北 京 邮 电 大 学

计 算 机 科 学 与 技 术 学 院

《下一代Internet技术与协议》

实验报告

姓名：\_\_\_\_\_鄭毓恒\_\_\_\_\_

学号：\_\_\_2020211262\_\_\_

班级：\_\_\_2020211302\_\_\_

2023年5月

**实验报告**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 实验名称 | | ICMPv6实验 | | |
| 实验目的 | | 通过Wireshark抓包，分析ICMPv6协议报文。 | | |
| 实验完成人 | | 鄭毓恒 | 完成时间 | 2023-05-29 |
| 实验环境 | Windows 11  WireShark 网络分析器 | | | |
| 实验步骤与结果分析 | | | | |
| 连接网络，打开IPv6协议，关闭IPv4协议。    在CMD命令行模式下输入ipconfig /all命令，得到以下本机IPv6信息。本机的IPv6地址为2001:da8:215:3c02:3049:73f2:dc55:ea00。    在CMD命令行模式下，使用nslookup命令对选定的网站域名www.bupt.edu.cn进行DNS解析，指定的IPv6服务器为2400:3200::1。可以看到获取到该网站的IPv6地址2001:da8:215:4038::161。    Wireshark抓到以下几个包。    其中，有两个DNS协议报文。首先是由本机发给DNS服务器，询问www.bupt.edu.cn的AAAA地址。然后服务器回复本机，包含该网站的AAAA地址。      对刚才获取到的IPv6地址进行ping操作。    Wireshark捕获到以下报文。    Ping命令将一个流程重复了4次。首先，本机向目的IPv6地址发Echo request报文，即向目标发送回复请求。ICMP的type字段为128，表示echo request类型。标识符为1，序列号为91。    然后，目标主机回复本机。ICMP的type字段为129，表示echo reply报文。标识符为1，序列号为91，表示这个报文回复的是序列号同为91的echo request报文。    对该网站的IPv6地址进行tracert操作，得到以下结果。结果输出了从本机到目标地址总共需要6跳，以及每一跳的目标地址。    命令tracert的工作方式是通过向目标地址发送不同跳数限制(hop limit)值的echo request回复请求数据报文，确定到目标所采取的路由。每个跳数限制发送3个请求报文。每个中间路由器在转发报文前将数据包上的 hop limit 递减 1。当hop limit字段减为0时，路由器向源地址发送超时报文。  Wireshark捕获的数据报文如下。跳数限制为1的请求报文没有收到路由器的超时报文，但也没有收到目标地址回复，本机判定为超时。跳数限制2-5的请求报文收到了路由器的超时报文，表示跳数已达上限。跳数限制为6的请求报文收到了目标地址的回复报文，表示从本机到目标地址最少需要6跳。    以下两个请求报文分别是跳数限制为2和3的请求报文，证明tracert通过更改IPv6协议的Hop Limit跳数限制字段，测试到目标地址的跳数。      这是跳数限制为3时，从路由器收到的超时报文，ICMP type字段为3。从报文源地址可知，是哪个路由器向本机发送的超时报文，也就是请求报文在前往目标地址路径上的那个路由器达到了跳数上限。    下图是从目标地址收到的echo reply回复报文    对网站的IPv6地址进行ping操作，加上参数 -l 3000，即用含有3000字节长度数据字段的报文进行ping操作。    Wireshark捕获到的数据报文。    与不带参数的ping操作对比，ping -l 3000不止在报文的数据字段长度有不同。同时，由于3000字节的数据过长，超出了转发接口的最大传输单元值MTU。因此，这次的数据报文都采用了IP分片技术，则在转发报文前，先将其分为更小的片，然后在到达目标地址时，由目标主机进行重组。  以下是本机发送的echo request请求报文。在IPv6协议头中，有Fragment Header分片头。其中，Offset字段表示这个分片报文的数据在总体数据中的偏移量，More Fragments字段表示这个报文之后还有同属一组的分片。从下图可见，这个报文的数据偏移量是2896，并且是该组最后一个报文。Wireshark软件不会显示所有的分片，但在IPv6字段的下方有提示消息，表示总共收到3个分片，组装后长度为3008字节。    以下是本机收到的echo reply回复报文。在IPv6协议头中，从下图可见，这个报文的数据偏移量是0，并且之后还有分片。在IPv6字段的下方有提示消息，表示总共收到3个分片，组装后长度为3008字节。 | | | | |
| 分析与思考 | | | | |
| 通过本次实验，抓取了DNS解析的DNS报文、ping、tracert和长报文ping过程的ICMPv6报文，并经过分析，学习到了echo request和echo reply等ICMPv6协议报文的内容、作用和各个字段的含义，更加掌握ICMPv6协议的原理和wireshark软件的使用方法。  在实验过程中，起初关闭本机的IPv4协议后，变成了离线状态，无法上网，也久无法进行nslookup和ping操作。后来通过ipconfig分析本机IP信息发现，当只使用IPv6协议时，本机使用的DNS服务器地址以fec0开头，代表站点本地地址，也就是暂时没有合适的IPv6 DNS服务器。后来发现，nslookup命令可以加入参数，选择指定的DNS服务器进行解析。使用了阿里巴巴公司的IPv6 DNS服务器，成功完成nslookup操作。 | | | | |