实验报告

|  |  |
| --- | --- |
| 实验名称：DNS域名服务协议 | |
| 实验台号：2 | 实验时间：2019年11月22日 |
| 实验小组：第2组  成员及本次实验分工:於文卓 | |
| 实验目的：  1.理解DNS实现的原理和实现方法  2.了解DNS解析的过程  3.通过编辑DNS请求数据包，了解DNS的报文格式  4.掌握nslookup命令和ipconfig命令的使用方法  5.通过dig命令可以显示整个DNS查询过程 | |
| 实验环境说明：  笔记本电脑一台(Win10系统)，Wireshark(Version 3.0.3) | |
| 实验过程、步骤（可另附页、使用网络拓扑图等辅助说明）及结果： 1.原理分析 DNS 域名系统是服务器和客户程序相互通信的一种协议。它提供了主机域名和 IP 地址之间的转换。域名服务器使用固定的端口号53，支持 UDP 和 TCP 访问。  DNS 是域名系统（Domain Name System）的缩写，它是一种用于 TCP/IP 应用程序的分布式数据库，它提供主机名字和 I P 地址之间的转换及有关电子邮件的选路信息。所谓“分布式”是指在 Internet 上的单个站点不能拥有所有的信息。每个站点（如大学中的系、校园、公司或公司中的部门）保留它自己的信息数据库，并运行一个服务器程序供 Internet上的其他系统（客户程序）查询。  域名解析需要由专门的域名解析服务器来完成，DNS 就是进行域名解析的服务器。它是一种分布式网络目录服务，主要用于域名与 IP 地址的相互转换，以及控制因特网的电子邮件的发送。大多数因特网服务依赖于 DNS 而工作，一旦DNS 出错，就无法连接 Web 站点，电子邮件的发送也会中止。  如图是DNS的解析流程，[图片来源](http://www.linuxdiyf.com/linux/21226.html)   2.实验步骤2.1 步骤一：使用Wireshark捕获数据包并进行分析 在Wireshark的工具栏输入框输入DNS即可筛选出DNS协议的记录    通过Wireshark的抓包，可以看到DNS报文的具体内容，如图所示   2.2 步骤二：使用nslookup工具解析域名 nslookup命令是查询域名对应ip的工具，其用法可以直接在windows系统的cmd中运行命令：nslookup 域名 来进行域名解析    也可以仅仅运行nslookup命令，不加任何参数。进入nslookup的交互界面，在“>”提示符后可以多次输入不同的域名，以实现多次的查询。如图实现了对[www.baidu.com、www.sina.com、www.hdu.edu.cn](http://www.baidu.com、www.sina.com、www.hdu.edu.cn)的查询    最后使用exit命令退出nslookup 2.3 步骤三：使用ipconfig命令查看DNS缓存 在Windows系统的cmd中，运行 ipconfig /displaydns 显示本机缓存区中的DNS解析内容。    而使用ipconfig /flushdns，可以清楚本机的DNS缓存记录 2.4 使用dig工具显示DNS查询过程 在Windows中使用dig命令需要安装相应程序，可以直接在网页查询，网址<https://www.diggui.com/>  在网页中可以选择要查询的类型、域名，选择公共的DNS服务器等。    对[www.baidu.com](http://www.baidu.com)的查询结果如下    可以看到[www.baidu.com](http://www.baidu.com)对应一个别名[www.a.shifen.com](http://www.a.shifen.com)，而这个域名又对应一个别名[www.wshifen.com](http://www.wshifen.com)。通过查询这个域名的ip地址，我们最终得到了两个ip，这两个ip为[www.baidu.com](http://www.baidu.com)域名对应的ip，在浏览器中输入这两个ip即可访问[www.baidu.com](http://www.baidu.com)。注意到，[www.baidu.com](http://www.baidu.com)后面还有个“.”，这是为什么呢。这并不是疏忽，其实所有域名的尾部，实际上都有一个根域名。比如[www.example.com](http://www.example.com)的真正域名其实是[www.baidu.com.root，之所以简写，是因为.root](http://www.baidu.com.root，之所以简写，是因为.root)对于所有域名都是一样的。   3.其他工具介绍3.1 host命令 Host命令可以看做dig命令的简化版本，返回当前请求域名的各种记录 3.2 whois命令 Whois命令用来查看域名的注册情况 | |
| 实验总结（遇到的问题及解决办法、体会）：  通过这次实验，我进一步了解了DNS的作用和工作流程。额外的通过Wireshark抓包，了解了DNS报文的结构。同时还了解了Windows中关于DNS的一些命令比如nslookup、ipconfig等。通过nslookup，我可以直接查询域名对应的IP地址，而通过ipconfig命令，我可以知道本地缓存了那些DNS解析内容。  此外了解使用了dig命令，可以显示DNS的查询过程。  域名服务分为客户端和服务器端，客户端提出请求，询问一个 Domain Name 的 IP 地址，服务器端必须回答客户端的请求。本地 DNS 首先查询自己的数据库，如果自己的数据库中没有对应的 IP 地址，则向本地 DNS 上所设的上一级 DNS 询问，得到结果之后，将收到的结果保存在高速缓冲区，并回答给客户端。  问题：域名与 IP 地址之间是否有一一对应的关系？  IP对域名是一对多的关系，一个IP地址可以对应多个域名；一个域名只能解析一个IP地址。 | |
| 器材、工具领用及归还负责人：於文卓 | 实验记录人：於文卓 |
| 实验执笔人：於文卓 | 报告协助人：於文卓 |
| 小组成员签名：於文卓 | |
| 验收人： | 成绩评定： |