hands-on-3

---

id: 519021910861

name: huidong xu

Q1. What's the role of DNS?

The domain name system(DNS) is a naming database in which Internet domain names are located and translated into Internet Protocol(IP) addresses. DNS maps the name people use to locate a website to the IP address that a computer uses to locate that website.

For example, if someone types "ipads.se.sjtu.edu.cn" into a web browser, a server behind the scenes maps that name to the corresponding IP address 202.120.40.85 which I get from a `dig`.

```
parallels@parallels-Parallels-Virtual-Platform:~/Desktop$ dig ipads.se.sjtu.edu.
cn

; <<>> DiG 9.16.1-Ubuntu <<>> ipads.se.sjtu.edu.cn
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 28822
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;ipads.se.sjtu.edu.cn.          IN      A

;; ANSWER SECTION:
ipads.se.sjtu.edu.cn.   0       IN      A       202.120.40.85

;; Query time: 4 msec
;; SERVER: 127.0.0.53#53(127.0.0.53)
;; WHEN: Fri Dec 17 03:27:11 PST 2021
;; MSG SIZE  rcvd: 65
```

What's more, web browsing and most other Internet activities rely on DNS to quickly provide the information necessary to connect users to remote hosts. DNS mapping is distributed throughout the Internet in a hierarchy of authority. Access providers and enterprises, as well as governments, universities and other organizations, typically have their own assigned ranges of IP addresses and an assigned domain name. They also typically run DNS servers to manage the mapping of those names to those addresses. Most Uniform Resource Locators(URLs) are built around the domain name of the web server that takes client requests.

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?

Use dig with specific command.

```
> dig @8.8.8.8 ipads.se.sjtu.edu.cn +norecurse
```

```
parallels@parallels-Parallels-Virtual-Platform:~/Desktop$ dig @8.8.8.8 ipads.se.
sjtu.edu.cn +norecurse

; <<>> DiG 9.16.1-Ubuntu <<>> @8.8.8.8 ipads.se.sjtu.edu.cn +norecurse
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 36951
;; flags: qr ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;ipads.se.sjtu.edu.cn.          IN      A

;; ANSWER SECTION:
ipads.se.sjtu.edu.cn.   3046    IN      A       202.120.40.85

;; Query time: 320 msec
;; SERVER: 8.8.8.8#53(8.8.8.8)
;; WHEN: Fri Dec 17 03:37:06 PST 2021
;; MSG SIZE  rcvd: 65
```

Use nslookup with specific command.

```
> nslookup ipads.se.sjtu.edu.cn 8.8.8.8
```

```
parallels@parallels-Parallels-Virtual-Platform:~/Desktop$ nslookup ipads.se.sjtu
.edu.cn 8.8.8.8
Server:         8.8.8.8
Address:        8.8.8.8#53

Non-authoritative answer:
Name:   ipads.se.sjtu.edu.cn
Address: 202.120.40.85
```

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.

There will be **5** queries.

1. Look up the root server, and get response address 'cn.'

```
parallels@parallels-Parallels-Virtual-Platform:~/Desktop$ dig @g.root-servers.net ipads.se.sjtu.edu.cn +norecurse

; <<>> DiG 9.16.1-Ubuntu <<>> @g.root-servers.net ipads.se.sjtu.edu.cn +norecurse
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 51336
;; flags: qr; QUERY: 1, ANSWER: 0, AUTHORITY: 8, ADDITIONAL: 11

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: 44541ef83fcb4df2e42f8be861bc787e01cdba818ddae6fb (good)
;; QUESTION SECTION:
;ipads.se.sjtu.edu.cn.          IN      A

;; AUTHORITY SECTION:
cn.                     172800  IN      NS      e.dns.cn.
cn.                     172800  IN      NS      a.dns.cn.
cn.                     172800  IN      NS      ns.cernet.net.
cn.                     172800  IN      NS      b.dns.cn.
cn.                     172800  IN      NS      f.dns.cn.
cn.                     172800  IN      NS      c.dns.cn.
cn.                     172800  IN      NS      d.dns.cn.
cn.                     172800  IN      NS      g.dns.cn.

;; ADDITIONAL SECTION:
a.dns.cn.               172800  IN      A       203.119.25.1
b.dns.cn.               172800  IN      A       203.119.26.1
c.dns.cn.               172800  IN      A       203.119.27.1
d.dns.cn.               172800  IN      A       203.119.28.1
e.dns.cn.               172800  IN      A       203.119.29.1
f.dns.cn.               172800  IN      A       195.219.8.90
g.dns.cn.               172800  IN      A       66.198.183.65
ns.cernet.net.          172800  IN      A       202.112.0.44
a.dns.cn.               172800  IN      AAAA    2001:dc7::1
d.dns.cn.               172800  IN      AAAA    2001:dc7:1000::1

;; Query time: 12 msec
;; SERVER: 192.112.36.4#53(192.112.36.4)
;; WHEN: Fri Dec 17 03:46:06 PST 2021
;; MSG SIZE  rcvd: 404
```

2. Ask '.cn' server, and get response address 'edu.cn.'

```
parallels@parallels-Parallels-Virtual-Platform:~/Desktop$ dig @a.dns.cn ipads.se.sjtu.edu.cn +norecurse

; <<>> DiG 9.16.1-Ubuntu <<>> @a.dns.cn ipads.se.sjtu.edu.cn +norecurse
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 34067
;; flags: qr; QUERY: 1, ANSWER: 0, AUTHORITY: 5, ADDITIONAL: 5

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;ipads.se.sjtu.edu.cn.          IN      A

;; AUTHORITY SECTION:
edu.cn.                 172800  IN      NS      deneb.dfn.de.
edu.cn.                 172800  IN      NS      dns2.edu.cn.
edu.cn.                 172800  IN      NS      ns2.cernet.net.
edu.cn.                 172800  IN      NS      ns2.cuhk.hk.
edu.cn.                 172800  IN      NS      dns.edu.cn.

;; ADDITIONAL SECTION:
dns.edu.cn.             172800  IN      A       202.38.109.35
dns2.edu.cn.            172800  IN      A       202.112.0.13
dns.edu.cn.             172800  IN      AAAA    2001:250:c006::35
dns2.edu.cn.            172800  IN      AAAA    2001:da8:1:100::13

;; Query time: 28 msec
;; SERVER: 203.119.25.1#53(203.119.25.1)
;; WHEN: Fri Dec 17 03:46:34 PST 2021
;; MSG SIZE  rcvd: 253
```

3. Ask 'edu.cn.' server, and get response address 'sjtu.edu.cn'

```
parallels@parallels-Parallels-Virtual-Platform:~/Desktop$ dig @dns.edu.cn ipads.se.sjtu.edu.cn +norecurse

; <<>> DiG 9.16.1-Ubuntu <<>> @dns.edu.cn ipads.se.sjtu.edu.cn +norecurse
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 37000
;; flags: qr; QUERY: 1, ANSWER: 0, AUTHORITY: 2, ADDITIONAL: 5

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: d401dd07690af6f4b510e77761bc78ada133d5cd4ac5e0b4 (good)
;; QUESTION SECTION:
;ipads.se.sjtu.edu.cn.          IN      A

;; AUTHORITY SECTION:
sjtu.edu.cn.            172800  IN      NS      dns.sjtu.edu.cn.
sjtu.edu.cn.            172800  IN      NS      apple.sjtu.edu.cn.

;; ADDITIONAL SECTION:
apple.sjtu.edu.cn.      172800  IN      A       202.112.26.43
dns.sjtu.edu.cn.        172800  IN      A       202.120.2.90
apple.sjtu.edu.cn.      172800  IN      AAAA    2001:da8:8000:6180:150:112:26:43
dns.sjtu.edu.cn.        172800  IN      AAAA    2001:da8:8000:1:202:120:2:90

;; Query time: 36 msec
;; SERVER: 202.38.109.35#53(202.38.109.35)
;; WHEN: Fri Dec 17 03:46:53 PST 2021
;; MSG SIZE  rcvd: 214
```

4. Ask 'sjtu.edu.cn.' server, and get response address 'se.sjtu.edu.cn'

```
parallels@parallels-Parallels-Virtual-Platform:~/Desktop$ dig @apple.sjtu.edu.cn ipads.se.sjtu.edu.cn +norecurse

; <<>> DiG 9.16.1-Ubuntu <<>> @apple.sjtu.edu.cn ipads.se.sjtu.edu.cn +norecurse
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 48583
;; flags: qr; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 2

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;ipads.se.sjtu.edu.cn.          IN      A

;; AUTHORITY SECTION:
se.sjtu.edu.cn.         3600    IN      NS      seserver.se.sjtu.edu.cn.

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

;; Query time: 4 msec
;; SERVER: 202.112.26.43#53(202.112.26.43)
;; WHEN: Fri Dec 17 03:47:02 PST 2021
;; MSG SIZE  rcvd: 88
```

5. Ask 'se.sjtu.edu.cn.' server, and get response address 'ipads.se.sjtu.edu.cn'

```
parallels@parallels-Parallels-Virtual-Platform:~/Desktop$ dig @202.120.40.2 ipads.se.sjtu.edu.cn +norecurse

; <<>> DiG 9.16.1-Ubuntu <<>> @202.120.40.2 ipads.se.sjtu.edu.cn +norecurse
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 17505
;; flags: qr aa; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4000
;; QUESTION SECTION:
;ipads.se.sjtu.edu.cn.          IN      A

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

;; Query time: 3 msec
;; SERVER: 202.120.40.2#53(202.120.40.2)
;; WHEN: Fri Dec 17 03:56:42 PST 2021
;; MSG SIZE  rcvd: 65
```

Q4. Did the default server have the answer in its cache? How do you know?
If it is obtained from the cache, it can be seen from the result of dig. There is a Time To Live(TTL), which is the number after `ipads.se.sjtu.edu.cn` in the picture. It can be seen that the same website is visited twice before and after, and the TTL has changed from 238 to 233. If it exceeds when no one visits at this time, it will be removed from the DNS cache.

```
parallels@parallels-Parallels-Virtual-Platform:~/Desktop$ dig ipads.se.sjtu.edu.cn

; <<>> DiG 9.16.1-Ubuntu <<>> ipads.se.sjtu.edu.cn
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 5251
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;ipads.se.sjtu.edu.cn.          IN      A

;; ANSWER SECTION:
ipads.se.sjtu.edu.cn.   238     IN      A       202.120.40.85

;; Query time: 0 msec
;; SERVER: 127.0.0.53#53(127.0.0.53)
;; WHEN: Fri Dec 17 04:05:42 PST 2021
;; MSG SIZE  rcvd: 65

parallels@parallels-Parallels-Virtual-Platform:~/Desktop$ dig ipads.se.sjtu.edu.cn

; <<>> DiG 9.16.1-Ubuntu <<>> ipads.se.sjtu.edu.cn
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 39552
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;ipads.se.sjtu.edu.cn.          IN      A

;; ANSWER SECTION:
ipads.se.sjtu.edu.cn.   233     IN      A       202.120.40.85

;; Query time: 0 msec
;; SERVER: 127.0.0.53#53(127.0.0.53)
;; WHEN: Fri Dec 17 04:05:47 PST 2021
;; MSG SIZE  rcvd: 65
```

I got verification from a website that is unlikely to have ever been visited.
When I visit `xhd.cn` for the first time, I can see that the TTL is 600 and the Query Time is very long because the URL does not exist and is not cached in dig.

```
parallels@parallels-Parallels-Virtual-Platform:~/Desktop$ dig xhd.cn

; <<>> DiG 9.16.1-Ubuntu <<>> xhd.cn
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 5955
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;xhd.cn.                                IN      A

;; ANSWER SECTION:
xhd.cn.                 600     IN      A       39.106.198.107

;; Query time: 304 msec
;; SERVER: 127.0.0.53#53(127.0.0.53)
;; WHEN: Fri Dec 17 04:09:58 PST 2021
;; MSG SIZE  rcvd: 51
```

When I visited again, because dig was already cached, the Query Time was very short, and the TTL was correspondingly substract from the interval between these two visits.

```
parallels@parallels-Parallels-Virtual-Platform:~/Desktop$ dig xhd.cn

; <<>> DiG 9.16.1-Ubuntu <<>> xhd.cn
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 18765
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;xhd.cn.                                IN      A

;; ANSWER SECTION:
xhd.cn.                 595     IN      A       39.106.198.107

;; Query time: 4 msec
;; SERVER: 127.0.0.53#53(127.0.0.53)
;; WHEN: Fri Dec 17 04:10:03 PST 2021
;; MSG SIZE  rcvd: 51
```