# 实验七 应用层实验

1. 选择DNS服务器第一次向Internet发出的DNS请求报文和对应的DNS应答报文（注意DNS报文的DNS协议树中有一个Transaction ID字段，这两个报文的此字段值肯定相同），将两条报文信息填入下表：

|  |  |  |  |
| --- | --- | --- | --- |
| No. | Source | Destination | Info. |
| 1 | 10.0.0.12 (PCB) | 10.0.0.11(DNS) | Transaction ID: 0x2c2e, Questions: 1, Answer RRs: 0, Authority RRs: 0, Additional RRs: 0, Flags: 0x0100 Standard query |
| 2 | 10.0.0.11(DNS) | 10.0.0.12 (PCB) | Transaction ID: 0x2c2e, Flags: 0x8180 Standard query response, No error, Questions: 1, Answer RRs: 4, Authority RRs: 4, Additional RRs: 8 |

查找DNS服务器的缓存，写出域名和IP地址对：

[www.buaa.edu.cn](http://www.buaa.edu.cn),

1. 客户机向本地DNS服务器发送的查询报文中Flags字段中Recursion desired位置1，表示使用递归查询；本地DNS服务器向Internet中的DNS服务器发送的查询报文中Flags字段中Recurion desired置0，表示使用迭代查询。试结合递归查询和迭代查询的特点分析这样做的原因：

1. DNS应答报文的协议树字段中应该包括“Queries”、“Answers”、“Authoritative nameservers”、“Additional records”四个字段，每个字段中会有多个相同的子协议树。

“Queries”字段中的一个子协议树，总的信息： www.buaa.edu.cn: type A, class IN

|  |  |  |  |
| --- | --- | --- | --- |
| 字段名 | 字段值 | 字段长度 | 字段信息 |
| Name | 4 | 15 | www.buaa.edu.cn |
| Type |  |  | A (Host Address) (1) |
| class |  | 16 Bit | IN |

“Answers” 字段所表达的信息：

* www.buaa.edu.cn: type A, class IN, addr 10.200.21.19

“Authoritative nameservers”字段所表达的信息：

* buaa.edu.cn: type NS, class IN, ns ns1.buaa.edu.cn
* buaa.edu.cn: type NS, class IN, ns ns2.buaa.edu.cn

“Additional records”字段所表达的信息：

* ns1.buaa.edu.cn: type A, class IN, addr 202.112.128.51
* ns2.buaa.edu.cn: type A, class IN, addr 202.112.128.50

1. 对比DNS请求报文和DNS应答报文，回答下面问题：

(1)．DNS客户端如何和DNS服务器协商是否使用递归查询？

(2)．对比DNS请求报文，DNS应答报文中多了那些字段？这些字段传递什么信息？

1. 根据DNS解析过程的分析，填写下表：

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **序号** | **类型** | **Source** | **Destination** | **主要内容（请求查询/应答返回）** | **查询类型** |
| 1 | 请求 | 10.0.0.12 | 10.0.0.11 | 请求查询(Standard query 0xfe4d A www.google.com) | IN |
| 2 |  | 10.0.0.11 | 10.0.0.12 | 应答返回（Standard query response 0xfe4d A [www.google.com](http://www.google.com) A 172.217.161.164） | IN |
| 3 |  | 10.0.0.12 | 10.0.0.11 | 请求查询（Standard query 0x7b11 A [www.buaa.edu.cn](http://www.buaa.edu.cn) ） |  |
| 4 |  | 10.0.011 | 128.9.0.107 |  |  |
| 5 |  | 128.9.0.107 | 10.0.011 |  |  |
| 6 |  | 10.0.011 | 10.0.0.12 |  |  |
| 7 |  |  |  |  |  |
| 8 |  |  |  |  |  |
| 9 |  |  |  |  |  |
| 10 |  |  |  |  |  |
| 11 |  |  |  |  |  |
| 12 |  |  |  |  |  |
| 13 |  |  |  |  |  |
| 14 |  |  |  |  |  |

(1).从报文②得知，DNS服务器所请求的根域名服务器IP地址为\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_。

(2).分析报文③，找出DNS服务器向哪一个.cn域名服务器发出请求报文，并写出它的域名和IP地址

(3).写出www.buaa.edu.cn的本地授权域名服务器的域名和IP地址：

|  |  |
| --- | --- |
| www.buaa.edu.cn的本地授权域名服务器 | IP地址 |
|  |  |
|  |  |

(4). 简述DNS域名解析的过程

。

1. DNS使用哪种传输层协议？为什么使用这种协议？

* DNS在进行区域传输的时候使用TCP协议，其它时候则使用UDP协议。UDP报文的最大长度为512字节，而TCP则允许报文长度超过512字节。
* 区域传送时使用TCP，主要有一下两点考虑：   
  1.辅域名服务器会定时（一般时3小时）向主域名服务器进行查询以便了解数据是否有变动。如有变动，则会执行一次区域传送，进行数据同步。区域传送将使用TCP而不是UDP，因为数据同步传送的数据量比一个请求和应答的数据量要多得多。   
  2.TCP是一种可靠的连接，保证了数据的准确性。
* 域名解析时使用UDP协议：   
  客户端向DNS服务器查询域名，一般返回的内容都不超过512字节，用UDP传输即可。不用经过TCP三次握手，这样DNS服务器负载更低，响应更快。虽然从理论上说，客户端也可以指定向DNS服务器查询的时候使用TCP，但事实上，很多DNS服务器进行配置的时候，仅支持UDP查询包。

1. 分析截获报文，与《计算机网络》教材P231的图6－5所述的过程有何不同？
2. 分析HTTP协议报文：从众多http报文中选择两条报文，一条是http请求报文（即get报文），另一条是http应答报文，将报文信息填入下表：

|  |  |  |  |
| --- | --- | --- | --- |
| No. | Source | Destination | Info. |
|  |  |  |  |
|  |  |  |  |

1. 总体分析截获的数据报文，概括http协议的工作过程（从在浏览器上输入网址，到出现网页，关闭网页）。

|  |  |  |
| --- | --- | --- |
| 步骤 | 所包括的报文序号 | 主要完成的功能（目的） |
| DNS解析过程 |  |  |
| TCP连接的建立过程 |  |  |
| HTTP的传文件过程 |  |  |
| TCP连接释放过程 |  |  |

1. 在TCP连接建立好后，将按以下步骤进行SMTP传输：（参考实验原理中SMTP的工作过程）

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| SMTP连接的建立过程 | No. | Source | Destination | 报文简要信息和参数 | 报文作用 |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
| 邮件的传送过程 | No. | Source | Destination | 报文简要信息和参数 | 报文作用 |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
| SMTP连接的释放过程 | No. | Source | Destination | 报文简要信息和参数 | 报文作用 |
|  |  |  |  |  |
|  |  |  |  |  |

1. 找到含有RCPT命令的报文，并对其进行分析，并说明RCPT命令的作用是什么？
2. 分析FTP报文的格式。指出在截获的报文中含有用户名和含有密码信息的报文。并将报文信息填入下表。

|  |  |  |  |
| --- | --- | --- | --- |
| No. | Source | Destination | Info. |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

1. 根据截获的报文进行总体分析，分析FTP协议的工作过程，分析控制连接和数据连接是如何工作的。
2. 从DHCP报文中选取四条报文，分析其功能，并将报文信息填入下表。

|  |  |  |  |
| --- | --- | --- | --- |
| No. | Source | Destination | Info. |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

1. 根据截获的报文进行总体分析，分析客户端从DHCP服务器上获得IP地址的过程。