



Communication Networks

Prof. Laurent Vanbever

Solution: Exercises week 13 – Application: DNS

DNS zone file

You are the administrator of SmartCompany (smart.com) responsible for the Internet service infrastructure of the company. SmartCompany runs its own web-services on a set of 8 static IP-Addresses (111.10.20.0 - 111.10.20.7). The file on the left is called a zone file^a and describes the DNS configuration of your zone (smart.com). Taking into consideration the zone file, respond to the following questions:

```
$TTL 3600
@           IN SOA ns.smart.com. adm.smart.com. (
           2002022401 ; serial
           3H ; refresh (hours)
           15m ; retry (minutes)
           1w ; expire (weeks)
           3h ; minimum (hours)
           )
IN         NS ns.clever.com.
IN         NS ns.smart.com.
@          IN A 111.10.20.3
www        IN A 111.10.20.5
upload     IN A 111.10.20.5
ns.smart.com. IN A 111.10.20.1
ns.clever.com. IN A 222.80.90.1
ftp        IN CNAME smart.com.
web        IN CNMAE smart.com.
```

Zone file for smart.com

a) What could be the meaning of the entries at the top (refresh, retry, ...)?

Solution:

- refresh - time for a secondary name server to wait until it should update its copy of the zone file again according to the primary name server's zone file.
- retry - time interval for the secondary name server that should elapse before a failed refresh should be retried.
- expire - time for a secondary name server to hold a zone before it is no longer considered authoritative.
- minimum - minimum TTL field that should be exported with any resource record (e.g., A record) from this zone.

^ahttps://en.wikipedia.org/wiki/Zone_file

b) Can you figure out which web-services are running on servers of the SmartCompany?

Solution: ftp, webservice

c) What is the IP address (if any) of the host www.smart.com?

Solution: It is 111.10.20.5

d) What is the IP address (if any) of the host ftp.smart.com?

Solution: It is 111.10.20.3. The CNAME record specifies that ftp is an alias for smart.com. Therefore, the IP address of ftp.smart.com is the same as the one of smart.com (as specified by @).

e) What are the FQDN (fully qualified domain name) and IP addresses of the primary and the secondary nameservers for the zone smart.com? Clearly indicate which is the primary and which is the secondary nameserver.

Solution: Primary: ns.smart.com - 111.10.20.1, secondary ns.clever.com - 222.80.90.1

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 the command:

```
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`.

Local vs. authoritative DNS server

Perform a DNS query for the URL `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 for additional output. 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 much more requests.

Multiple answers

Whenever a client (e.g., your computer) receives multiple IP addresses as answer to a DNS lookup, it picks the very first one. Only if that one does not work, it tries the next one in order.

When you run `dig yahoo.com`, you receive multiple IP addresses as an answer compared to, for example, `dig google.com`.

Can you think of a reason for answering with multiple IP addresses? Run the DNS lookup for `yahoo.com` multiple times.

Solution: (i) Resiliency: Should the first IP addresses not be reachable, you can try with the second one without having to do another DNS request.

(ii) Load of the authoritative DNS server: By giving multiple answers, you have a higher chance that one of the answers works for the entire lifetime of the reply (defined TTL value). Your DNS server will therefore get less frequent requests compared to a DNS server which only answers with one entry and a low TTL value.

(iii) Load balancing: You can use it as one way to do load balancing.