计算机网络实验报告-lab3

李远航

PB20000137

> 部分本地网络存在问题的实验使用vlab平台完成

- **Run nslookup to obtain the IP address of a Web server in Asia. What is the IP address of that server?**

```
(base) ubuntu@VM5522-bot:~$ nslookup ustc.edu.cn
Server:         172.31.0.1
Address:        172.31.0.1#53

Non-authoritative answer:
Name:   ustc.edu.cn
Address: 202.38.64.246
Name:   ustc.edu.cn
Address: 2001:da8:d800:642::248
```

```
Address: 202.38.64.246
Address: 2001:da8:d800:642::248
```

- **Run nslookup to determine the authoritative DNS servers for a university in Europe.**

```
(base) ubuntu@VM5522-bot:~$ nslookup -type=NS ox.ac.uk
Server:         172.31.0.1
Address:        172.31.0.1#53

Non-authoritative answer:
ox.ac.uk        nameserver = auth4.dns.ox.ac.uk.
ox.ac.uk        nameserver = dns1.ox.ac.uk.
ox.ac.uk        nameserver = dns0.ox.ac.uk.
ox.ac.uk        nameserver = auth6.dns.ox.ac.uk.
ox.ac.uk        nameserver = auth5.dns.ox.ac.uk.
ox.ac.uk        nameserver = dns2.ox.ac.uk.
ox.ac.uk        nameserver = ns2.ja.net.

Authoritative answers can be found from:
```

- **Run nslookup so that one of the DNS servers obtained in Question 2 is queried for the mail servers for Yahoo! mail. What is its IP address?**

```
(base) ubuntu@VM5522-bot:~$ nslookup mail.yahoo.com auth4.dns.ox.ac.uk
Server:         auth4.dns.ox.ac.uk
Address:        2600:3c00:e000:19::1#53

Non-authoritative answer:
mail.yahoo.com  canonical name = edge.gycpi.b.yahoodns.net.
Name:   edge.gycpi.b.yahoodns.net
Address: 119.161.8.12
Name:   edge.gycpi.b.yahoodns.net
Address: 119.161.8.11
Name:   edge.gycpi.b.yahoodns.net
Address: 2406:2000:a8:800::e6
Name:   edge.gycpi.b.yahoodns.net
Address: 2406:2000:a8:800::e7
```

```
1   Address: 119.161.8.12
2   Address: 119.161.8.11
3   Address: 2406:2000:a8:800::e6
4   Address: 2406:2000:a8:800::e7
```

- **Locate the DNS query and response messages. Are then sent over UDP or TCP?**

  UDP

- **What is the destination port for the DNS query message? What is the source port of DNS response message?**

  53 53

  ```
  > User Datagram Protocol, Src Port: 62745, Dst Port: 53
  > User Datagram Protocol, Src Port: 53, Dst Port: 62745
  ```

- **To what IP address is the DNS query message sent? Use ipconfig to determine the IP address of your local DNS server. Are these two IP addresses the same?**

  ```
  141 2.735727    61.132.163.68    192.168.0.104    DNS    431 Standard query response 0xeb94 A www.ietf.org CNAME www.ietf.org.cdn.
  ```

  192.168.0.104 本地查询相同

  ```
  无线局域网适配器 WLAN:

     连接特定的 DNS 后缀 . . . . . . . :
     IPv4 地址 . . . . . . . . . . . . : 192.168.0.104
     子网掩码 . . . . . . . . . . . . : 255.255.255.0
     默认网关. . . . . . . . . . . . . : 192.168.0.1
  ```

- **Examine the DNS query message. What "Type" of DNS query is it? Does the query message contain any "answers"?**

  ```
  v Queries
    > www.ietf.org: type A, class IN
    [Response In: 200]
  ```

  typeA

  no

- **Examine the DNS response message. How many "answers" are provided? What do each of these answers contain?**

  3

```
Answers
  www.ietf.org: type CNAME, class IN, cname www.ietf.org.cdn.cloudflare.net
      Name: www.ietf.org
      Type: CNAME (Canonical NAME for an alias) (5)
      Class: IN (0x0001)
      Time to live: 1239 (20 minutes, 39 seconds)
      Data length: 33
      CNAME: www.ietf.org.cdn.cloudflare.net
  www.ietf.org.cdn.cloudflare.net: type A, class IN, addr 104.16.45.99
  www.ietf.org.cdn.cloudflare.net: type A, class IN, addr 104.16.44.99
```

- **Consider the subsequent TCP SYN packet sent by your host. Does the destination IP address of the SYN packet correspond to any of the IP addresses provided in the DNS response message?**

一样

- **This web page contains images. Before retrieving each image, does your host issue new DNS queries?**

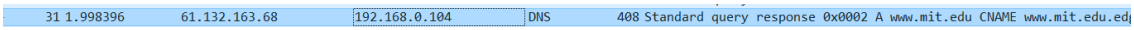
  没有

- **What is the destination port for the DNS query message? What is the source port of DNS response message?**

```
User Datagram Protocol, Src Port: 56281, Dst Port: 53
User Datagram Protocol, Src Port: 53, Dst Port: 56281
```

53 53

- **To what IP address is the DNS query message sent? Is this the IP address of your default local DNS server?**



和本机一样 192.168.0.104

- **Examine the DNS query message. What "Type" of DNS query is it? Does the query message contain any "answers"?**

```
Queries
  www.mit.edu: type A, class IN
[Response In: 31]
```

typeA

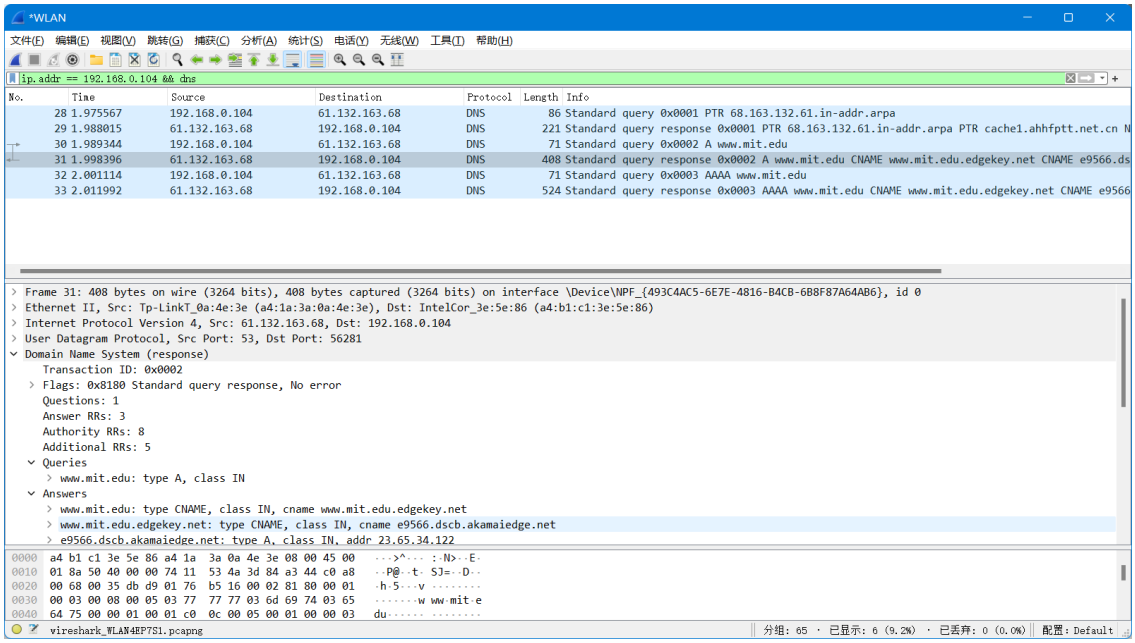
no answers

- **Examine the DNS response message. How many "answers" are provided? What do each of these answers contain?**

  3

```
Answers
  www.mit.edu: type CNAME, class IN, cname www.mit.edu.edgekey.net
      Name: www.mit.edu
      Type: CNAME (Canonical NAME for an alias) (5)
      Class: IN (0x0001)
      Time to live: 900 (15 minutes)
      Data length: 25
      CNAME: www.mit.edu.edgekey.net
  www.mit.edu.edgekey.net: type CNAME, class IN, cname e9566.dscb.akamaiedge.net
  e9566.dscb.akamaiedge.net: type A, class IN, addr 23.65.34.122
```

- **Provide a screenshot.**



- **To what IP address is the DNS query message sent? Is this the IP address of your default local DNS server?**

  21 1.551218 61.132.163.68 192.168.0.104 DNS 402 Standard query response 0x0002 NS mit.edu NS ns1-37.akam.net

  相同 192.168.0.104

- **Examine the DNS query message. What "Type" of DNS query is it? Does the query message contain any "answers"**

  > Queries
  > mit.edu: type NS, class IN
  > [Response In: 21]

  type NS

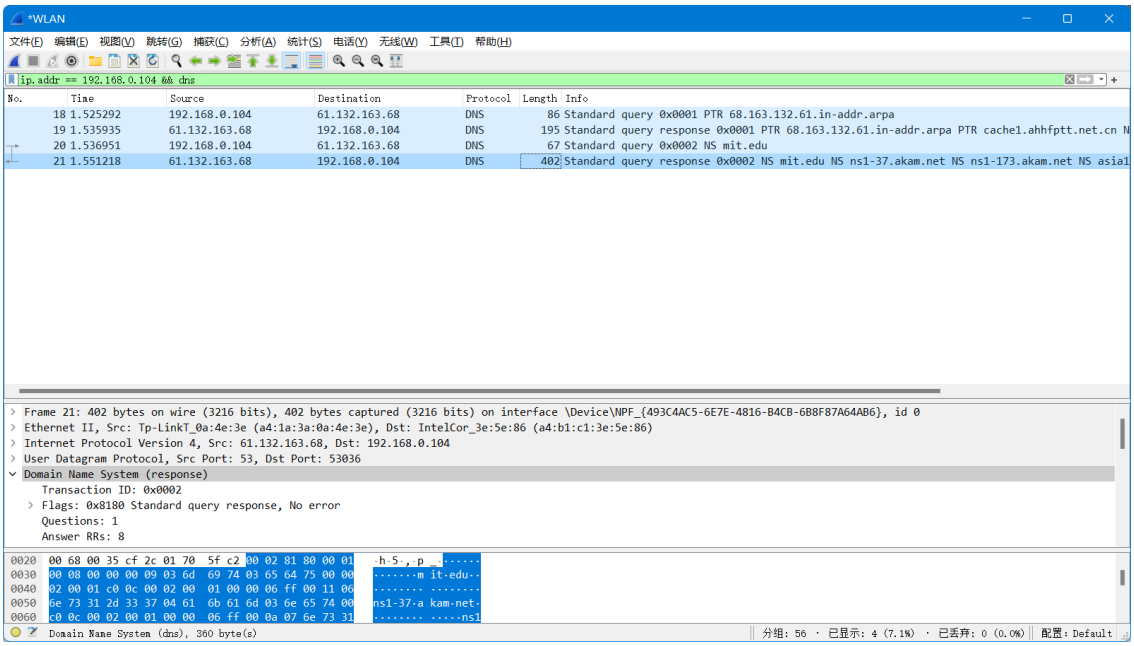
  no answers

- **Examine the DNS response message. What MIT nameservers does the response message provide? Does this response message also provide the IP addresses of the MIT namesers?**

```
Answers
    > mit.edu: type NS, class IN, ns ns1-37.akam.net
    > mit.edu: type NS, class IN, ns ns1-173.akam.net
    > mit.edu: type NS, class IN, ns asia1.akam.net
    > mit.edu: type NS, class IN, ns use2.akam.net
    > mit.edu: type NS, class IN, ns use5.akam.net
    > mit.edu: type NS, class IN, ns usw2.akam.net
    > mit.edu: type NS, class IN, ns eur5.akam.net
    > mit.edu: type NS, class IN, ns asia2.akam.net
Additional records
    > use2.akam.net: type A, class IN, addr 96.7.49.64
    > asia1.akam.net: type A, class IN, addr 95.100.175.64
    > eur5.akam.net: type A, class IN, addr 23.74.25.64
    > use5.akam.net: type A, class IN, addr 2.16.40.64
    > ns1-173.akam.net: type A, class IN, addr 193.108.91.173
    > usw2.akam.net: type A, class IN, addr 184.26.161.64
    > asia2.akam.net: type A, class IN, addr 95.101.36.64
    > use5.akam.net: type AAAA, class IN, addr 2600:1403:a::40
    > ns1-173.akam.net: type AAAA, class IN, addr 2600:1401:2::ad
    [Request In: 20]
    [Time: 0.014267000 seconds]
```

如图所示的域名服务器，提供了ip地址，如图在Additional records中展示

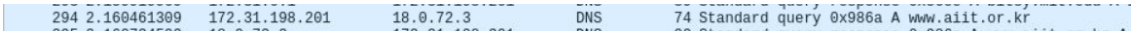
- **Provide a screenshot**



- **To what IP address is the DNS query message sent? Is this the IP address of your default local DNS server? If not, what does the IP address correspond to?**

```
(base) ubuntu@VM5522-bot:~$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 172.31.198.201  netmask 255.255.0.0  broadcast 172.31.255.255
        inet6 fe80::24e2:8fff:fe57:feb7  prefixlen 64  scopeid 0x20<link>
        inet6 2001:da8:d800:4bfc:24e2:8fff:fe57:feb7  prefixlen 64  scopeid 0x0<global>
        ether 26:e2:8f:57:fe:b7  txqueuelen 1000  (以太网)
        RX packets 21103509  bytes 3763110672 (3.7 GB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 523249  bytes 117761362 (117.7 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (本地环回)
        RX packets 50210  bytes 12780274 (12.7 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 50210  bytes 12780274 (12.7 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```



18.0.72.3

不是

是 `bitsy.mit.edu` 域名服务器的ip地址

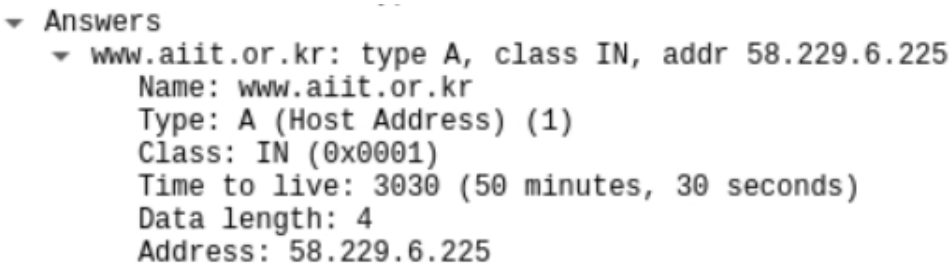
- **Examine the DNS query message. What "Type" of DNS query is it? Does the query message contain any "answers"?**

typeA

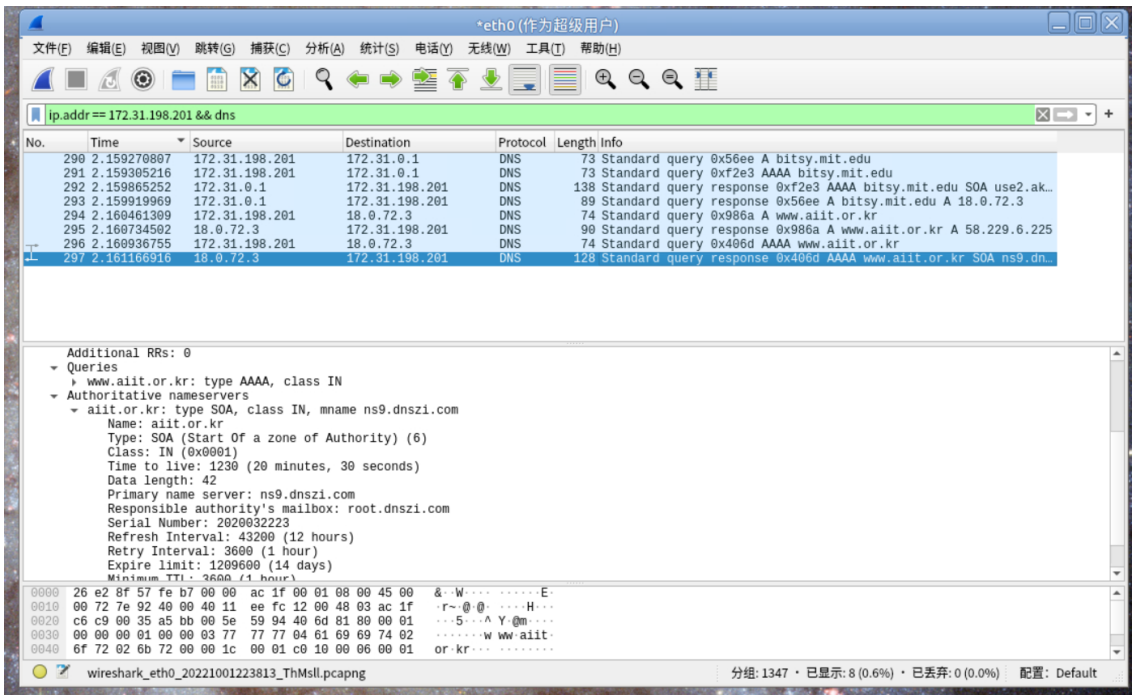
no anwers

- **Examine the DNS response message. How many "answers" are provided? What does each of these answers contain?**

1 如图所示



- **Provide a screenshot**


*eth0 (作为超级用户)
文件(F) 编辑(E) 视图(V) 跳转(G) 捕获(C) 分析(A) 统计(S) 电话(Y) 无线(W) 工具(T) 帮助(H)
ip.addr == 172.31.198.201 && dns
No. Time Source Destination Protocol Length Info
290 2.159270807 172.31.198.201 172.31.0.1 DNS 73 Standard query 0x56ee A bitsy.mit.edu
291 2.159305216 172.31.198.201 172.31.0.1 DNS 73 Standard query 0xf2e3 AAAA bitsy.mit.edu
292 2.159865252 172.31.0.1 172.31.198.201 DNS 138 Standard query response 0xf2e3 AAAA bitsy.mit.edu SOA use2.ak…
293 2.159919969 172.31.0.1 172.31.198.201 DNS 89 Standard query response 0x56ee A bitsy.mit.edu A 18.0.72.3
294 2.160461309 172.31.198.201 18.0.72.3 DNS 74 Standard query 0x986a A www.aiit.or.kr
295 2.160734502 18.0.72.3 172.31.198.201 DNS 90 Standard query response 0x986a A www.aiit.or.kr A 58.229.6.225
296 2.160936755 172.31.198.201 18.0.72.3 DNS 74 Standard query 0x406d AAAA www.aiit.or.kr
297 2.161166916 18.0.72.3 172.31.198.201 DNS 128 Standard query response 0x406d AAAA www.aiit.or.kr SOA ns9.dn…
Additional RRs: 0
Queries
www.aiit.or.kr: type AAAA, class IN
Authoritative nameservers
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: 1230 (20 minutes, 30 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)
0000 26 e2 8f 57 fe b7 00 00 ac 1f 00 01 08 00 45 00
0010 00 72 7e 92 40 00 40 11 ee fc 12 00 48 03 ac 1f
0020 c6 c9 00 35 a5 bb 00 5e 59 94 40 6d 81 80 00 01
0030 00 00 00 01 00 00 03 77 77 77 04 61 69 69 74 02
0040 6f 72 02 6b 72 00 00 1c 00 01 c0 10 00 06 00 01
wireshark_eth0_20221001223813_ThMsll.pcapng
分组: 1347 · 已显示: 8 (0.6%) · 已丢弃: 0 (0.0%)
配置: Default