Internet Engineering

© Amir Fazlollahi, 9722032

HW1

1.

HTTP version	Caching	Persistency	Pipelining	Multiplexing
1.0	✓	✗	✗	✗
1.1	✓	✓	✓	✗
2	✓	✓	✓	✓
3	✓	✓	✓	✓

HTTP/3 uses the UDP to fix head-of-line-blocking. In HTTP/2 with a packet loss or reordering, all parallel connections stop for the loss recovery in the TCP. HTTP/3 provides native multiplexing over the UDP to resolve this issue.

2.

1)

Stateless connections don't track or store the transactions. So, each new connection bears no information about the past transactions between the two peers. Stateful connections memorise past transactions and their results for future use; with each new connection coming, the peers track the history of the connections between them.

2)

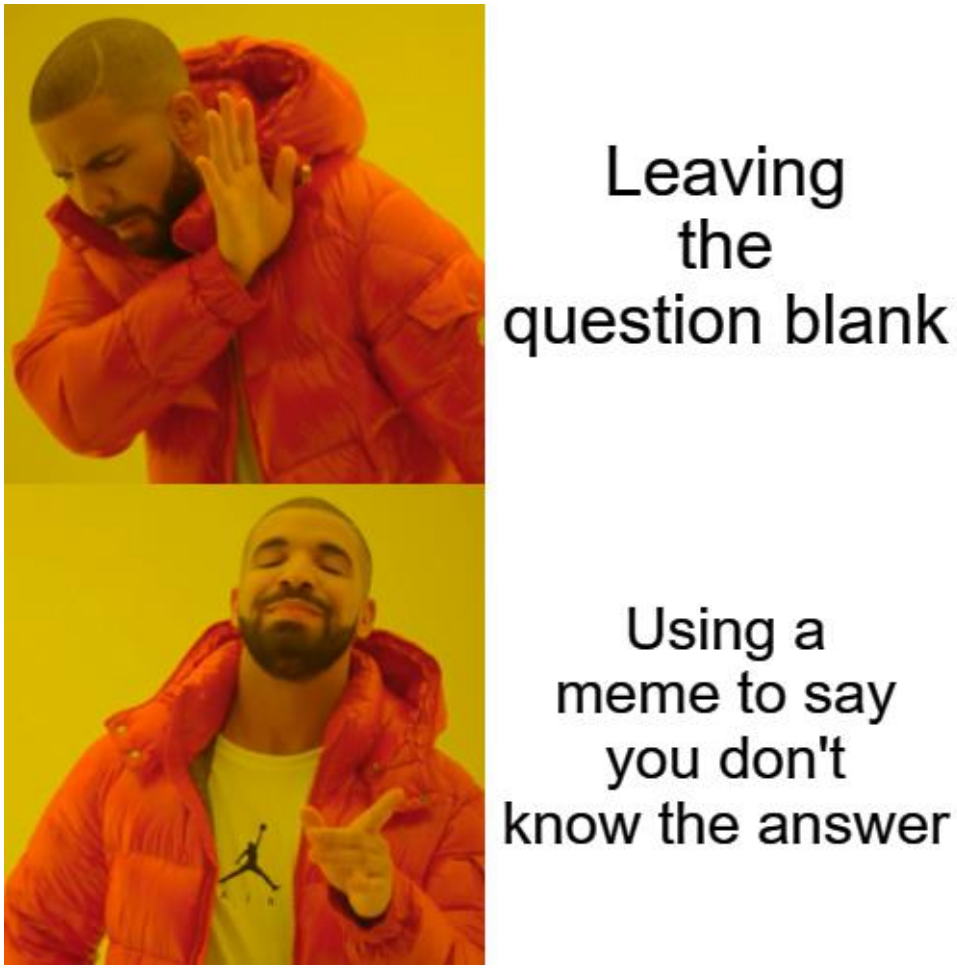
HTTP is a stateless connection. To tackle the challenges of this approach, HTTP uses cookies or web tokens; web servers usually store the state of their clients, and the clients with each HTTP connection send their IDs to the servers. This way, the servers can track the history of their clients' transactions.

3.

1)

Webhooks, web chatting and alerting operate based on unexpected transfer of data from the server to the client. The HTTP is a client/server protocol in which always the client starts the connection.

2)



4.

`ss://asghar:1234!!@ss.myproxy.com:1234\#shadowSocks1`

Protocol: ss

user: asghar

pass: 1234!!

host: ss.myproxy.com

port: 1234

frag: shadowSocks1

5.

1)

500; internal server error.

2)

404; not found.

3)

If moved permanently, use 301 or 308. If moved temporarily, use 302 or 307. Use 307 or 308 to force the client to use the same method in their new request.

4)

429; too many requests.

5)

200; renewing the token has been successful, and the new one resides in the response header.

6)

403; forbidden.

6.

1)

Packages are static content. We can cache such static content onto **reverse proxies t**o offload the main servers.

2)

We can use **reverse proxies** to distribute requests to several web servers.

3)

Use a **reverse proxy** to authenticate users before giving them access to the service.