钓鱼网站原理分析

一、 DNS知识

1. DNS 概述

1.1 什么是 DNS?

- **定义**：DNS 是将人类可读的域名（如 `google.com`）转换为机器可识别的 IP 地址（如 `172.217.14.110`）的系统。
- 作用：
  - 解析域名 → IP 地址
  - 支持分层域名结构（如 `.com` → `google.com` → `www.google.com`）
  - 管理网络资源的全局目录

1.2 DNS 的重要性

- **互联网核心服务**：没有 DNS，用户需手动输入 IP 地址访问网站。
- **分布式架构**：全球数十亿台服务器协同工作，确保高效解析。

---

2. DNS 的核心概念

2.1 域名结构-树状结构

- 根域（`.`）
- 顶级域（TLD）：`.com`、`.org`、`.cn`
- 二级域：`google.com`
- 子域：`mail.google.com`

2.2 DNS 服务器

互联网上的DNS域名服务器也是按照层次划分的，每一个域名服务器都只对域名体系中的一部分进行管辖。根据域名服务器所起的作用，可以把域名服务器划分为四种不同的类型：

根域名服务器： 根域名服务器是最高层次的域名服务器，也是最重要的域名服务器。根域名服务器知道所有顶级域名服务器的域名和IP地址。如果本地域名服务器无法对域名进行解析，就首先求助于根域名服务器。

顶级域名服务器： 顶级域名服务器负责管理在该服务器注册的所有二级域名。当收到 DNS查询请求时，就给出相应的回答（可能是最后的结果，也可能是下一步需要查询的域名服务器的 IP 地址）。

权威域名服务器：这就是前面已经讲过的负责一个区的域名服务器。当一个权限域名服务器还不能给出最后的查询回答时，就会告知发出查询请求的DNS客户，下一步应当找哪一个权威域名服务器。

本地域名服务器：本地域名服务器并不属于下图中的树状结构的DNS域名服务器，但是它对域名系统非常重要。当一个主机发出DNS查询请求时，这个查询请求报文就发送给本地域名服务器。每一个互联网服务提供者ISP都可以拥有一个本地域名服务器。

各个域的分层上都设有各自的域名服务器，各层域名服务器都了解该层以下分层中所有域名服务器的IP地址。因此它们从根域名服务器开始呈树状结构相互连接。由于所有域名服务器都了解根域名服务器的IP地址,所以若从根开始按照顺序追踪,可以访问世界上所有域名服务器的地址。

2.3 DNS 解析流程

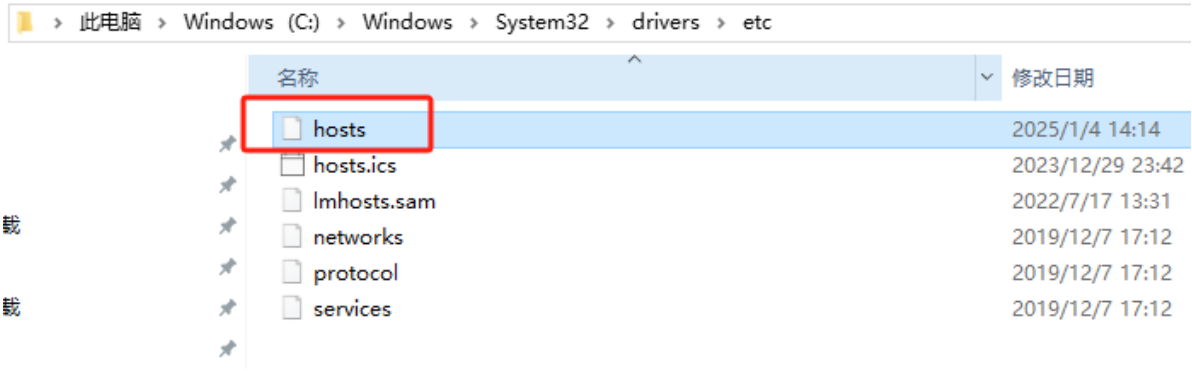
（1）查看浏览器缓存

当用户通过浏览器访问某域名时，浏览器首先会在自己的缓存中查找是否有该域名对应的 IP 地址（若曾经访问过该域名且没有清空缓存便存在）。

```
ipconfig /dispalydns
```

（2）查看系统缓存

当浏览器缓存中无域名对应 IP 则会自动检查用户计算机系统 Hosts 文件 DNS 缓存是否有该域名对应 IP。



（3）查看路由器缓存

当浏览器及系统缓存中均无域名对应 IP 则进入路由器缓存中检查，以上三步均为客服端的 DNS 缓存。

> 看不到，在头顶的路由器中

（4）查看ISP DNS 缓存

当在用户客服端查找不到域名对应 IP 地址，则将进入 ISP DNS 缓存中进行查询。比如你用的是电信的网络，则会进入电信的 DNS 缓存服务器中进行查找。

（5）询问根域名服务器

当以上均未完成，则进入根服务器进行查询。全球仅有 13 台根域名服务器，1 个主根域名服务器，其余 12
为辅根域名服务器。根域名收到请求后会查看区域文件记录，若无则将其管辖范围内顶级域名（如.com、.cn等）服务器 IP 告诉本地 DNS 服务器。

（6）询问顶级域名服务器

顶级域名服务器收到请求后查看区域文件记录，若无记录则将其管辖范围内权威域名服务器的 IP 地址告诉本地 DNS 服务器。

（7）询问权威域名（主域名）服务器

权威域名服务器接受到请求后查询自己的缓存，如果没有则进入下一级域名服务器进行查找，并重复该步骤直至找到正确记录。

（8）保存结果至缓存

本地域名服务器把返回的结果保存到缓存，以备下一次使用，同时将该结果反馈给客户端，客户端通过这个 IP地址即可访问目标Web服务器。至此，DNS递归查询的整个过程结束。

---

3. DNS 记录类型

通过设置不同的解析记录，可以实现对主机名不同的解析效果，从而满足不同场景下的域名解析需求。常见的域名解析记录，主要有以下几种类型。

A记录　zhuyu.com　A　49.232.21.222

A（Address）记录是用来指定主机名（或域名）对应的IP地址记录。用户可以将该域名下的网站服务器指向到自己的web server上，同时也可以设置域名的子域名。简单来讲，A记录就是指定域名对应的IP地址。如我们添加一条A记录将www的主机指向IP192.168.1.1，那么当你访问www主机时就会解析到192.168.1.1这个IP上。

CNAME记录

通常称别名解析，是主机名到主机名的映射。当需要将域名指向另一个域名，再由另一个域名提供 IP 地址，就需要添加 CNAME 记录，最常用到CNAME的场景包括做CDN、企业邮箱、全局流量管理等。与A记录不同的是，CNAME别名记录设置的值不是一个固定的IP，而是主机的别名地址。

别名解析可以提供更大的灵活性，便于统一管理。比如，当主机因某种因素的影响需要更换IP时，如果域名做了CNAME记录，就可以同时更新别名的解析指向，不需要进行新的解析操作。

NS记录

如果需要把子域名交给其他DNS服务商解析，就需要添加NS记录（NameServer）。NS记录是域名服务器记录，用来指定该域名由哪个DNS服务器来进行解析。NS记录中的IP即为该DNS服务器的IP地址。大多数域名注册商默认用自己的NS服务器来解析用户的DNS记录。DNS服务器NS记录地址一般以以下的形式出现：ns1.domain.com、ns2.domain.com等。

SOA记录

SOA，是起始授权机构记录，说明了在众多 NS 记录里哪一台才是主要的服务器。在任何DNS记录文件中，都是以SOA (Startof Authority)记录开始。SOA资源记录表明此DNS名称服务器是该DNS域中数据信息的最佳来源。

SOA记录与NS记录的区别：NS记录表示域名服务器记录，用来指定该域名由哪个DNS服务器来进行解析；SOA记录设置一些数据版本和更新以及过期时间等信息。

AAAA记录

AAAA记录(AAAArecord)是用来将域名解析到IPv6地址的DNS记录。用户可以将一个域名解析到IPv6地址上，也可以将子域名解析到IPv6地址上。国内大多数IDC不支持AAAA记录的解析，因此如果想进行AAAA记录解析，则需对域名NS记录设置一些专业的域名解析服务商，由他们提供AAAA记录的设置。中科三方云解析支持IPv6环境下的AAAA记录解析。

TXT记录

TXT记录，一般指某个主机名或域名的标识和说明。如：admin IN TXT “管理员, 电话：XXXXXXXXXX”，mail IN TXT“邮件主机，存放在xxx , 管理人：AAA”，Jim IN TXT “contact:abc@mailserver.com”，也就是说，通过设置TXT记录内容可以使别人更方便地联系到你。TXT 记录常用的方式还有做 SPF记录（反垃圾邮件）和SSL证书的DNS验证等。

MX记录

MX（MailExchanger）记录是邮件交换记录，主要用于邮箱解析，在邮件系统发送邮件时根据收信人的地址后缀进行邮件服务器的定位。MX记录允许设置一个优先级，当多个邮件服务器可用时，会根据该值决定投递邮件的服务器。

MX记录的权重对 Mail 服务非常重要，当发送邮件时，Mail 服务器先对域名进行解析，查找 MX记录。先找权重数最小的服务器（比如说是10），如果能连通，那么就将服务器发送过去；如果无法连通 MX 记录为 10 的服务器，才将邮件发送到权重更高的 mail 服务器上。

PTR记录

PTR是pointer 的简写，即“反向DNS”，domain namepointer，可以粗略的理解为DNS反向，是一个指针记录，用于将一个IP地址映射到对应的主机名，也可以看成是A记录的反向，即通过IP访问域名。

SRV记录

即服务定位（SRV）资源记录，用于定义提供特定服务的服务器的位置，如主机（hostname），端口（port number）等。

URL转发

URL转发，是指通过服务器的特殊设置，将当前访问的域名指向另一个指定的网络地址。根据目标地址的隐藏与否，URL转发可以分为显性URL和隐性URL两种。

显性URL：将域名指向一个http（s)协议地址，访问域名时，自动跳转至目标地址，地址栏显示为目标网站地址。

隐性URL：与显性URL类似，但隐性转发会隐藏真实的目标地址，地址栏中显示为仍为此前输入的地址。

二、实验环境搭建

1. 物理拓扑配置

- windows 设置自动获取IP地址，连接VMNET2网卡
- centos8按照如下配置

2.操作

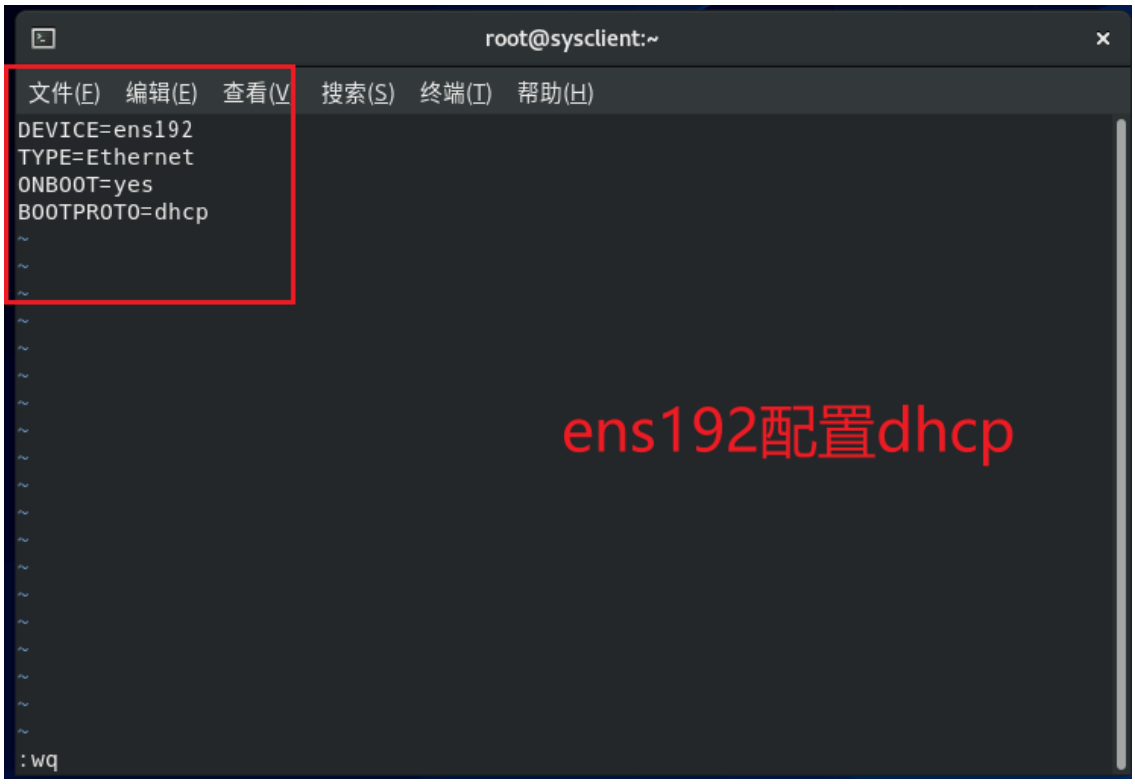
1.修改centos8 主机名为 `fishserver`

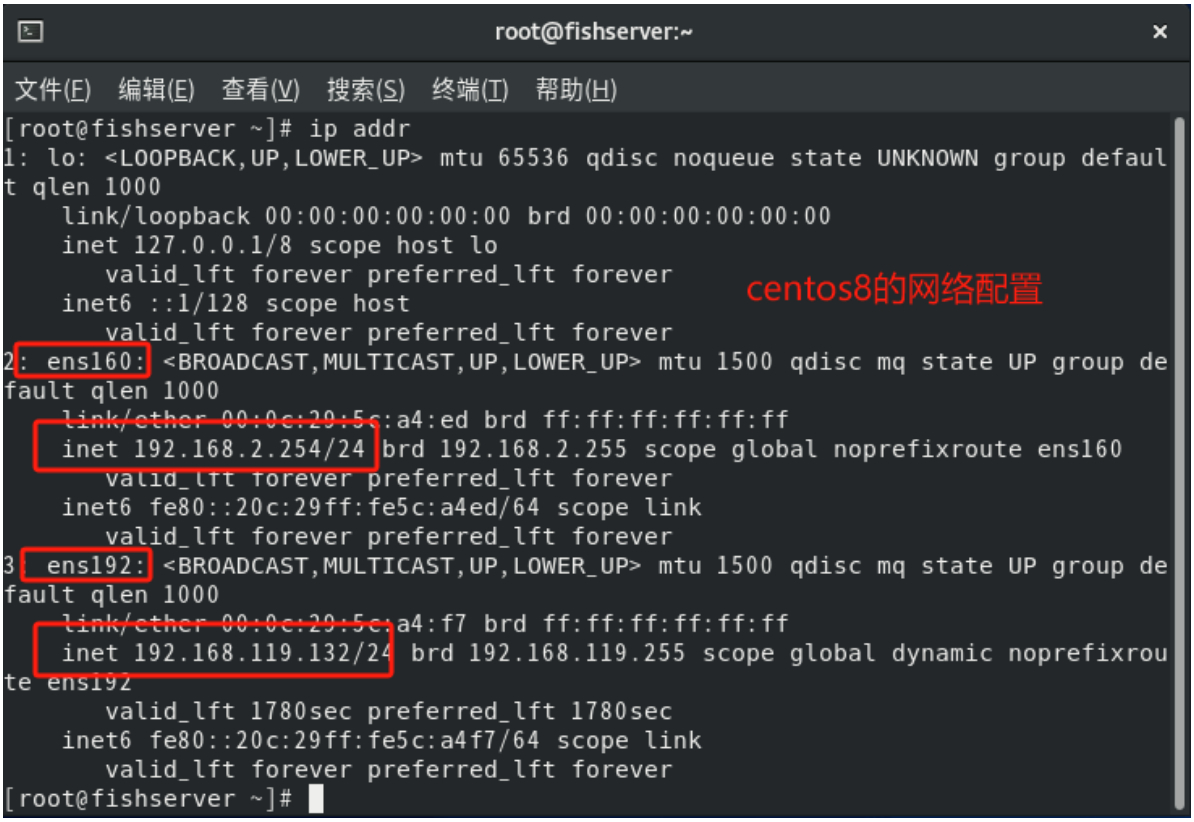
```
hostnamectl set-hostname fishsever
```

2.配置网络 ens160 vmnet2 静态地址 ens192 nat dhcp

- 将 `ens192` 设置成nat模式
- 修改 `ens192` 配置文件，重启查看配置是否生效

```
[root@fishserver ~]# vim /etc/sysconfig/network-scripts/ifcfg-ens192
```





- 测试连通性

```
[root@fishserver ~]# ping www.baidu.com
PING www.a.shifen.com (39.156.70.239) 56(84) bytes of data.
64 bytes from 39.156.70.239 (39.156.70.239): icmp_seq=1 ttl=128 time=11.2 ms
64 bytes from 39.156.70.239 (39.156.70.239): icmp_seq=2 ttl=128 time=10.10
ms
64 bytes from 39.156.70.239 (39.156.70.239): icmp_seq=3 ttl=128 time=12.4 ms
64 bytes from 39.156.70.239 (39.156.70.239): icmp_seq=4 ttl=128 time=10.9 ms
```

- 查看此时DNS配置，`/etc/resolv.conf`

3.DHCP服务器配置

- **安装DHCP服务**

```
[root@fishserver ~]# yum install dhcp-server -y
```

```
已升级：
  bind-export-libs-32:9.11.26-6.el8.x86_64  dhcp-client-12:4.3.6-45.el8.x8

已安装：
  dhcp-server-12:4.3.6-45.el8.x86_64
```

- **配置文件修改** `/etc/dhcp/dhcpd.conf`

  包含工作网段、地址池、分配的网关及DNS，还有租期

```
#
# DHCP Server Configuration file.
#   see /usr/share/doc/dhcp-server/dhcpd.conf.example
#   see dhcpd.conf(5) man page
#
~                                    引入模板文件
~
```

```
末行模式:r /usr/share/doc/dhcp-server/dhcpd.conf.example
```

```
# A slightly different configuration for an internal subnet.
subnet 10.5.5.0 netmask 255.255.255.224 {
  range 10.5.5.26 10.5.5.30;
  option domain-name-servers ns1.internal.example.org;
  option domain-name "internal.example.org";
  option routers 10.5.5.1;
  option broadcast-address 10.5.5.31;
  default-lease-time 600;                只要模板文件的这部分
  max-lease-time 7200;
```

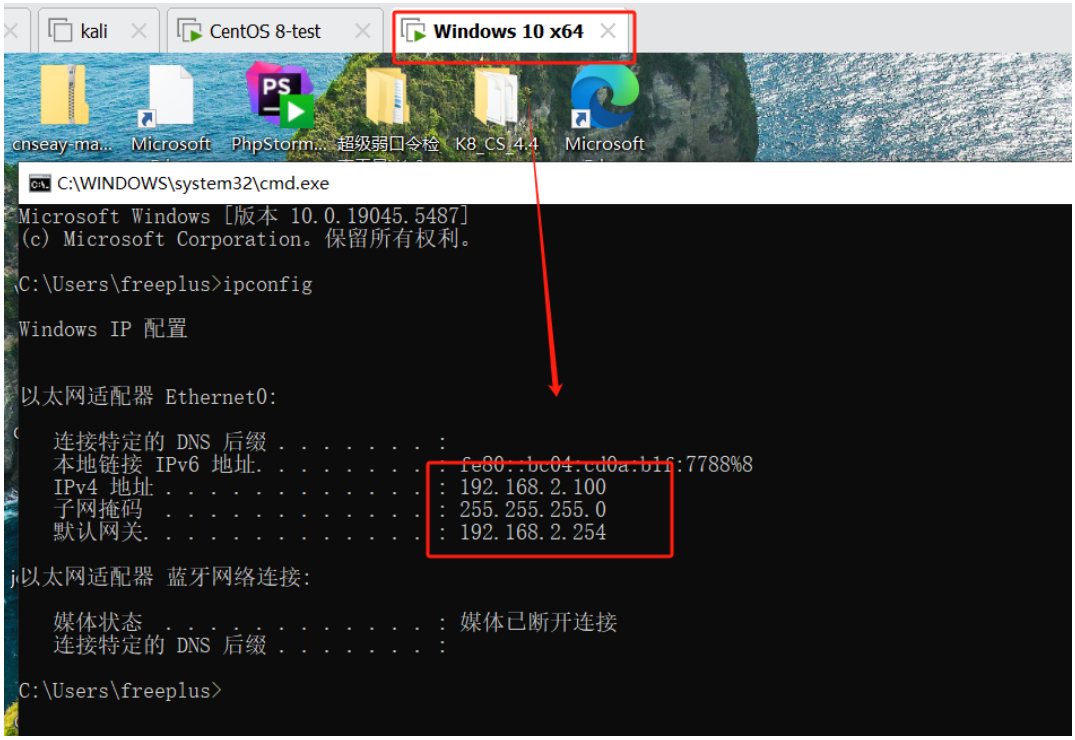
- 修改内容

```
1 # A slightly different configuration for an internal subnet.
2 subnet 192.168.2.0 netmask 255.255.255.0 {
3   range 192.168.2.100 192.168.2.200;
4   option domain-name-servers 192.168.2.254;
5   option routers 192.168.2.254;
6   default-lease-time 600;
7   max-lease-time 7200;
8 }
```

- 重启服务：

```
[root@fishserver yum.repos.d]# systemctl restart dhcpd
```

- **验证DHCP分配**
  - 在Windows Client执行`ipconfig`，确认获取到`192.168.2.100`及网关`192.168.2.254`



4.DNS服务器配置

- **安装BIND服务**（b：博客里大学 ind网络域名服务 ）

```
[root@fishserver yum.repos.d]# yum install -y bind
```

```
已升级：
  bind-libs-32:9.11.26-6.el8.x86_64          bind-libs-lite-32:9.11.26-6.el8.x86_64          bind-license-32:9.11.26-6.el8.noarch
  bind-utils-32:9.11.26-6.el8.x86_64         python3-bind-32:9.11.26-6.el8.noarch

已安装：
  bind-32:9.11.26-6.el8.x86_64                                       fstrm-0.6.1-2.el8.x86_64

完毕！
```

- **修改配置主文件** `/etc/named.conf`

```
[root@fishserver ~]# vim /etc/named.conf
```

```
options {
        listen-on port 53 { 192.168.2.254; }
        listen-on-v6 port 53 { ::1; };
        directory       "/var/named";
        dump-file       "/var/named/data/cache_dump.db";
        statistics-file "/var/named/data/named_stats.txt";
        memstatistics-file "/var/named/data/named_mem_stats.txt";
        secroots-file   "/var/named/data/named.secroots";
        recursing-file  "/var/named/data/named.recursing";
#       allow-query     { localhost; };

        /*
```

- 重启服务

```
[root@fishserver ~]# systemctl restart named
```

- 测试win10能否解析外网

```
C:\Users\freeplus>nslookup www.qq.com
服务器:  UnKnown
Address:  192.168.2.254

非权威应答:
名称:    ins-r23tsuuf.ias.tencent-cloud.net
Addresses:  2409:8702:4860:106::3e
          2409:8702:4860:1002::33
          111.30.185.195
          111.30.178.240
          111.30.185.60
Aliases:  www.qq.com
```

- 修改主配置文件`/etc/named.conf`，让named服务将www.jd.com解析到192.168.2.254

```
zone "jd.com" IN{
        type master;
        file "jd.com.zone";
};
```

声明对jd域名的权威解析

解析关系配置文件名

- 建立正向解析配置文件

```
[root@fishserver data]# touch /var/named/jd.com.zone
[root@fishserver data]# vim /var/named/jd.com.zone
```

```
$TTL 3H
@       IN SOA  jd.com. root.jd.com. (
                                        0       ; serial
                                        1D      ; refresh
                                        1H      ; retry
                                        1W      ; expire
                                        3H )    ; minimum
        NS      ns.jd.com.
ns      A       192.168.2.254
www     A       192.168.2.254
```

- 重启服务

```
[root@fishserver named]# systemctl restart named
```

- 测试www.jd.com的解析地址

```
C:\Users\freeplus>nslookup www.jd.com
服务器:  UnKnown
Address:  192.168.2.254

名称:    www.jd.com
Address:  192.168.2.254


C:\Users\freeplus>
```

5.路由与NAT配置

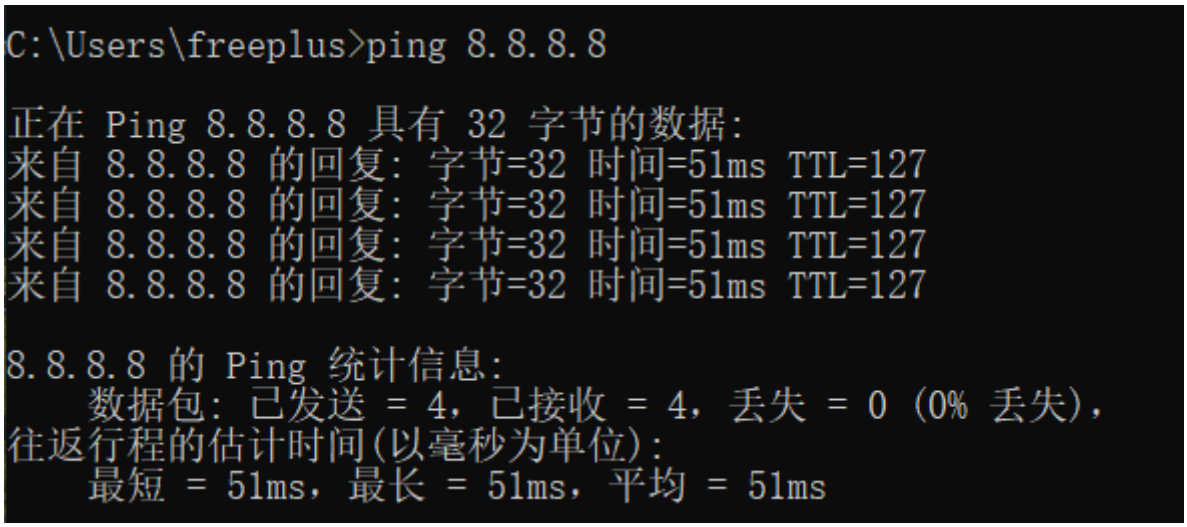
- **启用路由转发**

```
sudo sysctl -w net.ipv4.ip_forward=1
```

- 配置NAT规则

```
sudo iptables -t nat -I POSTROUTING -s 192.168.2.0/24 -p all -o ens192 -j SNAT --to-source 192.168.119.132
```

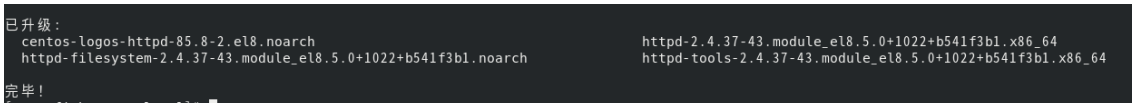
- 验证外网连通性



6.安装apache

- 通过yum进行安装

```
[root@fishserver local]# yun install httpd
```



- 启动httpd服务

```
[root@fishserver local]# systemctl start httpd
```

- 修改默认页面 `/var/www/html`

```
[root@fishserver local]# vim /var/www/html/index.html
```

```
<html>
<head>
</head>
<body>
        <h2>恭喜你中将了</h2>
</body>
</html>
`
```

- 使用win10访问京东