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

Read the following hands-on. Do as instructed, and submit your solutions **in English or Chinese** for the following quizes. Upload your answers to Canvas in a .pdf file. Due is 2021-12-17 23:59.

This hands-on would help you learn more about the Internet's Domain Name System (DNS).

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

We introduce a useful tool--- `dig`(Domain Information Groper), similar to `nslookup`. You may type `nslookup www.sina.com` to the terminal on your Windows. Either Windows or Ubuntu has dig (`sudo apt-get install dnsutils`).

```
cse@cse-lab:~$ dig www.sina.com

; <<>> DiG 9.11.4-P2-RedHat-9.11.4-26.P2.3.al7.7 <<>> www.sina.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 35037
;; flags: qr rd ra; QUERY: 1, ANSWER: 12, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;www.sina.com.                  IN      A

;; ANSWER SECTION:
www.sina.com.           60      IN      CNAME   spool.grid.sinaedge.com.
spool.grid.sinaedge.com. 30     IN      CNAME   ww1.sinaimg.cn.w.alikunlun.com.
ww1.sinaimg.cn.w.alikunlun.com. 30 IN   A       39.96.118.195
ww1.sinaimg.cn.w.alikunlun.com. 30 IN   A       39.96.118.196
ww1.sinaimg.cn.w.alikunlun.com. 30 IN   A       39.96.118.191
ww1.sinaimg.cn.w.alikunlun.com. 30 IN   A       39.96.118.193
ww1.sinaimg.cn.w.alikunlun.com. 30 IN   A       39.96.118.190
ww1.sinaimg.cn.w.alikunlun.com. 30 IN   A       39.96.118.147
ww1.sinaimg.cn.w.alikunlun.com. 30 IN   A       39.96.118.192
ww1.sinaimg.cn.w.alikunlun.com. 30 IN   A       39.96.118.148
ww1.sinaimg.cn.w.alikunlun.com. 30 IN   A       39.96.118.189
ww1.sinaimg.cn.w.alikunlun.com. 30 IN   A       39.96.118.194
```

We are particularly interested in the `ANSWER` section. The five fields of this section are name, expiration time, class, type, data. You can ignore the `class` field because this is nearly always IN for Internet. We can use `dig +short www.sina.com` for a short result of the domain. When you want to find the domain name of some IP, try `dig -x 173.194.127.80`. Many other interesting options like `-f`, `+domain` and `+trace` are free to try. Refer to `man dig` and take a fun tour.

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?

Dig only prints the final result of the recursive search. You can mimic the individual steps of a recursive search by sending a request to a particular DNS server and asking for no recursion using the `+norecurs` flag. For example, to send a non-recursive query to one of the root servers:

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

As can be seen, the server does not know the answer and instead provides information about the servers most likely to offer authoritative information.

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.

Assuming a DNS resolver knows nothing else about a name, it will ask a well-known root server. The root servers on the Internet are in the domain root-servers.net, and one way to get a list of them is with the command:

```
dig . ns
```

Use dig to ask *one* of the root servers the address of ipads.se.sjtu.edu.cn, *without* recursion.

It is unlikely that these servers know the answer, so they will *refer* you to a server (or list of servers) that might know. Go through the root hierarchy without recursion, follow the referrals manually until you have found the address.

Hint: you should start from "cn".

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

Hint: For each query that you run, please keep track of how long it took to get a response. If this information was cached, please find another host name that is not cached and *do differential testing*.