Internet Networking 236341 - Homework 2

Yosef Goren

May 13, 2023

Contents

1 DNS

1.1 `nslookup`

a. We looked up the address of the University of Amsterdam:

```
PS C:\Windows\system32> nslookup www.uva.nl
Server:  home.home
Address:  10.0.0.138

Non-authoritative answer:
Name:    uvacms-prd-fe-redir.lb.uva.nl
Address:  145.18.11.145
Aliases:  www.uva.nl
          redir-prd.cms.uva.nl
```

b. We looked up the authoritative DNS servers of MIT:

```
PS C:\Windows\system32> nslookup -type=NS mit.edu
Server:  home.home
Address:  10.0.0.138

Non-authoritative answer:
mit.edu nameserver = asia1.akam.net
mit.edu nameserver = usw2.akam.net
mit.edu nameserver = use2.akam.net
mit.edu nameserver = ns1-37.akam.net
mit.edu nameserver = use5.akam.net
mit.edu nameserver = asia2.akam.net
mit.edu nameserver = eur5.akam.net
mit.edu nameserver = ns1-173.akam.net
```

After that, we were able to confirm the first result '`asia1.akam.net`' is considered an authoritative name server in that domain by querying it directly:

```
PS C:\Windows\system32> nslookup www.mit.edu asia1.akam.net
Server:  UnKnown
Address:  95.100.175.64

Name:    www.mit.edu
```

Indeed here we can see the result is not preceeded by the note '`Non-Authoritative answer`'.

1.2 `ipconfig` & Wireshark

c. Multiple queries were sent. The queries and responses used the TCP protocol.

d. There were in-fact 3 different DNS queries initiated and 3 responses regarding my search:

dns and ip.addr == 10.0.0.23

No.	Time	Source	Destination	Protocol	Length	Info
11	1.680721	10.0.0.23	10.0.0.138	DNS	84	Standard query 0x15eb AAAA www.ietf.org
17	1.681103	10.0.0.23	10.0.0.138	DNS	84	Standard query 0x187c A www.ietf.org
19	1.681270	10.0.0.23	10.0.0.138	DNS	84	Standard query 0x01ca HTTPS www.ietf.org
26	1.684359	10.0.0.138	10.0.0.23	DNS	187	Standard query response 0x15eb AAAA www.ietf.o
30	1.688751	10.0.0.138	10.0.0.23	DNS	163	Standard query response 0x187c A www.ietf.org
36	1.751004	10.0.0.138	10.0.0.23	DNS	210	Standard query response 0x01ca HTTPS www.ietf.

On the server side the port was 53 in all of the packets (so 53 as destination of requests and as source of answers), and on the client side 3 different ports were used: 50883, 50884, 50885.

e. The DNS queries had a source IP's of my ethernet adapter `10.0.0.23` and destination IP of the default gateway `10.0.0.138`, the answers to the queries had the source IP of the gateway and destination address of my ethernet adapter:

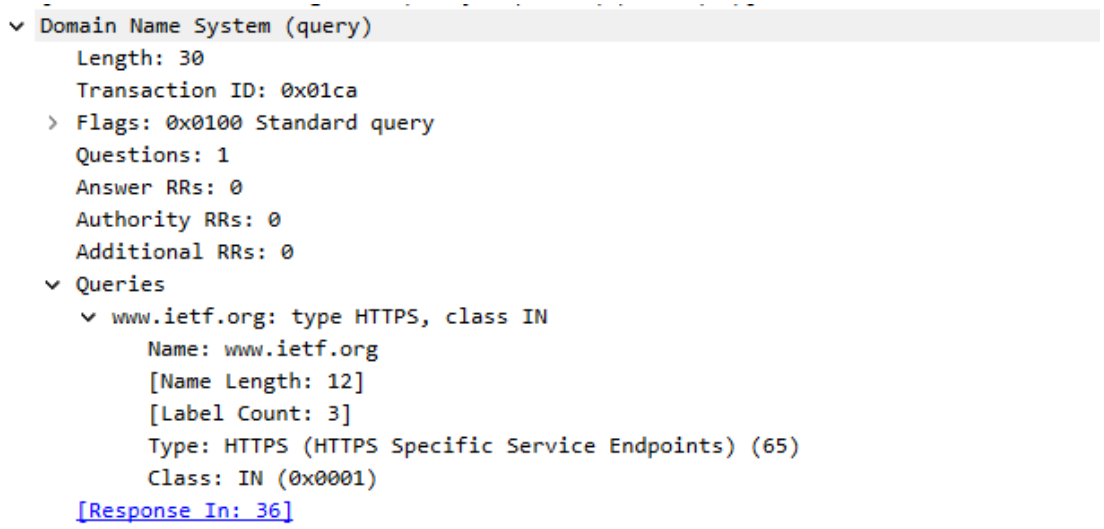
```
C:\Windows\System32>ipconfig
...
Ethernet adapter Ethernet:

Connection-specific DNS Suffix  . : home
IPv6 Address. . . . . . . . . . . : 2a06:c701:7241:5300:95d8:e6b8:e777:abcf
Temporary IPv6 Address. . . . . . : 2a06:c701:7241:5300:83d:935a:b003:26a5
Link-local IPv6 Address . . . . . : fe80::940f:4df:377e:f2cb%21
IPv4 Address. . . . . . . . . . . : 10.0.0.23
Subnet Mask . . . . . . . . . . . : 255.255.255.0
Default Gateway . . . . . . . . . : fe80::1%21
                                    10.0.0.138
```

So this means that the default gateway is the DNS provider for my host system.

f. Each of the 3 queries that were made had recived as single response to the port from which it was sent. Each such response contains a list of queries and responses.

g. The query content for the query coming out of 50885:



And the response:

```
▾ Queries
  ▾ www.ietf.org: type HTTPS, class IN
      Name: www.ietf.org
      [Name Length: 12]
      [Label Count: 3]
      Type: HTTPS (HTTPS Specific Service Endpoints) (65)
      Class: IN (0x0001)
▾ Answers
  ▾ www.ietf.org: type CNAME, class IN, cname www.ietf.org.cdn.cloudflare.net
      Name: www.ietf.org
      Type: CNAME (Canonical NAME for an alias) (5)
      Class: IN (0x0001)
      Time to live: 1760 (29 minutes, 20 seconds)
      Data length: 33
      CNAME: www.ietf.org.cdn.cloudflare.net
  › www.ietf.org.cdn.cloudflare.net: type HTTPS, class IN
  [Request In: 19]
  [Time: 0.069734000 seconds]
```

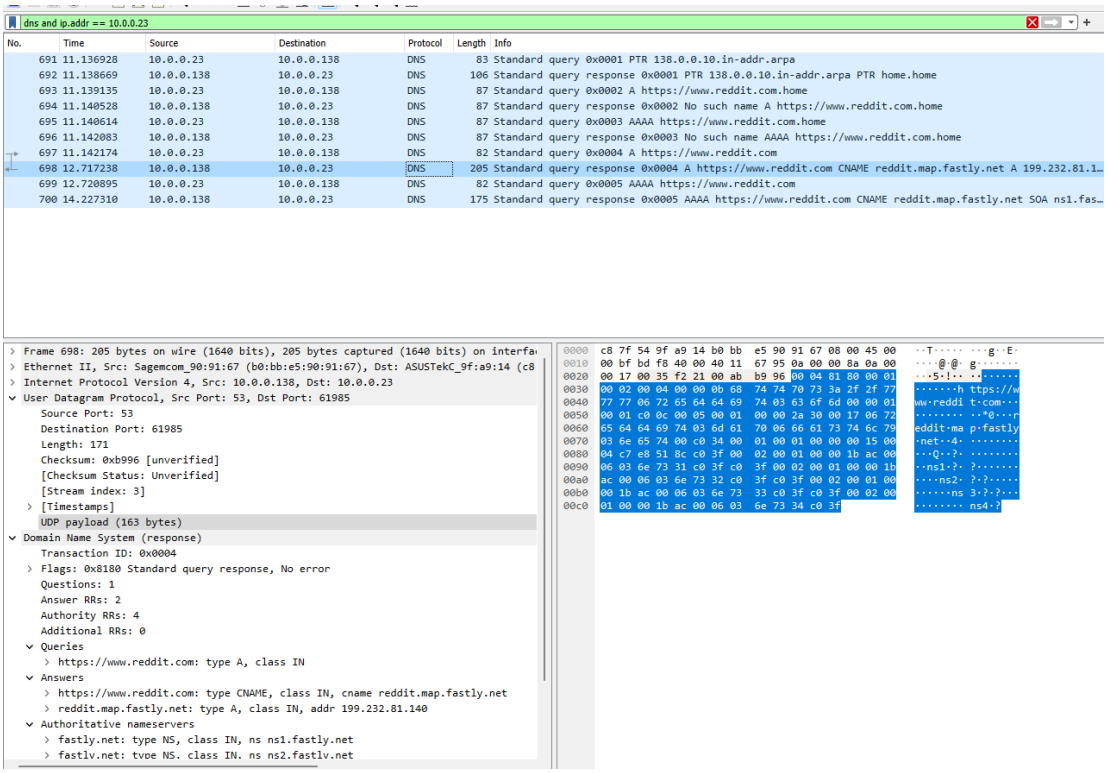
h. The client port is 61983 while the server port is still 53.

i. Like before, the DNS communication is between my computer and the default gateway. It is not a DNS itself - but acts as the DNS for my system.

j. The request was of type 'A' which requests a host address.

k. The response contained two host addresses, and a list of authoritative name servers.

l. In this photo we can see to two relevant request and response packets at the top, and also the content of the response packet below:

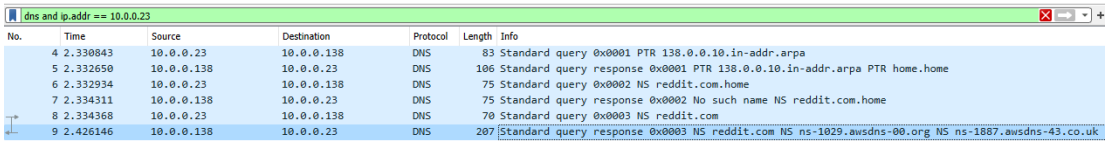


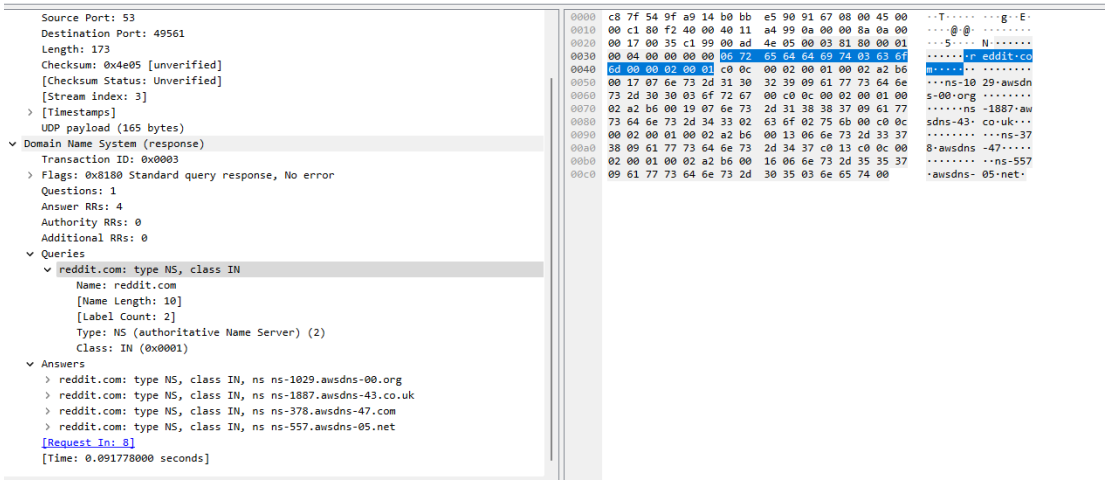
m. The server address is still the default gateway.

n. The query type is now 'NS' which means it is in search of a name server.

o. There are 4 answers, all of them contain the of a name server, but none conain the IP itself.

p. Wireshark:





q. A request to find who is `google-public-dns-a.google.com`.

r. The request to find `google-public-dns-a.google.com` was sent to the default gateway. It is my local DNS provider. The response also came from the default gateway.

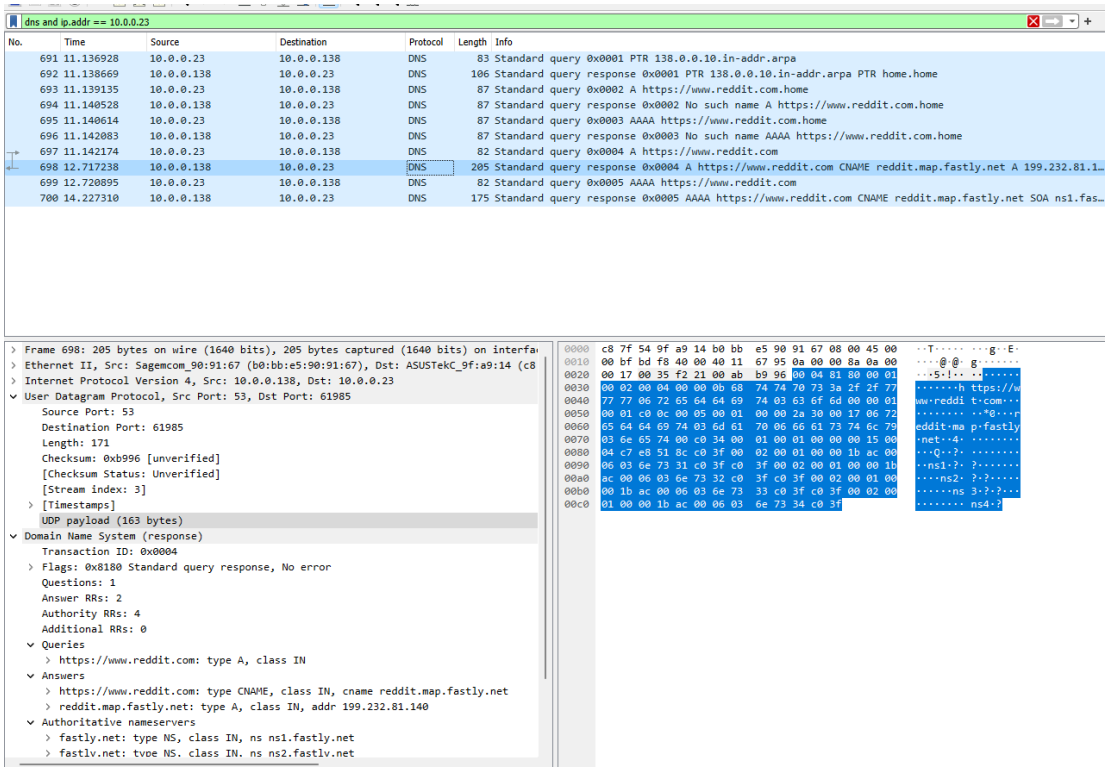
s. The request to find `reddit.com` was sent to the address `2001:4860:4860::8888` which resolved address of `google-public-dns-a.google.com` (which is not my local DNS server).

t. The IPv6 address of the google DNS server:

```
PS C:\Users\yosef> nslookup google-public-dns-a.google.com
Server:  home.home
Address:  10.0.0.138

Non-authoritative answer:
Name:    google-public-dns-a.google.com
Addresses:  2001:4860:4860::8888
          8.8.8.8
```

Wireshark: response packets at the top, and also the content of the response packet below:



2 ICMP

2.1 ICMP types and codes

a. The router sends an ICMP Time Exceeded packet to with `type=11` and `code=0` which means it is due to TTL running out.

b. The router sends an ICMP Destination Unreachable packet, with `type=3` and `code=4` which means that fragmantation was required but not allowed due to the DF flag.

c. The router sends an ICMP Destination Unreachable packet, with `type=3` and `code=1` which means the destination network is unreachable.

d. The router sends an ICMP Destination Unreachable packet, with `type=3` and `code=3` which means the destination port is unreachable.

e. It will send a packet with `type=5` and `code=0` which indicates that a packet was forwareded but the existing routing is used was not optimal in the sense that it should have been routed through the same LAN.

f. The router will return an ICMP echo reply packet which has `type=0`, `code=0`.

g. The router sends an ICMP Destination Unreachable packet, with `type=3` and `code=0` which means that the destination address could not be reached.

2.2 MTU discovery

MTU is the Maximum Transmission Unit, which is a number (in bytes) that describes the maximal size of a packet that will be sent.
MTU discovery is a process where on a specific socket - the two communicating parties attempt to find the MTU for the links that connect them - so they can send packets with the optimal size in their communication.

MTU discovery is done by attempting different message sizes (and `DF=1`) and seeing which are capable of passing and which do not return or result with an 'ICMP could not Fragment' - which means the packet was too large. A failiure indicates the packet size is larger than the MTU while a success indicates the packet size is smaller or equal to the MTU. To accelerate this process a binary search algorithm can be used.

2.3 ICMP and IP

ICMP is the Internet Control Message Protocol while IP is Internet Protocol.
The ICMP protocol enables the IP protocol to work, by transfering metadata about how IP messages are moving through the network (such as in the examples in the first part of the question).
It is also somewhat circular as ICMP packets are built upon the IP headers, while the routers and hosts that transfer IP packets relay on the ICMP protocol to be configured properly.

3 MiniNet

3.1 Router vs Switch

A switch is a device that operates at the data link layer (2). It uses the MAC addresses of devices to forward network traffic between them within the same LAN.
A router, on the other hand, operates at the IP layer (3). It uses IP addresses to forward network traffic between devices that are in different LAN's.