whenever the origin server provides the proxy server with it’s header, the proxy server then compare it’s current header to origin server’s header via Last-Modified Since method, If the origin server has updated in this period then the proxy server request for the data or the body. In this way, proxy server always gets up to date with the origin server.

1. The HTTP protocol is implemented in the Physical layer. Is this statement true or false?

Answer:

No the statement is false.

1. Can you receive mail using SMTP, why or why not?

Answer:

No I can’t receive mail using SMTP as it is not the protocol for receiving the mail. But we can use it for sending the mail. However, for receiving the mail we use POP3.

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

Answer:

SMTP is responsible for sending email from a client to a mail server, while POP3 is used to retrieve email from a mail server to a client. For sending a mail The client establishes an SMTP connection with the outgoing mail server. The client provides the sender's and recipient's email addresses, subject, and message content. The client sends the email as an SMTP message to the server. The server receives the SMTP message, performs recipient validation, and stores the email in the recipient's mailbox.

And to receive a mail the client establishes a POP3 connection with the incoming mail server. The client authenticates with the server using credentials. The client sends a POP3 command to list the emails in the mailbox. The server responds with the list of available emails and their unique identifiers. The client selects an email by specifying its identifier. The server sends the selected email to the client as a POP3 response. The client retrieves and displays the email content.

1. Why does root DNS servers maintain a hierarchical structure rather than a centralized structure?

Answer:

Root DNS servers maintain a hierarchical structure rather than a centralized structure for several reasons... Scalability, Redundancy and Resilience, Localized Resolution, Decentralization and Autonomy, Load Distribution. Where as if we used a centralized structure we wouldn’t have access to these benefits.

1. 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.

Answer:

Yes, I will be able to attend the quiz.

But I will be little bit late to enter the home page for the first time. As my local DNS server does not know the IP address It will do a Recursive DNS Resolution or use the DNS Hierarchy to resolve my IP address. As we know DNS system has a hierarchical structure. If my local DNS server doesn't have the IP address, it contacts other DNS servers higher in the hierarchy, such as root DNS servers, top-level domain (TLD) servers, and authoritative DNS servers for the specific domain.

1. 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?

Answer:

Yes, I still can browse the internet properly. However, for the very first request it would take more time than usual as my devices has to find out the local DNS server and other necessary things via broadcasting.

1. What is the size of an ARP request or reply packet (in bytes)?

Answer:

28 bytes.

1. 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?

Answer:

It simply didn’t response to the ARP request if it is not meant for it. Only the host that match the target IP address will reply to the request and in that way we can find our targeted devices.

10. What is the value of the 'operation' field in an ARP reply packet?

Answer:

In an ARP reply packet, the value of the 'operation' field is 2.

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

Answer:

During a TCP connection establishment process, the following flags are used…

SYN, ACK, SYN-ACK

During a TCP connection termination process, the following flags are used…

FIN, ACK, FIN-ACK

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?

Answer:

As from the question we can see here a server sends a TCP packet to a client it means it is in second way of the 3 way handshake. As we know only in middle phase of TCP connection process the server sends a response with ACK and SYN flags.

Here sequence number is 0 means it has sent data up to 0 bytes. And via sending acknowledgment number 1 means now it wants data from that range. i.e. it receives the data

upto 1.

13. In an outbound PDU packet, what does source port: 80 and destination port: 1027 means?

Answer:

An outbound PDU packet with source port 80 and destination port 1027 signifies that the packet is being sent from a web server or client using the HTTP protocol (commonly associated with port 80) to a destination port 1027, which could be a non-standard or dynamically assigned port associated with a specific application or service.