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：ICMP | | | |
| 实验学时：2 | | 实验日期： 2022-5-15 | |
| 实验目的：  探索ICMP协议：   1. Ping程序生成的ICMP消息 2. Traceroute程序生成的ICMP消息 3. ICMP消息的格式与内容 | | | |
| 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. 本机IP以及目标IP。 3. 为什么ICMP数据包没有端口信息？ 4. 请求ICMP的类型和代码。还有哪些其他字段？校验和，序列号和标识符字段所占字节数。 5. 响应。 6. 本机IP以及目标IP。 7. 如果ICMP发送了UDP数据包，那么探测数据包的IP协议号仍然是01吗？否则它是什么？ 8. 响应数据包和ping有何不同？ 9. 错误数据包比ICMP有更多字段，具体是？ 10. 源主机最后收到的3个数据包和ICMP错误数据包有何不同？ 11. 在tracert的跟踪中，是否有一个连接的延迟比其他连接长得多？这个连接末端的2个路由器的位置？ 12. 阐述基本方法   ICMP提供简明的出错报告信息，发送的错误报文返回到发送原数据的设备。从技术角度来说，ICMP是一个“错误侦测与回报机制”，可以通过其检测网络的连线状况。  报文格式：    通过type和code标识消息类型：     1. 实验结果展示与分析   Ping操作：     1. Source Address: 172.25.154.9   Destination Address: 143.89.12.134     1. ICMP报文仅仅传送到指定主机，而不是指定程序，所以没有端口号概念。 2. 类型8，代码0，还包括校验和、序列号、标识符各2B 3. 类型0，代码0，还包括校验和、序列号、标识符各2B   Tracert操作：     1. Source Address: 172.25.154.9   Destination Address: 128.93.162.83     1. 不是，应该是UDP的协议号为17 2. 具体字段内容不同 3. Type: 0 (Echo (ping) reply) -> 11 (Time-to-live exceeded)   增加：unused字段，包含请求的IP以及ICMP数据包的首部  减少：标识符Identifier 以及序列号Sequence Number字段     1. 最后3个接收到的数据包是目标主机的reply，表示成功接收request 2. 观察到第11跳相比前面的往返时延陡增，猜测是国际之间的路由连接。 | | | |
| 结论分析与体会：  这次实验深入了ICMP协议，学习了之前略有眼缘的ping与tracert命令，明白了为什么我们可以用其来检查网络状况。有意思的是，我们可以用tracert探测出网络通路，探明消息如何从大洋彼岸发送到我们的电脑上。  例如ping一下github.com:    可以“正常”访问，但是却ping不通，查询了可能是DNS解析的问题。  在hosts中加入：    好了，成功了！    看看github服务器距离我有多少路由“跳”：    19跳，对于计算机网络我们似乎可以给出一个确切结论：任意两台通讯设备的距离不超过K台路由！ | | | |