|  |
| --- |
| 实验目的：  使用wireshare来捕获DHCP协议  实验结果：  首先捕获DHCP：  1、先打开wireshark  2、win+Rcmd进行捕获icmp协议  屏幕截图 2023-04-21 170043  本地捕获如下所示：  屏幕截图 2023-04-21 170159 |

|  |
| --- |
| 实验内容：  1、您的主机的 IP 地址是多少？ 目标主机的 IP 地址是多少？  主机IP地址：172.25.156.185  目标主机IP地址：143.89.12.134  屏幕截图 2023-04-21 171200  2、为什么 ICMP 数据包没有源端口号和目的端口号？  因为ICMP协议是网络层间的通信协议，不涉及应用层间的通信，无需使用UDP和TCP协议，仅使用ip地址就可以实现数据报的传送  3、查看任意的请求 ICMP 数据包， ICMP 类型和代码是什么？ 该 ICMP 数据包还有哪些其他字段？ 校验和，序列号和标识符字段有多少字节  类型：8 代码：0 还包括：Checksum Identifier Sequence Number Data段  屏幕截图 2023-04-21 171218  校验和，序列号和标识符字段有2字节，其中一个如下图所示：  屏幕截图 2023-04-21 171349  4、查看任意的响应 ICMP 数据包， ICMP 类型和代码是什么？ 该 ICMP 数据包还有哪些其他字段？ 校验和，序列号和标识符字段有多少字节  屏幕截图 2023-04-21 171959  类型0 代码：0 还包括：Checksum Identifier Sequence Number Data段  校验和，序列号和标识符字段有2字节，  实验二：  屏幕截图 2023-04-23 201640  5、您的主机的 IP 地址是多少？ 目标目标主机的 IP 地址是多少？  屏幕截图 2023-04-23 215930  主机：172.25.202.159 目标主机：128.93.162.83  6、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？ 如果没有，它会是什么？  不会，因为icmp的协议号为01，如下图所示，  屏幕截图 2023-04-23 201857  udp的协议号为17，  协议号用来指出该数据传送采用了哪种协议，以便找到数据要上交到哪个传输层  7、检查屏幕截图中的 ICMP echo响应数据包。 这与本实验的前半部分中的 ICMP ping 查询数据包不同吗？ 如果不同，请解释为什么？  屏幕截图 2023-04-21 174847  不同，此时icmp的报文的报文类型为11，这说明在传递数据包时路由器检查到数据包发生超时了，因此路由器就丢包并且发送给该警告报文返回给原主机。  对比上一部分报文类型是0说明目的主机接收到原主机发送的报文并进行响应：  屏幕截图 2023-04-23 203334  8、检查屏幕截图中的 ICMP error数据包。 它具有比 ICMP 响应数据包更多的字段。 这个数据包含哪些内容？  对比发现多了错误包所针对的原始ICMP数据包的IP标头和前8个字节  屏幕截图 2023-04-23 203334屏幕截图 2023-04-21 174847  9、检查源主机收到的最后三个 ICMP 数据包。 这些数据包与 ICMP 错误数据包有何不同？ 他们为什么不同？  对比如下：  屏幕截图 2023-04-23 200647 屏幕截图 2023-04-23 200701  报文type不同，错误数据 的报文type=11说明访问超时  最后三个数据包type=0说明是回应请求，因为最后三个是响应包，在ttl到期之前一直到达目标主机，与中间路由器无关。   1. 在 tracert 跟踪测量中，是否有一个连接的延迟比其他连接长得多？ 请参阅图 4 中的屏幕截图，是否有连接的延迟明显长于其他连接？ 根据路由器名称，您能猜出这个连接末端的两个路由器的位置吗？   屏幕截图 2023-04-23 201640  第13到第14个延迟要比其他延迟更多，猜测两个路由器一个在亚洲一个在欧洲。  问题及收获：  学会了读取DHCP协议的字段含义，通过分析不同字段可以看出DHCP协议中报文的发送状态。 |