Midterm CNT William Dellinger

Question 1. Answers:

a. The major differences between TCP and UDP are: TCP relies on connection as opposed to UDP which does not, TCP is much slower than UDP because it guarantees data won't be lost if an error happens. DNS usually uses UDP instead of TCP because most DNS packets are small enough to fit inside of the smaller UDP headers, UDP is also significantly faster than TCP.
b. According to the textbook the internet has 5 layers:
    1. Application layer - https
    2. Transport layer - tcp
    3. network layer - ip
    4. Data link layer - ethernet
    5. Physical layer - hardware like an ethernet cable
c. TTL means time to live. TTL is used to determine how long a DNS record can still be cached. TTL is used to reduce the time a packet is active in the network.
d. The standard size of a TCP header is 20 bytes. The standard size of a UDP header is 8 bytes. Fields that exist in both are checksum, source port, and destination port.

Question 2. Answers:

The domain name is aol.com, to find this I used the command: dig MX aol.com
The ip addresses are :
67.195.204.75
67.195.204.80
67.195.228.84
67.195.228.86
98.136.96.92
98.136.96.93
To obtain these I used the same command as the previous question.

Question 3. Answers:

a.

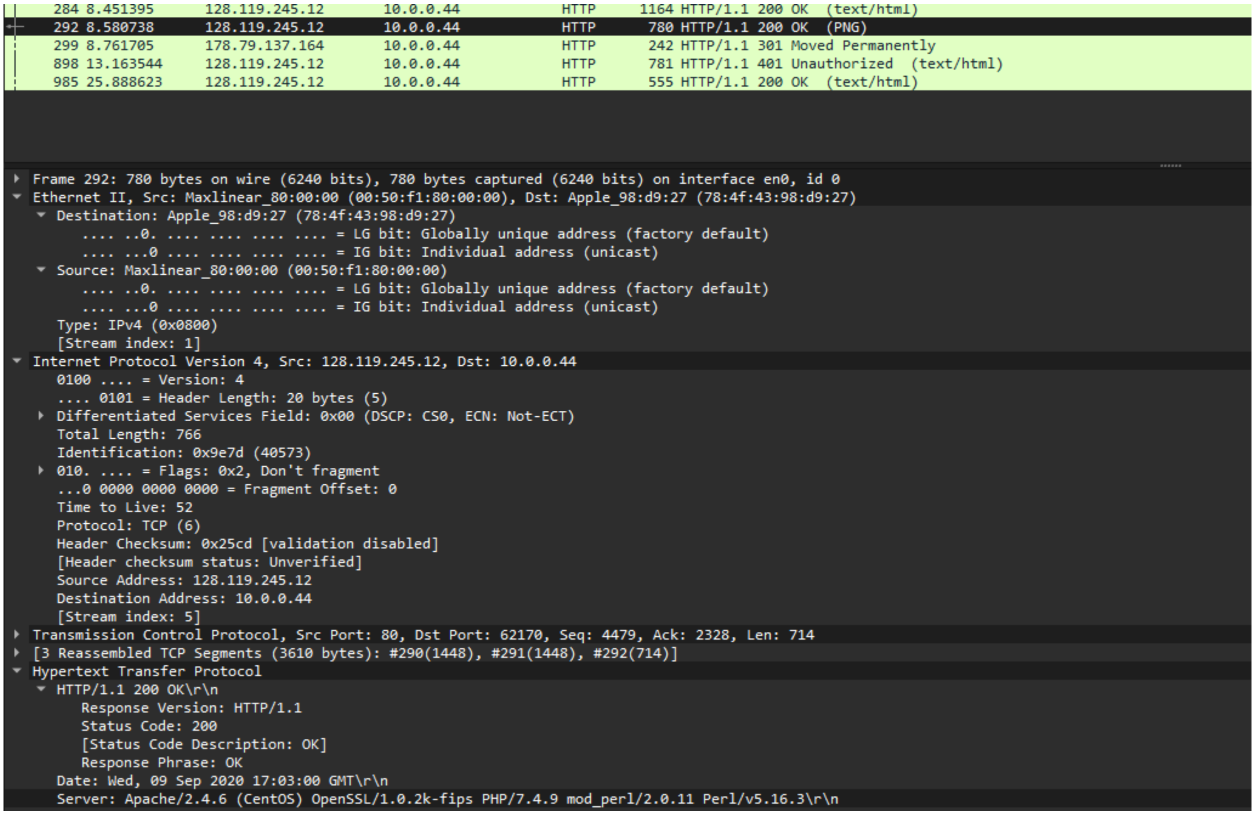
3.217.203.97
10.0.0.9
10.0.0.44
17.120.254.11
17.120.254.14
34.200.178.225
35.174.36.3
52.109.16.5
128.119.240.45
128.119.240.53

128.119.245.53
128.79.137.164
224.0.0.251

b. D

c. There are 4

d.



```
284 8.451395    128.119.245.12    10.0.0.44    HTTP    1164 HTTP/1.1 200 OK  (text/html)
292 8.580738    128.119.245.12    10.0.0.44    HTTP     780 HTTP/1.1 200 OK  (PNG)
299 8.761705    178.79.137.164    10.0.0.44    HTTP     242 HTTP/1.1 301 Moved Permanently
898 13.163544   128.119.245.12    10.0.0.44    HTTP     781 HTTP/1.1 401 Unauthorized  (text/html)
985 25.888623   128.119.245.12    10.0.0.44    HTTP     555 HTTP/1.1 200 OK  (text/html)

Frame 292: 780 bytes on wire (6240 bits), 780 bytes captured (6240 bits) on interface en0, id 0
Ethernet II, Src: Maxlinear_80:00:00 (00:50:f1:80:00:00), Dst: Apple_98:d9:27 (78:4f:43:98:d9:27)
  Destination: Apple_98:d9:27 (78:4f:43:98:d9:27)
    .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
    .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
  Source: Maxlinear_80:00:00 (00:50:f1:80:00:00)
    .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
    .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
  Type: IPv4 (0x0800)
  [Stream index: 1]
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 10.0.0.44
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
  Total Length: 766
  Identification: 0x9e7d (40573)
  010. .... = Flags: 0x2, Don't fragment
  ...0 0000 0000 0000 = Fragment Offset: 0
  Time to Live: 52
  Protocol: TCP (6)
  Header Checksum: 0x25cd [validation disabled]
  [Header checksum status: Unverified]
  Source Address: 128.119.245.12
  Destination Address: 10.0.0.44
  [Stream index: 5]
Transmission Control Protocol, Src Port: 80, Dst Port: 62170, Seq: 4479, Ack: 2328, Len: 714
[3 Reassembled TCP Segments (3610 bytes): #290(1448), #291(1448), #292(714)]
Hypertext Transfer Protocol
  HTTP/1.1 200 OK\r\n
    Response Version: HTTP/1.1
    Status Code: 200
    [Status Code Description: OK]
    Response Phrase: OK
  Date: Wed, 09 Sep 2020 17:03:00 GMT\r\n
  Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.9 mod_perl/2.0.11 Perl/v5.16.3\r\n
```

Question 4. Answers:

a. 10100101 + 11110111 + 01110001 =
10100101 +
11110111
____
110111100 carry 1

10111101 +
01110001
____
100101110 carry 1

Remove carry to get -> 00101111

Finally take ones compliment =
11010000

b. Error detection, using 1s complement handles overflow by using the carry. Additionally, it lets the interpreter check for errors against an all 1 result which would be ideally error free .
c. By checking it against 11111111 which would indicate no errors.
d. One bit errors can always be detected as the result will not equal the all 1 form. Two bit errors on the other hand sometimes can go unnoticed as the error can cancel itself out on the checksum calculation like if one bit is flipped from 1 to 0 and then a second error happens in which it results in the bit being flipped back to 1.

Question 5. Answer:

The names of the rdt protocol mechanisms and solutions are: Error detection, positive acknowledgement with retransmission, Negative acknowledgment (NAK, Sequence numbers, and timers.

Error detection uses checksums to check for corrupted packets. Positive acknowledgment with retransmission sends acknowledgements for correctly received packets, letting the sender know if they need to resend the packet. Negative acknowledgement, the receiver sends a message to sender in the case of a corrupted packet so that the sender knows to perform retransmission. Sequence numbers are used to keep track of the order and number of each packet to ensure that no duplication or skipping happens. Timers are used to detect lost packets by setting set time limits for how long to wait before an acknowledgment must be received.

"I certify that I have finished this exam solely by myself without any discussion or help from any other person".

Student Name: William Dellinger

PID: 5510058