

暨南大学本科实验报告专用纸

课程名称 计算机网络实验 成绩评定
实验项目名称 域名服务 (DNS) 指导老师 某某某
实验项目编号 7 实验项目类型 综合类 实验地点 N117
学生姓名 某某 学号 XXXXXXXX
学院 网络空间安全学院 系 专业 网络空间安全
实验时间 2020 年 11 月 25 日 晚 上 ~ 2020 年 11 月 25 日 晚 上

(一) 实验目的

1. 掌握 DNS 的报文格式
2. 掌握 DNS 的工作原理
3. 掌握 DNS 域名空间的分类
4. 理解 DNS 高速缓存的作用

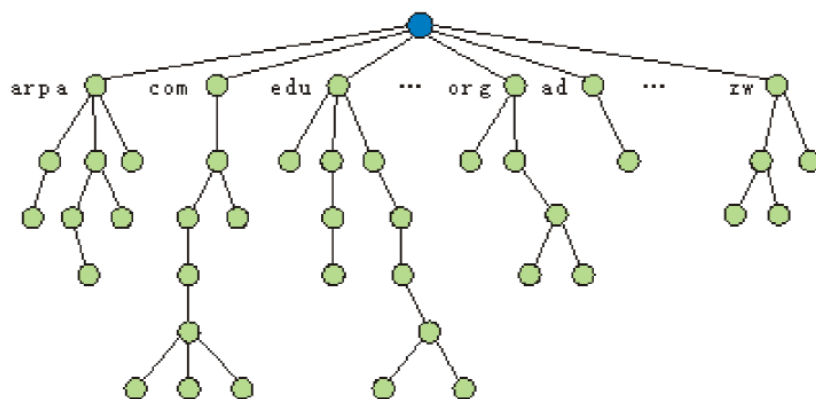
(二) 实验环境

本次使用能访问广域网的主机

(三) 实验原理

一、域名空间

在域名空间中，名字被定义在一个根在顶部的树型结构中。这个树结构最多有 128 层：第 0 层为根，如下图所示：



1. 标号

树上的每一个节点都有一个标号，标号是一个最多有 63 个字符的字符串。根节点的标号是空字符串。每一个节点的子节点都具有不同的标号，这样就保证了域名是惟一的。

2. 域名

一个完全的域名是用点“.”分隔开的标号序列。域名总是从节点标号向上读到根节点标号的。因为最后一个标号是根节点的标号，所以一个完全的域名总是以空标号结束。因为空字符串表示什么也没有，所以域名的最后一个字符是一个点。

(1) 完整域名

若域名以空字符串结束，那么这个域名就叫做完整域名（FQDN）。完整域名是包括主机全名的域名。它包括从最具体的到最一般的所有标号，并惟一地定义了该主机的名字。例如，域名：challenger.atc.fhda.edu 是名为 challenger 的计算机的完整域名。

(2) 不完整域名

若一个域名不是以空字符串结束，则它就叫做不完整域名（PQDN）。不完整域名从一个节点开始，它没有到达根节点。它适用于这样一种情况：当要被解析的域名和客户属于同一个场所时，解析程序可以自动加上缺少的部分，以便创建完整域名。例如，如果在场所 atc.fhda.edu 上的用户想得到计算机 challenger 的 IP 地址，用户就可以定义一个不完整域名：challenger。DNS 客户在把地址传递给 DNS 服务器之前，会加上后缀 atc.fhda.edu。

3. 域

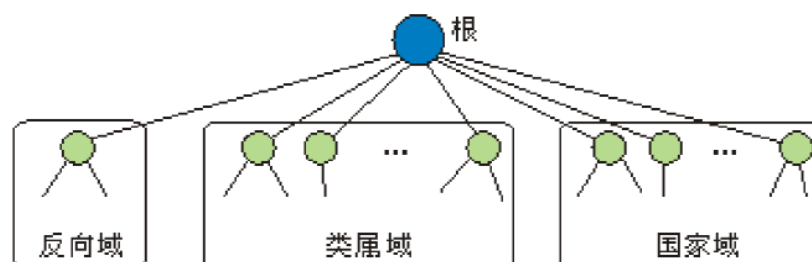
域（domain）是域名空间中的子树。域的名字就是这个子树顶部节点的域名。下图给出了一些域。域本身又可划分为若干个域（有时也称它们为子域）。

二. DNS 协议简介

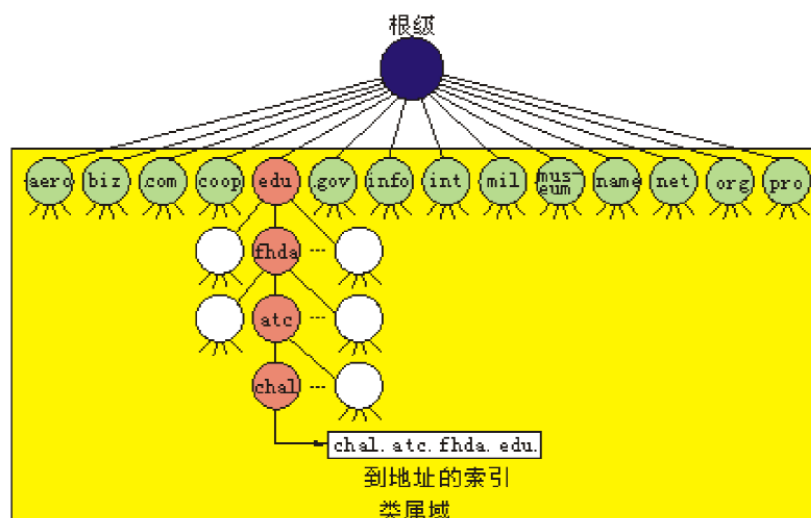
DNS（域名服务）是一种能够完成从域名到地址或从地址到域名的映射系统。使用 DNS，计算机用户可以间接的通过域名来完成通信。Internet 中的 DNS 被设计成为一个联机分布式数据库系统，采用客户/服务器方式工作。分布式的结构使 DNS 具有很强的容错性。

三. DNS 的域名分类

在 Internet 中，域名空间被划分为 3 个部分：类属域、国家域和反向域，如下图所示：



1. 类属域



在类属域的第一级允许有 14 个标号，这些标号描述了不同的机构类型。

2. 国家域

国家域使用两字符的国家或地区的缩写（例如，用 cn 代表中国）。第二级标号可以是机构的标号，或者是国家指定的标号。

3. 反向域

反向域用来把一个地址映射为域名。例如，有时服务器会收到来自客户的请求，要完成一个任务。但是服务器不能确定这个客户是否在授权的客户列表中，因为只有客户的 IP 地址（从收到的 IP 数据包中提取出来的）被列出。要确定这个客户是否在授权列表中，服务器可以使用它的解析程序向 DNS 发送查询，并请求把地址映射为名字。

这种类型的查询叫做反向查询或指针（PTR）查询。要处理反向查询，在域名空间中要增加反向域，且其第一级节点叫做 arpa（由于历史原因）。第二级节点叫做 in-addr（表示反向地址）。域的其余部分为 IP 地址。

处理反向域的服务器也是分级的。这就表示地址的网络号部分要比子网号部分的等级高，而子网号部分要比主机号部分的等级高。在与类属域和国家域相比较时，反向域看起来是反过来的，如 132.34.45.121 的 IP 地址在读出时应为 121.45.34.132.in-addr.arpa。下图是反向域配置的说明。

（四）实验步骤

练习1 Internet 域名空间的分类

各主机打开工具区的“拓扑验证工具”，选择相应的网络结构，配置网卡后，进行拓扑验证，如果通过拓扑验证，关闭工具继续进行实验，如果没有通过，请检查网络连接。本练习一人一组，现仅以主机 A 为例，其它主机的操作参考主机 A。

1. 类属域

将主机 A 的“首选 DNS 服务器”设置为公网 DNS 服务器，目的是能够访问 Internet。

- (1) 主机 A 启动协议分析器开始捕获数据并设置过滤条件（提取 DNS 协议）。
- (2) 主机 A 在命令行下运行“nslookup www.python.org”命令。
- (3) 主机 A 停止捕获数据。分析主机 B 捕获到的数据及主机 A 命令行返回的结果，回答以下问题：

- “www.python.org”对应的 IP 地址是什么？

151.101.108.223

- “www.python.org”域名的顶级域名的含义是什么？

.org 域名是互联网的通用顶级域之一，“org”是英文“organization（组织）”的缩写，表示其他类型的组织或非营利组织。

2. 国家域

- (1) 主机 A 启动协议分析器开始捕获数据并设置过滤条件（提取 DNS 协议）。
- (2) 主机 A 在命令行下运行“nslookup www.jl.gov.cn”命令。
- (3) 主机 A 停止捕获数据。分析主机 B 捕获到的数据及主机 A 命令行返回的结果，回答以下问题：

- “www.jl.gov.cn”对应的 IP 地址是什么？

121.32.243.81

- “www.jl.gov.cn”域名的顶级、二级、三级域名的含义是什么？

顶级域名表示中国国家域名，由中国国际互联网络信息中心（Inter NIC）注册并运行。.gov 表示政府行政机关域名。.jl 表示中国吉林省这个地区的域名。

3. 反向域

- (1) 将主机 A 的“首选 DNS 服务器”设置为服务器的 IP 地址。
- (2) 主机 A 启动协议分析器开始捕获数据并设置过滤条件（提取 DNS 协议）。
- (3) 主机 A 在命令行下运行“nslookup 192.168.10.8”命令。
- (4) 主机 A 停止捕获数据。分析主机 A 捕获到的数据及主机 A 命令行返回的结果，回答以下问题：

- 192.168.10.8 对应的域名是什么？

cachea.nic.jnu.edu.cn

- 反向域的顶级、二级域名分别是什么？

顶级域名为.cn，二级域名为.jnu

思考问题

1. Internet 的域名结构是怎样的？它与目前的电话网的号码结构有何异同之处？

(1) 域名的结构由标号序列组成，各标号之间用点隔开：. 三级域名、. 二级域名、. 顶级域名各标号分别代表不同级别的域名。

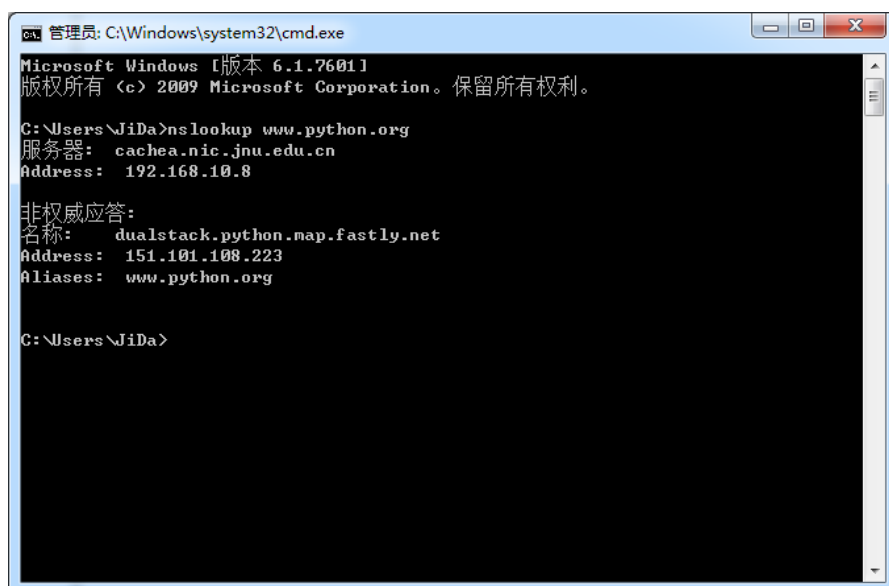
(2) 电话号码分为国家号（中国 +86），结构往下分为区号、本机号。

练习2 DNS 的应用及高速缓存

本练习将主机 A 和 B 作为一组，主机 C 和 D 作为一组，主机 E 和 F 作为一组。现仅以主机 A、B 所在组为例，其它组的操作参考主机 A、B 所在组的操作。

1. 该练习中，DNS 服务器及各主机 IP 地址配置同练习二。
2. 主机 A、B 分别在命令行下执行“ipconfig /flushdns”命令来清空 DNS 高速缓存。
3. 主机 A、B 分别启动协议分析器开始捕获数据并设置过滤条件（提取 DNS 协议和 ICMP 协议）。
4. 主机 A、B 分别在命令行下执行“ping 对方的域名”命令，然后执行“ipconfig/displaydns”命令来显示 DNS 高速缓存。在缓存中找到对方的域名所对应的记录。
5. 主机 A、B 在命令行下再次执行“ping 对方主机的域名”命令。
6. 主机 A、B 停止捕获，分析其捕获的数据及对方的 DNS 高速缓存中的内容，回答问题：
 - 简述在使用域名完成的通信中，DNS 协议所起到的作用。
将域名解析为 IP 地址
 - 简述 DNS 高速缓存的作用。
可大大减轻根域名服务器的负荷，使因特网上的 DNS 查询请求和回答报文的数量大为减少，同时也减少查询时间，提高效率。
 - 参考“会话分析”视图的显示结果，绘制此次访问过程的报文交互图（包括 ICMP 协议）。(报文交互图附在附页处)
7. 恢复网络环境，将“首选 DNS 服务器”清空。

（五）实验结果与分析

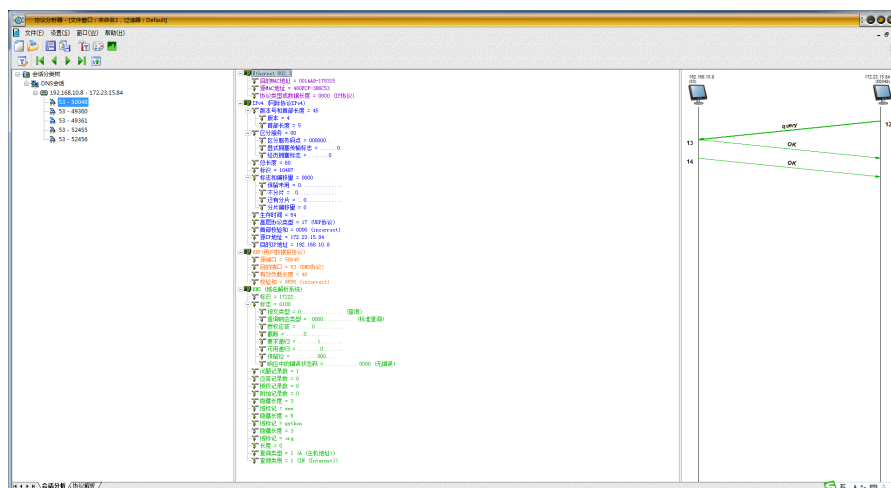


```
C:\Windows\system32\cmd.exe
Microsoft Windows [版本 6.1.7601]
版权所有 (c) 2009 Microsoft Corporation。保留所有权利。

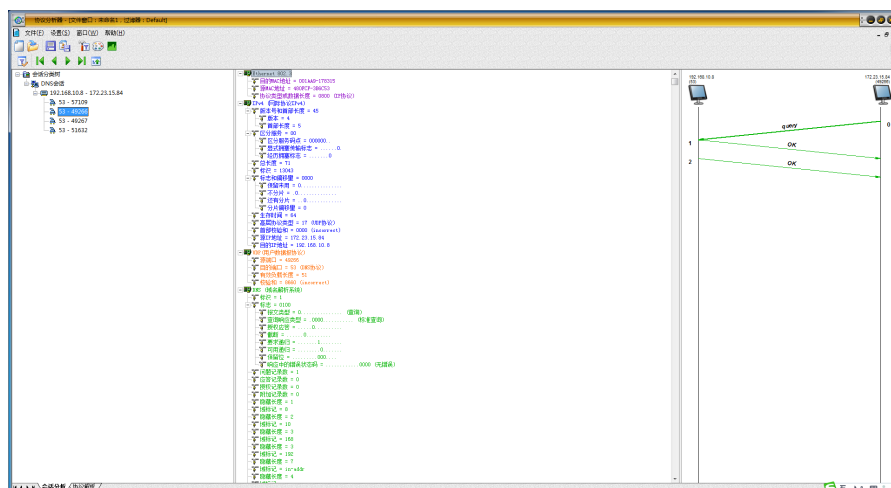
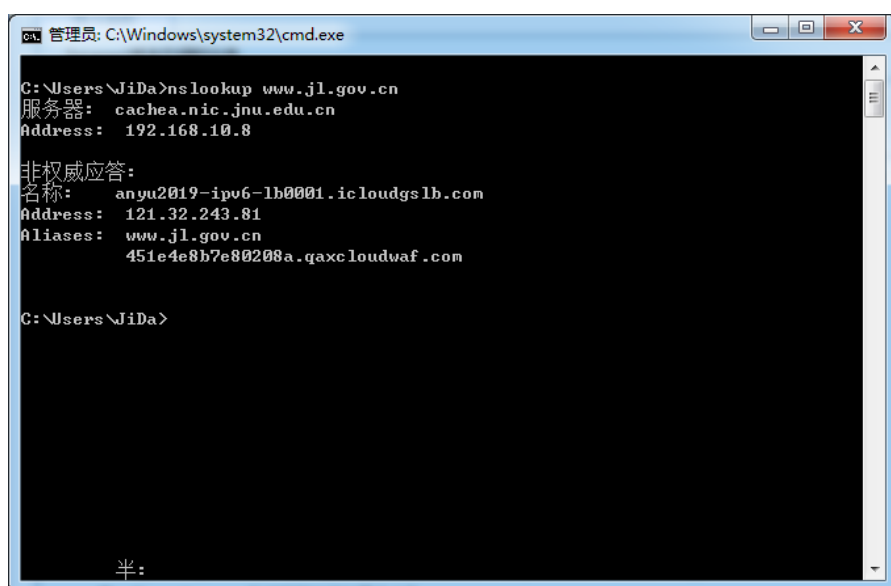
C:\Users\JiDa>nslookup www.python.org
服务器:  cachea.nic.jnu.edu.cn
Address:  192.168.10.8

非权威应答:
名称:    dualstack.python.map.fastly.net
Address: 151.101.108.223
Aliases: www.python.org

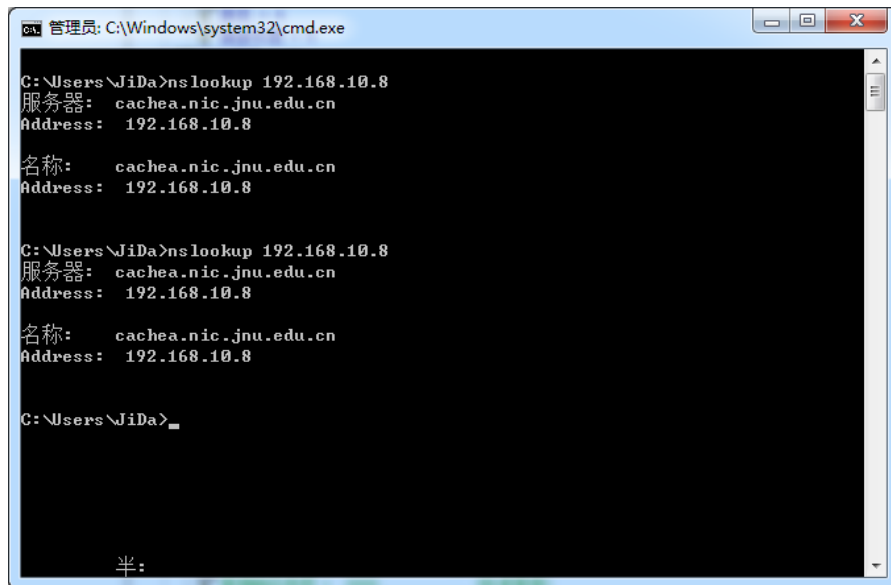
C:\Users\JiDa>
```



分析:使用 nslookup 命令发送 DNS 查询报文,查询类属域的 IP 地址。cachea.nic.jnu.edu.cn 表示本地域名服务器的名字, 192.168.10.8 表示本地域名服务器的 IP 地址。dual-stack.python.map.fastly.net 表示网站的真实域名, 151.101.108.223 表示网站的 IP 地址, 下同。



分析: 使用 nslookup 命令发送 DNS 查询报文, 查询国家域的 IP 地址。同时也可以看到, DNS 协议是基于 IP 协议和 UDP 协议的, 如图所示, 每个 DNS 查询报文的标识位不同, 但其标志位都是相同的 (0100), 报文中记录了报文类型 (即查询报文还是响应报文)、查询的问题记录数、应答记录数、授权记录数、附加记录数、相应错误码等等。除此之外, DNS 报文中还保存着查询的型别, 通常查询类型为 A 类型, 表示由域名获取对应的 IP 地址。查询类为地址类型, 通常为互联网地址, 值为 1。



```
管理员: C:\Windows\system32\cmd.exe

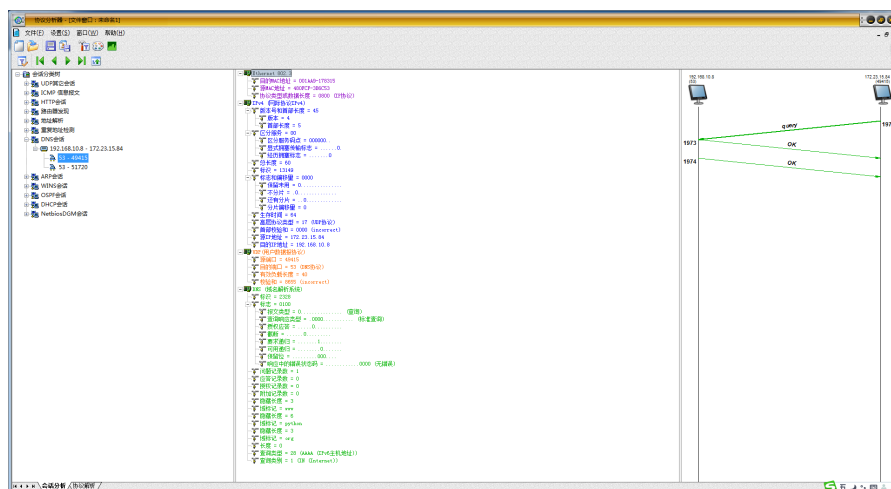
C:\Users\JiDa>nslookup 192.168.10.8
服务器:  cachea.nic.jnu.edu.cn
Address:  192.168.10.8

名称:    cachea.nic.jnu.edu.cn
Address:  192.168.10.8

C:\Users\JiDa>nslookup 192.168.10.8
服务器:  cachea.nic.jnu.edu.cn
Address:  192.168.10.8

名称:    cachea.nic.jnu.edu.cn
Address:  192.168.10.8

C:\Users\JiDa>
```



分析: 使用 nslookup 命令发送 DNS 查询报文, 查询对应 IP 的域名。DNS 协议支持 “反向查询”, 即通过 IP 地址查询对应的域名。同时, 由于 DNS 查询有两种方式, 即递归查询和迭代查询, 所以报文中含有要求递归和可用递归字段, 要求递归被请求设置, 应答的时候使用的相同的值返回。如果设置了, 就建议域名服务器进行递归解析, 递归查询的支持是可选的。而可用递归字段在应答中设置或取消, 用来代表服务器是否支持递归查询。

```
C:\Windows\system32\cmd.exe
Microsoft Windows [版本 6.1.7601]
版权所有 (c) 2009 Microsoft Corporation。保留所有权利。

C:\Users\JiDa>ipconfig /flushdns

Windows IP 配置

已成功刷新 DNS 解析缓存。

C:\Users\JiDa>ping www.python.org

正在 Ping dualstack.python.map.fastly.net [151.101.108.223] 具有 32 字节的数据:
来自 151.101.108.223 的回复: 字节=32 时间=58ms TTL=48
来自 151.101.108.223 的回复: 字节=32 时间=58ms TTL=48
来自 151.101.108.223 的回复: 字节=32 时间=59ms TTL=48
来自 151.101.108.223 的回复: 字节=32 时间=58ms TTL=48

151.101.108.223 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),
    往返行程的估计时间(以毫秒为单位):
        最短 = 58ms, 最长 = 59ms, 平均 = 58ms

C:\Users\JiDa>ipconfig /displaydns

Windows IP 配置

www.python.org
-----
记录名称 . . . . . : www.python.org
记录类型 . . . . . : 5
生存时间 . . . . . : 398
数据长度 . . . . . : 8
部分 . . . . . : 答案
CNAME 记录 . . . . . : dualstack.python.map.fastly.net

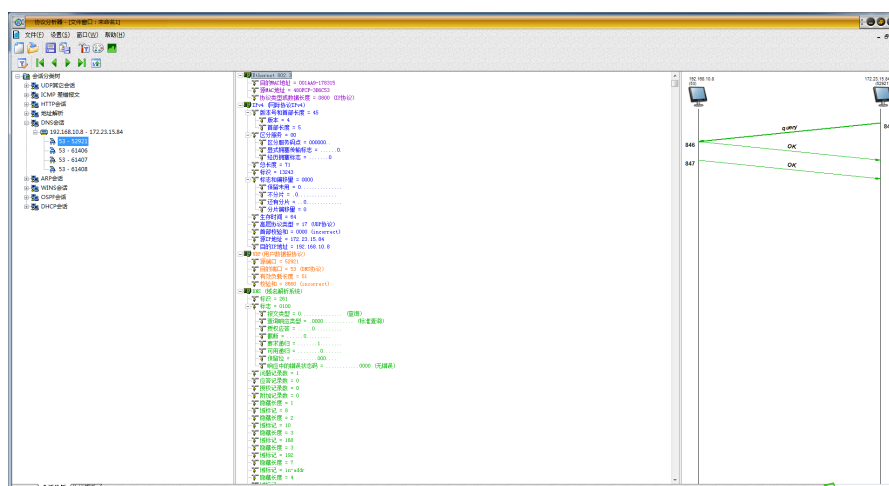
C:\Users\JiDa>ping www.python.org

正在 Ping dualstack.python.map.fastly.net [151.101.108.223] 具有 32 字节的数据:
来自 151.101.108.223 的回复: 字节=32 时间=58ms TTL=48
来自 151.101.108.223 的回复: 字节=32 时间=58ms TTL=48
来自 151.101.108.223 的回复: 字节=32 时间=58ms TTL=48
来自 151.101.108.223 的回复: 字节=32 时间=58ms TTL=48

151.101.108.223 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),
    往返行程的估计时间(以毫秒为单位):
        最短 = 58ms, 最长 = 58ms, 平均 = 58ms

C:\Users\JiDa>
```

半:



分析：使用 `nslookup` 命令发送 DNS 查询报文，学习 DNS 高速缓存。DNS 服务器可以高速缓存从其他 DNS 服务器收到的 DNS 记录，也可以在 DNS 客户服务中使用高速缓存，将其作为 DNS 客户端保存在最近的查询过程中得到的信息高速缓存，如此一来可提高解析速度。如上图所示，我们 ping 了某个域名，然后 display 高速缓存，便能查到刚刚 ping 的域名的查询信息，下一次查询时会优先在高速缓存区中查询。

（六）附录

利用 `gethostbyname` 函数实现域名到 ip 地址的简单映射。

暨南大学本科实验报告专用纸(附页)

```
File Actions Edit View Help
[root@kali ~/Desktop/myarp]# make
g++ tmp.cpp -o query
[root@kali ~/Desktop/myarp]# ./query
please input the domain: www.jnu.edu.cn
address: 36.156.46.43 hptr->h_name: upichq.v.ctxcdn.cn
addr.sin_addr[614215211]
address: 36.156.46.41 hptr->h_name: upichq.v.ctxcdn.cn
addr.sin_addr[614215209]
address: 36.156.46.42 hptr->h_name: upichq.v.ctxcdn.cn
addr.sin_addr[614215210]
address: 36.156.46.40 hptr->h_name: upichq.v.ctxcdn.cn
addr.sin_addr[614215208]
address: 36.156.46.39 hptr->h_name: upichq.v.ctxcdn.cn
addr.sin_addr[614215207]
address: 36.156.46.38 hptr->h_name: upichq.v.ctxcdn.cn
addr.sin_addr[614215206]
address: 36.156.46.44 hptr->h_name: upichq.v.ctxcdn.cn
addr.sin_addr[614215212]
address: 36.156.46.49 hptr->h_name: upichq.v.ctxcdn.cn
addr.sin_addr[614215217]
address: 36.156.46.36 hptr->h_name: upichq.v.ctxcdn.cn
addr.sin_addr[614215204]
address: 36.156.46.45 hptr->h_name: upichq.v.ctxcdn.cn
addr.sin_addr[614215213]
[root@kali ~/Desktop/myarp]#
```

```
C:\WINDOWS\system32\cmd.exe

C:\Users\HM520>ping 36.156.46.42

正在 Ping 36.156.46.42 具有 32 字节的数据:
来自 36.156.46.42 的回复: 字节=32 时间=92ms TTL=51
来自 36.156.46.42 的回复: 字节=32 时间=84ms TTL=51

36.156.46.42 的 Ping 统计信息:
    数据包: 已发送 = 2, 已接收 = 2, 丢失 = 0 (0% 丢失),
往返行程的估计时间(以毫秒为单位):
    最短 = 84ms, 最长 = 92ms, 平均 = 88ms
Control-C
^C
C:\Users\HM520>ping www.jnu.edu.cn

正在 Ping upichq.v.ctxcdn.cn [36.156.46.41] 具有 32 字节的数据:
来自 36.156.46.41 的回复: 字节=32 时间=80ms TTL=52
来自 36.156.46.41 的回复: 字节=32 时间=66ms TTL=52
来自 36.156.46.41 的回复: 字节=32 时间=62ms TTL=52
来自 36.156.46.41 的回复: 字节=32 时间=70ms TTL=52

36.156.46.41 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),
往返行程的估计时间(以毫秒为单位):
    最短 = 62ms, 最长 = 80ms, 平均 = 69ms

C:\Users\HM520>
```