# 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 |
| --- | --- | --- | --- |
| | | | |

教师评语：

# 一 实验环境

1. 实验环境：运行 Arch Linux x86_64 操作系统的 PC 机一台
2. PacketTracer 版本：7.0.0.0202

# 二 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。

# 三 实验内容及步骤

## 3.1 网络拓扑配置

打开 PacketTracker，配置网络拓扑如下图。

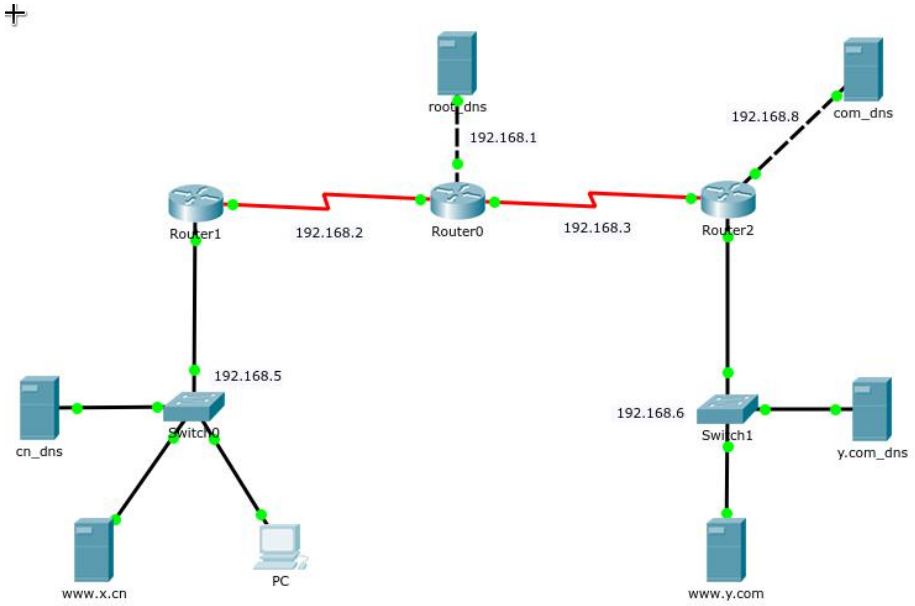


图 1 网络拓扑配置

其中，各台主机 IP 地址配置如下表：

表 1 实验拓扑中各台设备 IP 地址

| 设备 | IP 地址 |
|---|---|
| cn_dns | 192.168.5.1 |
| www.x.cn | 192.168.5.2 |
| PC | 192.168.5.3 |
| root_dns | 192.168.1.1 |

| | |
|---|---|
| y.com_dns | 192.168.5.1 |
| www.y.com | 192.168.5.2 |
| com_dns | 192.168.8.1 |

接着为三台路由器配置网口 IP 值以及路由转发表，配置完成之后打开网口，可以看到所有的指示灯变成绿色，网络拓扑配置完毕。

### 3.2 观察本地域名解析过程

首先点击 Simulation，进入模拟模式。

点击 PC/Desktop，点击浏览器 Web Browser，输入域名 www.x.cn/index.html，观察 DNS 报文的发送和 DNS 解析的过程。

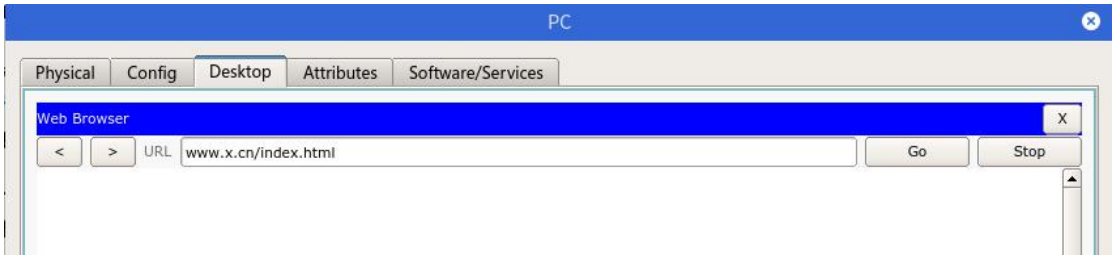


图 2 浏览器输入域名 www.x.cn/index.html

完成后，单击 Reset Simulation，重置模拟，将原有事件全部清空，同时关闭 PC 的 Web Browser 窗口。

### 3.3 观察外网域名解析过程

重新打开 PC 的 Web Browser，输入外网域名 www.y.com/index.html，再次观察 DNS 报文的发送和域名解析的过程。

完成后，仍然重置模拟，同时关闭 PC 的 Web Browser 窗口。

### 3.4 观察 DNS 缓存的作用

重复 3.3 步骤，在已有 DNS 缓存的情况下，观察此次外网域名解析的过程，并分析 DNS 的作用。

## 四 实验结果

### 4.1 观察本地域名解析过程

当在浏览器中输入域名之后，Event List 中出现一个 DNS 报文，不断点击 Capture/Forward 按钮，一步步观察报文发送的步骤，当浏览器显示出请求的网页之后，捕获到的 Event List 如下图：

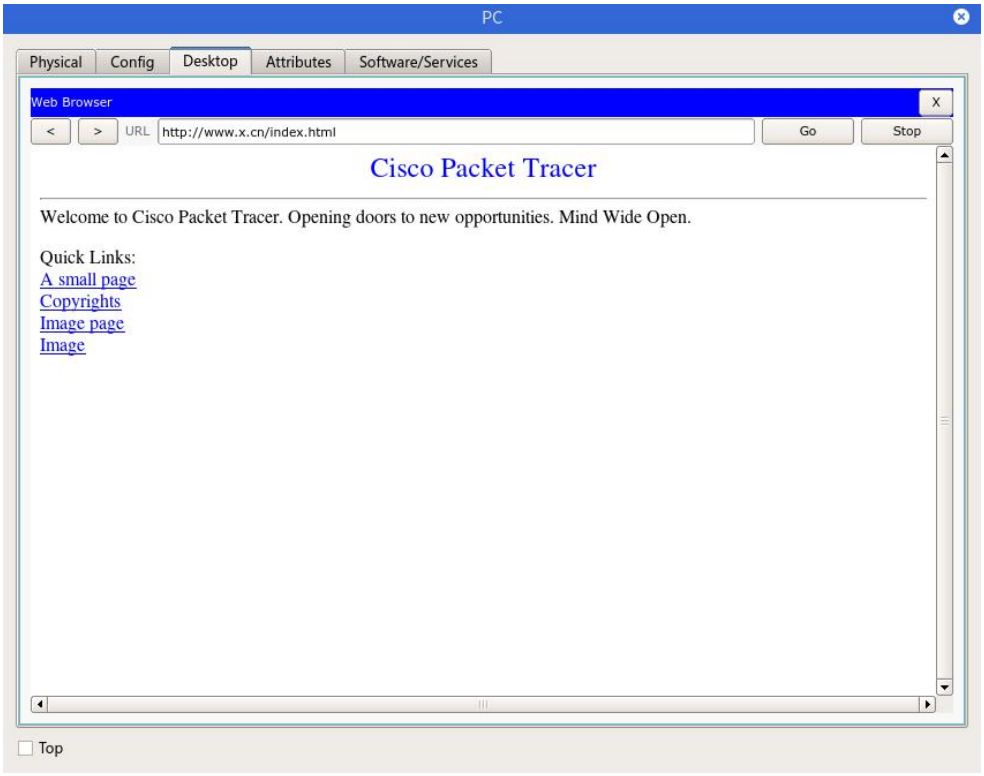


图 3 浏览器显示网页

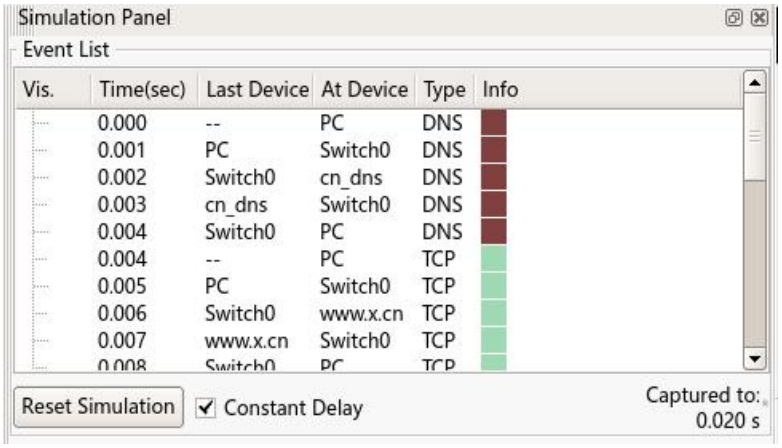


图 4 浏览器显示网页

从 Event List 中，我们可以看到，报文发送的过程如下：（忽略 ARP）

1. PC -> cn_dns，DNS，PC 从本地 DNS 服务器查询域名。

2. cn_dns -> PC，DNS，本地 DNS 服务器在本地文件中找到了对应域名的记录，返回查询的结果给 PC。

3. PC -> www.x.cn，TCP，PC 已经从 DNS 服务器知道了网站服务器的 IP 地址，于是就可以和网站服务器之间建立 TCP 连接了。

DNS 查询报文和响应报文如下图：

UDP

| 0 | 16 | 31 Bits |
|---|---|---|
| SRC PORT: 1029 | DEST PORT: 53 | |
| LENGTH: 0x20 | CHECKSUM: 0x0 | |
| DATA (VARIABLE) | | |

DNS Header

| 0 1 | 5 | 8 9 | 12 | 15 Bits |
|---|---|---|---|---|
| ID | | | | |
| OPCODE | AA TC RD RA | | Z | RCODE |
| QDCOUNT: 1 | | | | |
| ANCOUNT: 0 | | | | |
| NSCOUNT: 0 | | | | |
| ARCOUNT: 0 | | | | |

DNS Query

| 0 | 16 | 31 Bits |
|---|---|---|
| NAME: www.x.cn | | |
| TYPE: 0x0001 | CLASS: 0x0001 | |

图 5 DNS 请求报文

UDP

| 0 | 16 | 31 Bits |
|---|---|---|
| SRC PORT: 53 | DEST PORT: 1029 | |
| LENGTH: 0x36 | CHECKSUM: 0x0 | |
| DATA (VARIABLE) | | |

DNS Header

| 0 1 | 5 | 8 9 | 12 | 15 Bits |
|---|---|---|---|---|
| ID | | | | |
| OPCODE | AA TC RD RA | | Z | RCODE |
| QDCOUNT: 1 | | | | |
| ANCOUNT: 1 | | | | |
| NSCOUNT: 0 | | | | |
| ARCOUNT: 0 | | | | |

DNS Query

| 0 | 16 | 31 Bits |
|---|---|---|
| NAME: www.x.cn | | |
| TYPE: 0x0001 | CLASS: 0x0001 | |

DNS Answer

| 0 | 16 | 31 Bits |
|---|---|---|
| NAME: www.x.cn | | |
| TYPE: 0x0001 | CLASS: 0x0001 | |
| TTL: 86400 | | |
| LENGTH: 4 | ADDRESS: 192.168.5.2 | |
| ... | | |

图 6 DNS 响应报文

DNS 响应报文中，包括请求报文的全部内容，还包括 TTL（缓存在主机上的时间），LENGTH（数据长度），ADDRESS（域名对应的 IP 地址）。

在 DNS 首部中，查询记录数 QDCOUNT 为 1，应答记录数 ANCOUNT 为 1。

## 4.5 观察外网域名解析过程

重新观察 PC 请求 www.y.com/index.html 的过程，根据捕获到的 Event List，分析 DNS 服务器之间的域名解析的过程如下：

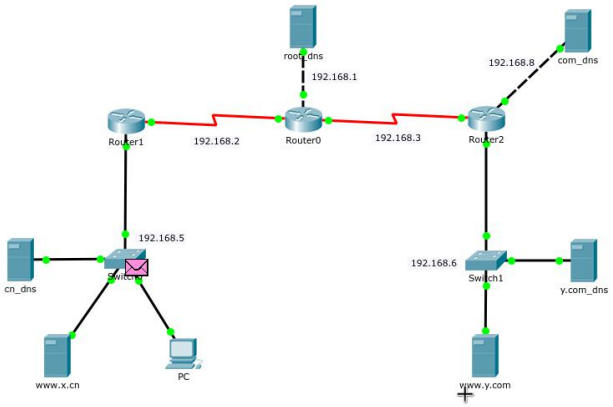


图 7 网络拓扑

1. PC -> cn_dns，DNS，PC 向其 DNS 服务器查询域名。

2. cn_dns -> root_dns，DNS，本地 DNS 服务器 cn_dns 发现无法解析这个域名，在本地文件中找到根 DNS 服务器的记录，于是向根 DNS 服务器请求查询。

3. root_dns -> com_dns，DNS，根 DNS 服务器 root_dns 收到 cn_dns 发来的 DNS 查询请求之后，在本地文件中未能直接解析出域名 www.y.com，但找到能解析.com 域名的顶级域名服务器 com_dns，于是 root_dns 向 com_dns 发送 DNS 查询。

4. com_dns -> y.com_dns，DNS，顶级域名服务器 com_dns 收到 DNS 查询请求之后，在本地文件中未能直接解析出域名 www.y.com，但找到能解析 y,com 后缀的权威域名服务器 y.com_dns，于是 com_dns 向 y.com_dns 发送 DNS 查询。

5. y.com_dns -> com_dns，DNS，权威域名服务器 y.com_dns 收到 DNS 查询周，在本地文件中找到了对应域名的记录，将查询结果写入应答报文中返回给 com_dns。

6. com_dns -> root_dns，DNS，com_dns 收到 DNS 应答报文之后，取出查询结果并写入应答报文中返回给 root_dns。

7. root_dns -> cn_dns，DNS，根 DNS 服务器 root_dns 收到 DNS 应答报文之后，取出查询结果并写入应答报文中返回给 cn_dns。

8. cn_dns -> PC，DNS，本地 DNS 服务器 cn_dns 收到 DNS 应答报文之后，取出查询结果并写入应答报文中返回给 PC。

9. PC -> www.y.com，TCP，PC 和网站服务器建立 TCP 连接。

记录各个 DNS 应答中字段的值，结果如下图：

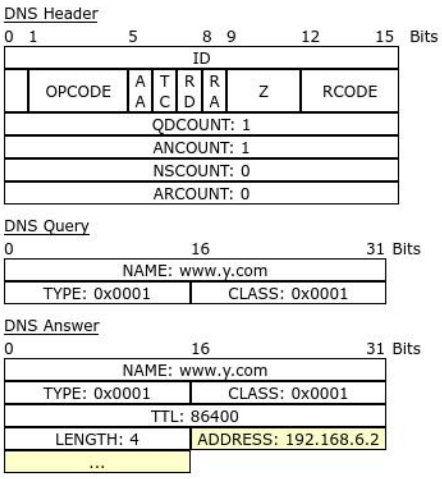


图 8 DNS：y.com_dns 返回

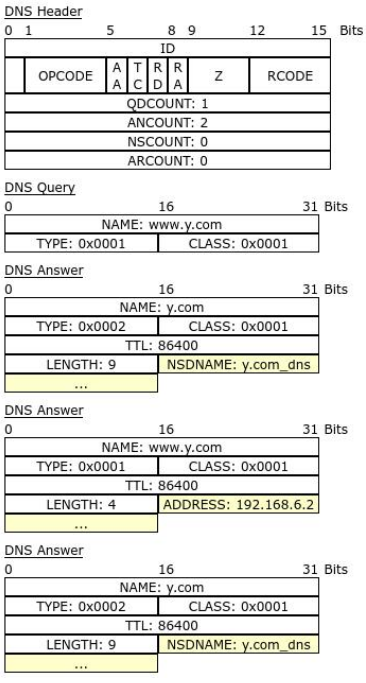


图 9 DNS：com_dns 返回

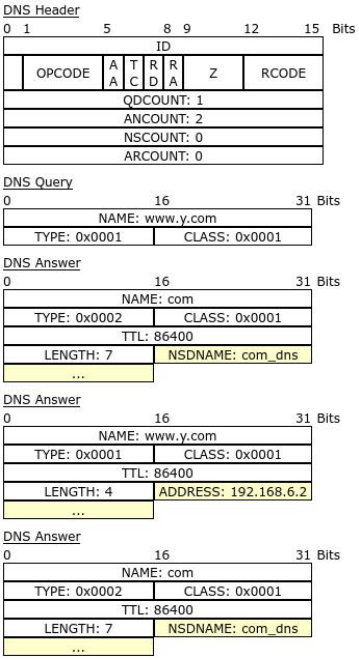


图 10 DNS：root_dns 返回

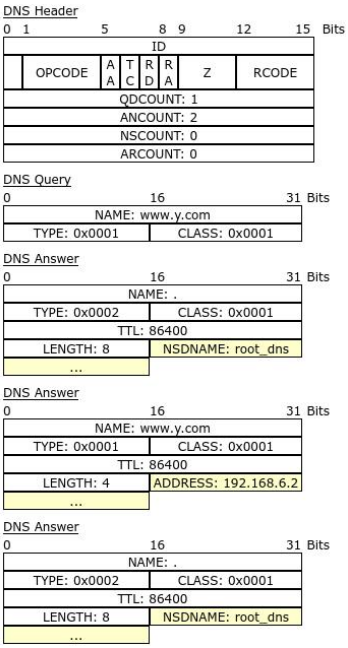


图 11 DNS：cn_dns 返回

观察发现，不同 DNS 应答报文的首部中查询记录数（QDCOUNT）及应答记录数（ANCOUNT）不一样，第一个报文只有一个应答，后面的几个报文内容都有两个应答条目。

我们再记录下各个 DNS 服务器内的 DNS 缓存作对比，如下图：

DNS Cache Table for cn_dns

| Name | Record Type | Record Value | Time stamp |
|---|---|---|---|
| com | NS | server: com_dns | 周二 11月 6 11:39:43 2018 |
| www.y.com | A | IP:192.168.6.2 | 周二 11月 6 11:39:43 2018 |

图 12 cn_dns 内的 DNS 缓存

DNS Cache Table for root_dns

| Name | Record Type | Record Value | Time stamp |
|---|---|---|---|
| www.y.com | A | IP:192.168.6.2 | 周二 11月 6 11:39:43 2018 |
| y.com | NS | server: y.com_dns | 周二 11月 6 11:39:43 2018 |

图 13 root_dns 内的 DNS 缓存

DNS Cache Table for com_dns

| Name | Record Type | Record Value | Time stamp |
|---|---|---|---|
| www.y.com | A | IP:192.168.6.2 | 周二 11月 6 11:39:35 2018 |

图 14 com_dns 内的 DNS 缓存

将 DNS 缓存表和应答报文对比就发现，缓存的条目刚好就是应答报文中有的几个条目。

其中 NS 类型指 Name Server，用来指定该域名由哪个 DNS 服务器来解析，A 类型值 Address，即指定主机名（或域名）对应的 IP 地址记录。

查阅资料可知，DNS 各字段的含义如下：

QR（1bit）：查询/响应标志，0 为查询，1 为响应。

opcode（4bit）： 0 表示标准查询，1 表示反向查询，2 表示服务器状态请求。

AA（1bit）：表示授权回答。

TC（1bit）：表示可截断的。

RD（1bit）：表示期望递归。

RA（1bit）：表示可用递归。

Z（3bit）：用 0 填充的位。

RCODE（4bit）：表示返回码，0 表示没有差错，3 表示名字差错，2 表示服务器错误（Server Failure）。

QDCOUNT（16bit）：表示查询记录数。

ANCOUNT（16bit）：表示应答记录数。

NSCOUNT（16bit）：表示授权区域数。

ARCOUNT（16bit）：表示附加区域数。

## 4.6 观察 DNS 缓存的作用

重复上一个步骤，在已有 DNS 缓存的情况下，请求 www.y.com/index.html，观察到如下的结果：

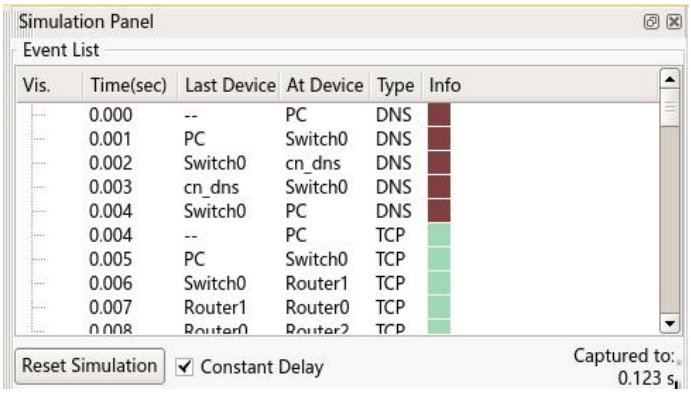


图 15 Event List

此时，PC 只向本地 DNS 服务器发送了一个 DNS 查询，就获取了网站服务器的 IP 地址，这是因为根据图 12 中的 DNS 缓存表，PC 就直接获了 www.y.co

m 的 IP 地址。

# 五 实验中的问题及心得

## 5.1 实验中的问题

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，因为 Web 服务器是一种被动接受主机连接的服务器，不需要自己去向其他的域名请求数据，因此不需要配置 DNS Server。

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。

路由器之间采用串口连接和用以太网口连接相比保密性和可靠性较高，但速度不如以太网口连接。

3. DNS 协议使用运输层的什么协议？

UDP 协议。

4. DNS 缓存有什么用？在 Packet Tracer 中如何清空 DNS 缓存？

DNS 缓存用来存放最近解析过的域名信息，如果又需要查询同一个域名，就可以快速的返回查询结果，提高解析的效率。清空缓存时，可以进入该 DNS 服务器的 Config 窗口，点击窗口下方的 DNS Cache 按钮，在弹出的窗口中单击下方的 Clear Cache 俺就即可把 DNS 缓存清空。

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，则域名服务器之间的 DNS 请求和应答的交互过程应如何？

本实验中 PC 与本地域名服务器 cn_dns 之间的解析的递归查询，本地域名服务器 cn_dsn 与根域名服务之间的解析也是递归查询。

如果是另一种解析方法，则当 root_dns 查询到下一步该向谁查询时，会让 cn_dns 自己向目标进行查询。

## 5.2 实验总结

通过本次实验，我理解了 DNS 系统的工作原理，熟悉了 DNS 的工作过程以及 DNS 报文格式，同时也更加熟练了网络拓扑的 IP 配置，路由器转发表配置，把以前几次实验中还有没有搞懂的地方都解决了。