**暨南大学本科实验报告专用纸**

课程名称 计算机网络实验 成绩评定

实验项目名称 DNS 协议分析实验 指导教师 雷小林 、魏林锋

实验项目编号 实验项目类型 综合 实验地点 N117

学生姓名 陈宇 学号 2020101642

学院 信息科学技术学院 系 计算机系 专业 软件工程

实验时间 2022 年 11 月 15 日 下 午～ 11 月 15 日 下 午

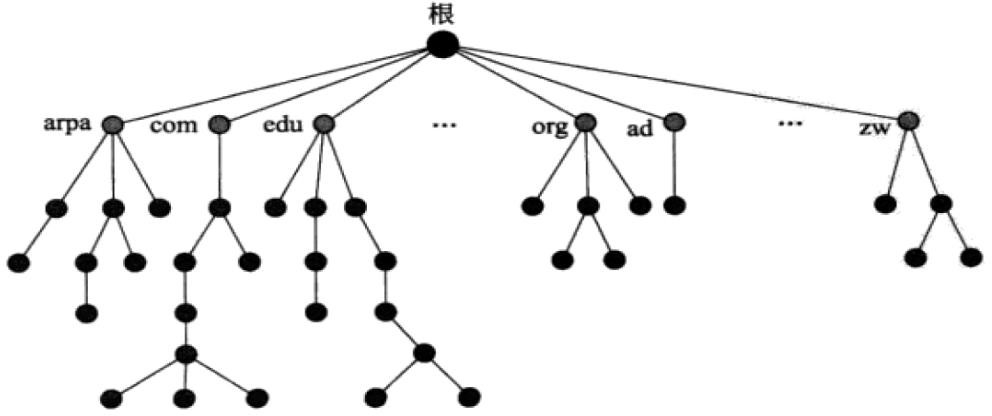
## 实验目的

1. 掌握 DNS 的报文格式
2. 掌握 DNS 的工作原理
3. 掌握 DNS 域名空间的分类
4. 理解 DNS 高速缓存的作用

## 实验原理

1. 域名空间

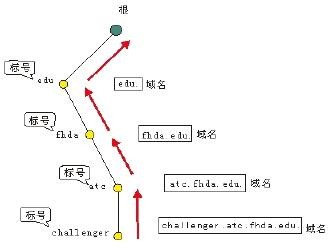
在域名空间中，名字被定义在一个根在顶部的树型结构中。这个树结构最多有 128 层：

第 0 层为根，如下图所示：

* 标号

树上的每一个节点都有一个标号，标号是一个最多有 63 个字符的字符串。根节点的标号是空字符串。每一个节点的子节点都具有不同的标号，这样就保证了域名是惟一的。

* 域名

一个完全的域名是用点“.”分隔开的标号序列。域名总是从节点标号向上读到根点标号的。因为最后一个标号是根节点的标号，所以一个完全的域名总是以空标号结束。因为空字符串表示什么也没有，所以域名的最后一个字符是一个点。下图给出了一个域名示例。

2．DNS 协议简介

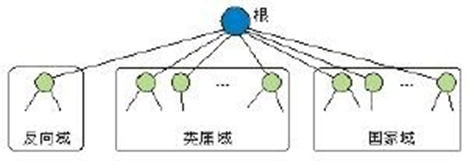
DNS 是域名系统 （Domain Name System）的缩写，是一种分层次的、基于域的命名方案，

主要用来将主机名和电子邮件目标地址映射成 IP 地址。当用户在应用程序中输入 DNS 名称

时，DNS 通过一个分布式数据库系统将用户的名称解析为与此名称相对应的 IP 地址。

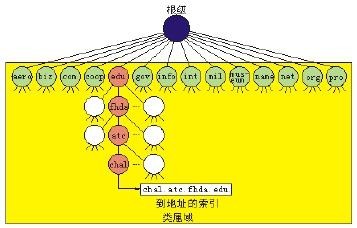
（1）DNS 的域名分类

在 Internet 中，域名空间被划分为 3 个部分：类属域、国家域和反向域，如下图所示：



* 类属域

类属域按照主机的类属行为分类。树中的每一个节点定义一个域，它是到域名空间数据库的一个索引，如下图所示：



在类属域的第一级允许有 14 个标号。这些标号描述了不同的机构类型，如下表所示：

|  |  |  |  |
| --- | --- | --- | --- |
| 标号 | 说明 | 标号 | 说明 |
| aero | 航空和航天公司 | int | 国际机构 |
| biz | 企业或商行（与“com”相 | mil | 军事机构 |
| com | 商业机构 | museum | 博物馆和其它非盈利组织 |
| coop | 协作的企业组织 | name | 人名字（个人的） |
| edu | 教育机构 | net | 网络支持中心 |
| gov | 政府机构 | org | 非盈利机构 |
| info | 信息服务提供者 | pro | 专业个体组织 |

* 国家域

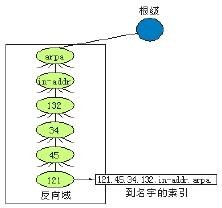
国家域使用两字符的国家或地区的缩写（例如，用 cn 代表中国）。第二级标号可以是机构的标号，或者是国家指定的标号。

* 反向域

反向域用来把一个地址映射为域名。例如，有时服务器会收到来自客户的请求，要完成一个任务。但是服务器不能确定这个客户是否在授权的客户列表中，因为只有客户的 IP 地址（从收到的 IP 数据包中提取出来的）被列出。要确定这个客户是否在授权列表中，服务器可以使用它的解析程序向 DNS 发送查询，并请求把地址映射为名字。

这种类型的查询叫做反向查询或指针（PTR）查询。要处理反向查询，在域名空间中要增加反向域，且其第一级节点叫做 arpa（由于历史原因）。第二级节点叫做 in-addr（表示反向地址）。域的其余部分为 IP 地址。

处理反向域的服务器也是分级的。这就表示地址的网络号部分要比子网号部分的等级高， 而子网号部分要比主机号部分的等级高。在与类属域和国家域相比较时，反向域看起来是反过来的，如 132.34.45.121 的 IP 地址在读出时应为 121.45.34.132.in-addr.arpa。下图是反向域配置的说明。



（2）DNS 报文格式

DNS 报文由 12 字节长的首部和 4 个长度可变的字段组成，如下图所示：

|  |  |
| --- | --- |
| 标识（16 位） | 标志（16 位） |
| 问题记录数（16 位） | 应答记录数（16 位） |
| 授权记录数（16 位） | 附加记录数（16 位） |
| 查询问题 | |
| 回答（资源记录数可变） | |
| 授权（资源记录数可变） | |
| 额外信息（资源记录数可变） | |

标识：该字段占两个字节，由客户程序设置并由服务器返回。客户程序通过它来确定响应与查询是否匹配。

标志：16 位的标志字段被划分为若干子字段，如下图所示：

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| QR | Opcode | AA | TC | RD | RA | 保留 | AD | CD | rcode |
| 1 位 | 4 位 | 1 位 | 1 位 | 1 位 | 1 位 | 1 位 | 1 位 | 1 位 | 4 位 |

标志字段的各子字段含义如下：

* + QR（查询/响应）：该位为 0 时是查询报文；为 1 时是响应报文。
  + Opcode：该位为 0 时是标准查询；为 1 时是反向查询；为 2 时是服务器状态请求。
  + AA（授权回答）：这是 1 位字段。当它设置为 1 时，表示名字服务器是权限服务器。它只用在响应报文中有效。
  + TC（截断的）：该位只在响应报文中有效，它表示响应报文被切割，因为响应报文过大而无法适用于数据包的数据部分。例如，如果响应包含大量名称服务器，数据包可能会超过允许的 MTU。这时，数据包将被切割，并且将 TC 域位设置为 1。
  + RD（要求递归）：如果目标名称服务器不包含所请求的信息，该域表示客户端请求递归查询。
  + RA（递归可用）：该域在响应中有效，它表示响应名称服务器是否提供递归查询。
  + AD（可信数据）：这位用来指定所有的数据已经被服务器认证。
  + CD（验证无效）：这位指定了没有被认证的数据对于询问者来说是可以接受的。
  + Rcode：该域长度为 4 位，用于 DNS 响应中，表示是否出现错误。问题记录数：该字段占两个字节，查询问题部分包含的条目数量。

应答记录数：该字段占两个字节，表示回答部分包含的回答记录数。在查询报文中它的值是 0。

授权记录数：该字段占两个字节，包含在响应报文的授权部分的授权记录数。在查询报文中它的值是 0。

附加记录数：该字段占两个字节，包含在响应报文的附加部分的附加记录数。在查询报文中它的值是 0。

查询问题：DNS 查询或响应报文中会有查询部分。查询部分中每个问题的格式如下图所示：

|  |  |
| --- | --- |
| 查询名 | |
| 查询类型 | 查询类 |

* + 查询名：表示要查找的名字，它是一个或多个标识符序列。
  + 查询类型：表示查询问题时的类型。最常用的查询类型是 A 类型，表示期望获得查询名的 IP 地址；而一个PTR 查询则请求获得一个 IP 地址对应的域名。
  + 查询类：表示查询的类别。其值通常是 1，表示 Internet 类型。

回答（资源记录数可变）：DNS 响应报文中会有回答部分。回答部分包括从服务器到客户（解析程序）的回答。其资源记录的格式如下图所示：

|  |  |
| --- | --- |
| 域名 | |
| 类型 | 类 |
| 生存时间 | |
| 资源数据长度 | 资源数据 |

* + 域名：表示记录中资源数据对应的名字。它的格式和查询名字字段格式相同。
  + 类型：表示资源记录的类型。它的值和查询类型的值是一样的。
  + 类：表示资源记录的类别。它的值和查询类的值是一样的。
  + 生存时间：表示客户程序保留该资源记录的秒数。
  + 资源数据长度：表示资源数据的数量。该数据的格式依赖于类型字段的值。
  + 资源数据：表示该资源数据的内容。

授权（资源记录数可变）：DNS 响应报文中会有授权部分。授权部分为该查询给出关于一个或多个授权服务器的信息（域名）。其资源记录的格式如下图所示：

|  |  |
| --- | --- |
| 域名 | |
| 类型 | 类 |
| 生存时间 | |
| 资源数据长度 | 资源数据 |

* + 域名：表示记录中资源数据对应的名字。它的格式和查询名字字段格式相同。
  + 类型：表示资源记录的类型。它的值和查询类型的值是一样的。
  + 类：表示资源记录的类别。它的值和查询类的值是一样的
  + 生存时间：表示客户程序保留该资源记录的秒数。
  + 资源数据长度：表示资源数据的数量。该数据的格式依赖于类型字段的值
  + 资源数据：表示该资源数据的内容。

额外信息（资源记录数可变）：DNS 响应报文中会有额外信息部分。额外信息部分提供有助于解析程序的附加信息。其资源记录格式如下图所示：

|  |  |
| --- | --- |
| 域名 | |
| 类型 | 类 |
| 生存时间 | |
| 资源数据长度 | 资源数据 |

* + 域名：表示记录中资源数据对应的名字。它的格式和查询名字段格式相同。
  + 类型：表示资源记录的类型。它的值和查询类型的值是一样的。
  + 类：表示资源记录的类别。它的值和查询类的值是一样的。
  + 生存时间：表示客户程序保留该资源记录的秒数。
  + 资源数据长度：表示资源数据的数量。该数据的格式依赖于类型字段的值。
  + 资源数据：表示该资源数据的内容。

（3）域名服务器和域名解析

DNS 解析程序是客户/服务器模式的应用程序。需要把地址映射为域名或把域名映射为地址的主机要调用DNS 解析程序。解析程序用映射请求找到最近的 DNS 服务器。若 DNS 服务器有这个信息，则满足解析程序的要求；否则，或者让解析程序找其它的服务器，或者再请其它服务器提供这个信息。

当解析程序收到响应后，就解释这个响应，看它是正确的解析还是错误的解析，最后把解析结果交给请求映射的进程。

* + 正向解析

通常，解析程序把域名交给服务器，请求服务器给出相应的地址，服务器检查类属域或国家域并查找映射。

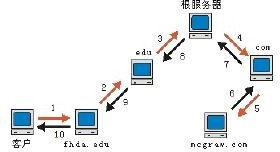
如果需要查询的域名是类属域名或国家域名，解析程序就把这个需要查询的域名发送到本地 DNS 服务器进行解析。若本地服务器不能解析这个域名，它就让解析程序再找其它的DNS 服务器，或者直接询问其它 DNS 服务器。

* + 反向解析

有时客户会要求将 IP 地址映射到相应的域名，客户把 IP 地址发送到 DNS 服务器并请求服务器映射出相应的域名，这种查询叫做反向解析，也叫做 PTR 查询。要回答这类查询， DNS 使用反向域。在请求中，IP 地址需要反过来，同时还要附上两个标号 in-addr 和 arpa， 以创建可以被反向域部分所接受的域。例如，若解析程序收到的 IP 地址是 132.34.45.121， 解析程序首先把地址反过来，并在发送前加上两个标号。 发送出的域名是“121.45.34.132.in-addr.arpa”，它由 DNS 服务器接受和解析。

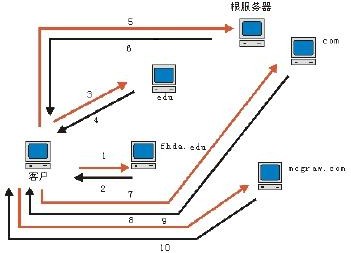
（4）递归解析和迭代解析

* + 递归解析

客户（解析程序）可以向域名服务器请求递归回答。这就表示解析程序期望服务器提供最终解答。若服务器是这个域名的权限服务器，就检查它的数据库并作出响应。若服务器不是权限服务器，它就将请求发送给另一个服务器（通常是父服务器）并等待响应。若父服务器是权限服务器，则响应；否则，就将查询再发送给另一个服务器。当查询最终被解析时， 响应就返回，直到最后到达发出请求的客户。下图给出了这个过程：

* + 迭代解析

客户（解析程序）可以向域名服务器请求迭代回答。若服务器是这个域名的权限服务器， 它就发送解答。若不是，就返回它认为可以解析这个查询的服务器的 IP 地址。客户就向第二个服务器重复查询。若新找到的服务器能够解决这个问题，就回答这个查询；否则，就向客户返回一个新的服务器的 IP 地址。现在客户必须向第三个服务器重复查询。这个过程称为迭代，客户向多个服务器重复发送同样的查询。在下图中，客户在从 mcgraw.com 服务器获得解答之前，查询了 4 个服务器。



（5）DNS 高速缓存

每个域名服务器都维护着一个高速缓存，存放最近用到过的域名信息和此记录的来源。 当客户请求域名解析时，域名服务器首先检查它是否被授权管理该域名，若未被授权，则查看自己的高速缓存，检查该域名是否最近被转换过。如果有这个域名信息，域名服务器就会将有关域名和IP 地址的绑定信息报告给客户，并标志为非授权绑定，同时给出获得此绑定的域名服务器的域名，本地域名服务器也会将该绑定通知客户。但该绑定信息可能是过时的。 根据是强调高效还是准确性，客户可以选择接受该绑定信息还是直接与该绑定信息的授权服 务器联系。

3．实验环境与说明

（1）实验设备和连接

实验设备和连接图如图 37 所示，一台锐捷 S2126G 交换机连接了 2 台 PC 机，分别命

名为主机 A、主机 B，交换机命名为 Switch。

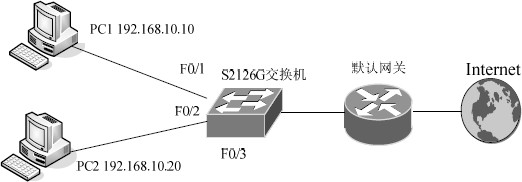


图 37 DNS 协议分析实验连接图

（2）实验分组

每六名同学为一组，其中每两人一小组，每小组各自独立完成实验。将主机 A 和 B 作为一组，主机 C 和 D 作为一组，主机 E 和 F 作为一组。现仅以主机 A、B 所在组为例， 其它组的操作参考主机 A、B 所在组的操作。

## 实验步骤

练习一、Internet 域名空间的分类

本练习一人一组，现仅以主机 A 为例，其它主机的操作参考主机 A。

**类属域**

步骤 1：将主机 A 的“首选 DNS 服务器”设置为公网 DNS 服务器，目的是能够访问 Internet。

步骤 2：主机 A 运行 Wireshark 捕获数据并设置过滤条件（提取 DNS 协议）。步骤 3：主机 A 在命令行下运行“nslookup [www.python.org](http://www.python.org/)”命令。

步骤 4：主机 A 停止捕获数据。分析主机 B 捕获到的数据及主机 A 命令行返回的结果，回答以下问题：

* + “[www.python.org](http://www.python.org/)”对应的 IP 地址是什么？

**答：146.75.112.223**

文本

描述已自动生成

* + “[www.python.org](http://www.python.org/)”域名的顶级域名的含义是什么？

**答： .org = 各类组织机构（包括非盈利团体）**

**国家域**

步骤 5：主机 A 运行 Wireshark 捕获数据并设置过滤条件（提取 DNS 协议）。

步骤 6：主机 A 在命令行下运行“nslookup [www.gd.gov.cn](http://www.gd.gov.cn/)”命令。

步骤 7：主机 A 停止捕获数据。分析主机 B 捕获到的数据及主机 A 命令行返回的结果，

回答以下问题：

* + “[www.gd.gov.cn](http://www.gd.gov.cn/)”对应的 IP 地址是什么？

文本

描述已自动生成

**答：120.197.33.11**

* + “[www.gd.gov.cn](http://www.gd.gov.cn/)”域名的顶级、二级、三级域名的含义是什么？

答：**.cn = 中国域名**

**.gov = 政府部门**

**.gd = 广东省**

反向域

步骤 8：将主机 A 的“首选 DNS 服务器”设置为 DNS 服务器的 IP 地址（按所在环境实际情况来配置或者自动获取）。

步骤 9：主机 A 运行 Wireshark 捕获数据并设置过滤条件（提取 DNS 协议）。步骤 10：主机 A 在命令行下运行“nslookup 8.8.8.8”命令。

步骤 11：主机 A 停止捕获数据。分析主机 A 捕获到的数据及主机 A 命令行返回的结果，

回答以下问题：

* + 8.8.8.8 对应的域名是什么？

文本

描述已自动生成

答：dns.google

* + 反向域的顶级、二级域名分别是什么？

答：**.google = 谷歌公司**

**.dns = dns服务器**

练习二、查看DNS 查询请求

步骤 1： 将主机 A 的“首选 DNS 服务器”设置为 DNS 服务器的 IP 地址（按所在环境实际情况来配置或者自动获取）。

步骤 2：利用 ipconfig /flushdns 命令清空主机 A 上的 DNS 缓存。

步骤 3 ： 在主机 A 启动 Wireshark ， 设置主机 A 的截获条件为通过主机 IP： “ip.addr==your\_IP\_address”，开始截获报文。

步骤 4：在主机A 上打开命令行窗口，执行nslookup –type=NS jnu.edu.cn。

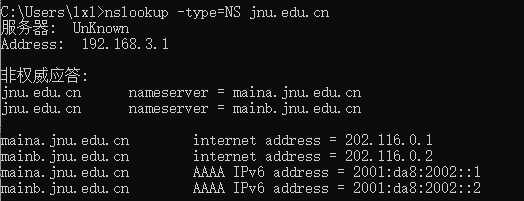


图 38 NSLOOKUP 操作示意

步骤 5：停止截获报文并将截获的结果分别保存为 DNS-S 和 DNS-C。分析 DNS 的请求和应答报文，完成下面的要求。

1）从 DNS-C 中选择一条计算机发出的 DNS 请求报文和相应的 DNS 应答报文 （它们的Transaction ID 字段的值相同），将两条报文的信息填入表 5.15。

表 15 DNS 请求报文和应答报文信息

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| DNS 报文  类型 | 报文序号 | 源站点 | 目的站点 | 报文信息 |
| DNS 请求  报文 | 0001 | 10.45.241.125 | 192.168.11.8 | 8.11.168.192.in-addr.arpa |
| DNS 应答报文 | 0001 | 192.168.11.8 | 10.45.241.125 | Standard query response 0x0001 PTR 8.11.168.192.in-addr.arpa PTR cacheb.nic.jnu.edu.cn NS cachea.nic.jnu.edu.cn NS cacheb.nic.jnu.edu.cn A 192.168.10.8 AAAA 2001:da8:2002::10:8 A 192.168.11.8 AAAA 2001:da8:2002::11:8 |

2）分析报，找出 DNS 服务器所请求的根域名服务器 IP 地址为多少？

**答：8.11.168.192**

3）上述命令输出内容的AAAA 记录是什么？有什么作用？

答：AAAA记录(AAAA record)是用来将域名解析到IPv6地址的DNS记录。与之相对的A记录只能将域名解析到IPv4地址上，如果需要将域名解析到一个IPv6地址上，就需要添加一条AAAA记录。

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

练习三、DNS 的应用及高速缓存

本练习将主机 A 和 B 作为一组，主机 C 和 D 作为一组，主机 E 和 F 作为一组。现仅以主机

A、B 所在组为例，其它组的操作参考主机 A、B 所在组的操作。

该练习中，DNS 服务器及各主机 IP 地址配置同练习二。

步骤 1：主机 A、B 分别在命令行下执行“ipconfig/flushdns”命令来清空 DNS 高速缓存。步骤 2：主机 A、B 分别启动 Wireshark 捕获数据并设置过滤条件（提取 DNS 协议和 ICMP 协议）。

步骤 3 ： 主机 A 、B 分别在命令行下执行“ ping 对方的域名” 命令， 然后执行“ipconfig/displaydns”命令来显示 DNS 高速缓存。在缓存中找到对方的域名所对应的记录。

步骤 5：主机 A、B 在命令行下再次执行“ping 对方主机的域名”命令。

步骤 5：主机 A、B 停止捕获，分析其捕获的数据及对方的 DNS 高速缓存中的内容，回答问题：

* 简述在使用域名完成的通信中，DNS 协议所起到的作用。

**答：将域名解析为IP 地址，客户端向DNS服务器（DNS服务器有自己的IP地址）发送域名查询请求**

* 简述 DNS 高速缓存的作用。

**答：当某个访问请求解析过一个域名以后，该解析记录就放置在缓存中，以后再有同样的解析请求，就直接从缓存中提供结果，加快了访问者的应答速度。**

* 参考“会话分析”视图的显示结果，绘制此次访问过程的报文交互图（包括 ICMP 协议）。

## 实验总结

1. 通过实验掌握了 DNS 的报文格式
2. 通过实践掌握了 DNS 的工作原理
3. 通过学习掌握了 DNS 域名空间的分类
4. 通过查阅资料理解了 DNS 高速缓存的作用