Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

Networked Systems
ETH Zürich — seit 2015

Communication Networks

Prof. Laurent Vanbever

Solution: Exercise 10 – DNS part II & HTTP

10.1 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
```

```
nslookup nyu.edu
```

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

  Solution: Note that the actual IP address can depend on the local DNS server you use. We got the following answer:

  ```
  ;; ANSWER SECTION:
  nyu.edu.   60   IN   A   216.165.47.10
  ```

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

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

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

- Why does the answer differ compared to the one from your local DNS server?

  Solution: The request is not sent to an open DNS resolver, but to a DNS server that only provides answers about its own zone. Therefore, the root DNS server only points you to the name servers responsible for the next zone in the hierarchy, the edu zone.

  We got the following answer:

  ```
  ;; AUTHORITY SECTION:
  edu.  172800  IN  NS  a.edu-servers.net.
  edu.  172800  IN  NS  c.edu-servers.net.
  edu.  172800  IN  NS  d.edu-servers.net.
  ...
  ```

- How would you proceed with this answer to find the IP address behind `nyu.edu`?

  Solution: Now that we know which servers are responsible for the edu zone, we can continue step-by-step just like your local DNS server would. Next, we would send a request to one of the edu name servers:

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

  The reply points us to the name servers in charge of the zone of NYU. By sending a request to them, we finally get the IP address behind the URL `nyu.edu`.

10.2 Local vs. authoritative DNS server

Perform a DNS query for `uzh.ch` using first the authoritative DNS server (`ns1.uzh.ch`) and then your local server.

Note: When using `nslookup` on Windows, you need to specify the `-debug` flag to get the relevant information for this task. For example:

```
nslookup -debug uzh.ch
```

- Compare the `ANSWER SECTION` of the responses. Can you see differences between the answers from your local DNS server and the authoritative server? Run the query to your local server multiple times to make the differences more obvious.

  Solution: The answers differ in the time to live (TTL). While the TTL is constant in the replies from the authoritative DNS server, it varies in the replies from the local server.

- What is the reason for this difference?

  Solution: The local DNS server caches replies to requests. To ensure that it does not keep outdated information in its cache, each authoritative name server attaches a TTL to its replies. The TTL tells the local DNS server how long it can store the reply in the cache and use it to reply to requests.

- As you have seen in the lecture, DNS can be used to balance the incoming load. What are the considerations one has to make when using DNS load balancing with respect to the TTL?

  Solution: With low TTLs we can ensure that we can shift the load quickly. However, low TTLs also mean that our authoritative DNS server will get many more requests.

10.3 Curious students

Consider that ITET has a local DNS server serving the DNS requests for all students' devices connected in the department. How could you determine if an external website has been visited recently by a fellow colleague of yours? Explain.

Solution: You can simply use `dig` to issue a query for any external website you're interested in and observe the response time. If the external website has been visited recently, the response time should be close to immediate (as the local DNS server is located close by). If not, the response time will be slower as the local DNS server would have to initiate a new remote query.

You could also look at the TTL value returned by the local server and compare it to the TTL you get when querying directly the authoritative DNS server for that domain. If the TTL returned by the local server is lower than the one from the authoritative DNS server, you know that the entry has been cached by the local server and hence, someone has visited the website recently.

10.4 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?

Solution: You could assign the server multiple IP addresses and link each IP address to a single website. The biggest drawback of this solution is the need for multiple IP addresses. IPv4 addresses are limited and hence expensive.