Hands-on-3: Domain Name Service (DNS)

> **Q1: What's the role of DNS? Please describe it using your own words.**

DNS is responsible for mapping a domain name to its corresponding ip address. It's not user friendly for the users to always visit a website through ip address, for it's difficult to remember. With DNS, users can type a string of url (like www.baidu.com) instead of ip address. Therefore, the role of DNS is to make it easier to visit a website or use a web service.

> **Q2: How can you ask a specific DNS server (instead of the default) for information about a domain name? For example, once the default server crashes and you wish to ask the other server 8.8.8.8, what command should you use?**

We can use command:

```
dig @8.8.8.8 www.sina.com
```

If the default server crashes and I wish to ask the other server 8.8.8.8

We can use the parameter `+trace` to trace the stack of recursive search.

For example, if we try to:

```
dig www.sina.com +trace
```

Then we will get:

```
...
Received 262 bytes from 127.0.0.53#53(127.0.0.53) in 4 ms
...
Received 1200 bytes from 199.7.91.13#53(d.root-servers.net) in 28 ms
...
Received 791 bytes from 192.5.6.30#53(a.gtld-servers.net) in 220 ms
...
Received 75 bytes from 114.134.80.144#53(ns1.sina.com) in 64 ms
```

We can then use ***@xxx*** to search the domain name at ***xxx***. In this way, we are free to specify the DNS server.

```
dig @8.8.8.8 www.sina.com
```

Furthermore, parameter ***+norecurse*** can be used to prevent default recursive search.

```
dig @a.root-servers.net www.sina.com +norecurse
```

> **Q3: Do you know the process of solving the domain name of "ipads.se.sjtu.edu.cn"? How many queries did it take to find the IP address for ipads? Include the sequence of commands that you used.**

The sequence of commands I used:

- First, get a list of the root servers.

```
dig . ns
```

- Then search at ***j.root-servers.net***

```
dig @j.root-servers.net ipads.se.sjtu.edu.cn +norecurse
```

- Then at ***c.dns.cn***

```
dig @c.dns.cn ipads.se.sjtu.edu.cn +norecurse
```

- Then at ***dns.edu.cn***

```
dig @dns.edu.cn ipads.se.sjtu.edu.cn +norecurse
```

- Then at ***dns.sjtu.edu.cn***

```
dig @dns.sjtu.edu.cn ipads.se.sjtu.edu.cn +norecurse
```

- Then we got a ***glue record***

```
;; ADDITIONAL SECTION:
seserver.se.sjtu.edu.cn. 3600   IN  A   202.120.40.2
```

- Then at ***202.120.40.2***

```
dig @202.120.40.2 ipads.se.sjtu.edu.cn
```

- Finally we got the answer:

```
;; ANSWER SECTION:
ipads.se.sjtu.edu.cn.   3600    IN  A   202.120.40.85
```

- The ip address of ***ipads.se.sjtu.edu.cn*** is ***202.120.40.85***

  There are **5** queries in total.

> **Q4: Did the default server have the answer in its cache? How do you know?**

The default server have the answer cached.

Because you will get a response with a relatively high latency: 40ms at first, but then the responses will only take 0-4ms. After a little time, you will experience a relatively high latency again.

If I change to ***8.8.8.8*** for query. The response latency is about 150ms at first, then it decreases to about 60 - 80 ms. It turns out that all DNS has its cache.

Moreover, I try to visit a rarely known website https://yokohei.com/docs/dns-trace.html. The response latency at first is really high: 212 ms. But after that, when I dig it again, the latency has become 0 ms.

Interestingly, I tried a non-existent host name: ***232saaxa.com***, It seems that it has also been cached.

So, there is no doubt that the default DNS will **cache** the answer.