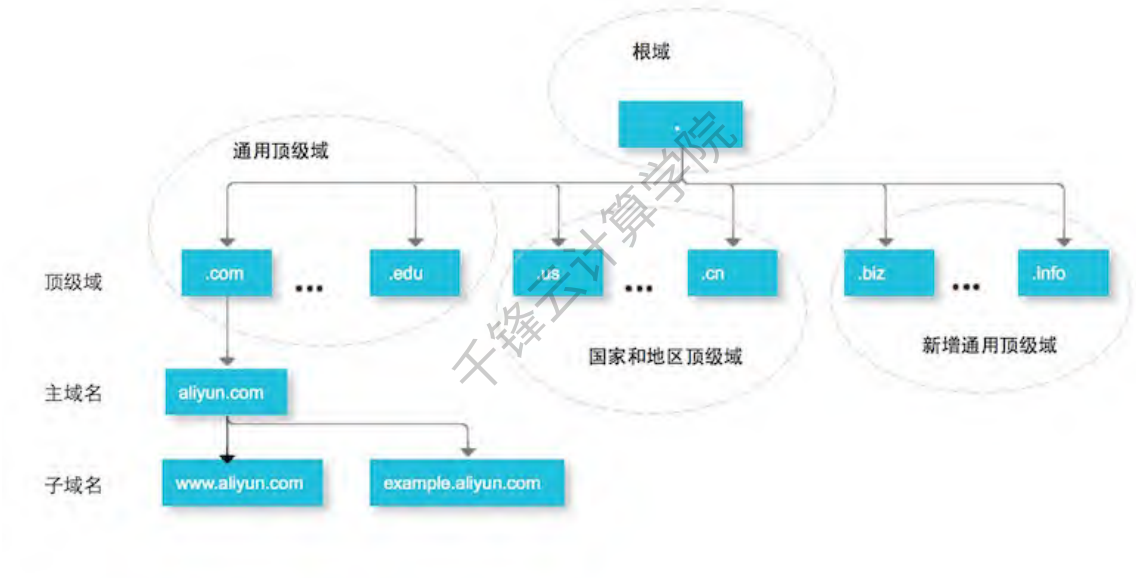
第4天-域名申请及解析

一、DNS 基本概念

- DNS 是域名系统 (Domain Name System) 的缩写，是因特网的一项核心服务，它作为可以将域名和IP地址相互映射的一个分布式数据库，能够使人更方便的访问互联网，而不用去记住能够被机器直接读取的IP数串。

二、域名的分层结构

- 由于因特网的用户数量较多，所以因特网在命名时采用的是层次树状结构的命名方法。任何一个连接在因特网上的主机或路由器，都有一个唯一的层次结构的名字，即域名(domain name)。这里，“域”(domain)是名字空间中一个可被管理的划分。从语法上讲，每一个域名都是有标号(label)序列组成，而各标号之间用点(小数点)隔开。域名可以划分为各个子域，子域还可以继续划分为子域的子域，这样就形成了顶级域、主域名、子域名等。关于域名层次结构如下图：



三、域名分层举例

- “.com”是顶级域名；
- “aliyun.com”是主域名（也可称托管一级域名），主要指企页名；
- “example.aliyun.com”是子域名（也可称为托管二级域名）；
- “www.example.aliyun.com”是子域名的子域（也可称为托管三级域名）。

四、DNS的分层结构

- 域名是分层结构，域名DNS服务器也是对应的层级结构。有了域名结构，还需要有域名DNS服务器去解析域名，且是需要由遍及全世界的域名DNS服务器去解析，域名DNS服务器实际上就是装有域名系统的主机。域名解析过程涉及4个DNS服务器，分别如下：

分类	作用
根DNS服务器	英文：Root nameserver。本地域名服务器在本地查询不到解析结果时，则第一步会向它进行查询，并获取顶级域名服务器的IP地址。
顶级域名服务器	英文：Tld nameserver。负责管理在该顶级域名服务器下注册的二级域名，例如“www.example.com”，.com则是顶级域名服务器，在向它查询时，可以返回二级域名“example.com”所在的权威域名服务器地址
权威域名服务器	英文：authoritative nameserver。在特定区域内具有唯一性，负责维护该区域内的域名与IP地址之间的对应关系，例如云解析DNS。
本地域名服务器	英文：DNS resolver或Local DNS。本地域名服务器是响应来自客户端的递归请求，并最终跟踪直到获取到解析结果的DNS服务器。例如用户本机自动分配的DNS、运营商ISP分配的DNS、谷歌/114公共DNS等

- 每个层的域名上都有自己的域名服务器，最顶层的是根域名服务器
- 每一级域名服务器都知道下级域名服务器的IP地址，以便于一级一级向下查询

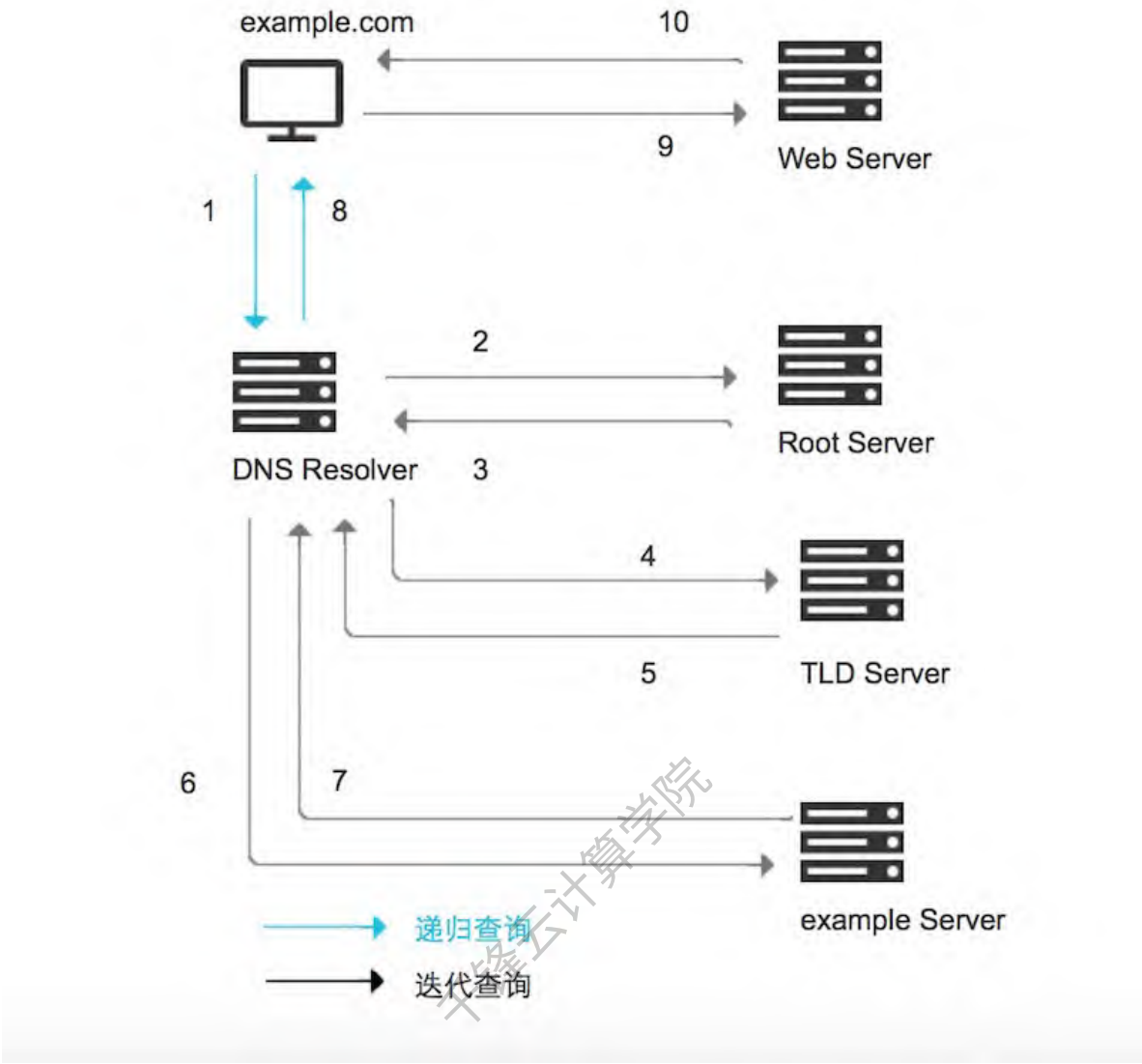
五、DNS 解析过程

- DNS查询的结果通常会在本地域名服务器中进行缓存，如果本地域名服务器中有缓存的情况下，则会跳过如下DNS查询步骤，很快返回解析结果。下面的示例则概述了本地域名服务器没有缓存的情况下，DNS查询所需的8个步骤：

1. 用户在Web浏览器中输入“example.com”， 则由本地域名服务器开始进行递归查询。
2. 本地域名服务器采用迭代查询的方法，向根域名服务器进行查询 。
3. 根域名服务器告诉本地域名服务器，下一步应该查询的顶级域名服务器.com TLD的IP地址
4. 本地域名服务器向顶级域名服务器.com TLD进行查询
5. .com TLD服务器告诉本地域名服务器，下一步查询example.com权威域名服务器的IP地址
6. 本地域名服务器向example.com权威域名服务器发送查询
7. example.com权威域名服务器告诉本地域名服务器所查询的主机IP地址
8. 本地域名服务器最后把查询的IP地址响应给web浏览器

- 一旦DNS查询的8个步骤返回了example.com的IP地址，浏览器就能够发出对网页的请求：

9. 浏览器向IP地址发出HTTP请求
10. 该IP处的web服务器返回要在浏览器中呈现的网页



六、DNS术语

1、递归查询

- 是指DNS服务器在收到用户发起的请求时，必须向用户返回一个准确的查询结果。如果DNS服务器本地没有存储与之对应的信息，则该服务器需要询问其他服务器，并将返回的查询结构提交给用户。

2、迭代查询

- 是指DNS服务器在收到用户发起的请求时，并不直接回复查询结果，而是告诉另一台DNS服务器的地址，用户再向这台DNS服务器提交请求，这样依次反复，直到返回查询结果。

3、DNS缓存

- DNS缓存是将解析数据存储在靠近发起请求的客户端的位置，也可以说DNS数据是可以缓存在任意位置，最终目的是以此减少递归查询过程，可以更快的让用户获得请求结果。

4、TTL

- 英文全称Time To Live ，这个值是告诉本地域名服务器，域名解析结果可缓存的最长时间，缓存时间到期后本地域名服务器则会删除该解析记录的数据，删除之后，如有用户请求域名，则会重新进行递归查询/迭代查询的过程。

5、IPV4、IPV6双栈技术

- 双栈英文Dual IP Stack，就是在一个系统中可同时使用IPv6/ IPv4这两个可以并行工作的协议栈

6、TLD Server

- 英文全称Top-level domains Server，指顶级域名服务器。

7、DNS Resolver

- 指本地域名服务器，它是DNS查找中的第一站，是负责处理发出初始请求的DNS服务器。运营商ISP分配的DNS、谷歌8.8.8.8等都属于DNS Resolver。

8、Root Server

- 指根域名服务器，当本地域名服务器在本地查询不到解析结果时，则第一步会向它进行查询，并获取顶级域名服务器的IP地址。

9、DNS Query Flood Attack

- 指域名查询攻击，攻击方法是通过操纵大量傀儡机器，发送海量的域名查询请求，当每秒域名查询请求次数超过DNS服务器可承载的能力时，则会造成解析域名超时从而直接影响业务的可用性。

10、URL转发

- 英文 Url Forwarding，也可称地址转向，它是通过服务器的特殊设置，将一个域名指向到另外一个已存在的站点

11、edns-client-subnet

- google提交了一份DNS扩展协议，允许DNS resolver传递用户的ip地址给authoritative DNS server.

12、DNSSEC

- 域名系统安全扩展（DNS Security Extensions），简称DNSSEC。它是通过数字签名来保证DNS应答报文的真实性和完整性，可有效防止DNS欺骗和缓存污染等攻击，能够保护用户不被重定向到非预期地址，从而提高用户对互联网的信任。

七、DNS 记录类型

- DNS支持A、CNAME、MX、TXT、SRV、AAAA、NS、CAA记录类型

记录类型	功能描述
A	IPV4记录，支持将域名映射到IPv4地址使用
AAAA	IPV6记录，支持将域名映射到IPv6地址使用
CNAME	别名记录，支持将域名指向另外一个域名
MX	电邮交互记录，支持将域名指向邮件服务器地址
TXT	文本记录，是任意可读的文本DNS记录
SRV	服务器资源记录，用来标识某台服务器使用了某个服务，常见于微软系统的目录管理
NS	名称服务器记录，支持将子域名委托给其他DNS服务商解析
CAA	CAA资源记录，可以限定域名颁发证书和CA（证书颁发机构）之间的联系

八、DNS 客户端检测工具

- 正、反解查询命令：host、nslookup、dig

1、host

- 解析域名对应的IP地址和别名等信息

1. 语法

```
host [选项] [主机名或IP] [server]
```


2. 常用选项

- -a：列出该主机详细的各项主机名称设定资料

3. 常用参数

- server： host 命令默认是使用 /etc/resolv.conf 文件中的 DNS 主机来查询的，若设置该参数，则使用这里设置的 DNS 主机进行查询。

4. 应用实例

1、解析域名对应的IP地址等信息

- host 域名

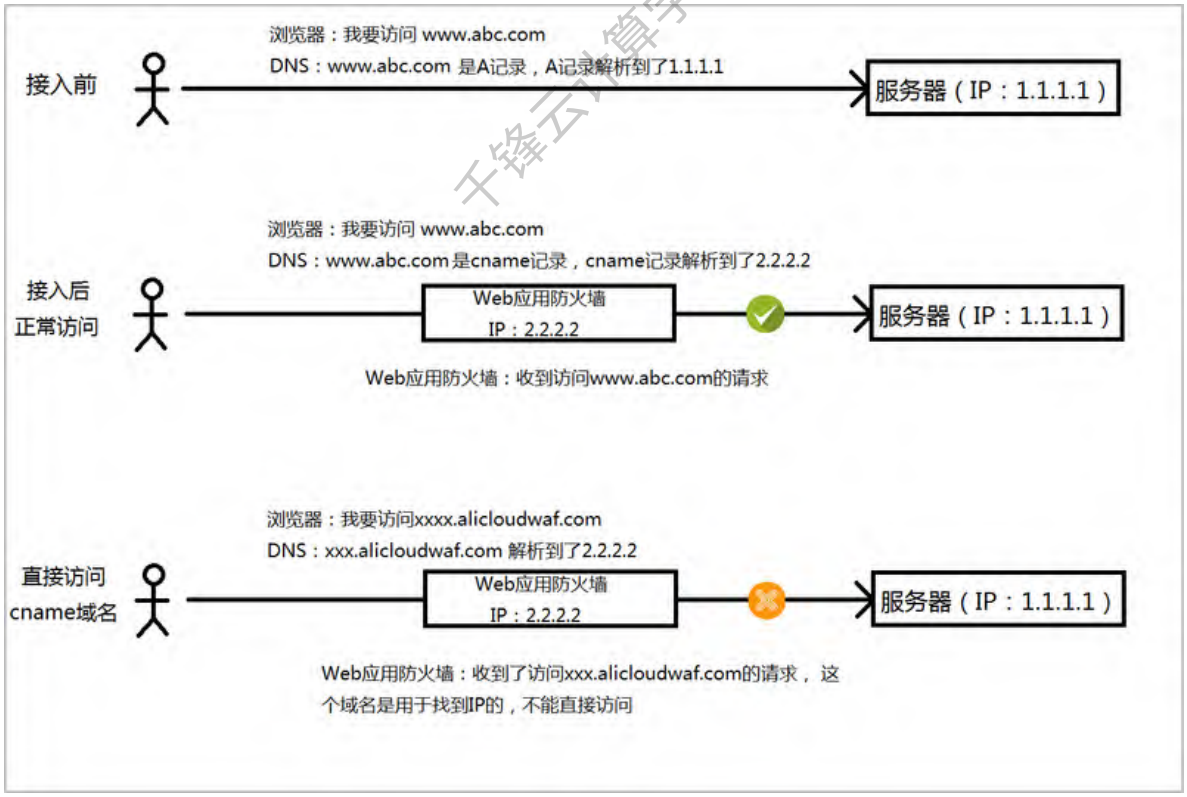
```
[root@qfedu.com ~]# host www.baidu.com
www.baidu.com is an alias for www.a.shifen.com.
www.a.shifen.com has address 61.135.169.125
www.a.shifen.com has address 61.135.169.121
```

- host -a 域名

```
[root@qfedu.com ~]# host -a www.baidu.com
Trying "www.baidu.com"
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 29562
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 5, ADDITIONAL: 5
```

```
;; QUESTION SECTION:
;www.baidu.com.                 IN      ANY

;; ANSWER SECTION:
www.baidu.com.          1000    IN      CNAME   www.a.shifen.com.

;; AUTHORITY SECTION:
baidu.com.              52656   IN      NS      ns7.baidu.com.
baidu.com.              52656   IN      NS      ns3.baidu.com.
baidu.com.              52656   IN      NS      ns2.baidu.com.
baidu.com.              52656   IN      NS      ns4.baidu.com.
baidu.com.              52656   IN      NS      dns.baidu.com.

;; ADDITIONAL SECTION:
dns.baidu.com.          52853   IN      A       202.108.22.220
ns2.baidu.com.          65473   IN      A       61.135.165.235
ns3.baidu.com.          52760   IN      A       220.181.37.10
ns4.baidu.com.          65473   IN      A       220.181.38.10
ns7.baidu.com.          53740   IN      A       180.76.76.92

Received 228 bytes from 10.0.2.3#53 in 9 ms
```

- www.baidu.com 通过 CNAME 映射到 www.a.shifen.com，但是无法直接访问 www.a.shifen.com 。
- Web应用防火墙或高防IP生产的CNAME域名，是用于DNS解析的，不能直接访问。



2、使用自定义的 DNS主机 解析域名对应的IP地址等信息

- host 域名 DNS主机名或IP

```
[root@qfedu.com ~]# host www.baidu.com 168.95.1.1
Using domain server:
Name: 168.95.1.1
```

```
Address: 168.95.1.1#53
Aliases:

www.baidu.com is an alias for www.a.shifen.com.
www.a.shifen.com has address 180.97.33.108
www.a.shifen.com has address 180.97.33.107

[root@qfedu.com ~]# host www.baidu.com dns.hinet.net
Using domain server:
Name: dns.hinet.net
Address: 168.95.1.1#53
Aliases:

www.baidu.com is an alias for www.a.shifen.com.
www.a.shifen.com has address 180.97.33.108
www.a.shifen.com has address 180.97.33.107

[root@qfedu.com ~]# host www.baidu.com 8.8.8.8
Using domain server:
Name: 8.8.8.8
Address: 8.8.8.8#53
Aliases:

www.baidu.com is an alias for www.a.shifen.com.
www.a.shifen.com has address 61.135.169.121
www.a.shifen.com has address 61.135.169.125
```


2、nslookup

- 域名解析工具，就是查DNS信息用的命令。使用 /etc/resolv.conf 这个文件作为 DNS 服务器的来源选择。

1、语法

```
nslookup [主机名或IP]
```

2、应用实例

1、解析域名对应的IP地址

- nslookup 域名

```
[root@qfedu.com ~]# nslookup www.baidu.com
Server:         10.0.2.3
Address:        10.0.2.3#53

Non-authoritative answer:
Name:   www.baidu.com
Address: 61.135.169.121
Name:   www.baidu.com
Address: 61.135.169.125
```

2、解析IP地址对应的主机名

- 并不是所有的IP地址都能解析成功
- nslookup IP

```
[root@qfedu.com ~]# nslookup 168.95.1.1
Server:         10.0.2.3
Address:        10.0.2.3#53

Non-authoritative answer:
1.1.95.168.in-addr.arpa name = dns.hinet.net.

Authoritative answers can be found from:
95.168.in-addr.arpa     nameserver = ans1.hinet.net.
95.168.in-addr.arpa     nameserver = ans2.hinet.net.
ans1.hinet.net  internet address = 168.95.192.15
ans1.hinet.net  has AAAA address 2001:b000:168::1:100:1
ans2.hinet.net  internet address = 168.95.1.15
ans2.hinet.net  has AAAA address 2001:b000:168::2:100:1
```

3、查看本机DNS服务器

- nslookup server

```
[root@qfedu.com ~]# nslookup server
Server:         10.0.2.3
Address:        10.0.2.3#53

** server can't find server: NXDOMAIN
```


3、dig

- 域名查询工具，可以用来测试域名系统工作是否正常。
- 功能与 nslookup 类似，建议使用 dig 来取代 nslookup

1、安装

- 若系统默认没有 dig 命令，则使用下面命令进行安装。

```
[root@qfedu.com ~]# yum install bind-utils
```

2、语法

```
dig [选项] [主机名]
```

3、常用选项

- @：dig 命令默认使用 /etc/resolv.conf 文件中的 DNS 主机来解析域名，若设置该参数，则使用这里设置的 DNS 主机进行解析。
- -b ：当主机具有多个IP地址，指定使用本机的哪个IP地址向域名服务器发送域名查询请求。

4、应用实例

1、解析域名对应的IP地址等信息

```
[root@qfedu.com ~]# dig www.baidu.com
; <<>> DiG 9.9.4-RedHat-9.9.4-61.el7 <<>> www.baidu.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 50280
```

```
;; flags: qr rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 5, ADDITIONAL: 6

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

;; ANSWER SECTION:
www.baidu.com.          1096    IN      CNAME   www.a.shifen.com.
www.a.shifen.com.       290     IN      A       61.135.169.121
www.a.shifen.com.       290     IN      A       61.135.169.125

;; AUTHORITY SECTION:
a.shifen.com.           34      IN      NS      ns3.a.shifen.com.
a.shifen.com.           34      IN      NS      ns4.a.shifen.com.
a.shifen.com.           34      IN      NS      ns1.a.shifen.com.
a.shifen.com.           34      IN      NS      ns5.a.shifen.com.
a.shifen.com.           34      IN      NS      ns2.a.shifen.com.

;; ADDITIONAL SECTION:
ns1.a.shifen.com.       411     IN      A       61.135.165.224
ns2.a.shifen.com.       435     IN      A       180.149.133.241
ns3.a.shifen.com.       431     IN      A       61.135.162.215
ns4.a.shifen.com.       431     IN      A       115.239.210.176
ns5.a.shifen.com.       435     IN      A       119.75.222.17

;; Query time: 11 msec
;; SERVER: 10.0.2.3#53(10.0.2.3)
;; WHEN: Wed May 16 08:40:42 UTC 2018
;; MSG SIZE  rcvd: 271
```


- HEADER(标题)：显示查询的内容有哪些，包括1个 QUERY, 3个 ANSWER 及5个AUTHORITY。
- QUESTION(问题)：显示所要查询的内容。
- ANSWER(回答)：依据刚刚的 QUESTION 去查询所得到的结果。
- AUTHORITY(验证)：从这里我们可以知道 www.baidu.com 是由 哪些DNS服务器提供的 ANSWER。

2、使用自定义的 DNS服务器解析域名对应的IP地址等信息

```
[root@qfedu.com ~]# dig @168.95.1.1 www.baidu.com
; <<>> DiG 9.9.4-RedHat-9.9.4-61.el7 <<>> @168.95.1.1 www.baidu.com
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 48040
;; flags: qr rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 3072
;; QUESTION SECTION:
;www.baidu.com.                 IN      A

;; ANSWER SECTION:
www.baidu.com.          1034    IN      CNAME   www.a.shifen.com.
www.a.shifen.com.       241     IN      A       180.97.33.107
www.a.shifen.com.       241     IN      A       180.97.33.108
```

```
;; Query time: 70 msec
;; SERVER: 168.95.1.1#53(168.95.1.1)
;; WHEN: Wed May 16 08:39:13 UTC 2018
;; MSG SIZE  rcvd: 101
```

九、DNS 客户端配置

- Centos7 手动设置 /etc/resolv.conf 里的 DNS,系统会重新覆盖或者清除了，使用以下下三种方法解决。

1、使用命令行工具 nmcli

1、查看网络连接

```
[root@qfedu.com ~]# nmcli connection show
NAME  UUID                                  TYPE      DEVICE
eth0  662a58e0-f4cb-40d0-a01f-d39a354baaba  ethernet  eth0
```

2、nmcli 配置 DNS

- 修改当前网络连接对应的DNS服务器，这里的网络连接可以用名称或者UUID来标识

```
[root@qfedu.com ~]# nmcli con mod eth0 ipv4.dns "114.114.114.114 8.8.8.8"
```

3、启动 DNS 配置

```
[root@qfedu.com ~]# nmcli con up eth0
Connection successfully activated (D-Bus active path:
/org/freedesktop/NetworkManager/ActiveConnection/4)
```


4、nmcli 命令的详细帮助

```
[root@qfedu.com ~]# man NetworkManager.conf
[root@qfedu.com ~]# man nmcli
```

2、使用传统方法

1、修改 NetworkManager 配置

- 修改 /etc/NetworkManager/NetworkManager.conf 文件，在main部分添加 “dns=none” 选项：

```
[root@qfedu.com ~]# vim /etc/NetworkManager/NetworkManager.conf
[main]
plugins=ifcfg-rh
dns=nonevim
```

2、重启 NetworkManager 服务

```
[root@qfedu.com ~]# systemctl restart NetworkManager.service
```

3、手工修改 /etc/resolv.conf

```
[root@qfedu.com ~]# vim  /etc/resolv.conf
nameserver 114.114.114.114
nameserver 8.8.8.8
```

3、网卡配置文件指定 DNS

1、修改网卡配置文件

```
[root@qfedu.com ~]# cd  /etc/sysconfig/network-scripts/      # 进入网络配置文件目录
[root@qfedu.com ~]# vim  ifcfg-eth0                          # 编辑配置文件，添加修改以下内容
TYPE="Ethernet"
BOOTPROTO="static"                          # 启用静态IP地址
DEFROUTE="yes"
IPV4_FAILURE_FATAL="no"
IPV6INIT="yes"
IPV6_AUTOCONF="yes"
IPV6_DEFROUTE="yes"
IPV6_FAILURE_FATAL="no"
NAME="eth0"
UUID="8071cc7b-d407-4dea-a41e-16f7d2e75ee9"
ONBOOT="yes"                                # 开启自动启用网络连接
IPADDR0="192.168.21.128"                    # 设置IP地址
PREFIX0="24"                                # 设置子网掩码
GATEWAY0="192.168.21.2"                     # 设置网关
DNS1="8.8.8.8"                              # 设置主DNS
DNS2="8.8.4.4"                              # 设置备DNS
HWADDR="00:0C:29:EB:F2:B3"
IPV6_PEERDNS="yes"
IPV6_PEERROUTES="yes"
```


2、重启网络

```
[root@qfedu.com ~]# service network restart
```

3、测试网络是否正常

```
[root@qfedu.com ~]# ping www.baidu.com
```

4、查看IP地址

```
[root@qfedu.com ~]# ip addr
```

十、DNS 实战

- 公网域名申请（阿里云万网/新网）操作
- 域名服务商后台配置公网域名解析操作
- 使用dns客户端测试工具测试公网域名解析结果