

# Internet Networking 236341 - Homework 2

Yosef Goren

May 13, 2023

## Contents

<b>1</b>	<b>DNS</b>	<b>1</b>
1.1	nslookup . . . . .	1
1.2	ipconfig & Wireshark . . . . .	2
<b>2</b>	<b>ICMP</b>	<b>7</b>
2.1	ICMP types and codes . . . . .	7
2.2	MTU discovery . . . . .	8
2.3	ICMP and IP . . . . .	8
<b>3</b>	<b>MiniNet</b>	<b>8</b>
3.1	Router vs Switch . . . . .	8

## 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-redirect.lb.uva.nl
Address: 145.18.11.145
Aliases: www.uva.nl
         redirect.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 preceded 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.org
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.org

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 received 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:

```

v Queries
  v 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)
  v Answers
    v 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 199.232.81.140
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.fastly.net

  

> Frame 698: 205 bytes on wire (1640 bits), 205 bytes captured (1640 bits) on interface > Ethernet II, Src: Sagemcom_90:91:67 (b0:bbe:590:91:67), Dst: ASUSTek_9f:a9:14 (c8:00:0e:14:a9:14) > Internet Protocol Version 4, Src: 10.0.0.138, Dst: 10.0.0.23 > User Datagram Protocol, Src Port: 53, Dst Port: 61985	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 11 67 95 0a 00 00 8a 0a 00 ...@.g..... 0020 00 17 00 35 f2 21 00 ab b5 96 00 04 01 00 00 00 ...5.l...P.... 0030 00 02 00 04 00 00 00 68 74 74 70 73 3a 2f 2f 77 .....h.https:// 0040 77 77 06 72 65 64 64 69 74 03 63 6f 6d 00 00 01 ..w-reddi t-com- 0050 00 01 c0 0c 00 05 00 01 00 00 2a 30 00 17 06 72 .....:g...r 0060 65 64 64 69 74 03 6d 61 70 06 66 61 73 74 6c 79 reddit-ma p-fastly 0070 03 6e 65 74 00 c0 34 00 01 00 01 00 00 00 15 00 net-d..... 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-?>...
---	--

  

> [Timestamps] > [UDP payload (163 bytes)] > Domain Name System (response) Transaction ID: 0x0004 > Flags: 0x0100 Standard query response, No error Questions: 1 Answer RRs: 2 Authority RRs: 4 Additional RRs: 0 > Queries > https://www.reddit.com: type A, class IN > 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 > Authoritative nameservers > fastly.net: type NS, class IN, ns ns1.fastly.net > fastly.net: type NS, class IN, ns ns2.fastly.net	
---	--

- 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	2.338843	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	0000	c8 7f 54 9f a9 14 b0 bb e5 90 91 67 08 00 45 00	--T.....g..E:
Destination Port: 49561	0010	00 c1 80 f2 40 00 40 11 a4 99 0a 00 00 8a 0a 00	...@.@.....
Length: 173	0020	00 17 00 35 c1 99 00 ad 4e 05 00 03 61 80 00 01	...S...n.....
Checksum: 0x4e05 [unverified]	0030	00 04 00 00 00 00 00 72 65 64 64 69 74 03 63 6f	.....r.eddit.co
[Checksum Status: Unverified]	0040	6d 00 00 02 00 01 c0 0c 00 02 00 01 00 02 a2 b6	a.....
[Stream Index: 3]	0050	00 17 07 6e 73 2d 31 30 32 39 09 61 77 73 64 6e	....ns-10 29:awsdn
> [Timestamps]	0060	73 2d 30 30 03 6f 72 67 00 c0 0c 00 02 00 01 00	s-00.org.....
UDP payload (165 bytes)	0070	02 a2 b6 00 19 07 6e 73 2d 31 38 38 37 09 61 77	.....ns -1887:aw
Domain Name System (response)	0080	73 64 6e 73 2d 34 33 02 63 6f 02 75 6b 00 c0 0c	sdns-43- co-uk...
Transaction ID: 0x0003	0090	00 02 00 01 00 02 a2 b6 00 13 06 6e 73 2d 33 37	.....ns-37
> Flags: 0x8180 Standard query response, No error	00a0	38 09 61 77 73 64 6e 73 2d 34 37 c0 13 c0 0c 00	8:awsdns -47.....
Questions: 1	00b0	02 00 01 00 02 a2 b6 00 16 06 6e 73 2d 35 35 37	.....ns-557
Answer RRs: 4	00c0	09 61 77 73 64 6e 73 2d 30 35 03 6e 65 74 00	:awsdns- 05-net:
Authority RRs: 0			
Additional RRs: 0			
Queries			
reddit.com: type NS, class IN			
Name: reddit.com			
[Name Length: 10]			
[Label Count: 2]			
Type: NS (authoritative Name Server) (2)			
Class: IN (0x0001)			
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]			

- 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
```

**dns and ip.addr := 10.0.0.13**

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
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 199.232.81.14
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.fastly.net

```

> Frame 698: 205 bytes on wire (1640 bits), 205 bytes captured (1640 bits) on interface0
> Ethernet II, Src: Sagemcom_90:91:67 (b0:bb:es:90:91:67), Dst: ASUSTekC_9f:a9:14 (c8:27:4d:9f:a9:14)
> Internet Protocol Version 4, Src: 10.0.0.138, Dst: 10.0.0.23
✓ 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)
    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
    ✓ Queries
      > https://www.reddit.com: type A, class IN
    ✓ 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
    ✓ Authoritative nameservers
      > fastly.net: type NS, class IN, ns ns1.fastly.net
      > fastlv.net: type NS, class IN, ns ns2.fastlv.net
  
```

Hex dump of the packet data (Frame 698):

```

0000 c0 7f 54 9f a9 14 b0 bb e5 00 91 67 00 00 45 00 ...T...:g:E
0010 00 bf bd f8 40 00 00 11 67 95 0a 00 00 8a 0a 00 ...@:g:
0020 00 17 00 35 f2 21 00 ab b9 96 04 81 00 00 01 00 ...5:l:
0030 00 02 00 04 00 00 00 68 74 74 70 73 3a 2f 2f 77 .....hhttps://
0040 77 77 06 72 65 64 64 69 74 03 63 6f 6d 00 00 01 ...wreddit.com
0050 00 01 c0 0c 00 05 00 01 00 00 20 00 17 06 72 .....Ap
0060 65 64 64 69 74 03 64 61 70 06 66 61 73 74 6c 75 ...editmapfastly
0070 03 6e 65 74 00 c0 34 00 01 00 01 c0 00 15 00 .....net:4:
0080 c4 07 e5 51 8c c0 3f 00 02 01 00 00 1b ac 00 .....Q:2:
0090 06 03 6e 73 31 c0 3f c0 3f 00 02 00 00 1b .....ns1:2:
00a0 ac 00 06 03 6e 73 32 c0 3f c0 3f 00 02 01 00 .....ns2:2:
00b0 00 1b ac 00 06 03 6e 73 33 c0 3f c0 3f 00 02 00 .....ns3:2:
00c0 01 00 00 1b ac 00 06 03 6e 73 34 c0 3f .....ns4:2:
  
```

- e. It will send a packet with `type=5` and `code=0` which indicates that a packet was forwarded 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 failure 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 transferring 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 rely 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.