

实验名称	DNS 实验		
姓名	刘培源	学号	2023214278
实验步骤	<p>实验环境：Mac Parallel Desktop 19; Ubuntu 22.04</p> <p>1. 首先使用 <code>sudo apt-get install bind9</code> 在 ubuntu 上安装 bind9，安装成功截图如下：</p> <div data-bbox="411 537 1332 600"><pre>nat@nat-Parallels-ARM-Virtual-Machine:/etc/init.d\$ whereis bind bind: /usr/lib/aarch64-linux-gnu/bind /etc/bind</pre></div> <p>2. 然后使用 <code>sudo gedit /etc/resolv.conf</code> 修改 DNS 服务器，将 nameserver 修改为 127.0.0.1，修改截图如下：</p> <div data-bbox="411 712 1316 1249"><pre>Open ▾ [icon] resolv.conf /etc Save 1# This is /run/systemd/resolve/stub-resolv.conf managed by man:systemd-resolved(8). 2# Do not edit. 3# 4# This file might be symlinked as /etc/resolv.conf. If you're looking at 5# /etc/resolv.conf and seeing this text, you have followed the symlink. 6# 7# This is a dynamic resolv.conf file for connecting local clients to the 8# internal DNS stub resolver of systemd-resolved. This file lists all 9# configured search domains. 10# 11# Run "resolvectl status" to see details about the uplink DNS servers 12# currently in use. 13# 14# Third party programs should typically not access this file directly, but only 15# through the symlink at /etc/resolv.conf. To manage man:resolv.conf(5) in a 16# different way, replace this symlink by a static file or a different symlink. 17# 18# See man:systemd-resolved.service(8) for details about the supported modes of 19# operation for /etc/resolv.conf. 20 21nameserver 127.0.0.1 22options edns0 trust-ad 23search localdomain</pre></div> <p>3. 然后在配置文件 <code>/etc/bind/named.conf.local</code> 中添加新的域，我添加的是 <code>peiyuanliu.com</code>，截图如下：</p> <div data-bbox="411 1366 1316 1713"><pre>Open ▾ [icon] named.conf.local /etc/bind 1// 2// Do any local configuration here 3// 4 5// Consider adding the 1918 zones here, if they are not used in your 6// organization 7//include "/etc/bind/zones.rfc1918"; 8zone "peiyuanliu.com"{ 9 type master; 10 file "/etc/bind/db.peiyuanliu.com"; 11};</pre></div> <p>4. 以 <code>db.local</code> 为模版设置自己的 DNS 映射，通过如下命令：</p> <p>(1) <code>sudo cp db.local db.peiyuanliu.com</code></p> <p>(2) <code>sudo gedit db.peiyuanliu.com</code></p> <p>来进行配置，配置截图如下：</p>		

```
Open  db.peiyuanliu.com /etc/bind
1;
2; BIND data file for local loopback interface
3;
4 $TTL      604800
5 @        IN      SOA      peiyuanliu.com. mail.peiyuanliu.com. (
6          2          ; Serial
7          604800     ; Refresh
8          86400      ; Retry
9          2419200    ; Expire
10         604800 )    ; Negative Cache TTL
11;
12 @        IN      NS       peiyuanliu.com.
13 @        IN      A        180.97.33.108
14 @        IN      AAAA     ::1
15 *        IN      A        180.97.33.108
```

5. 然后启动 bind9，以及清空 DNS 缓存，注意 ubuntu22.04 的版本，与实验指导书的命令是不一致的，需要通过如下截图的命令来启动 bind9 和清空 DNS 缓存。

```
nat@nat-Parallels-ARM-Virtual-Machine:/etc/init.d$ sudo systemctl restart bind9
nat@nat-Parallels-ARM-Virtual-Machine:/etc/init.d$ sudo /etc/init.d/nscd restart
Restarting nscd (via systemctl): nscd.service.
```

6. 测试 ping peiyuanliu.com 是否成功，成功截图如下：

```
nat@nat-Parallels-ARM-Virtual-Machine:/etc/init.d$ ping peiyuanliu.com
PING peiyuanliu.com(ip6-localhost (::1)) 56 data bytes
64 bytes from ip6-localhost (::1): icmp_seq=1 ttl=64 time=0.083 ms
64 bytes from ip6-localhost (::1): icmp_seq=2 ttl=64 time=0.141 ms
64 bytes from ip6-localhost (::1): icmp_seq=3 ttl=64 time=0.145 ms
64 bytes from ip6-localhost (::1): icmp_seq=4 ttl=64 time=0.146 ms
64 bytes from ip6-localhost (::1): icmp_seq=5 ttl=64 time=0.144 ms
```

7. Wireshark 的 DNS 信息在数据分析给出。

1. DNS 查询请求包分析：

在尝试访问 `www.peiyuanliu.com` 时，由于主机未知百度的 IP 地址，发起了对 `www.peiyuanliu.com` 的 DNS 查询。设置的 DNS 服务器地址为本地 `127.0.0.1`，因此 DNS 查询的源和目标地址都是 `127.0.0.1`。发送的 DNS 请求显示源 IP 和目标 IP 都是 `127.0.0.1`，源端口为 `51668`，目标端口为 `53`，符合 DNS 查询的标准通信模式。

Position	Protocol	Length	Info
0.0.1	DNS	87	Standard query 0xd5ad A peiyuanliu.com OPT
0.0.1	DNS	87	Standard query 0x61dc AAAA peiyuanliu.com OPT
0.0.1	DNS	103	Standard query response 0xd5ad A peiyuanliu.com A 180.97.33.108 OPT
0.0.1	DNS	115	Standard query response 0x61dc AAAA peiyuanliu.com AAAA ::1 OPT
	ICMPv6	120	Echo (ping) request id=0x000d, seq=1, hop limit=64 (reply in 407)
	ICMPv6	120	Echo (ping) reply id=0x000d, seq=1, hop limit=64 (request in 406)

0000	00 00 03 04 00 06 00 00	00 00 00 00 2b c0 08 00+....
0010	45 00 00 47 d8 2e 40 00	40 11 64 75 7f 00 00 01	E..G..@. @.du....
0020	7f 00 00 01 c9 d4 00 35	00 33 fe 46 d5 ad 01 205..3.F....
0030	00 01 00 00 00 00 00 01	0a 70 65 69 79 75 61 6epeiyuan
0040	6c 69 75 03 63 6f 6d 00	00 01 00 01 00 00 29 04	liu.com.....)

2. DNS 查询返回包分析

收到 DNS 查询后，DNS 服务器从端口 `53`（本地地址 `127.0.0.1`）向客户端的端口 `51668`（同样的本地地址）回传了对应的 IP 地址。查询结果显示 `www.peiyuanliu.com` 的 IP 地址为 `180.97.33.108`，与之前配置的地址一致。这标志着 DNS 查询流程的完成，使得主机能通过此 IP 地址与目标网站通信。由于使用 `ping` 命令测试与 `www.peiyuanliu.com` 的连通性，接下来的数据包遵循 ICMP 协议，其目的地址即为新获得的 IP 地址。

Position	Protocol	Length	Info
0.0.1	DNS	87	Standard query 0xd5ad A peiyuanliu.com OPT
0.0.1	DNS	87	Standard query 0x61dc AAAA peiyuanliu.com OPT
0.0.1	DNS	103	Standard query response 0xd5ad A peiyuanliu.com A 180.97.33.108 OPT
0.0.1	DNS	115	Standard query response 0x61dc AAAA peiyuanliu.com AAAA ::1 OPT
	ICMPv6	120	Echo (ping) request id=0x000d, seq=1, hop limit=64 (reply in 407)
	ICMPv6	120	Echo (ping) reply id=0x000d, seq=1, hop limit=64 (request in 406)

0000	00 00 03 04 00 06 00 00	00 00 00 00 3d 65 08 00=e..
0010	45 00 00 57 c5 eb 00 00	40 11 b6 a8 7f 00 00 01	E..W...@.....
0020	7f 00 00 01 00 35 c9 d4	00 43 fe 56 d5 ad 85 805..C.V....
0030	00 01 00 01 00 00 00 01	0a 70 65 69 79 75 61 6epeiyuan
0040	6c 69 75 03 63 6f 6d 00	00 01 00 01 c0 0c 00 01	liu.com.....

思考题	<p>1、一个 DNS 查询的答复中是否会包含几个应答记录?如果是，对同一查询多执行几次，看看每次应答记录的顺序是否相同，试分析为什么。</p> <p>答： DNS 答复可包含多个记录，顺序可能变化，反映负载均衡或缓存更新。</p> <p>2、思考一下如何劫持 <code>www.naichabiao.com</code> 到 <code>www.jd.com</code>。</p> <p>答： 通过对 DNS 服务器的攻击，篡改 DNS 记录，将 <code>www.naichabiao.com</code> 的 IP 地址改为与 <code>www.jd.com</code> 相同。</p>
经验总结	<p>1. 若使用 Ubuntu 22.04 的话，要用 <code>sudo systemctl restart bind9</code> 代替 <code>sudo /etc/init.d/bind9 start</code> 来启动 bind9; 并用 <code>sudo /etc/init.d/nscd restart</code> 代替 <code>sudo /etc/init.d/dns-clean start</code> 来清空 dns 缓存。</p> <p>2. 如果第一步 nscd 没有的话，用 <code>sudo apt-get install ncsd</code> 安装即可。</p>