Homework 2

Wireshark Lab DNS

15. See assignment submission
16. 2603:9001:20f0:7290:1; Yes, this is local DNS
17. Type NS no Answers
18. use5.akam.net, use2akam.net... Yes
19. See assignment submission
20. The query sent to bitsy.mit.edu is sent to 18.0.72.3
21. There are type A and AAAA query sent with info containing bitsy and ait
22. There is 1 answer with the authoritative nameserver
23. See assignment submission

Homework 2

Wireshark Lab HTTP

5. HTTP Authentication
   18. 401 Unauthorized
   19. Authorization with <username>:<password>

Wireshark Lab DNS

1. nslookup
   1. alibaba.asia → 165.160.1520
   2. An authorative server for www.cam.ac.uk is auth0.dns.cam.ac.uk
   3. Server Refused
2. ipconfig → No tasks
3. Tracing DNS with Wireshark
   4. It was sent over User Datagram Protocol (UDP)
   5. Src: 60333 Dst: 53
   6. Sent to 192.168.1.1, yes it is the same
   7. AAAA, a standard query, the query message does not contain answers
   8. 2 answers which seem to be data about the site including Name, Type, TTL & address
   9. I cannot notice anything that stands out
   10. No, it does not.
   11. Dst: 53 Src: 54020
   12. 2603:9001:26f0:7a0::1, Yes
   13. Type A, answers: 0
   14. 3 answers are provided

HTTP Overview

Homework 2

Wireshark Lab HTTP

1. Basic HTTP GET/Response Interaction
    1. Both client and server using 1.1
    2. en-US, en
    3. 192.168.1.55, 128.119.245.12
    4. 200 OK
    5. Tue, Oct 3 2023 18:33:37
    6. 128 bytes
    7. Acknowledgement #
2. Conditional HTTP GET/response interaction
    8. I do not see an if modfied since header
    9. Yes, the server responded with 200 OK
    10. Yes, if-modified-since: Tue, 03 Oct 2023 05:59:02 GMT
    11. 304 Not Modified, no it did not return the contents of the file, it is not included in the body.
3. Retrieving Long Documents
    12. 1 GET request was sent, in my Wireshark Frame #773
    13. 803
    14. 200 ok
    15. 4
4. HTML Documents w/ Embedded Objects
    16. 3 GET requests were sent. The requests were sent to 128.119.245.12 & 178.79.137.164
    17. Parallel, I know this by opening Developer tools on Chrome

Securing TCP

Home Work 2

4. www.ufl.edu
   a. m.root-servers.net → f.edu-servers.net → ens.nane.ufl.edu
   b. www.google.com : m.root-servers.net → ns4.google.com

5. a. Upon clicking the link, an HTTP GET request message is sent, with the source host being the device the site is being accessed From (client) & the destination host would be the server hosting the target URL (www.amazon.com)
   b. The referer likely looks like "www.smartwatchreview.com" so that Amazon can know which site sent the user.
   c. User Agent refers to the browser that made the request: Eg Chrome, Firefox URI Reference is where we are coming from: http://www.smartwatch... Target URI is where the link is bringing us: http://www.amazon.com

6. a. A DATA Frame is being created. The value of the Type field would be 0x0
   b. Length = 1000 + 8 = 1008 bytes
   c. 9 octets + Data (1000) + Padding (8) = 1017 bytes

Wireshark Lab Intro

1. UDP, TCP, QUIC
2. 2 milliseconds
3. 128.119.245.12, 192.168.1.55
4. ✓

Homework 2

Charles
Richardson

1. a. False b. True c. False d. True e. False

2. The client sends the DNS query to the local DNS name server, which checks its cache for the translation of the query. If it is not in the cache, then the local DNS name server contacts a Root level server and awaits for directions to the top level domain server, upon response, it sends a request to the top level server for the authoritative server which contains the address of www.mit.edu/research.html. This all assumes that the local name server is using iterated queries, which are more commonly used than recursive queries due to the burden of recursive queries on the network DNS.

3. Access Link Bandwidth = 15 Mbps $\Delta_{cache} = 10$ millisecond

LAN bandwidth = 100 Mbps

Obj Size = 1,000,000 bits = 125 Kb

Avg Request Rate (B) 14/sec

Internet Response Time = 3 sec

Avg Access Delay (s) = $\Delta / 1 - \Delta B$: Δ - avg time required to send obj over access link (s)

Δ = (s) = $66.\bar{6}$ ms $= \frac{66.\bar{6}ms}{1-(\frac{14}{15})(.067)} \approx$ (1sec) B = arrival rate of objects to access link

Avg Access Delay = $\frac{10 \text{ smill}}{1-(10)(14)r} = \frac{10}{-139}$ s

−140

Total Average Response Time (s) = Internet Response Time + Avg Access Delay

4 sec = 3 sec + 1 sec

Total Response Time with Cache = Total Avg Response Time (0.6) + Cache Response Time (0.4)

= 4(0.6) + microseconds(0.4)

= ~1.6 seconds

Absolutely (something) Fundamental