山东大学 计算机 学院

计算机网络 课程实验报告

|  |  |  |  |
| --- | --- | --- | --- |
| 学号：202000130143 | 姓名： 郑凯饶 | | 班级： 2020级1班 |
| 实验题目：DNS | | | |
| 实验学时：2 | | 实验日期： 2022-3-22 | |
| 实验目的：  学习域名解析系统（DNS），包括本地DNS服务器，DNS缓存，DNS记录和信息，报文各个字段。 | | | |
| 硬件环境：  Dell Latitude 5411  Intel(R) Core(TM) i5-10400H CPU @ 2.60GHz(8GPUs),~2.6GHz | | | |
| 软件环境：  Windows 10 家庭中文版64位（10.0，版本18363）  Wireshark-win64-3.6.2 | | | |
| 实验步骤与内容：   1. 问题： 2. 运行nslookup获取一台亚洲服务器的IP地址。 3. 查询一所欧洲大学的authoritative DNS服务器。 4. 使用问题（2）中的DNS服务器向Yahoo!mail发起询问，它的IP地址？ 5. 定位DNS询问及回复信息，是通过UDP还是TCP发送？ 6. DNS询问信息的目标端口是多少？DNS回复的源端口？ 7. DNS询问信息向哪个IP发送？使用ipconfig查询本地的DNS服务器，判断两者是否一致。 8. 测试DNS询问信息。它属于什么类型的DNS询问？是否包含了回答？ 9. 测试DNS回复信息。有多少回答提供？它们各自包含什么？ 10. 思考随后本机发出的TCP SYN包。它的目的地是否是DNS回复信息中的IP？ 11. 在取回图像之前，主机是否发出新的DNS询问？ 12. 询问的目标端口？回复的源端口？ 13. 目的地IP？是否是本地DNS服务器？ 14. DNS询问类型。是否包含回答? 15. 多少回复被提供？分别包含什么内容？ 16. 截屏。 17. 目的地IP？是否是本地DNS服务器？ 18. DNS询问类型。是否包含回答? 19. DNS回复提供了哪些MIT nameservers,是否包含他们的IP？ 20. 截图。 21. 目的地IP？是否是本地DNS服务器？若不是它对应的IP？ 22. DNS询问类型。是否包含回答? 23. 多少回复被提供？分别包含什么内容？ 24. 截图。 25. 阐述基本方法   使用nslookup进行指定DNS服务器进行域名解析，使用ipconfig清除DNS缓存，使用Wireshark分析DNS报文的各个字段。参考资源如下：  nslookup命令：<https://blog.csdn.net/xg_ren/article/details/80782338>  ipconfig命令：<https://blog.csdn.net/bcbobo21cn/article/details/51759140>  DNS记录：<https://blog.csdn.net/u013920085/article/details/42552987>   1. 实验结果展示与分析   （1）查询阿里巴巴的IP：    （2）查询牛津大学的DNS服务器：    （3）使用牛津的DNS服务器响应超时，谷歌的OK.    （4）通过UDP发送。    （5）询问时的目标端口为53，回复的源端口也是53.  （6）8.8.8.8，谷歌的DNS服务器（手动设置），和本地的一致  （7）A类型。包含指向DNS回复的链接。    （8）      （9）TCP SYN包的目的地就是前DNS回复中解析的IP结果。    （10）还发出了新的DNS询问，图片域名不同要重新解析。实际并没有，使用F12开发者工具查看图片源，发现来自统一域名。（8）中nav.smartscreen.microsoft.com应该是与Edge筛选器相关的请求，analytics.ietf.org请求的JS脚本，与登录相关。  （11）前两条为nslookup专用的DNS信息。仍然都是53  （12）仍然是8.8.8.8，相同  （13）有A类型以及AAAA类型两种DNS询问，包含指向回复的链接（应该是Wireshark软件提供）  （14）针对每个询问各有一个回复。第一个回复包含两条CNAME类型的DNS询问，分别解析向[www.mit.edu](http://www.mit.edu)和前者返回的[www.mit.edgekey.net，以及向e9566.dscb.akamaiedge.net](http://www.mit.edgekey.net，以及向e9566.dscb.akamaiedge.net)发送的询问，最后得到域名对应的主机IP为23.15.106.234.以上是使用IPV4进行的，另外AAAA类型应该是基于IPV6协议的解析过程，只有最后返回的IP不同为2600:140b:4800:583:255e.  （15）    （16）8.8.8.8，是  （17）NS（authoritative Name Server）,似乎没有  （18）nameservers如（19）所示，没有提供它们的IP  （19）    （20）bitsy.mit.edu服务器似乎访问不了，使用百度公共DNS替代。DNS询问发往180.76.76.76，不是指定的DNS服务器，命令的第三个字段是指定DNS服务器。  （21）A类型，从DNS报文头部Answer RRs字段等于0我们知道该报文不包含回复。    （22）提供了1个Authority RRs,SOA（Start Of a zone of Authority）类型，包含序列号，主服务器，负责人邮箱，刷新间隔等信息。    （23） | | | |
| 结论分析与体会：  这次实验从DNS客户端的角度初步窥探了一下DNS，了解DNS大致的运作流程，熟悉了DNS报文。之前我的电脑自动获取本地的DNS server进行域名解析时有问题，实验中我将它手动设置为谷歌DNS服务器8.8.8.8。DNS是一个复杂的分布式系统，希望以后能更进一步学习，尝试优化域名解析。 | | | |