# 山东大学 计算机 学院

## 计算机网络 课程实验报告

| 学号：202000130143 | 姓名： 郑凯饶 | 班级： 2020 级 1 班 |
|---|---|---|
| 实验题目：DNS | | |
| 实验学时：2 | 实验日期： 2022-3-22 | |

实验目的：

学习域名解析系统（DNS），包括本地 DNS 服务器，DNS 缓存，DNS 记录和信息，报文各个字段。

硬件环境：

Dell Latitude 5411

Intel(R) Core(TM) i5-10400H CPU @ 2.60GHz(8GPUs),~2.6GHz

软件环境：

Windows 10 家庭中文版 64 位（10.0，版本 18363）

Wireshark-win64-3.6.2

实验步骤与内容：

1. 问题：

（1） 运行 nslookup 获取一台亚洲服务器的 IP 地址。

（2） 查询一所欧洲大学的 authoritative DNS 服务器。

（3） 使用问题（2）中的 DNS 服务器向 Yahoo!mail 发起询问，它的 IP 地址？

（4） 定位 DNS 询问及回复信息，是通过 UDP 还是 TCP 发送？

（5） DNS 询问信息的目标端口是多少？DNS 回复的源端口？

（6） DNS 询问信息向哪个 IP 发送？使用 ipconfig 查询本地的 DNS 服务器，判断两者是否一致。

（7） 测试 DNS 询问信息。它属于什么类型的 DNS 询问？是否包含了回答？

（8） 测试 DNS 回复信息。有多少回答提供？它们各自包含什么？

（9） 思考随后本机发出的 TCP SYN 包。它的目的地是否是 DNS 回复信息中的 IP？

（10）在取回图像之前，主机是否发出新的 DNS 询问？

（11）询问的目标端口？回复的源端口？

（12）目的地 IP？是否是本地 DNS 服务器？

（13）DNS 询问类型。是否包含回答?

（14）多少回复被提供？分别包含什么内容？

（15）截屏。

（16）目的地 IP？是否是本地 DNS 服务器？

（17）DNS 询问类型。是否包含回答?

（18）DNS 回复提供了哪些 MIT nameservers,是否包含他们的 IP？

（19）截图。

（20）目的地 IP？是否是本地 DNS 服务器？若不是它对应的 IP？

（21）DNS 询问类型。是否包含回答?

（22）多少回复被提供？分别包含什么内容？

（23）截图。

2. 阐述基本方法

使用 nslookup 进行指定 DNS 服务器进行域名解析，使用 ipconfig 清除 DNS 缓存，使用 Wireshark 分析 DNS 报文的各个字段。参考资源如下：

nslookup 命令：https://blog.csdn.net/xg_ren/article/details/80782338
ipconfig 命令：https://blog.csdn.net/bcbobo21cn/article/details/51759140
DNS 记录：https://blog.csdn.net/u013920085/article/details/42552987

3. 实验结果展示与分析

（1）查询阿里巴巴的 IP：

```
C:\Users\DELL>nslookup re.1688.com
服务器:  dns.google
Address:  8.8.8.8

非权威应答:
名称:    1688-na61-na62.wagbridge.alibaba.1688.com.gds.alibabadns.com
Addresses:  2401:b180:2000:20::3c
          2401:b180:2000:20::21
          2401:b180:2000:20::20
          2401:b180:2000:20::1f
          2401:b180:2000::16
          2401:b180:2000::15
          2401:b180:2000::14
          2401:b180:2000::13
          203.119.213.3
Aliases:  re.1688.com
          1688-na61-na62.wagbridge.alibaba.1688.com
```

（2）查询牛津大学的 DNS 服务器：

```
C:\Users\DELL>nslookup www.ox.ac.uk
服务器:  dns.google
Address:  8.8.8.8

非权威应答:
名称:    www.ox.ac.uk
Addresses:  151.101.66.216
          151.101.130.216
          151.101.194.216
          151.101.2.216


C:\Users\DELL>
```

（3）使用牛津的 DNS 服务器响应超时，谷歌的 OK.

```
C:\Users\DELL>nslookup mail.yahoo.com 151.101.66.216
DNS request timed out.
    timeout was 2 seconds.
服务器:  UnKnown
Address:  151.101.66.216

DNS request timed out.
    timeout was 2 seconds.
DNS request timed out.
    timeout was 2 seconds.
DNS request timed out.
    timeout was 2 seconds.
DNS request timed out.
    timeout was 2 seconds.
*** 请求 UnKnown 超时

C:\Users\DELL>nslookup mail.yahoo.com 8.8.8.8
服务器:  dns.google
Address:  8.8.8.8

非权威应答:
名称:    edge.gycpi.b.yahoodns.net
Addresses:  2406:2000:9c:800::12
          2406:2000:a0:807::1
          2406:2000:a0:807::2
          2406:2000:9c:800::11
          119.161.15.251
```

（4）通过 UDP 发送。

```
    23 2022-03-22 17:43:09.051958 8.8.8.8          172.25.188.178      DNS
User Datagram Protocol, Src Port: 53, Dst Port: 62509
    Source Port: 53
    Destination Port: 62509
    Length: 115
    Checksum: 0xee9d [unverified]
    [Checksum Status: Unverified]
    [Stream index: 1]
  > [Timestamps]
    UDP payload (107 bytes)
Domain Name System (response)
```

（5）询问时的目标端口为 53，回复的源端口也是 53.

（6）8.8.8.8，谷歌的 DNS 服务器（手动设置），和本地的一致

（7）A 类型。包含指向 DNS 回复的链接。

```
Domain Name System (query)
    Transaction ID: 0xd8da
  > Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  v Queries
    > www.ietf.org: type A, class IN
    [Response In: 27]
```

（8）

| Source | Destination | Protocol | Length | Info |
|---|---|---|---|---|
| 172.25.188.178 | 8.8.8.8 | DNS | 72 | Standard query 0xd8da A www.ietf.org |
| 172.25.188.178 | 8.8.8.8 | DNS | 72 | Standard query 0x2967 AAAA www.ietf.org |
| 8.8.8.8 | 172.25.188.178 | DNS | 173 | Standard query response 0x2967 AAAA www.ietf.org CNAME www. |
| 8.8.8.8 | 172.25.188.178 | DNS | 149 | Standard query response 0xd8da A www.ietf.org CNAME www.iet |
| 172.25.188.178 | 8.8.8.8 | DNS | 89 | Standard query 0xe78a AAAA nav.smartscreen.microsoft.com |
| 172.25.188.178 | 8.8.8.8 | DNS | 89 | Standard query 0xaf7d A nav.smartscreen.microsoft.com |
| 8.8.8.8 | 172.25.188.178 | DNS | 264 | Standard query response 0xe78a AAAA nav.smartscreen.microso |
| 8.8.8.8 | 172.25.188.178 | DNS | 220 | Standard query response 0xaf7d A nav.smartscreen.microsoft. |
| 172.25.188.178 | 8.8.8.8 | DNS | 78 | Standard query 0x5a28 A analytics.ietf.org |
| 172.25.188.178 | 8.8.8.8 | DNS | 78 | Standard query 0x01ba AAAA analytics.ietf.org |
| 8.8.8.8 | 172.25.188.178 | DNS | 106 | Standard query response 0x01ba AAAA analytics.ietf.org AAAA |
| 8.8.8.8 | 172.25.188.178 | DNS | 94 | Standard query response 0x5a28 A analytics.ietf.org A 4.31. |

```
  v Queries
    v www.ietf.org: type AAAA, class IN
        Name: www.ietf.org
        [Name Length: 12]
        [Label Count: 3]
        Type: AAAA (IPv6 Address) (28)
        Class: IN (0x0001)
  v Answers
    > www.ietf.org: type CNAME, class IN, cname www.ietf.org.cdn.cloudflare.net
    > www.ietf.org.cdn.cloudflare.net: type AAAA, class IN, addr 2606:4700::6810:2d63
    > www.ietf.org.cdn.cloudflare.net: type AAAA, class IN, addr 2606:4700::6810:2c63
    [Request In: 23]
    [Time: 0.072627000 seconds]
```

（9）TCP SYN 包的目的地就是前 DNS 回复中解析的 IP 结果。

| | | | | |
|---|---|---|---|---|
| 2001:250:5800:1002:… | 2606:4700::6810:2d63 | TCP | 86 | 52917 → 443 [SYN] Seq=0 Win=64800 Len=0 MSS=1440 WS= |
| 2001:250:5800:1002:… | 2606:4700::6810:2d63 | TCP | 86 | 52918 → 443 [SYN] Seq=0 Win=64800 Len=0 MSS=1440 WS= |

（10）还发出了新的 DNS 询问，图片域名不同要重新解析。实际并没有，使用 F12 开发者工具查看图片源，发现来自统一域名。（8）中 nav.smartscreen.microsoft.com 应该是与 Edge 筛选器相关的请求，analytics.ietf.org 请求的 JS 脚本，与登录相关。

（11）前两条为 nslookup 专用的 DNS 信息。仍然都是 53

（12）仍然是 8.8.8.8，相同

（13）有 A 类型以及 AAAA 类型两种 DNS 询问，包含指向回复的链接（应该是 Wireshark 软件提供）

（14）针对每个询问各有一个回复。第一个回复包含两条 CNAME 类型的 DNS 询问，分别解析向 www.mit.edu 和前者返回的 www.mit.edgekey.net，以及向 e9566.dscb.akamaiedge.net 发送的询问，最后得到域名对应的主机 IP 为 23.15.106.234.以上是使用 IPV4 进行的，另外 AAAA 类型应该是基于 IPV6 协议的解析过程，只有最后返回的 IP 不同为 2600:140b:4800:583:255e.

（15）

| Destination | Protocol | Length | Info |
|---|---|---|---|
| 8.8.8.8 | DNS | 80 | Standard query 0x0001 PTR 8.8.8.8.in-addr.arpa |
| 172.25.188.178 | DNS | 104 | Standard query response 0x0001 PTR 8.8.8.8.in-addr.arpa PTR d… |
| 8.8.8.8 | DNS | 71 | Standard query 0x0002 A www.mit.edu |
| 172.25.188.178 | DNS | 160 | Standard query response 0x0002 A www.mit.edu CNAME www.mit.ed… |
| 8.8.8.8 | DNS | 71 | Standard query 0x0003 AAAA www.mit.edu |
| 172.25.188.178 | DNS | 200 | Standard query response 0x0003 AAAA www.mit.edu CNAME www.mit… |

（16）8.8.8.8，是

（17）NS（authoritative Name Server），似乎没有

（18）nameservers 如（19）所示，没有提供它们的 IP

（19）

```
C:\Users\DELL>nslookup -type=NS mit.edu
服务器:  dns.google
Address:  8.8.8.8

非权威应答:
mit.edu nameserver = asia1.akam.net
mit.edu nameserver = asia2.akam.net
mit.edu nameserver = use2.akam.net
mit.edu nameserver = eur5.akam.net
mit.edu nameserver = usw2.akam.net
mit.edu nameserver = use5.akam.net
mit.edu nameserver = ns1-173.akam.net
mit.edu nameserver = ns1-37.akam.net
```

（20）bitsy.mit.edu 服务器似乎访问不了，使用百度公共 DNS 替代。DNS 询问发往 180.76.76.76，不是指定的 DNS 服务器，命令的第三个字段是指定 DNS 服务器。

（21）A 类型，从 DNS 报文头部 Answer RRs 字段等于 0 我们知道该报文不包含回复。

```
Domain Name System (query)
  Transaction ID: 0x0002
> Flags: 0x0100 Standard query
  Questions: 1
  Answer RRs: 0
  Authority RRs: 0
  Additional RRs: 0
> Queries
  [Response In: 1991]
```

（22）提供了 1 个 Authority RRs，SOA（Start Of a zone of Authority）类型，包含序列号，主服务器，负责人邮箱，刷新间隔等信息。

```
v aiit.or.kr: type SOA, class IN, mname ns9.dnszi.com
    Name: aiit.or.kr
    Type: SOA (Start Of a zone of Authority) (6)
    Class: IN (0x0001)
    Time to live: 3583 (59 minutes, 43 seconds)
    Data length: 42
    Primary name server: ns9.dnszi.com
    Responsible authority's mailbox: root.dnszi.com
    Serial Number: 2020032223
    Refresh Interval: 43200 (12 hours)
    Retry Interval: 3600 (1 hour)
    Expire limit: 1209600 (14 days)
    Minimum TTL: 3600 (1 hour)
```

（23）

```
C:\Users\DELL>nslookup www.aiit.or.kr 180.76.76.76
服务器:  public-dns-a.baidu.com
Address:  180.76.76.76

非权威应答:
名称:    www.aiit.or.kr
Address:  58.229.6.225
```

| Source | Destination | Protocol | Length | Info |
|---|---|---|---|---|
| 172.25.216.231 | 180.76.76.76 | DNS | 85 | Standard query 0x0001 PTR 76.76.76.180.in-addr.arpa |
| 180.76.76.76 | 172.25.216.231 | DNS | 321 | Standard query response 0x0001 PTR 76.76.76.180.in-addr.arp |
| 172.25.216.231 | 180.76.76.76 | DNS | 74 | Standard query 0x0002 A www.aiit.or.kr |
| 180.76.76.76 | 172.25.216.231 | DNS | 193 | Standard query response 0x0002 A www.aiit.or.kr A 58.229.6. |
| 172.25.216.231 | 180.76.76.76 | DNS | 74 | Standard query 0x0003 AAAA www.aiit.or.kr |
| 180.76.76.76 | 172.25.216.231 | DNS | 128 | Standard query response 0x0003 AAAA www.aiit.or.kr SOA ns9. |

结论分析与体会：

这次实验从 DNS 客户端的角度初步窥探了一下 DNS，了解 DNS 大致的运作流程，熟悉了 DNS 报文。之前我的电脑自动获取本地的 DNS server 进行域名解析时有问题，实验中我将它手动设置为谷歌 DNS 服务器 8.8.8.8。DNS 是一个复杂的分布式系统，希望以后能更进一步学习，尝试优化域名解析。