**华中科技大学计算机学院**

**《计算机通信与网络》实验报告**

实验名称 DNS解析实验

|  |  |  |  |
| --- | --- | --- | --- |
| 姓 名 | 班 级 | 学 号 | 得 分 |
| 潘翔 | IOT1601 | U201614898 |  |

教师评语：

# Lab7 DNS解析实验

## 7.1 环境

操作系统: Manjaro-4.18.10-1 x86\_64 (Arch-Based Distribution)

开发语言: C/C++

编辑器: Visual Studio Code 1.27.2 x64

编译器: g++ (GCC) 8.2.1 20180831

调试器: GNU gdb (GDB) 8.2

构建工具: GNU Make 4.2.1

网络环境：

Link encap:Ethernet  HWaddr a0:8c:fd:24:5d:4c     
inet addr:222.20.100.153  Bcast:222.20.101.255  Mask:255.255.254.0   
inet6 addr: fe80::2476:27:cd9d:d75b/64 Scope:Link   
inet6 addr: 2001:250:4000:803c:e3c1:b69:d9f2:67b0/64 Scope:Global

## 7.2 实验目的

1. 理解 DNS 系统的工作原理；
2. 熟悉 DNS 服务器的工作过程；
3. 熟悉 DNS 报文格式；
4. 理解 DNS 缓存的作用。

## 7.3 实验内容及步骤

### 7.3.1 任务一： 观察本地域名解析过程

1. 步骤 1： 在 PC 的浏览器窗口请求内部 Web 服务器的网页
2. 步骤 2： 捕获 DNS 事件并分析本地域名解析过程

本步骤注意观察并完成以下几项内容：

* 1. 分析本地 DNS 服务器的域名解析过程；
  2. 分析 DNS 的响应报文的组成；
  3. 记录 DNS 首部中的查询记录数（QDCOUNT） 及应答记录数（ANCOUNT） ；
  4. 记录 DNS QUERY（DNS 查询）及 DNS ANSWER（DNS应答）部分各字段的值及含义。

完成后单击Reset Simulation（重置模拟）按钮， 将原有的事件全部清空；

同时关闭 PC 的Web Browser（Web浏览器）窗口。

### 7.3.2 任务二： 观察外网域名解析过程

1. 步骤 1： 在 PC 的浏览器窗口请求外部 Web 服务器的网页
2. 步骤 2： 捕获 DNS 事件并分析外网域名解析过程

本步骤注意观察并完成以下几项内容：

* 1. 分析 DNS 服务器之间的域名解析过程；
  2. 各个 DNS 应答报文的首部中查询记录数（QDCOUNT） 及应答记录数（ANCOUNT）是否一样；
  3. 不同的 DNS ANSWER（DNS 应答） 中各字段的值及含义。

完成后单击 Reset Simulation（重置模拟）按钮，将原有的事件全部清空；

同时关闭PC的 Web Browser（Web 浏览器）窗口。

### 7.3.3 任务三： 观察缓存的作用

1. 步骤 1： 查看本地域名服务器 cn\_dns 的缓存
2. 步骤 2： 在 PC 的浏览器窗口请求外部 Web 服务器的网页

重复任务二， 再次观察此次解析外网域名的过程。

完成后单击 Reset Simulation（重置模拟）按钮， 将原有的事件全部清空； 同时关闭 PC 机的 Web Browser（Web 浏览器）窗口。

### 思考

1. 除了 PC 需要配置 DNS Server 外， Web 服务器是否需要 DNS Server 配置？ 如果需要，为什么？
2. 图 7.1 中路由器之间采用串口连接， 路由器为什么要采用这种连接方式。 查阅资料了解串口连接的优缺点。
3. DNS 协议使用运输层的什么协议？
4. DNS 缓存有什么作用？ 在 Packet Tracer 中如何清空 DNS 缓存？
5. 本实验中 PC 与本地域名服务器cn\_dns之间的解析是递归还是迭代？ 本地域名服务器cn\_dns与根域名服务器root\_dns之间呢？ 若后者用另一种解析方法， 则域名服务器之间DNS的请求和应答的交互过程应如何？

## 7.4 实验准备

### 7.4.1 搭建网络拓扑

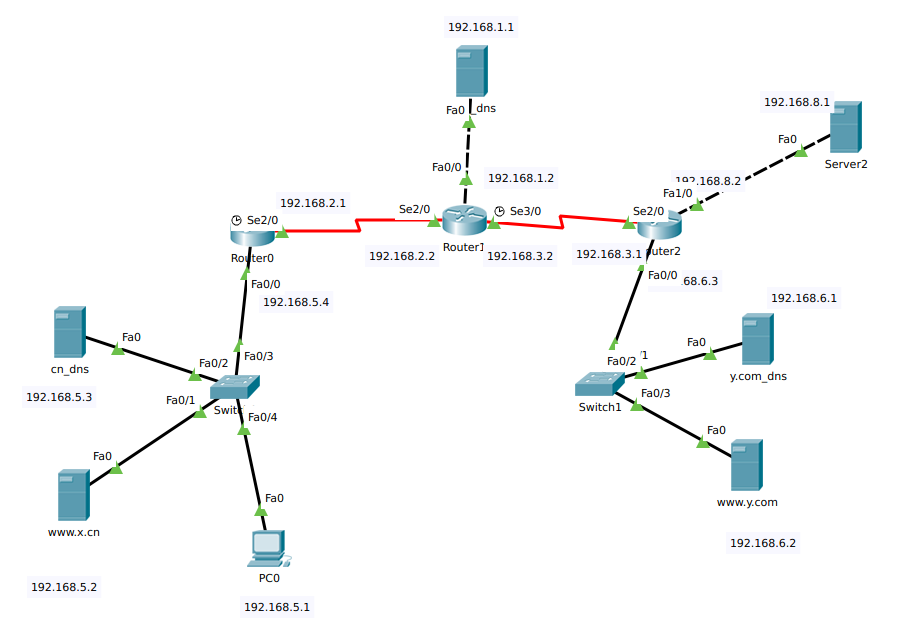


图7-1 网络拓扑图

### 7.4.2 配置主机 IP、 网关、 DNS

### 7.4.3 配置各设备 IP、 网关、 DNS 等

### 7.4.4 配置服务器

1. 域名服务器
   1. 顶级域名服务器 cn\_dns 配置

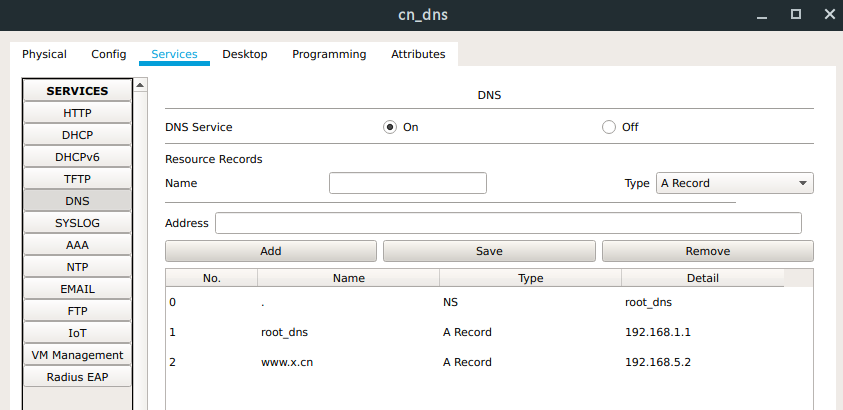


图7-1 顶级域名服务器 cn\_dns 配置图

* 1. 本地域名（权威） 服务器 y.com\_dns 配置

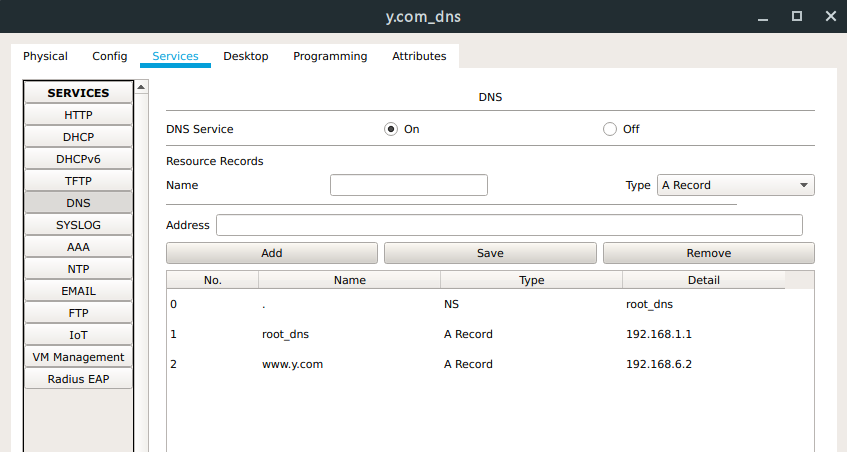


图7-2 本地域名（权威）服务器y.com\_dns配置图

* 1. 顶级域名服务器 com\_dns 配置

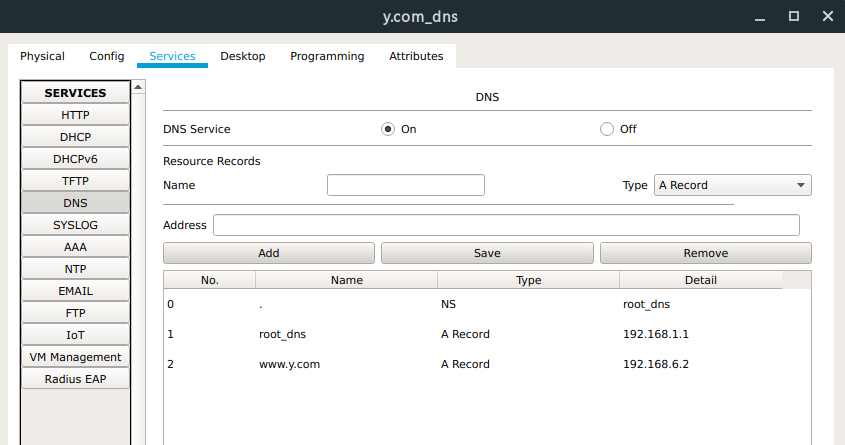


图7-2 顶级域名服务器 com\_dns 配置图

* 1. 根域名服务器 root\_dns 配置

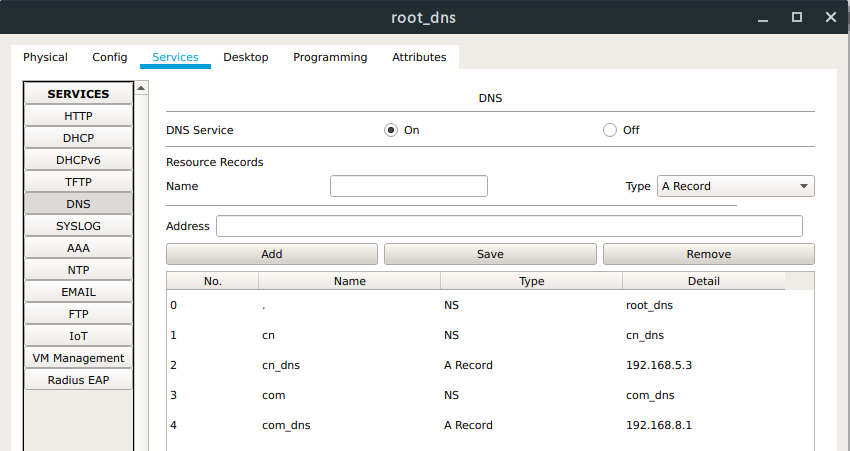


图7-2 根域名服务器root\_dns配置图

1. Web 服务器
   1. [www.x.cn](http://www.x.cn)

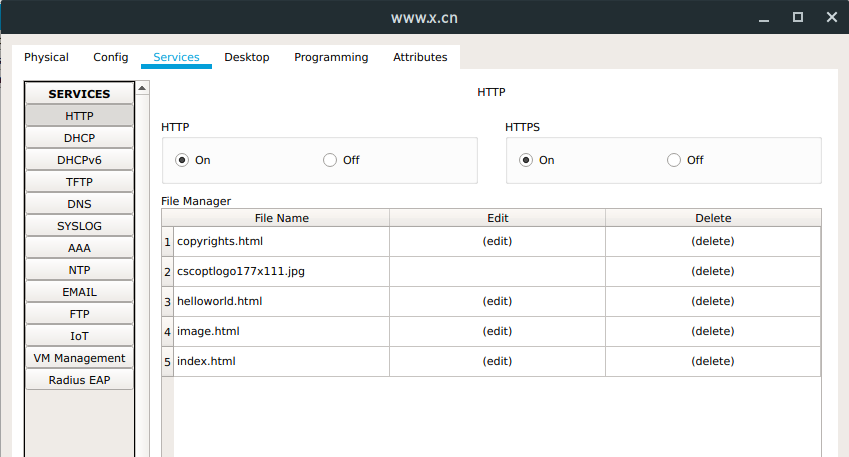


图7-1 [www.x.cn](http://www.x.cn)配置图

* 1. [www.y.com](http://www.y.com)

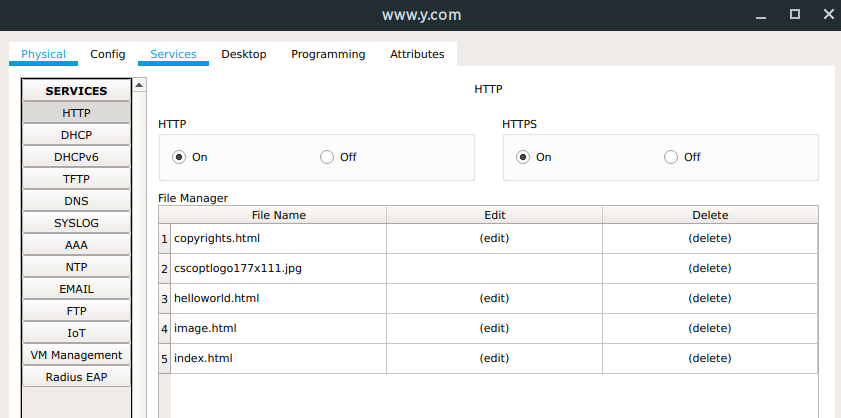


图7-1 [www.y.com](http://www.y.com)配置图

### 7.4.5 路配置由器静态路由表

1. Router0

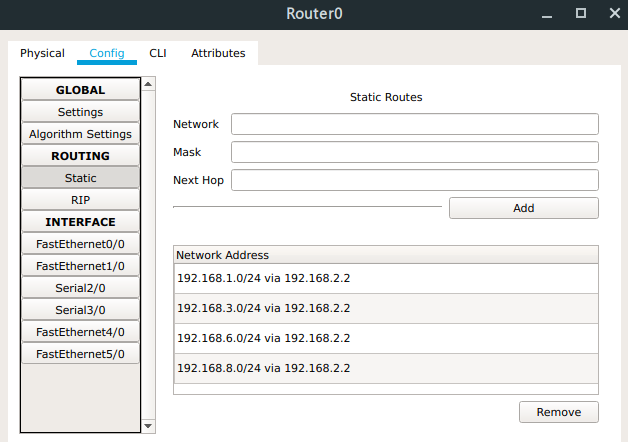


图7-1 Router0静态路由表配置

1. Router1

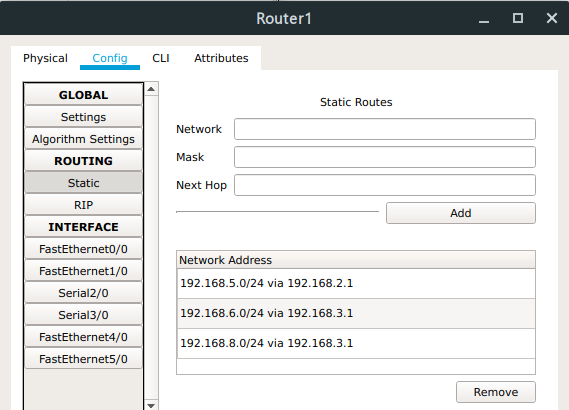


图7-1 Router1静态路由表配置

1. Router2

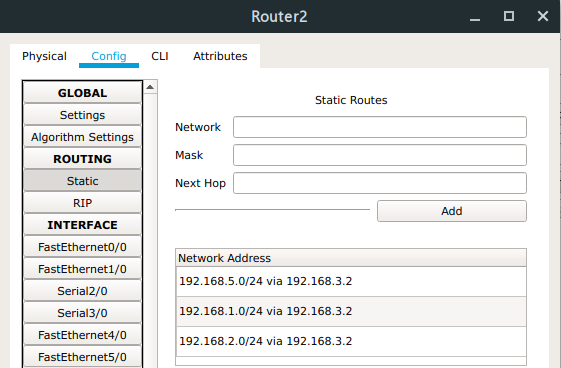


图7-1 Router2静态路由表配置

## 7.5 实验结果

### 7.5.1 任务一： 观察本地域名解析过程

1. 步骤 1： 在 PC 的浏览器窗口请求内部 Web 服务器的网页
2. 步骤 2： 捕获 DNS 事件并分析本地域名解析过程
   1. 分析本地 DNS 服务器的域名解析过程；
      1. NS服务器接收到PC0的请求www.x.cn后，本地存在目标的解析
      2. 封装DNS响应报文回复PC0
   2. 分析 DNS 的响应报文的组成；

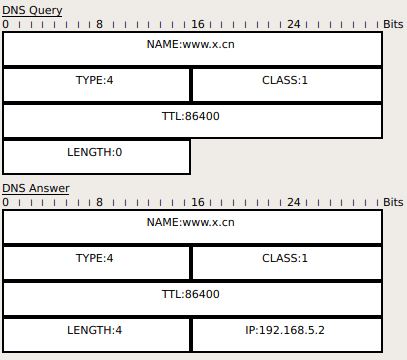


图7-1 DNS响应报文

* 1. 记录 DNS 首部中的查询记录数（QDCOUNT） 及应答记录数（ANCOUNT）；

QDCOUNT=1

ANCOUNT=1

* 1. 记录 DNS QUERY（DNS 查询）及 DNS ANSWER（DNS 应答）部分各字段的值及含义。



查询类型：4

查询类：通常为1，表明是Internet数据(IN)

TTL:86400

Data Length:4

Address:192.168.5.2

### 7.5.2 任务二： 观察外网域名解析过程

1. 步骤 1： 在 PC 的浏览器窗口请求外部 Web 服务器的网页
2. 步骤 2： 捕获 DNS 事件并分析外网域名解析过程

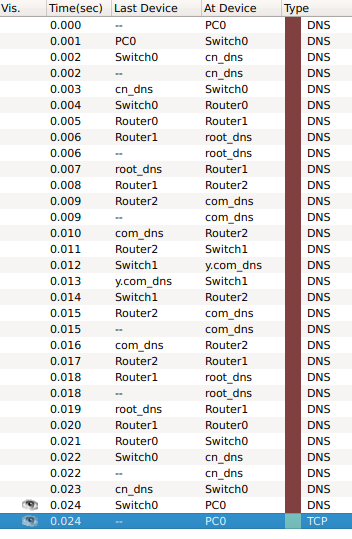


图7-1 外网域名解析过程图

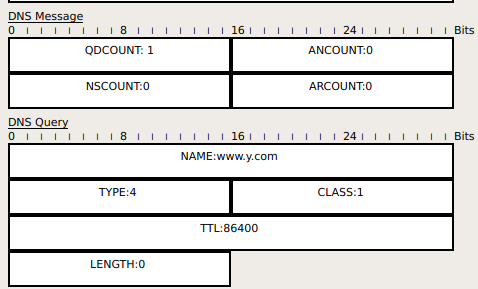


图7-1 问询DNS报文图

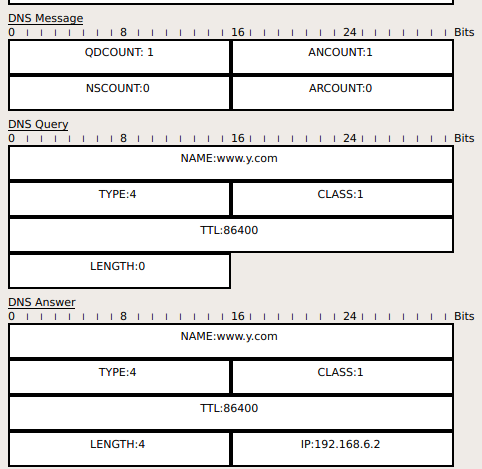


图7-1 y.com\_dns回复com\_dns报文图

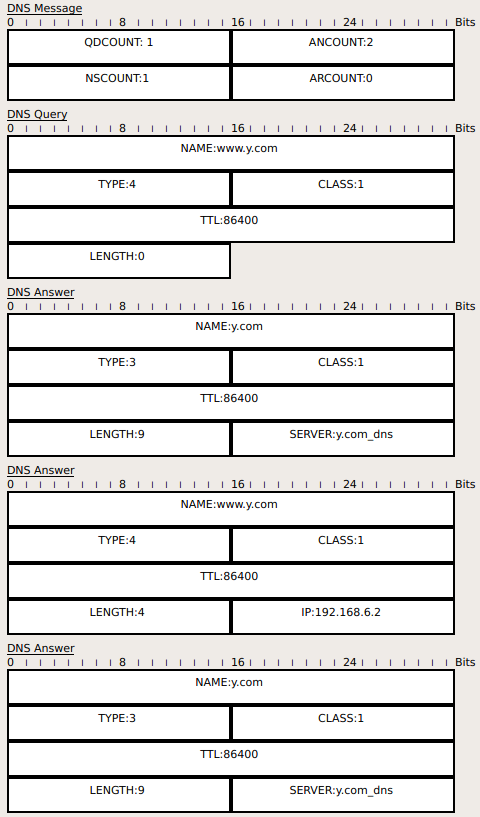


图7-1 com\_dns回复root\_dns报文图

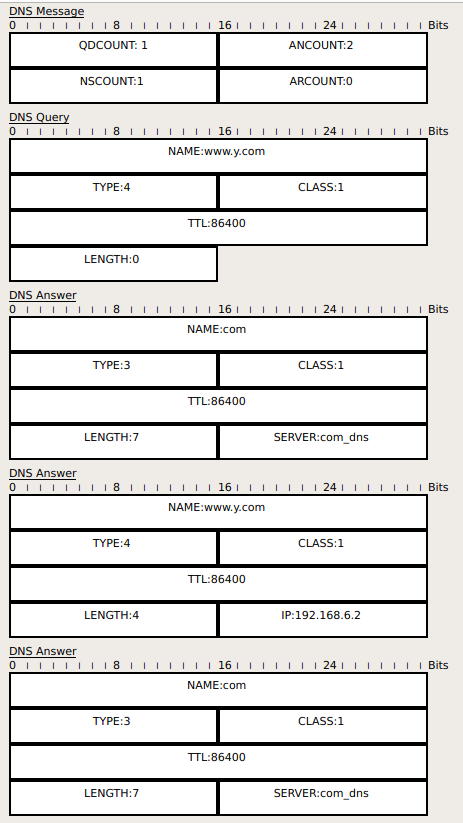


图7-1root\_dns回复cn\_dns报文图

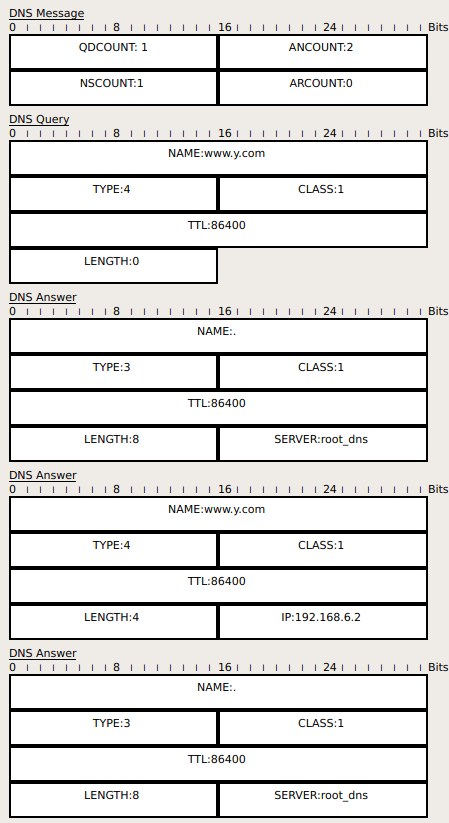


图7-1cn\_dns回复PC0报文图

* 1. 分析 DNS 服务器之间的域名解析过程；

为递归查询

* + 1. 主机192.168.5.1先向顶级域名服务器 cn\_dns (192.168.5.3)进行递归查询，此时充当本地域名服务器
    2. 本地域名服务器采用递归查询，向root\_dns根域名服务器进行查询
    3. 根域名服务器root\_dns问询顶级域名服务器com\_dns
    4. 顶级域名服务器com\_dns向本地服务器y.com\_dns进行问询，获取IP地址
    5. 本地服务器y.com\_dns回复顶级域名服务器com\_dns，com\_dns进行缓存，并产生回复报文
    6. 顶级域名服务器com\_dns回复根域名服务器root\_dns，root\_dns进行缓存，并产生回复报文
    7. 根域名服务器root\_dns回复顶级域名服务器cn\_dns，cn\_dns进行缓存，并产生回复报文
    8. 顶级域名服务器cn\_dns回复PC0
  1. 各个 DNS 应答报文的首部中查询记录数（QDCOUNT）及应答记录数（ANCOUNT）是否一样；

表7-1 查询记录数（QDCOUNT）及应答记录数（ANCOUNT）表

|  |  |  |  |
| --- | --- | --- | --- |
| SRC | DST | QDCOUNT | ANCOUNT |
| PC0 | cn\_dns | 1 | 0 |
| cn\_dns | root\_dns | 1 | 0 |
| root\_dns | com\_dns | 1 | 0 |
| com\_dns | y.com\_dns | 1 | 0 |
| y.com\_dns | com\_dns | 1 | 1 |
| com\_dns | root\_dns | 1 | 2 |
| root\_dns | cn\_dns | 1 | 2 |
| cn\_dns | PC0 | 1 | 2 |

* 1. 不同的 DNS ANSWER（DNS 应答） 中各字段的值及含义。

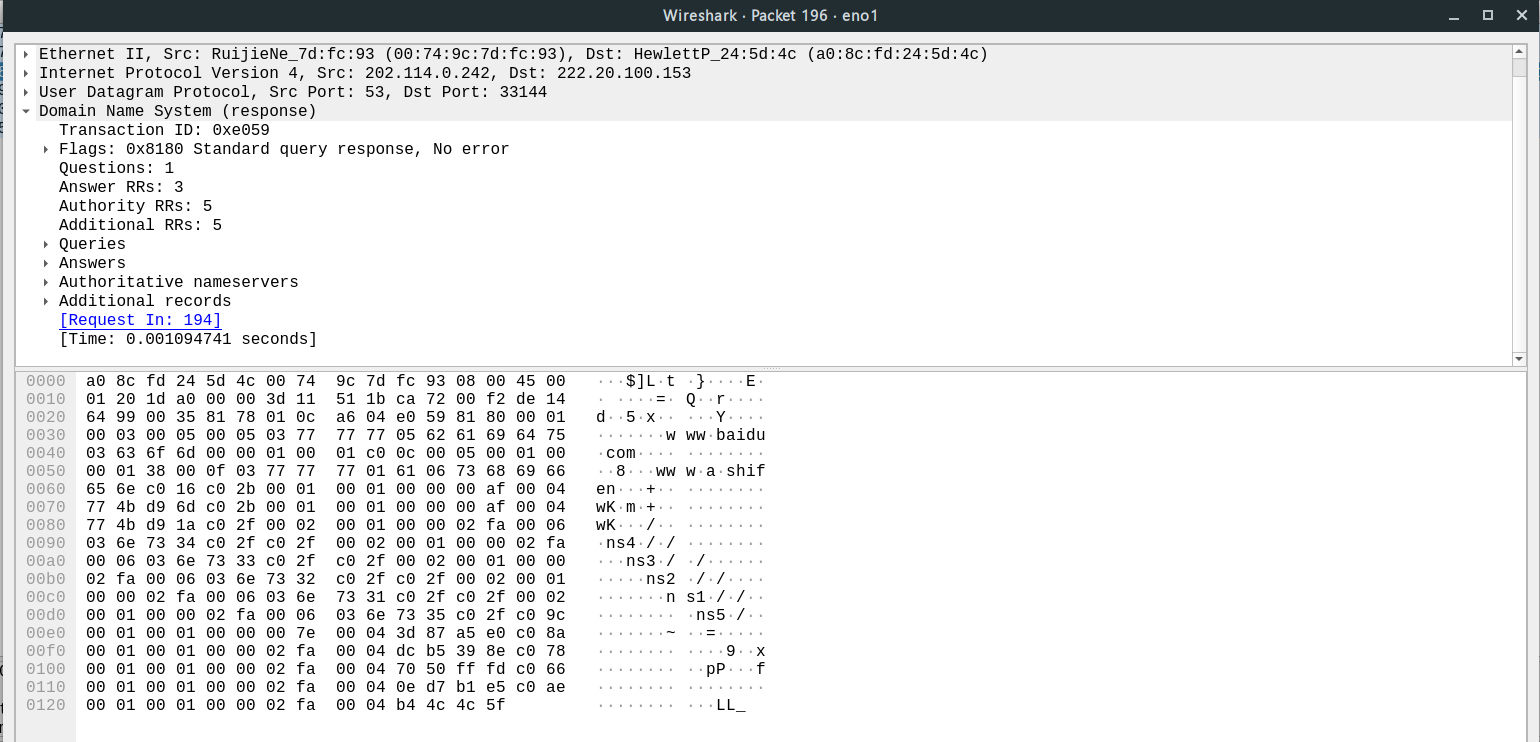
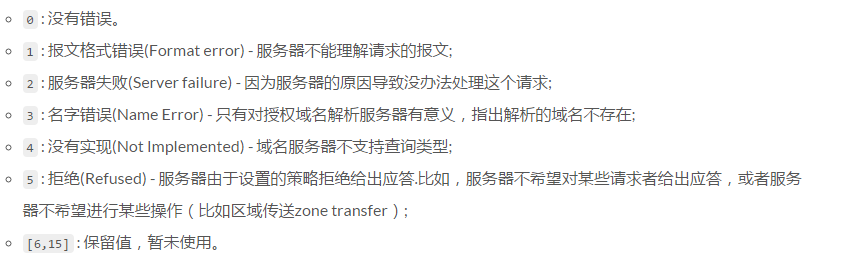


图7-1 ping [www.baidu.com](http://www.baidu.com) DNS回复报文

1. ID: 2个字节(16bit)，标识字段，客户端会解析服务器返回的DNS应答报文，获取ID值与请求报文设置的ID值做比较，如果相同，则认为是同一个DNS会话。

Transaction ID: 0xe059

1. FLAGS: 2个字节(16bit)的标志字段。包含以下属性:
   1. QR: 0表示查询报文，1表示响应报文;
   2. opcode: 通常值为0（标准查询），其他值为1（反向查询）和2（服务器状 态请求）,[3,15]保留值;
   3. AA: 表示授权回答（authoritative answer）– 这个比特位在应答的时候才有意义，指出给出应答的服务器是查询域名的授权解析服务器;
   4. TC: 表示可截断的（truncated）–用来指出报文比允许的长度还要长，导致被截断;
   5. RD: 表示期望递归(Recursion Desired) – 这个比特位被请求设置，应答的时候使用的相同的值返回。如果设置了RD，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;
   6. RA: 表示支持递归(Recursion Available) – 这个比特位在应答中设置或取消，用来代表服务器是否支持递归查询;
   7. Z : 保留值，暂未使用;
   8. RCODE: 应答码(Response code) - 这4个比特位在应答报文中设置，代表的含义如下:



Flags: 0x8180 Standard query response, No error

1. QDCOUNT: 无符号16bit整数表示报文请求段中的问题记录数。

Questions: 1

1. ANCOUNT: 无符号16bit整数表示报文回答段中的回答记录数。

Answer RRs: 3

1. NSCOUNT: 无符号16bit整数表示报文授权段中的授权记录数。

Authority RRs: 5

1. ARCOUNT: 无符号16bit整数表示报文附加段中的附加记录数。

Additional RRs: 5

1. Queries

www.baidu.com: type A, class IN

Name: [www.baidu.com](http://www.baidu.com)

Type: A (Host Address) (1)

Class: IN (0x0001)

1. Answers

www.baidu.com: type CNAME, class IN, cname [www.a.shifen.com](http://www.a.shifen.com)

www.a.shifen.com: type A, class IN, addr 119.75.217.109

www.a.shifen.com: type A, class IN, addr 119.75.217.26

1. Authoritative nameservers
2. Additional records

### 7.5.3 任务三： 观察缓存的作用

1. 步骤 1： 查看本地域名服务器 cn\_dns 的缓存
2. 步骤 2： 在 PC 的浏览器窗口请求外部 Web 服务器的网页

### 思考

1. 除了 PC 需要配置 DNS Server 外， Web 服务器是否需要 DNS Server 配置？ 如果需要，为什么？

不需要需要，如果是Web的link指向其他地址，或者需要直接访问其他域 名的资源，但通常此过程交给客户端的浏览器解决，所以通常不需要

1. 路由器之间采用串口连接， 路由器为什么要采用这种连接方式。 查阅资料了解串口连接的优缺点。
   1. 串口：专为广域网设计，它可以做ISDN,PPP,帧中继等网络类型的连接可以接很多网络类型，要使用它必须设置时钟频率（DCE、DTE），路由表的算法也在此接口上形成。

在路由器的广域网连接中，应用最多的端口：“高速同步串口”（SERIAL）

在企业网之间有时也通过DDN或X.25等广域网连接技术进行专线 连接。这种同步端口一般要求速率非常高，因为一般来说通过这种 端口所连接的网络的两端都要求实时同步。

* 1. 以太网口是对局域网内的，它只有拥有局域网所需要的所有功能。没有广域网接口所需要的功能，而广域网串口也没有局域网以太网口接口的功能，两个接口是不能对调的

而在实际个人使用中，更多的使用串口线做路由的管理。

1. DNS 协议使用运输层的什么协议？

UDP

1. DNS 缓存有什么作用？ 在 Packet Tracer 中如何清空 DNS 缓存？

缓存最近访问的域名，在下次查找时不用进行递归或迭代查询，从而提高 DNS的查询效率。

DNS Service->DNS cache->clean cache

1. 本实验中 PC 与本地域名服务器cn\_dns之间的解析是递归还是迭代？ 本地域名服务器cn\_dns与根域名服务器root\_dns之间呢？ 若后者用另一种解析方法， 则域名服务器之间DNS的请求和应答的交互过程应如何？

递归查询。

若为迭代查询，每次将下一次需要查询的地址返回给本地DNS服务器，由本地DNS进行逐级问询，在此过程中，问询路径上的DNS服务器无法对最终的目的地址进行缓存。

## 7.6 实验中的问题及心得

本次实验模拟了最终DNS在网络中的解析过程，涉及到子网的配置，路由static配置和DNS服务器的配置。

而在实际的环境中，可以使用nslookup查看DNS解析情况，并使用dig +trace <domain> 查看详细的解析过程，追踪每一步的DNS过程。

而对于DNS其中，发现存在CNAME(别名)，MX(邮件)等其他的设置，在实际的使用中，可以基于DNS实现服务器的负载均衡化，对于同一个服务器资源访问，维护DNS服务器池进行论询，是一种不用知道服务器实际运行状况的有效的均衡化方式。

实验过程中，发现DNS Server中返回的报文存在两份，考虑PacketTracer报文解析存在一定的问题，故使用TraceRoute进行报文的解析。

本次实验对于DNS的报文字段设计有了更深的理解，同时体会其设计思想，DNS为了维护对于特定报文匹配的回复，采用1QNA的回复方式，进行对应问题的匹配，而不会造成DNS问询过多而混淆。