

**实验报告**

**课程名称： 计算机网络原理**

**学生姓名： 朱方灏钧 学号： 210111316**

**年级专业： 19级软件工程 班级： 19.11**

**指导教师： 张毅**

**开课学期： 2021 年— 2022 年 1 学期**

**宜宾学院人工智能与大数据学部实验教学中心**

**宜宾学院人工智能与大数据学部**

**实验报告**

**年级：19级**  **专业：软件工程** **上课日期： 2021**年 12月12日

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **实验名称** | **ICMP协议分组结构** | | | | | |
| **学生姓名** | **朱方灏钧** | **学号** | **210111316** | **实验合作者 姓名** | **无** | |
| **指导教师(签名)** |  | **评 阅 日 期** | |  | **实验报告分** |  |
| **实验报告基本内容：**一、实验目的；二、实验内容；三、实验原理；四、实验步骤及结果；五、实验遇到问题及解决方法；六、实验结论 | | | | | | |
| 1. 实验目的：   掌握网络层ICMP协议   1. 实验内容： 2. 在命令提示符中，利用ipconfig /all查看自己主机的ip及MAC地址，查看自己的网关ip地址并记录，方法同实验1。IMG_256 3. 运行wireshark抓包分析工具，在命令提示符输入”ping 网关地址”， 然后输入“ping 125.88.254.3 -i 4”过一段时间后停止捕获，观察捕获到的数据包。        1. 在过滤栏中，设置过滤条件过滤本机ip地址发出和接受的ICMP数据包，找到ICMP echo request与reply及TTL过期的数据包，查看捕获数据包的ICMP协议分组结构，并记录下表，其中报头内后四个字节的内容请根据实际捕获数据包填写（注意LE：little-endian与BE：big-endian大小端的数据存储模式）。   ICMP echo request:   |  |  |  |  | | --- | --- | --- | --- | | 类型 | 代码 | 校验和 | | | 8 | 0 | 0x4c84 | | | 8 | 0 | 0x002f | 0x2f00 | | 8 | 0 | 0x0030 | 0x3000 |   ICMP echo reply:   |  |  |  |  | | --- | --- | --- | --- | | 类型 | 代码 | 校验和 | | | 0 | 0 | 0x5484 | | | 0 | 0 | 0x002f | 0x2f00 | | 0 | 0 | 0x0030 | 0x3000 |   TTL exceeded:   |  |  |  |  | | --- | --- | --- | --- | | 类型 | 代码 | 校验和 | | | 11 | 0 | 0x9fa3 | | | 11 | 0 | 0x0038 | 0x3800 | | 11 | 0 | 0x003a | 0x3a00 |   根据捕获的数据包信息思考并回答以下问题：   1. ICMP echo request与reply以及TTL exceeded三个报文的类型与代码字段分别是多少？请查阅相关资料了解这两个字段可能的取值与含义。   答：类型字段分别是8,0,11，代码字段为0  TYPE CODE Description Query  0 0 Echo Reply——回显应答（Ping应答） x  3 0 Network Unreachable——网络不可达  3 1 Host Unreachable——主机不可达  3 2 Protocol Unreachable——协议不可达  3 3 Port Unreachable——端口不可达  3 4 Fragmentation needed but no frag. bit set——需要进行分片但设置不分片比特  3 5 Source routing failed——源站选路失败  3 6 Destination network unknown——目的网络未知  3 7 Destination host unknown——目的主机未知  3 8 Source host isolated (obsolete)——源主机被隔离（作废不用）  3 9 Destination network administratively prohibited——目的网络被强制禁止  3 10 Destination host administratively prohibited——目的主机被强制禁止  3 11 Network unreachable for TOS——由于服务类型TOS，网络不可达  3 12 Host unreachable for TOS——由于服务类型TOS，主机不可达  3 13 Communication administratively prohibited by filtering——由于过滤，通信被强制禁止  3 14 Host precedence violation——主机越权  3 15 Precedence cutoff in effect——优先中止生效  4 0 Source quench——源端被关闭（基本流控制）  5 0 Redirect for network——对网络重定向  5 1 Redirect for host——对主机重定向  5 2 Redirect for TOS and network——对服务类型和网络重定向  5 3 Redirect for TOS and host——对服务类型和主机重定向  8 0 Echo request——回显请求（Ping请求） x  9 0 Router advertisement——路由器通告  10 0 Route solicitation——路由器请求  11 0 TTL equals 0 during transit——传输期间生存时间为0  11 1 TTL equals 0 during reassembly——在数据报组装期间生存时间为0  12 0 IP header bad (catchall error)——坏的IP首部（包括各种差错）  12 1 Required options missing——缺少必需的选项  13 0 Timestamp request (obsolete)——时间戳请求（作废不用） x  14   Timestamp reply (obsolete)——时间戳应答（作废不用） x  15 0 Information request (obsolete)——信息请求（作废不用） x  16 0 Information reply (obsolete)——信息应答（作废不用） x  17 0 Address mask request——地址掩码请求 x  18 0 Address mask reply——地址掩码应答 x   1. 在这三个报文中，报头的后四个字节分别是什么内容？表示什么含义？   答：是：0x002f，0x2f00，0x0030，0x3000，0x0038，0x3800，0x003a，0x3a00，表示TCP序列号和确认号(Sequence Number)，用来跟踪该端发送的数据量，如果发出和收到的的序列号和确认号相同，则可判断为同一个报文   1. 对比ICMP echo request与reply报文的数据部分，请问是否一样？说明echo请求时发送方与接受方的操作。   答：一样，发送端发送带数据的request请求，接受方收到相同数据的request请求时发送带有相同数据的reply回复。   1. 仔细观察TTL exceeded报文的ICMP数据部分，请问该数据部分包括了哪些部分？为什么这样？   答：没有包括数据部分，因为收到请求失败了，无法接受数据   1. 思考：请根据今天实验的所有实验结果 2. 说明ICMP的触发机制是什么？   答：发送ping等属于ICMP类型的网络请求   1. 尝试捕获其他类型的ICMP报文。   答：如 traceart www.baidu.com 端口不可达。类型为3，代码为3   1. 当IP数据包传输出错时ICMP协议如何封装差错报文？   答：封装差错报文相关的type，code，checksum，Unused等属性，没有Data等其他属性   1. 实验原理：   利用wireshark的软件功能实现   1. 实验步骤及结果 2. 实验遇到问题及解决方法   无   1. 实验结论   通过wireshark的使用，把课堂上学到的理论知识用到了实践中，真正理解了什么是ICMP数据包的知识 | | | | | | |
| **指**  **导**  **教**  **师**  **评**  **语** | | | | | | |