Internet Networking 236341 - Homework 2

Yosef Goren

May 14, 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
```

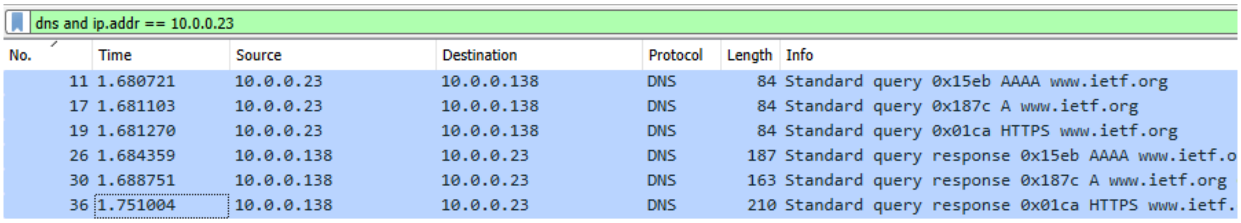
Indeed here we can see the result is not preceeded by the note '`Non-Authoritative answer`'.

1.2 `ipconfig` & Wireshark

c. Multiple queries were sent. The queries and responses used both TCP and UDP under different circumstances; when using Edge browser (as in the photos) - the protocol was TCP [1] , and when using Firefox - UDP was used.

[1] likely due to the fact DNS over HTTPS was used - which is built on TLS - which is built on TCP

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:

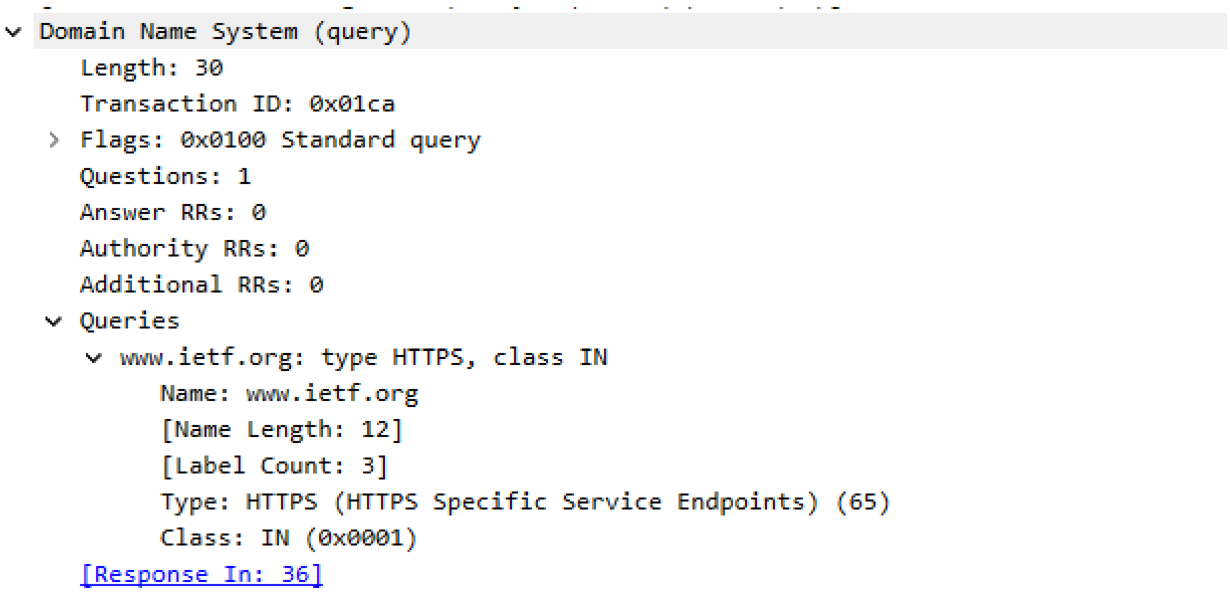
```
C:\Windows\System32>ipconfig
...
Ethernet adapter Ethernet:

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.

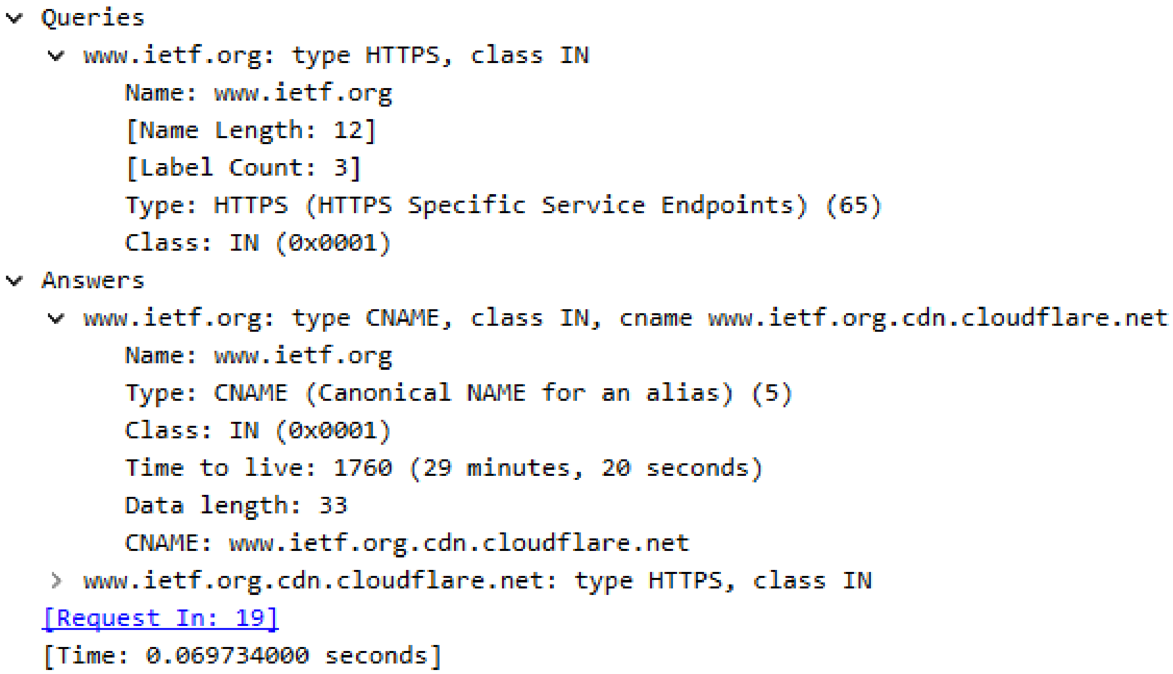
f. Each of the 3 queries that were made had recived as single response to the port from which it was sent. Each such response contains a list of queries and responses.

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



```
⌄ Domain Name System (query)
    Length: 30
    Transaction ID: 0x01ca
  › Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  ⌄ 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)
    [Response In: 36]
```

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]
```

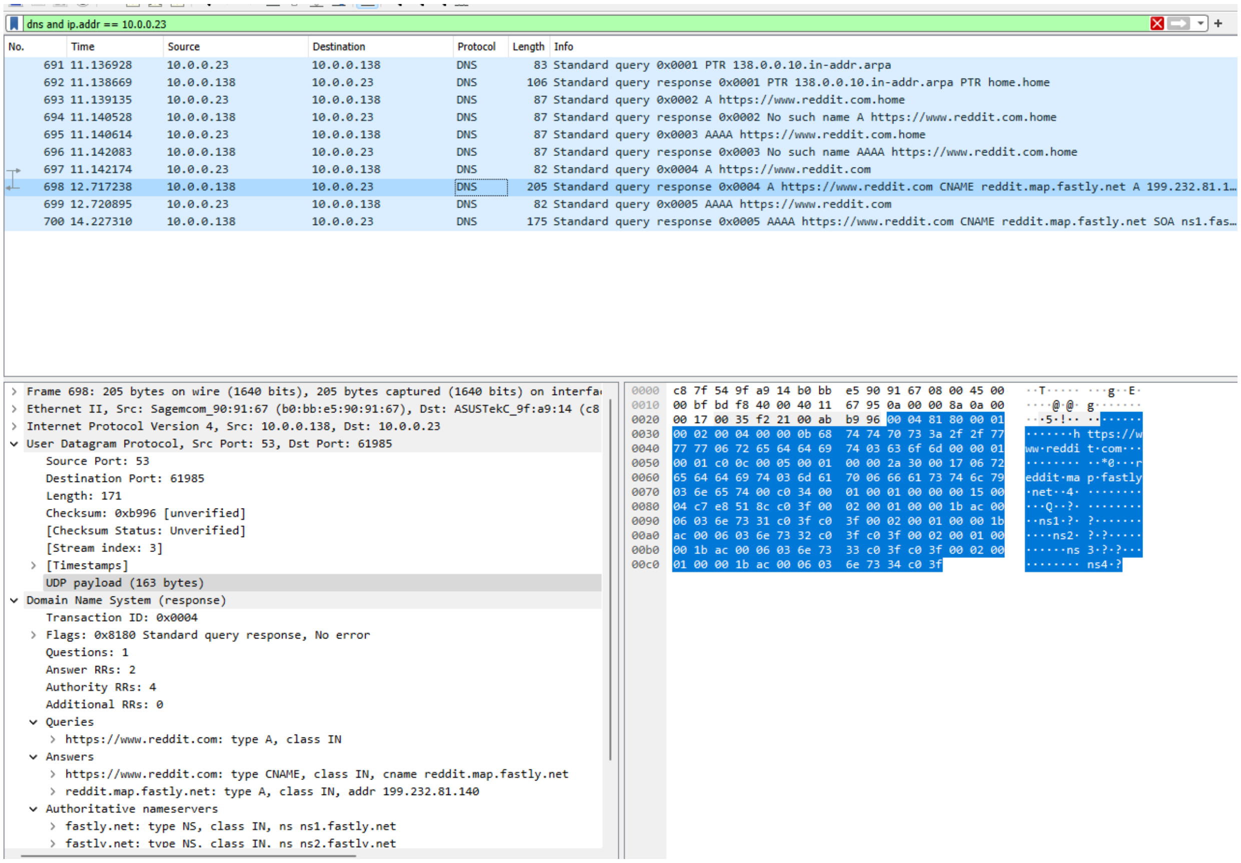
h. The client port is 61983 while the server port is still 53.

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:



```
dns and ip.addr == 10.0.0.23
```

```
No.     Time       Source        Destination   Protocol  Length Info
    691 11.136928  10.0.0.23     10.0.0.138    DNS         83 Standard query 0x0001 PTR 138.0.0.10.in-addr.arpa
    692 11.138669  10.0.0.138    10.0.0.23     DNS        106 Standard query response 0x0001 PTR 138.0.0.10.in-addr.arpa PTR home.home
    693 11.139135  10.0.0.23     10.0.0.138    DNS         87 Standard query 0x0002 A https://www.reddit.com.home
    694 11.140528  10.0.0.138    10.0.0.23     DNS         87 Standard query response 0x0002 No such name A https://www.reddit.com.home
    695 11.140614  10.0.0.23     10.0.0.138    DNS         87 Standard query 0x0003 AAAA https://www.reddit.com.home
    696 11.142083  10.0.0.138    10.0.0.23     DNS         87 Standard query response 0x0003 No such name AAAA https://www.reddit.com.home
    697 11.142174  10.0.0.23     10.0.0.138    DNS         82 Standard query 0x0004 A https://www.reddit.com
    698 12.717238  10.0.0.138    10.0.0.23     DNS        205 Standard query response 0x0004 A https://www.reddit.com CNAME reddit.map.fastly.net A 199.232.81.1…
    699 12.720895  10.0.0.23     10.0.0.138    DNS         82 Standard query 0x0005 AAAA https://www.reddit.com
    700 14.227310  10.0.0.138    10.0.0.23     DNS        175 Standard query response 0x0005 AAAA https://www.reddit.com CNAME reddit.map.fastly.net SOA ns1.fas…
```

```
> Frame 698: 205 bytes on wire (1640 bits), 205 bytes captured (1640 bits) on interfa
> Ethernet II, Src: Sagemcom_90:91:67 (b0:bb:e5:90:91:67), Dst: ASUSTekC_9f:a9:14 (c8
> Internet Protocol Version 4, Src: 10.0.0.138, Dst: 10.0.0.23
v User Datagram Protocol, Src Port: 53, Dst Port: 61985
    Source Port: 53
    Destination Port: 61985
    Length: 171
    Checksum: 0xb996 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 3]
  > [Timestamps]
    UDP payload (163 bytes)
v Domain Name System (response)
    Transaction ID: 0x0004
  > Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 2
    Authority RRs: 4
    Additional RRs: 0
  v Queries
    > https://www.reddit.com: type A, class IN
  v Answers
    > https://www.reddit.com: type CNAME, class IN, cname reddit.map.fastly.net
    > reddit.map.fastly.net: type A, class IN, addr 199.232.81.140
  v Authoritative nameservers
    > fastly.net: type NS, class IN, ns ns1.fastly.net
    > fastly.net: type NS, class IN, ns ns2.fastly.net
```

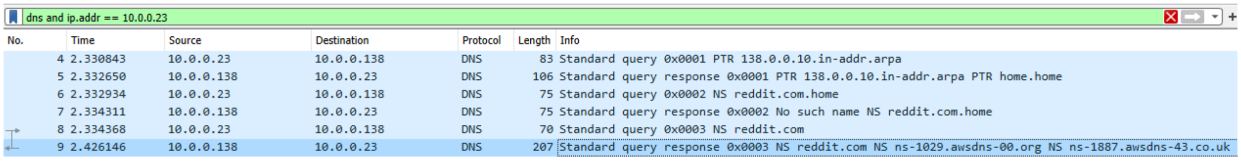
```
0000  c8 7f 54 9f a9 14 b0 bb  e5 90 91 67 08 00 45 00   ··T····· ···g··E·
0010  00 bf bd f8 40 00 40 11  67 95 0a 00 00 8a 0a 00   ····@·@· g·······
0020  00 17 00 35 f2 21 00 ab  b9 96 00 04 81 80 00 01   ···5·!·· ········
0030  00 02 00 04 00 00 0b 68  74 74 70 73 3a 2f 2f 77   ·······h ttps://w
0040  77 77 06 72 65 64 64 69  74 03 63 6f 6d 00 00 01   ww·reddi t·com···
0050  00 01 c0 0c 00 05 00 01  00 00 2a 30 00 17 06 72   ········ ··*0···r
0060  65 64 64 69 74 03 6d 61  70 06 66 61 73 74 6c 79   eddit·ma p·fastly
0070  03 6e 65 74 00 c0 34 00  01 00 01 00 00 00 15 00   ·net··4· ········
0080  04 c7 e8 51 8c c0 3f 00  02 00 01 00 00 1b ac 00   ···Q··?· ········
0090  06 03 6e 73 31 c0 3f c0  3f 00 02 00 01 00 00 1b   ··ns1·?· ?·······
00a0  ac 00 06 03 6e 73 32 c0  3f c0 3f 00 02 00 01 00   ····ns2· ?·?·····
00b0  00 1b ac 00 06 03 6e 73  33 c0 3f c0 3f 00 02 00   ······ns 3·?·?···
00c0  01 00 00 1b ac 00 06 03  6e 73 34 c0 3f            ········ ns4·?
```

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.

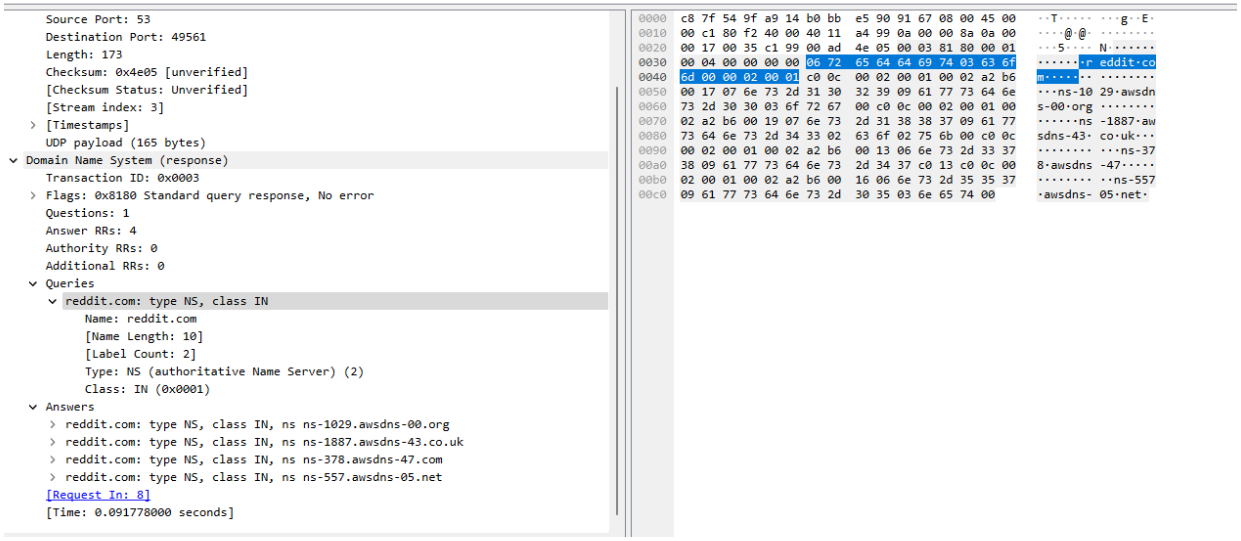
o. There are 4 answers, all of them contain the of a name server, but none conain the IP itself.

p. Wireshark:



dns and ip.addr == 10.0.0.23

```
No.    Time       Source       Destination   Protocol  Length Info
     4 2.330843   10.0.0.23    10.0.0.138    DNS           83 Standard query 0x0001 PTR 138.0.0.10.in-addr.arpa
     5 2.332650   10.0.0.138   10.0.0.23     DNS          106 Standard query response 0x0001 PTR 138.0.0.10.in-addr.arpa PTR home.home
     6 2.332934   10.0.0.23    10.0.0.138    DNS           75 Standard query 0x0002 NS reddit.com.home
     7 2.334311   10.0.0.138   10.0.0.23     DNS           75 Standard query response 0x0002 No such name NS reddit.com.home
     8 2.334368   10.0.0.23    10.0.0.138    DNS           70 Standard query 0x0003 NS reddit.com
     9 2.426146   10.0.0.138   10.0.0.23     DNS          207 Standard query response 0x0003 NS reddit.com NS ns-1029.awsdns-00.org NS ns-1887.awsdns-43.co.uk
```



```
    Source Port: 53
    Destination Port: 49561
    Length: 173
    Checksum: 0x4e05 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 3]
  > [Timestamps]
    UDP payload (165 bytes)
v Domain Name System (response)
    Transaction ID: 0x0003
  > Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 4
    Authority RRs: 0
    Additional RRs: 0
  v Queries
    v reddit.com: type NS, class IN
        Name: reddit.com
        [Name Length: 10]
        [Label Count: 2]
        Type: NS (authoritative Name Server) (2)
        Class: IN (0x0001)
  v Answers
    > reddit.com: type NS, class IN, ns ns-1029.awsdns-00.org
    > reddit.com: type NS, class IN, ns ns-1887.awsdns-43.co.uk
    > reddit.com: type NS, class IN, ns ns-378.awsdns-47.com
    > reddit.com: type NS, class IN, ns ns-557.awsdns-05.net
    [Request In: 8]
    [Time: 0.091778000 seconds]
```

```
0000  c8 7f 54 9f a9 14 b0 bb  e5 90 91 67 08 00 45 00   ··T····· ···g··E·
0010  00 c1 80 f2 40 00 40 11  a4 99 0a 00 00 8a 0a 00   ····@·@· ········
0020  00 17 00 35 c1 99 00 ad  4e 05 00 03 81 80 00 01   ···5···· N·······
0030  00 04 00 00 00 00 06 72  65 64 64 69 74 03 63 6f   ·······r eddit·co
0040  6d 00 00 02 00 01 c0 0c  00 02 00 01 00 02 a2 b6   m······· ········
0050  00 17 07 6e 73 2d 31 30  32 39 09 61 77 73 64 6e   ···ns-10 29·awsdn
0060  73 2d 30 30 03 6f 72 67  00 c0 0c 00 02 00 01 00   s-00·org ········
0070  02 a2 b6 00 19 07 6e 73  2d 31 38 38 37 09 61 77   ······ns -1887·aw
0080  73 64 6e 73 2d 34 33 02  63 6f 02 75 6b 00 c0 0c   sdns-43· co·uk···
0090  00 02 00 01 00 02 a2 b6  00 13 06 6e 73 2d 33 37   ········ ···ns-37
00a0  38 09 61 77 73 64 6e 73  2d 34 37 c0 13 c0 0c 00   8·awsdns -47·····
00b0  02 00 01 00 02 a2 b6 00  16 06 6e 73 2d 35 35 37   ········ ··ns-557
00c0  09 61 77 73 64 6e 73 2d  30 35 03 6e 65 74 00      ·awsdns- 05·net·
```

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.

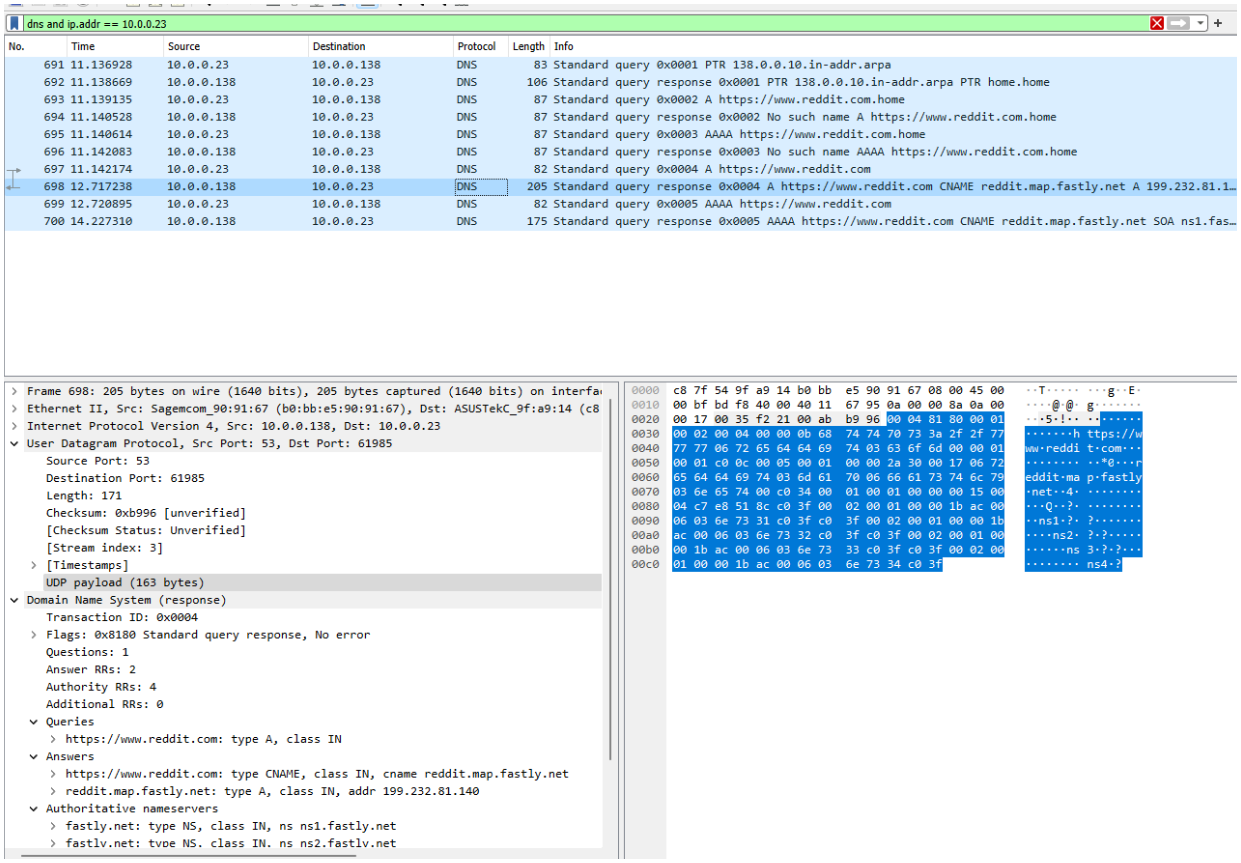
s. The request to find `reddit.com` was sent to the address `2001:4860:4860::8888` which resolved address of `google-public-dns-a.google.com` (which is not my local DNS server).

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:



```
dns and ip.addr == 10.0.0.23

No.   Time       Source      Destination Protocol Length Info
  691 11.136928  10.0.0.23   10.0.0.138  DNS       83 Standard query 0x0001 PTR 138.0.0.10.in-addr.arpa
  692 11.138669  10.0.0.138  10.0.0.23   DNS      106 Standard query response 0x0001 PTR 138.0.0.10.in-addr.arpa PTR home.home
  693 11.139135  10.0.0.23   10.0.0.138  DNS       87 Standard query 0x0002 A https://www.reddit.com.home
  694 11.140528  10.0.0.138  10.0.0.23   DNS       87 Standard query response 0x0002 No such name A https://www.reddit.com.home
  695 11.140614  10.0.0.23   10.0.0.138  DNS       87 Standard query 0x0003 AAAA https://www.reddit.com.home
  696 11.142083  10.0.0.138  10.0.0.23   DNS       87 Standard query response 0x0003 No such name AAAA https://www.reddit.com.home
  697 11.142174  10.0.0.23   10.0.0.138  DNS       82 Standard query 0x0004 A https://www.reddit.com
  698 12.717238  10.0.0.138  10.0.0.23   DNS      205 Standard query response 0x0004 A https://www.reddit.com CNAME reddit.map.fastly.net A 199.232.81.1…
  699 12.720895  10.0.0.23   10.0.0.138  DNS       82 Standard query 0x0005 AAAA https://www.reddit.com
  700 14.227310  10.0.0.138  10.0.0.23   DNS      175 Standard query response 0x0005 AAAA https://www.reddit.com CNAME reddit.map.fastly.net SOA ns1.fas…
```

```
> Frame 698: 205 bytes on wire (1640 bits), 205 bytes captured (1640 bits) on interfa
> Ethernet II, Src: Sagemcom_90:91:67 (b0:bb:e5:90:91:67), Dst: ASUSTekC_9f:a9:14 (c8
> Internet Protocol Version 4, Src: 10.0.0.138, Dst: 10.0.0.23
v User Datagram Protocol, Src Port: 53, Dst Port: 61985
    Source Port: 53
    Destination Port: 61985
    Length: 171
    Checksum: 0xb996 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 3]
  > [Timestamps]
    UDP payload (163 bytes)
v Domain Name System (response)
    Transaction ID: 0x0004
  > Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 2
    Authority RRs: 4
    Additional RRs: 0
  v Queries
    > https://www.reddit.com: type A, class IN
  v Answers
    > https://www.reddit.com: type CNAME, class IN, cname reddit.map.fastly.net
    > reddit.map.fastly.net: type A, class IN, addr 199.232.81.140
  v Authoritative nameservers
    > fastly.net: type NS, class IN, ns ns1.fastly.net
    > fastly.net: type NS, class IN, ns ns2.fastly.net
```

```
0000  c8 7f 54 9f a9 14 b0 bb  e5 90 91 67 08 00 45 00   ··T····· ···g··E·
0010  00 bf bd f8 40 00 40 11  67 95 0a 00 00 8a 0a 00   ····@·@· g·······
0020  00 17 00 35 f2 21 00 ab  b9 96 00 04 81 80 00 01   ···5·!·· ········
0030  00 02 00 04 00 00 0b 68  74 74 70 73 3a 2f 2f 77   ·······h ttps://w
0040  77 77 06 72 65 64 64 69  74 03 63 6f 6d 00 00 01   ww·reddi t·com···
0050  00 01 c0 0c 00 05 00 01  00 00 2a 30 00 17 06 72   ········ ··*0···r
0060  65 64 64 69 74 03 6d 61  70 06 66 61 73 74 6c 79   eddit·ma p·fastly
0070  03 6e 65 74 00 c0 34 00  01 00 01 00 00 00 15 00   ·net··4· ········
0080  04 c7 e8 51 8c c0 3f 00  02 00 01 00 00 1b ac 00   ···Q··?· ········
0090  06 03 6e 73 31 c0 3f c0  3f 00 02 00 01 00 00 1b   ··ns1·?· ?·······
00a0  ac 00 06 03 6e 73 32 c0  3f c0 3f 00 02 00 01 00   ····ns2· ?·?·····
00b0  00 1b ac 00 06 03 6e 73  33 c0 3f c0 3f 00 02 00   ······ns 3·?·?···
00c0  01 00 00 1b ac 00 06 03  6e 73 34 c0 3f            ········ ns4·?
```

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 Source Quench packet, with `type=4` and `code=0` which means the buffer was full.

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.

3.2

The output is:

```
mininet> h1 ifconfig
h1-eth0   Link encap:Ethernet  HWaddr d6:e9:4b:ad:4c:62
        inet addr:10.0.0.1  Bcast:10.255.255.255  Mask:255.0.0.0
        inet6 addr: fe80::d4e9:4bff:fead:4c62/64 Scope:Link
        UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
        RX packets:7 errors:0 dropped:0 overruns:0 frame:0
        TX packets:8 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:1000
        RX bytes:558 (558.0 B)  TX bytes:648 (648.0 B)

lo        Link encap:Local Loopback
        inet addr:127.0.0.1  Mask:255.0.0.0
        inet6 addr: ::1/128 Scope:Host
        UP LOOPBACK RUNNING  MTU:65536  Metric:1
        RX packets:0 errors:0 dropped:0 overruns:0 frame:0
        TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:0
        RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)
```

1. The MAC is: `d6:e9:4b:ad:4c:62`.

2. The IP is: `10.0.0.1`, subnet mask: `255.0.0.0`, so there are 24 bits to specify different hosts in the subnet meaning there can be up to 2^{24} hosts in it.

3. The IPv6 address is `fe80::d4e9:4bff:fead:4c62/64`.

4. The MTU is 1500 (bytes).

5. `txqueuelen` refers to the length of the transmission queue of this interface, which is a buffer that holds packets that are waiting to be transmitted by the interface.

3.3

A loopback interface is an interface that connects the host to itself.
These interfaces are useful for many things; among the most important ones I can think of are for platform-independent IPC, and for testing network services (for example I can run `ssh localhost` before attempting to log in somewhere else to make sure my ssh client is working properly).
The associated IP address `127.0.0.1` is a special address dedicated to loopback adapters.

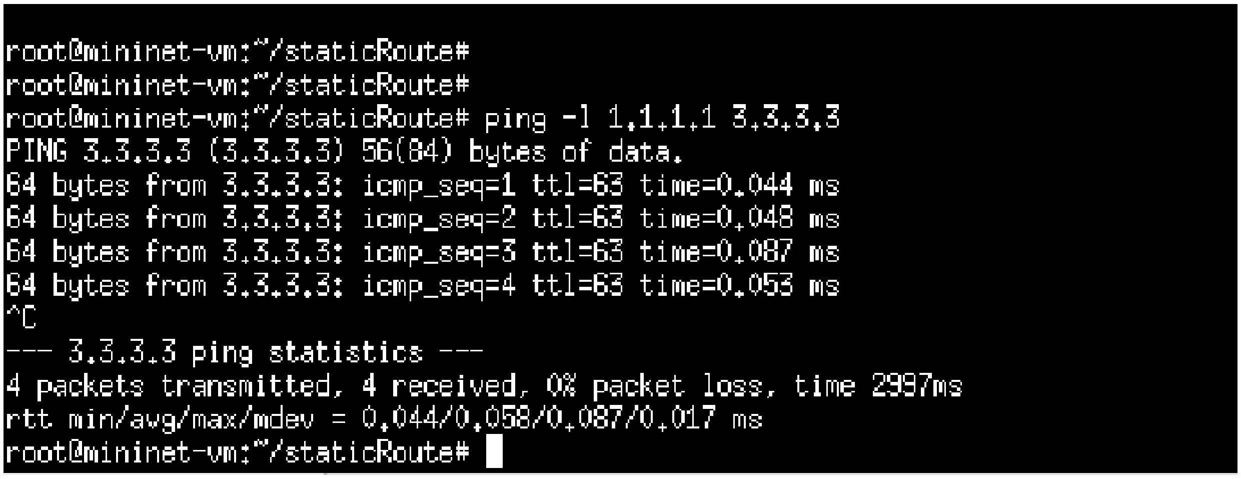
3.4

The output is almost identical - but the two have different IP and MAC addresses. They are both in a private network `10.*.*.*` - (which we know is the same private network). This also means that the first 8 bits of their IPv4 address match (in-fact the first 30 bits do, but that is more of a coincident).

3.5

We have used the following commands to configure the routers:

- For R1: 'ip route 2.2.2.0/24 192.168.1.2'
- For R2: 'ip route 3.3.3.0/24 192.168.2.2'
- For R3: 'ip route 192.168.1.0/24 192.168.2.1'



```
root@mininet-vm:~/staticRoute#
root@mininet-vm:~/staticRoute#
root@mininet-vm:~/staticRoute# ping -I 1.1.1.1 3.3.3.3
PING 3.3.3.3 (3.3.3.3) 56(84) bytes of data.
64 bytes from 3.3.3.3: icmp_seq=1 ttl=63 time=0.044 ms
64 bytes from 3.3.3.3: icmp_seq=2 ttl=63 time=0.048 ms
64 bytes from 3.3.3.3: icmp_seq=3 ttl=63 time=0.087 ms
64 bytes from 3.3.3.3: icmp_seq=4 ttl=63 time=0.053 ms
^C
--- 3.3.3.3 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 2997ms
rtt min/avg/max/mdev = 0.044/0.058/0.087/0.017 ms
root@mininet-vm:~/staticRoute#
```

3.6

The main disadvantage of using static routing is that it needs to be manually defined by the network administrator, which can be very time consuming and unscalable, moreover - static routing is also less resilient to router crashes.

3.7

In the 'count to infinity' The 'count to infinity' problem is a problem in which the router loses the link to a specific destination before it can update its neighbors. It receives a message from one of them that there is an alternate route that is much shorter than the one to the destination that was lost. However, the alternate route actually passes through the first router, which does not exist because one of the links has failed. The result is that both routers will update each other with incorrect routes to a specific destination and packets that will arrive at these routers in order to reach the destination will be stuck. The process will continue until the routes that the routers exchange between them are less efficient than another route (since their cost only increases).

3.8

The mechanism is an addition to split horizon, so that instead of a router receiving reports from routers that may be using routes through it, it will receive them and define their use as an infinite cost, thus preventing the sending router from being poisoned.

3.9

Triggered updates is a protocol designed to try to speed up the solution of the count to infinity problem. In cases where the ”misleading cycle” is more than two routers, split horizon will not help us. The way to do this is to send update messages as soon as an update message is received, even if it is not the time when we (as a router) are supposed to send update messages, and thus speed up the convergence of the count-to-infinity problem and accelerate the network’s recovery.

3.10

The protocol is restricted to networks where the longest path requires no more than 15 hops. The protocol relies on ”counting to infinity” to address certain uncommon scenarios, which can lead to lengthy convergence periods. Additionally, the protocol utilizes ”hop count” exclusively and disregards other real-time parameters, such as measured delay, reliability, or load.

3.11

Every datagram has a specific purpose, and the command field is used as a header to the datagram, where its purpose is mentioned. This includes types such as response, request, trace off, trace on, and reserved.

3.12

Based on our count, it takes an average of `20` seconds between each response.

3.13

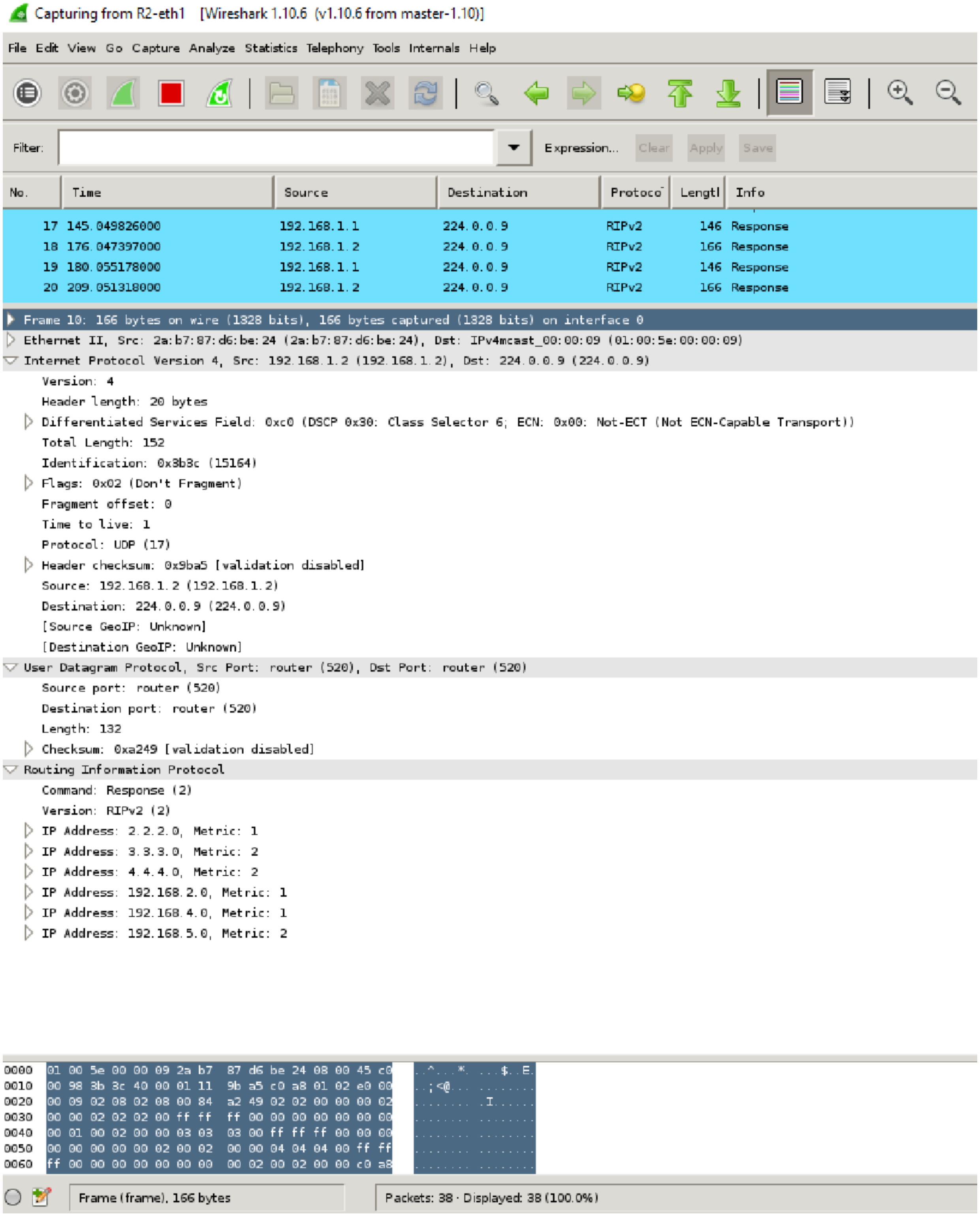
The message is sent via UDP, on port `17`.

3.14

The IP address of the destination is `224.0.0.9`, whats important about this address is that it is used by the RIP for multicast.

3.15

The important detail that the responce message contains is the Metric, Which represents the hop count. That is the number of router that a message needs to go through to reach its destination.



Capturing from R2-eth1 [Wireshark 1.10.6 (v1.10.6 from master-1.10)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter:
Expression...
Clear
Apply
Save

```
No.  Time              Source          Destination    Protoco  Lengtl  Info
 17  145.049826000     192.168.1.1     224.0.0.9      RIPv2       146  Response
 18  176.047397000     192.168.1.2     224.0.0.9      RIPv2       166  Response
 19  180.055178000     192.168.1.1     224.0.0.9      RIPv2       146  Response
 20  209.051318000     192.168.1.2     224.0.0.9      RIPv2       166  Response
```

```
▶ Frame 18: 166 bytes on wire (1328 bits), 166 bytes captured (1328 bits) on interface 0
▷ Ethernet II, Src: 2a:b7:87:d6:be:24 (2a:b7:87:d6:be:24), Dst: IPv4mcast_00:00:09 (01:00:5e:00:00:09)
▽ Internet Protocol Version 4, Src: 192.168.1.2 (192.168.1.2), Dst: 224.0.0.9 (224.0.0.9)
    Version: 4
    Header length: 20 bytes
  ▷ Differentiated Services Field: 0xc0 (DSCP 0x30: Class Selector 6; ECN: 0x00: Not-ECT (Not ECN-Capable Transport))
    Total Length: 152
    Identification: 0x3b3c (15164)
  ▷ Flags: 0x02 (Don't Fragment)
    Fragment offset: 0
    Time to live: 1
    Protocol: UDP (17)
  ▷ Header checksum: 0x9ba5 [validation disabled]
    Source: 192.168.1.2 (192.168.1.2)
    Destination: 224.0.0.9 (224.0.0.9)
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
▽ User Datagram Protocol, Src Port: router (520), Dst Port: router (520)
    Source port: router (520)
    Destination port: router (520)
    Length: 132
  ▷ Checksum: 0xa249 [validation disabled]
▽ Routing Information Protocol
    Command: Response (2)
    Version: RIPv2 (2)
  ▷ IP Address: 2.2.2.0, Metric: 1
  ▷ IP Address: 3.3.3.0, Metric: 2
  ▷ IP Address: 4.4.4.0, Metric: 2
  ▷ IP Address: 192.168.2.0, Metric: 1
  ▷ IP Address: 192.168.4.0, Metric: 1
  ▷ IP Address: 192.168.5.0, Metric: 2
```

```
0000  01 00 5e 00 00 09 2a b7  87 d6 be 24 08 00 45 c0   ..^...*. ...$..E.
0010  00 98 3b 3c 40 00 01 11  9b a5 c0 a8 01 02 e0 00   ..;<@... ........
0020  00 09 02 08 02 08 00 84  a2 49 02 02 00 00 00 02   ........ .I......
0030  00 00 02 02 02 00 ff ff  ff 00 00 00 00 00 00 00   ........ ........
0040  00 01 00 02 00 00 03 03  03 00 ff ff ff 00 00 00   ........ ........
0050  00 00 00 00 00 02 00 02  00 00 04 04 04 00 ff ff   ........ ........
0060  ff 00 00 00 00 00 00 00  00 02 00 02 00 00 c0 a8   ........ ........
```

Frame (frame), 166 bytes

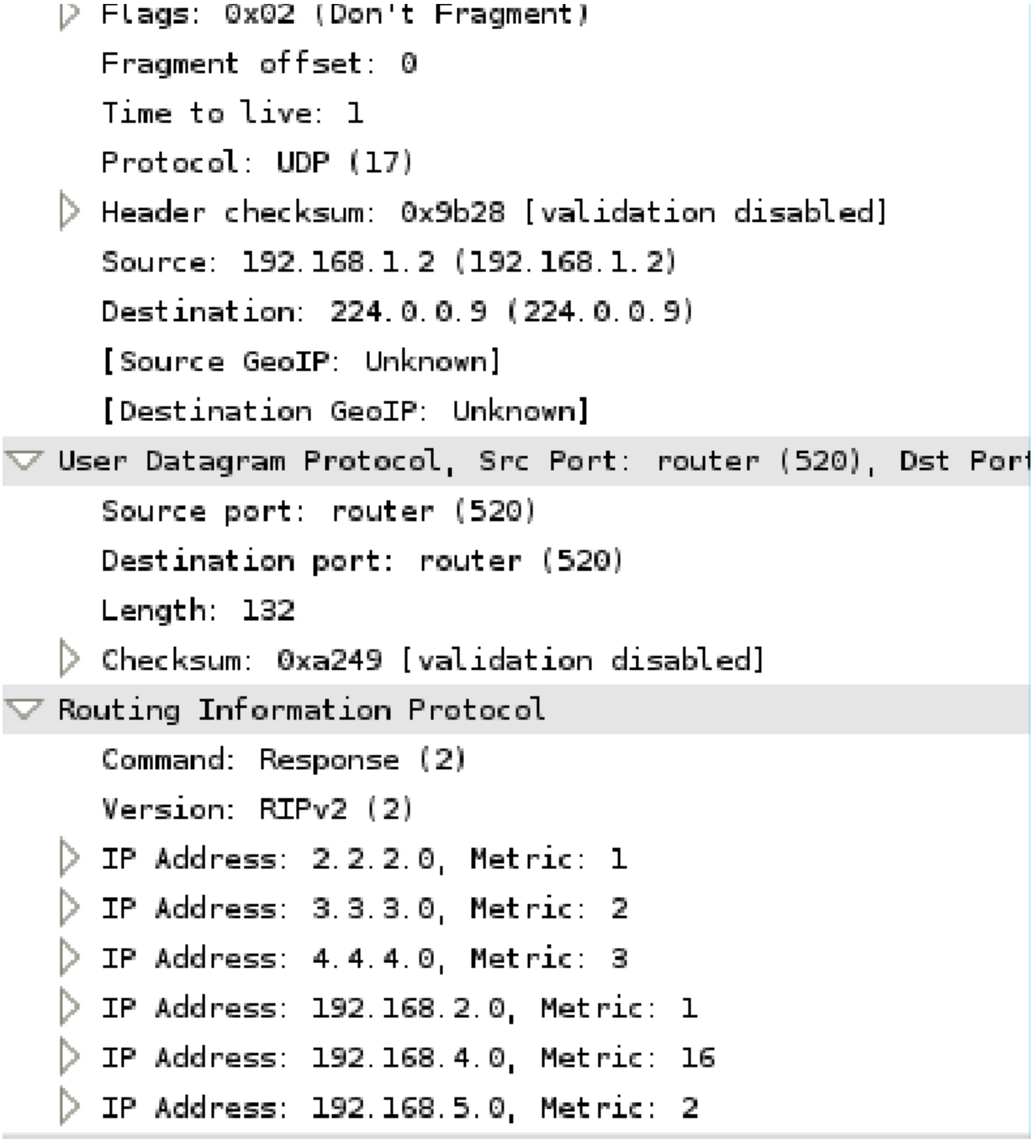
Packets: 38 · Displayed: 38 (100.0%)

3.16

In our tests, the infinity metric was 16, this should be relatively long compared to the other routes in the network (there shouldn't be any other router with longer route)

3.17

Shortly after the link went down, the other nodes (routers) realized that they had a better way to reach node 4. Thanks to the Triggered Updates mechanism. They send their own responses with updates about better paths as soon as they realized the previous path was no longer the better one.



```
   ▷ Flags: 0x02 (Don't Fragment)
     Fragment offset: 0
     Time to live: 1
     Protocol: UDP (17)
   ▷ Header checksum: 0x9b28 [validation disabled]
     Source: 192.168.1.2 (192.168.1.2)
     Destination: 224.0.0.9 (224.0.0.9)
     [Source GeoIP: Unknown]
     [Destination GeoIP: Unknown]
▽ User Datagram Protocol, Src Port: router (520), Dst Port
     Source port: router (520)
     Destination port: router (520)
     Length: 132
   ▷ Checksum: 0xa249 [validation disabled]
▽ Routing Information Protocol
     Command: Response (2)
     Version: RIPv2 (2)
   ▷ IP Address: 2.2.2.0, Metric: 1
   ▷ IP Address: 3.3.3.0, Metric: 2
   ▷ IP Address: 4.4.4.0, Metric: 3
   ▷ IP Address: 192.168.2.0, Metric: 1
   ▷ IP Address: 192.168.4.0, Metric: 16
   ▷ IP Address: 192.168.5.0, Metric: 2
```