Communication Networks
Prof. Laurent Vanbever

Exercise 12 – DNS, Web, and Email

DNS

12.1 Local DNS server

On Linux and Mac computers you can use the command line tool `dig` to perform DNS lookups. The corresponding tool for Windows is `nslookup`. First, perform a lookup for `nyu.edu` using your default DNS server by running the command `dig nyu.edu` or `nslookup nyu.edu`.

- What is the IP address of the server behind `nyu.edu`?

Now, perform the same lookup, but use one of the DNS root servers (e.g., `a.root-servers.net`) by running[a]

```
dig @a.root-servers.net nyu.edu
nslookup nyu.edu a.root-servers.net
```

---
[a]If the `nslookup` command does not yield helpful output for you, try adding `-type=soa` after `nslookup`. (For some, it may be the other way round—adding this option may hide the relevant part in the output.)

- Why does the answer differ compared to the one from your local DNS server?
- How would you proceed with this answer to find the IP address behind `nyu.edu`?

12.2 Name it or Route it: pick one

| DNS | *vs.* | BGP Anycast |
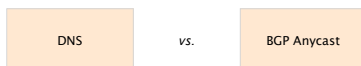
Any clear winner?

In the course, we saw two ways to replicate and load-balance content: *(i)* using Anycast routing; or *(ii)* using DNS.

a) List and briefly justify three pros and cons of each;

b) We saw that CDNs often rely on DNS for distributing their load. Could they also use Anycast routing instead? Explain why or why not.

Web and Email

12.3 HTTP host header

Perform a DNS lookup for `google.ch` and open `http://172.217.168.35` in your browser. What do you observe?

Now try to repeat the same process for `nsg.ee.ethz.ch` and `comm-net.ethz.ch`. Open the websites in your browser using the IP(s) from the DNS lookup. Do you see the expected websites?

Normally, one machine can host multiple websites at the same time. To distinguish which website has to be provided by the server, clients can add a so called "host header" in their HTTP request which specifies the website they want to access. You can try that yourself with the two websites from above. For example with the following commands:

```
telnet comm-net.ethz.ch 80
```

```
GET / HTTP/1.1
Host: comm-net.ethz.ch
```

Do you see another way how you could host multiple websites on the same machine? Can you see potential problems with this approach compared to the host header?

12.4 E-mail

Answer the following questions about e-mail with True or False and justify your choice.

a) SMTP and IMAP can be used to forward e-mails from one e-mail server to another one.

b) Looking at the header of a received e-mail, you can reconstruct through which e-mail servers the message was forwarded.

c) IMAP is the encrypted counter-part of POP.

d) It is not possible to verify that the e-mail was actually sent by the given FROM address.

e) The IP address of the mail server of a domain can be found by issuing a DNS query asking for the A record of that domain.

f) Images attached to an e-mail are transformed to text for transmission.

12.5 E-Mail analysis (Exam Style Question)

You received an email with the raw content shown in Figure 2.

```
1   Received: from edge20.ethz.ch (82.130.99.26) by CAS10.d.ethz.ch
2    (172.31.38.210) with SMTP Server (TLS) id 14.3.408.0; Thu, 2 Aug
3    2018 11:17:27 +0200
4   Received: from phil2.ethz.ch (129.132.65.3) by edge20.ethz.ch (82.130.99.26)
5    with SMTP Server id 14.3.408.0; Thu, 2 Aug 2018 11:17:23 +0200
6   Received: from filter.spam.ch ([5.152.185.154]  helo=filter.spam.ch)
7    by phil2.ethz.ch with esmtps  (TLSv1:AES128-SHA:128)   (Exim 4.69)
8    (envelope-from <john.doe@anonymous.ch>)        id 1fl9j0-0004C9-7T
9    for lvanbever@ethz.ch; Thu, 02 Aug 2018 11:17:15 +0200
10  X-Note: This Email was scanned by filter.spam.ch
11  Received: by filter.spam.ch with PIPE id
12   93122453; Thu, 02 Aug 2018 11:17:13 +0200
13  Received: from [10.40.0.131] (HELO smtp.ch.exg7.mailhost.com)  by
14   filter.spam.ch with ESMTPS id 93122443
15   for lvanbever@ethz.ch; Thu, 02 Aug 2018 11:17:10 +0200
16  Received: from exg7.mailhost.local (192.168.40.105) by
17   exg7.mailhost.local (192.168.40.107) with SMTP Server
18   (version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256_P256) id
19   15.1.1531.3; Thu, 2 Aug 2018 11:17:09 +0200
20  From: Anonymous Student <john.doe@anonymous.ch>
21  To: Laurent Vanbever <lvanbever@ethz.ch>
22  Subject: Exam solutions
23  Date: Thu, 2 Aug 2018 09:17:09 +0000
24  Message-ID: <11A5442F-4D6E-436F-A873-2E3DA3656C06@anonymous.ch>
25  Accept-Language: de-CH, en-US
26  Content-Language: en-US
27  Content-Type: text/plain; charset="us-ascii"
28  Content-ID: <F43C7219ADA84040984B4640587C2B70@fwd7.mailhost.com>
29  Content-Transfer-Encoding: quoted-printable
30  MIME-Version: 1.0
31
32  Hey, can you give me the solutions for the exam?
```

Raw content of a received email

a) According to Figure 2, what are the e-mail addresses of the sender and the receiver of this message?

b) List the IP addresses of all servers that have seen this email according to Figure 2 in chronological order starting with the server that saw the email *first*.

c) According to the header in Figure 2, the email passed a spam filter (`filter.spam.ch`). Could one of the other servers have added this entry without the email actually passing `filter.spam.ch`? If yes: why and which server(s) could have done it? If no: why not?

d) Which servers (according to Figure 2) could modify the email message ("Hey, ... ")? Why?

e) Assume you have `telnet` access to an open SMTP server that does not appear in Figure 2 and you want to fake the email shown in Figure 2. That is, your goal is that the receiver of the email in Figure 2 receives the same email again (with the same sender). Which parts of the email in Figure 2 can you replicate in your email and which parts will be different? Use the line numbers in Figure 2 to list parts that are equal or different in your email and briefly explain the reasons why they are equal or different.