COMP9331 Lab3 课堂笔记

Exercise 1 DNS Types:

- **A** record - The record that holds the IP address of a domain (IP 地址)
- **CNAME** record - Forwards one domain or subdomain to another domain, does NOT provide an IP address
- **MX** record - Directs mail to an email server (邮件)
- TXT record - Lets an admin store text notes in the record
- **NS** record - Stores the name server for a DNS entry (权威应答所在服务器)
- SOA record - Stores admin information about a domain
- SRV record - Specifies a port for specific services
- PTR record - Provides a domain name in reverse-lookups

Exercise 2:

如何在 Wireshark 里面查看 DNS 信息(见录屏)

Exercise 3:

Dig 用法:

1. dig *domain*

   `$ dig google.com` -- 查询 google.com 的 DNS 信息

2. dig *@ip_addr domain*

   `$ dig @129.94.242.33 google.com` -- 使用指定服务器(129.94.242.33)查询 google.com 的 DNS 信息

3. dig *@ip_addr domain DNStype*

   `$ dig @129.94.242.33 google.com MX` -- 使用指定服务器(129.94.242.33)查询 google.com 指定类型的 DNS 信息

做题思路:

Exercise 3

Q1

运行 dig 命令, 查看对应 A 类型的结果:

```
$ dig www.eecs.berkeley.edu
```

Q2

查看 CNAME 类型的结果

Q3

Authority section: The name server which are authoritative for the record.

Additional section: IP addresses of the nameservers in authority section.

Q4

查看 dig 输出结果的最后几行:

```
;; Query time: 24 msec
;; SERVER: 129.94.242.2#53(129.94.242.2)
;; WHEN: Fri Oct 09 22:29:09 AEDT 2020
;; MSG SIZE  rcvd: 425
```

Q5

运行 dig 命令, 查看对应 NS 类型的结果:

```
$ dig eecs.berkeley.edu NS
```

```
;; ANSWER SECTION:
eecs.berkeley.edu.      86400   IN      NS      adns2.berkeley.edu.
eecs.berkeley.edu.      86400   IN      NS      ns.eecs.berkeley.edu.
eecs.berkeley.edu.      86400   IN      NS      adns1.berkeley.edu.
eecs.berkeley.edu.      86400   IN      NS      adns3.berkeley.edu.
eecs.berkeley.edu.      86400   IN      NS      ns.CS.berkeley.edu.

;; ADDITIONAL SECTION:
ns.CS.berkeley.edu.     42846   IN      A       169.229.60.61
ns.eecs.berkeley.edu.   43654   IN      A       169.229.60.153
adns1.berkeley.edu.     5564    IN      A       128.32.136.3
adns1.berkeley.edu.     3318    IN      AAAA    2607:f140:8000:fffe::3
adns2.berkeley.edu.     3318    IN      A       128.32.136.14
adns2.berkeley.edu.     5564    IN      AAAA    2607:f140:ffff:fffe::e
adns3.berkeley.edu.     10169   IN      A       192.107.102.142
adns3.berkeley.edu.     3318    IN      AAAA    2607:f140:a000:d::abc
```

这些都是

ip在这里

Q6

运行 dig 命令, 查看对应 PTR 类型的结果:

```
$ dig -x 111.68.101.54
```

Q7

运行 dig 命令, 查看对应 MX 类型的结果:

```
$ dig @129.94.242.33 yahoo.com MX
```

如何判断是否权威应答:

观察 flags 里面是否有 “aa”!

```
; <<>> DiG 9.9.5-9+deb8u19-Debian <<>> @129.94.242.33 yahoo.com MX
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 51380
;; flags: qr rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 5, ADDITIONAL: 10

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;yahoo.com.                     IN      MX
```

非权威应答

```
; <<>> DiG 9.9.5-9+deb8u19-Debian <<>> @68.180.131.16 yahoo.com MX
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 39350
;; flags: qr aa rd; QUERY: 1, ANSWER: 3, AUTHORITY: 5, ADDITIONAL: 10
;; WARNING: recursion requested but not available
```

权威应答

Q8

同上题, 不过使用的是 Q5 里面的 ip 地址.

Q9

运行 dig 命令, 查看对应 **MX** 类型的结果:

```
$ dig @68.180.131.16 yahoo.com MX
```

```
;; ADDITIONAL SECTION:
ns1.yahoo.com.          1209600 IN      A       68.180.131.16
ns2.yahoo.com.          1209600 IN      A       68.142.255.16
ns3.yahoo.com.          1800    IN      A       27.123.42.42
ns4.yahoo.com.          1209600 IN      A       98.138.11.157
ns5.yahoo.com.          86400   IN      A       202.165.97.53
ns1.yahoo.com.          86400   IN      AAAA    2001:4998:130::1001
ns2.yahoo.com.          86400   IN      AAAA    2001:4998:140::1002
ns3.yahoo.com.          1800    IN      AAAA    2406:8600:f03f:1f8::10
ns5.yahoo.com.          86400   IN      AAAA    2406:2000:ff60::53
```

(用这些 IP 地址都行)

Q10

第一步:

运行 dig 命令, 查看对应 NS 类型的结果:

```
$  dig . NS
```

```
;; ADDITIONAL SECTION:
a.root-servers.net.     307903  IN      A       198.41.0.4
a.root-servers.net.     412702  IN      AAAA    2001:503:ba3e::2:3
b.root-servers.net.     421817  IN      A       199.9.14.201
b.root-servers.net.     143292  IN      AAAA    2001:500:200::b
c.root-servers.net.     257832  IN      A       192.33.4.12
c.root-servers.net.     257832  IN      AAAA    2001:500:2::c
d.root-servers.net.     257832  IN      A       199.7.91.13
d.root-servers.net.     257832  IN      AAAA    2001:500:2d::d
e.root-servers.net.     349711  IN      A       192.203.230.10
e.root-servers.net.     404288  IN      AAAA    2001:500:a8::e
```

第二步:

根据第一步拿到的 NS 服务器, 进一步查询 au.的权威服务器

运行 dig 命令, 查看对应 NS 类型的结果:

```
$  dig @198.41.0.4 au. NS
```

```
;; AUTHORITY SECTION:
au.                     172800  IN      NS      m.au.
au.                     172800  IN      NS      d.au.
au.                     172800  IN      NS      q.au.
au.                     172800  IN      NS      t.au.
au.                     172800  IN      NS      s.au.
au.                     172800  IN      NS      r.au.
au.                     172800  IN      NS      n.au.
au.                     172800  IN      NS      a.au.
au.                     172800  IN      NS      c.au.

;; ADDITIONAL SECTION:
m.au.                   172800  IN      A       156.154.100.24
m.au.                   172800  IN      AAAA    2001:502:2eda::24
d.au.                   172800  IN      A       162.159.25.38
d.au.                   172800  IN      AAAA    2400:cb00:2049:1::a29f:1926
q.au.                   172800  IN      A       65.22.196.1
q.au.                   172800  IN      AAAA    2a01:8840:be::1
t.au.                   172800  IN      A       65.22.199.1
```

第三步:

根据第二步拿到的 NS 服务器, 进一步查询 edu.au.的权威服务器

运行 dig 命令, 查看对应 NS 类型的结果:

```
$  dig @156.154.100.24 edu.au. NS
```

```
;; ANSWER SECTION:
edu.au.                 900     IN      NS      s.au.
edu.au.                 900     IN      NS      r.au.
edu.au.                 900     IN      NS      t.au.
edu.au.                 900     IN      NS      q.au.

;; ADDITIONAL SECTION:
q.au.                   1906    IN      A       65.22.196.1
q.au.                   58896   IN      AAAA    2a01:8840:be::1
r.au.                   4910    IN      A       65.22.197.1
r.au.                   49938   IN      AAAA    2a01:8840:bf::1
s.au.                   17418   IN      A       65.22.198.1
s.au.                   69984   IN      AAAA    2a01:8840:c0::1
t.au.                   40832   IN      A       65.22.199.1
t.au.                   71514   IN      AAAA    2a01:8840:c1::1
```

第四步:

根据第三步拿到的 NS 服务器, 进一步查询 unsw.edu.au 的权威服务器

运行 dig 命令, 查看对应 NS 类型的结果:

```
$  dig @65.22.196.1 unsw.edu.au NS
```

```
;; AUTHORITY SECTION:
unsw.edu.au.            900     IN      NS      ns3.unsw.edu.au.
unsw.edu.au.            900     IN      NS      ns2.unsw.edu.au.
unsw.edu.au.            900     IN      NS      ns1.unsw.edu.au.

;; ADDITIONAL SECTION:
ns1.unsw.edu.au.        900     IN      A       129.94.0.192
ns2.unsw.edu.au.        900     IN      A       129.94.0.193
ns3.unsw.edu.au.        900     IN      A       192.155.82.178
ns1.unsw.edu.au.        900     IN      AAAA    2001:388:c:35::1
ns2.unsw.edu.au.        900     IN      AAAA    2001:388:c:35::2
```

第五步:

根据第四步拿到的 NS 服务器, 进一步查询 cse.unsw.edu.au 的权威服务器

运行 dig 命令, 查看对应 NS 类型的结果:

```
$  dig @129.94.0.192 cse.unsw.edu.au NS
```

```
;; AUTHORITY SECTION:
cse.unsw.edu.au.        10800   IN      NS      maestro.orchestra.cse.unsw.edu.au.
cse.unsw.edu.au.        10800   IN      NS      beethoven.orchestra.cse.unsw.edu.au.

;; ADDITIONAL SECTION:
beethoven.orchestra.cse.unsw.edu.au. 10800 IN A 129.94.242.2
beethoven.orchestra.cse.unsw.edu.au. 10800 IN A 129.94.172.11
beethoven.orchestra.cse.unsw.edu.au. 10800 IN A 129.94.208.3
maestro.orchestra.cse.unsw.edu.au. 10800 IN A   129.94.242.33
```

第六步:

根据第五步拿到的 NS 服务器, 进一步查询你的 ip 地址

运行 dig 命令, 查看对应 A 类型的结果:

```
$  dig @129.94.242.2 lyre00.cse.unsw.edu.au A
```

最终结果:

```
;; ANSWER SECTION:
lyre00.cse.unsw.edu.au. 3600    IN      A       129.94.210.20
```

Question11

Yes, one physical machine can have several names and/or IP addresses associated with it.

A physical machine may have several network interfaces, and an interface may associate with several IP addresses. For example, a computer can have several IP addresses by install several network interfaces cards.

Exercise 4

参见代码 **WebServer.py**

运行方式 :

1. Terminal 里面运行: **python3 WebServer.py 5678**
2. 浏览器访问地址: 127.0.0.1:5678/index.html