**《下一代Internet技术与协议》**

**课程实验报告**



**学院：计算机学院（国家示范性软件学院）**

**班级： 2018211314**

**姓名： 李志毅**

**学号： 2018211582**

**实验一 IPv6的使用和测试实验**

**一、实验内容和目的**

本次实验内容：

1.如何打开Windows系统的ipv6协议，关闭ipv4协议

2.如何使用ipconfig/all命令和ping命令测试ipv6协议的成功使用

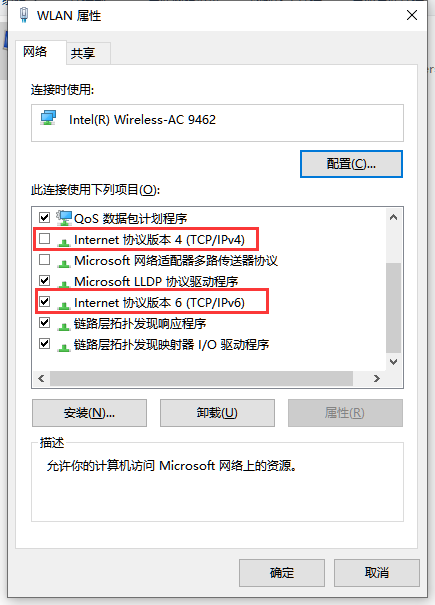
通过本次实验，可以了解ipv6协议在Windows如何使用，并熟悉常见的地址结合和ping命令数据包分析，以及判断该地址类型。

**二、实验环境**

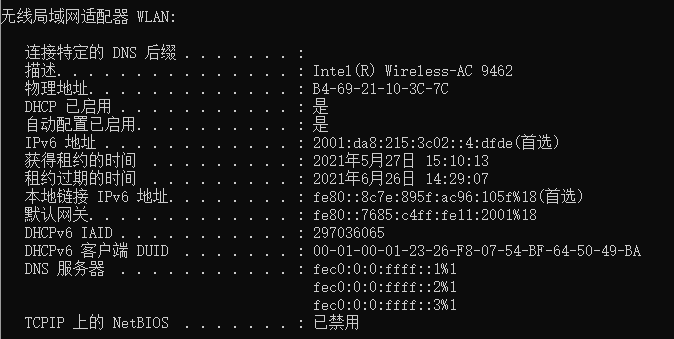
1 台装有 Windows 操作系统的 pc 机，要求能够连接到 Internet，并安装 Wireshark 等软件。1 部使用 SIM 卡连接网络的手机。

**三、实验准备**

**1.关闭IPv4，打开IPv6**



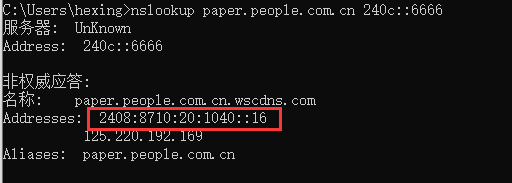
**2.打开PowerShell窗口，输入ipconfig -all命令**



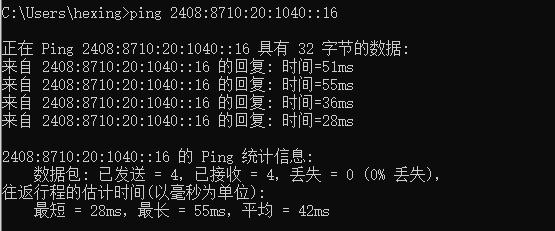
与IPv6相关的地址的相关信息整理为：

|  |  |  |
| --- | --- | --- |
| **名称** | **地址** | **描述** |
| IPv6地址 | 2001:da8:215:3c02::4:dfde | 属于2000-3FFF范围，为可汇聚全球单播地址 |
| 本地链接IPv6地址 | fe80::8c7e:895f:ac96:105f%18 | FE80-FEBF范围，为链路本地单播地址 |
| 默认网关 | fe80::7685:c4ff:fe11:2001%18 | 链路本地网关地址 |
| DNS服务器 | fec0:0:0:ffff::1%1  fec0:0:0:ffff::2%1  fec0:0:0:ffff::3%1 | IPv6网络上的DNS服务器地址，FEC0开头代表站点本地地址 |

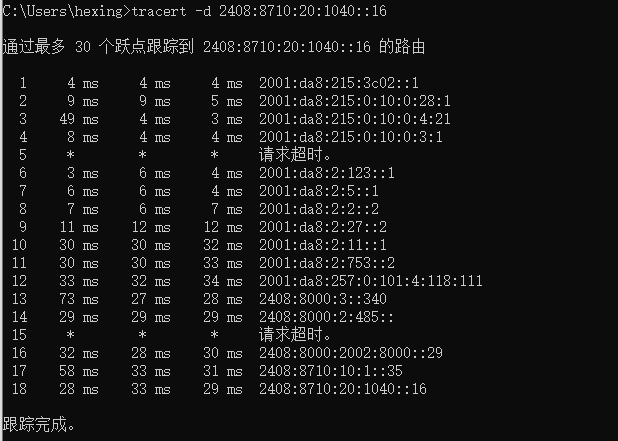
**3.使用nslookup命令对选定的网站域名进行DNS解析，截图并记录其IPv6地址**



**4.对此网站的IPv6地址进行ping操作，截图记录**



**5.对此网站的IPv6地址进行tracert操作，使用tracert -d XXXX:XXXX的命令和参数-d，截图记录**

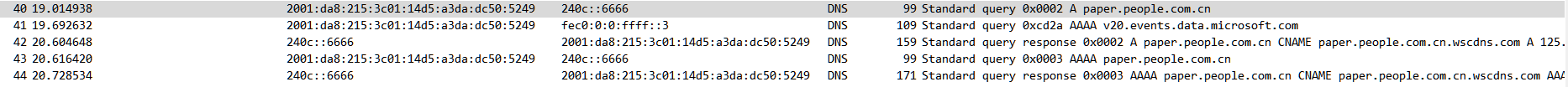


**四、抓包内容与分析**

**1.使用nslookup命令对选定网站进行DNS解析**

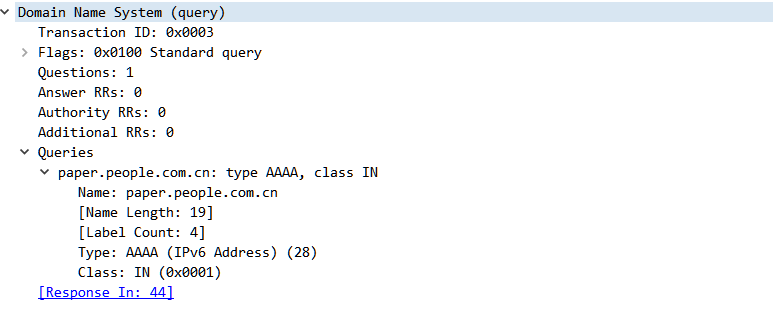
本次实验中，我选取的支持IPv6的网站为人民日报-人民网，域名为<http://paper.people.com.cn/>，利用nslookup命令对该域名进行解析，指定IPv6服务器为**240c::6666**，最终获取到的地址为**2408:8710:20:1040::16**

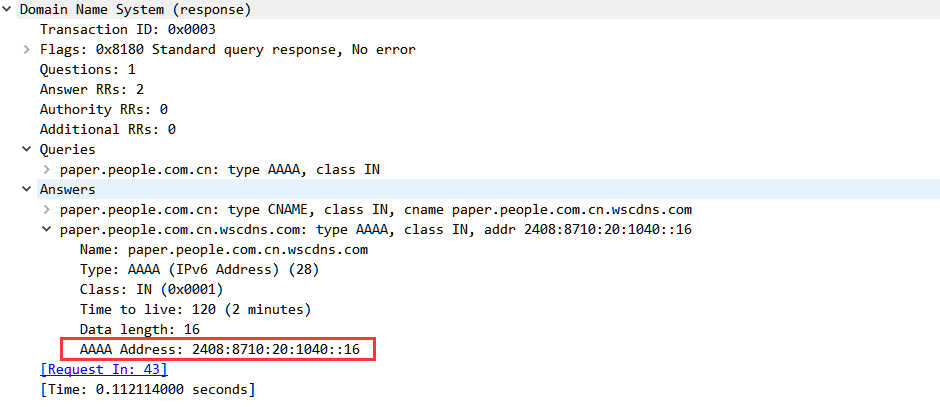
使用Wireshark抓包可以看到：



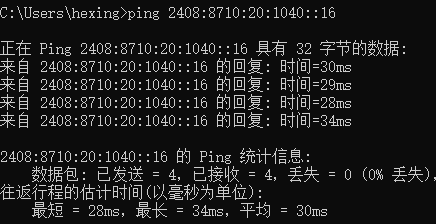
本地向DNS服务器发送DNS请求报文，请求paper.people.com.cn的AAAA地址，而后DNS服务器向本地返回DNS响应报文，在报文中给paper.people.c

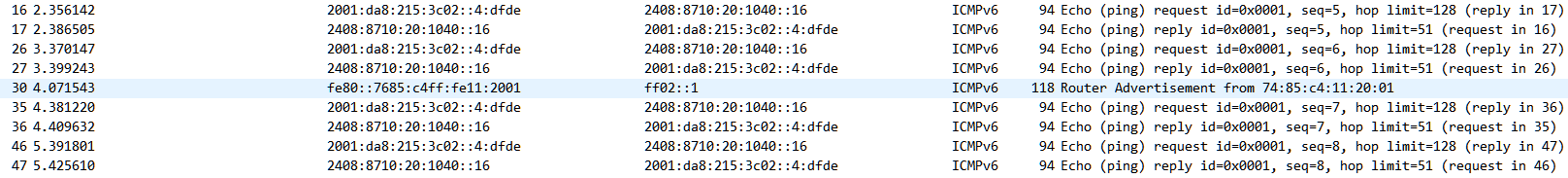
om.cn的IPv6地址信息，与CMD中显示一致





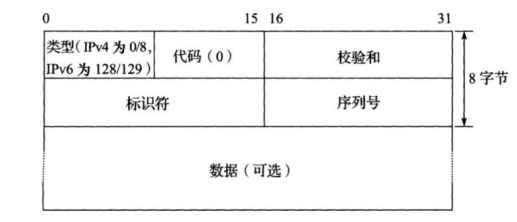
**2.对此网站的IPv6地址进行ping操作**



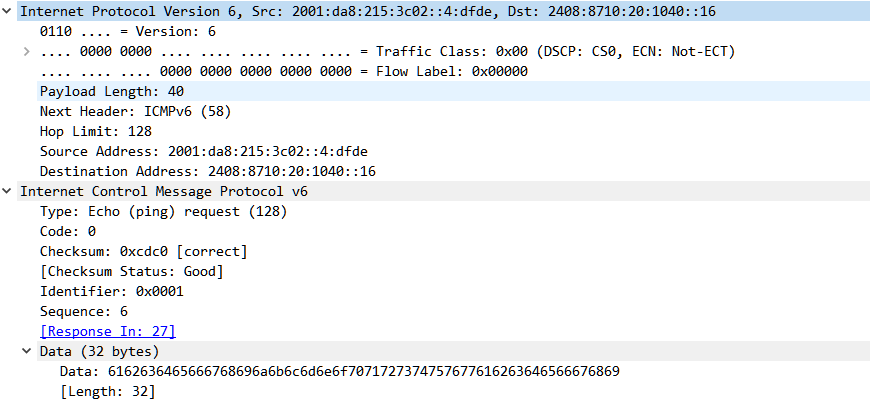


ping 指令的作用是随机生成固定长度的数据包，通过 ICMP（Internet 控制消息协议）协议将数据包发送到指定主机，并侦听回显回复报文来探测与目标主机之间的连接。在本机的 CMD 当中显示出发送的数据、回复的时间等信息。

观察 CMD 中的输出可知：通过 ping 指令向**2408:8710:20:1040::16** 发送了四段报文，并均得到了回复。再对比观察 wireshark 当中抓取到的报文，也同样捕获到了四组 ICMP 的 ping 报文，每组报文有两个包构成。

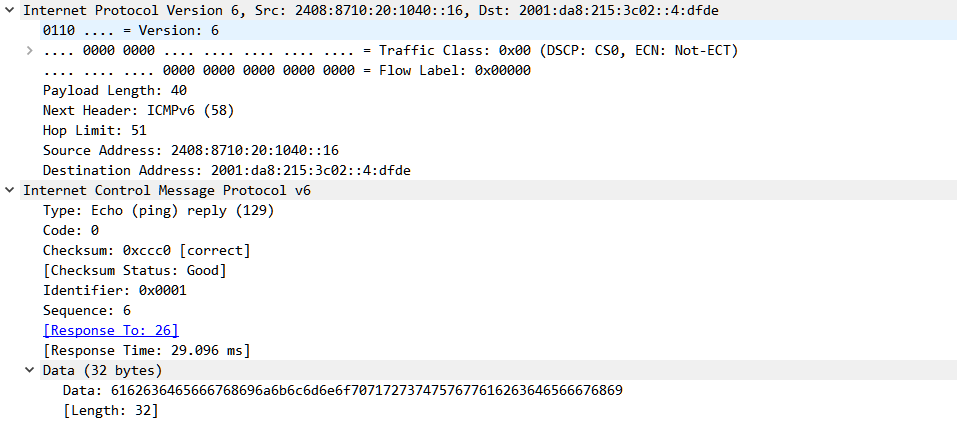
一个包是由本机向目标主机（**2408:8710:20:1040::16**）发送的 Echo request包；另一个包是由目标主机接受到本机发送的 Echo request 后回复的 Echo reply包。由于四组报文的内容基本一致，因此在此只对第一组报文进行详细分析。 

* ICMPv6-Echo request



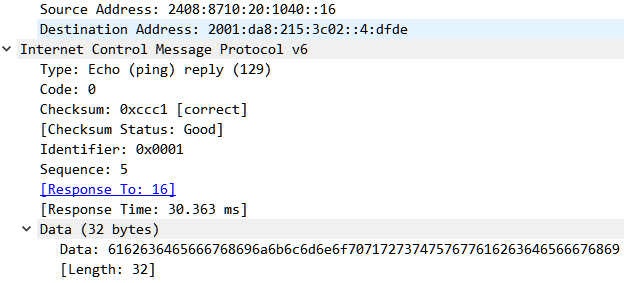
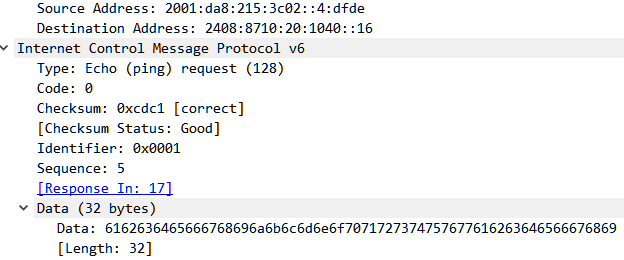
该报文是由本机发往目标主机（**2408:8710:20:1040::16**）的 echo request 报文，即向目标主机发送回显请求。其中 ICMP 报文 Type 字段为 128，代表该报文为 echo request 报文；code 字段内容为 0,checksum 校验和根据报文内容生成；标识符为 1；序列号为 6；数据内容由 ping 指令随机生成长度 32bytes。

* ICMPv6-Echo reply

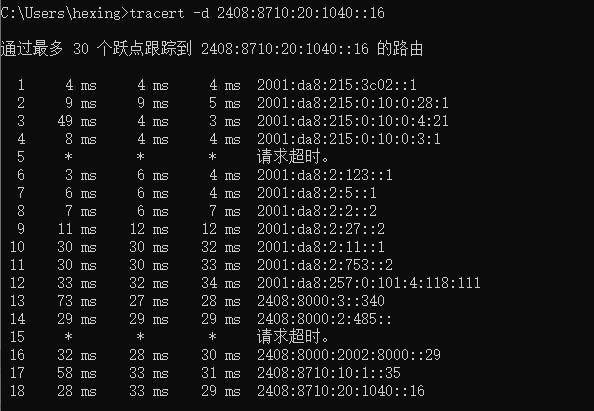


该报文是由目标主机（**2408:8710:20:1040::16**）发往本机的 echo reply 报文，即向目标主机发送回复报文。其中 ICMP 报文 Type 字段为 129，代表该报文为 echo reply 报文；code 字段内容为 0；checksum 校验和根据报文内容生成；标识符为1；序列号为 6；数据内容 data 与 echo request 报文中数据一致.

对比同组报文，传送方向分别为本机到目标主机、目标主机到本机；类型分别为 128（echo request）、129（echo reply）；校验和不同，根据报文生成；序列号相同均为6；数据 data 由 ping 指令随机生成。 其余报文同理：



**3.对此网站的IPv6地址进行tracert操作**



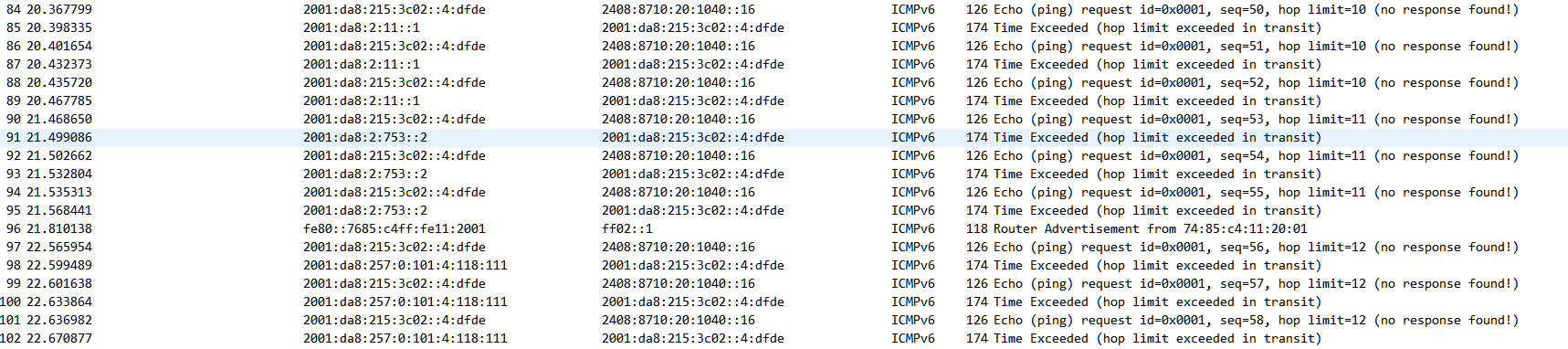
通过向目标地址发送不同跳数限制(hop limit)值的“Internet 控制消

息协议 (ICMP)”回显请求数据包，tracert 诊断程序确定到目标所采取的路由。要求路径上的每个路由器在转发数据包之前至少将数据包上的 hop limit 递减 1。当数据 包上的 hop limit 减为 0 时，路由器应该将“已超时”的消息发回源地址。

tracert 先发送 hop limit 为 1 的回显请求数据包，并在随后的每次发送过 程将 hop limit 递增 1，直到目标响应或 hop limit（最大为 30）达到最大值， 从而确定路由。通过检查中间路由器发回的“已超时”的消息确定路由。某些路 由器不经询问直接丢弃 hop limit 过期的数据包，这在捕获报文时不会存在回显 应答报文。

跟踪路由（Tracert）是路由跟踪实用程序，用于确定 IP 数据包访问目标所 采取的路径，其工作原理是通过向目标发送不同跳转限制 (hop limit) 值的 “Internet 控制消息协议（ICMP）”回应数据包，跟踪路由诊断程序确定到目标 所采取的路由。实际应用中可以使用跟踪路由命令确定数据包在网络上的停止位 置。

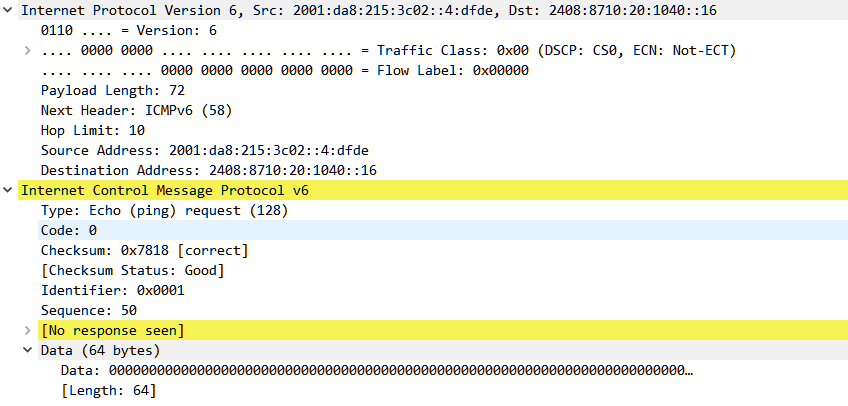
Wireshark 软件中捕获的报文情况如下：



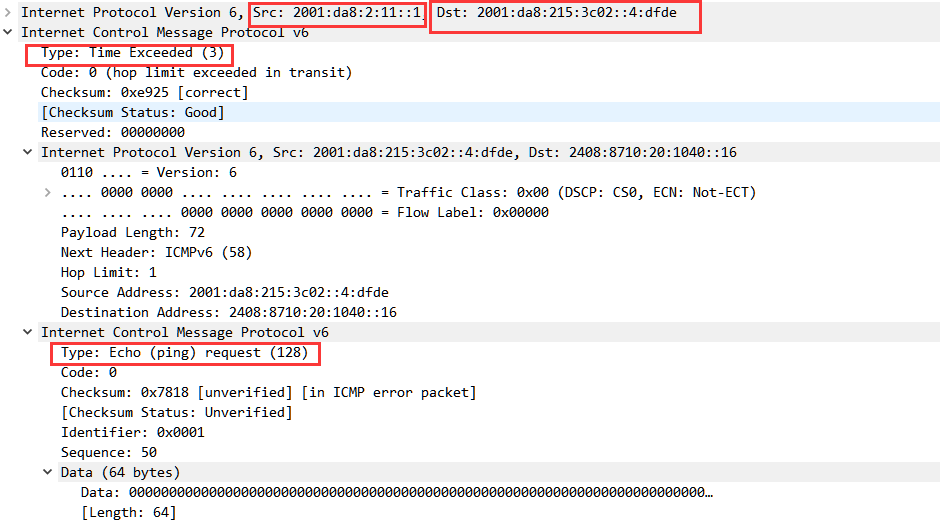
结合命令行显示以及抓包分析结果可知，每次主机向目标地址发送递增的hop 限制的 Echo request 报文，并且每次发送三个为一组。当 hop limit 减为 0 时，中间路由将会向主机回发超时报文，主机以此获得每一跳的路由信息。在实际实验过程中，总共进行了 hop limit 1~21 的 echo request，其中除了 5 以外，每个跳数限制下的请求报文均得到了回应。

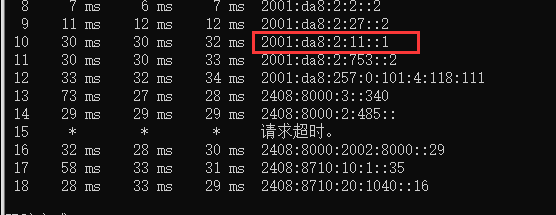
总体而言，我们可以将整个过程分为三类：发送的 request 有收到超时 time exceeded 的（1-4 & 6-20）；发送的 request 没有收到超时 time exceeded 的（5）；发送的 echo request 收到了 echo reply 报文的回复（21）。

* **ICMPv6-Echo Request**



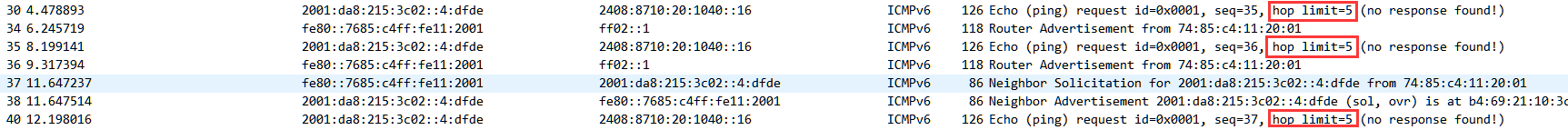
* **ICMPv6-time Exceeded**

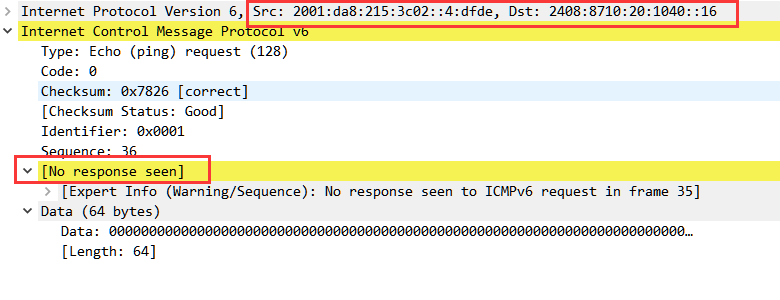




由如上报文可以看出，本机向目标主机发送了 hop limit 为 1 的报文，在经过一跳到达一个路由节点后，由于 hop limit 被减为 0，对应路由返回 time exceeded 报文。在返回的 time exceeded 的报文中可以看到对应的源地址与最终得出的路由结果里对应节点的地址一致

同时发现，当hop limit=5时：



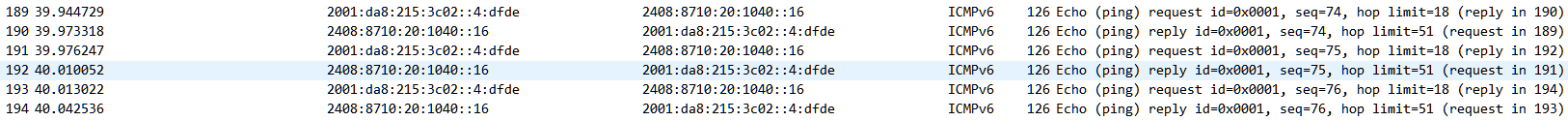


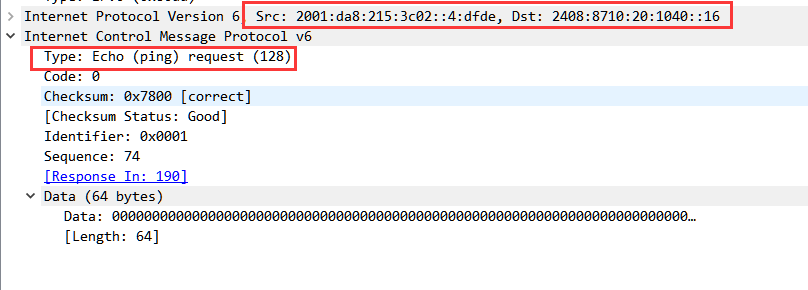
hop limit为5并未收到类似的time exceed报文回复，说明没有报文回复，可能原因是：那一跳禁止ping、不对TTL超时响应处理等

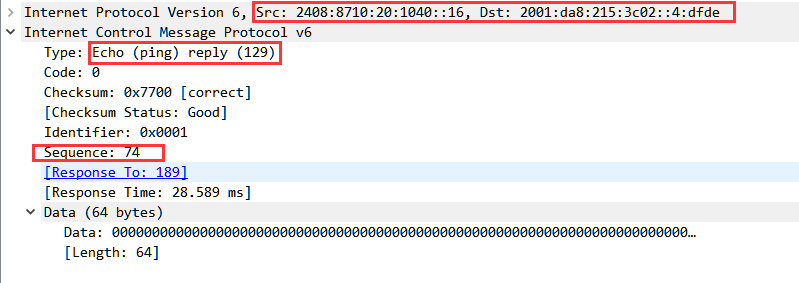
当hop limit达到18时，echo request抵达目标地址

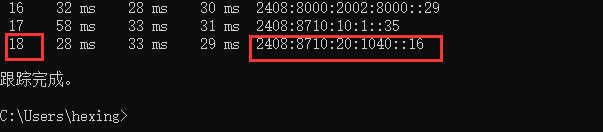
（**2408:8710:20:1040::16**）

这三组request均收到了reply报文









**五、实验问题与心得**

本次实验使用Wireshark抓包分析了ping命令和tracert命令执行过程中的报文收发情况，主要分析了ICMPv6报文的各项字段和整个过程，通过本实验，让我对于ICMPv6协议的具体内容有了更深的理解，对Wireshark抓包软件的使用更加熟练，对ICMPv6协议下的各种类型包有了更好的掌握，锻炼了我的实践能力和分析能力，让我进一步理解了ping、tarcert命令的工作原理，以及计算机网络路由的相关性知识。