**暨南大学本科实验报告专用纸**

课程名称 计算机网络实验 成绩评定

实验项目名称TCP/IP协议配置与网络实用命令指导教师 潘 冰

实验项目编号 实验二 实验项目类型 验证性 实验地点 实验室

学生姓名 周录塔 学号 2019050383

学院 智能科学与工程 系 　专业 信息安全

实验时间 2021 年 9 月 10 日 午～ 月 日 午

1. **实验目的**
   * 熟悉TCP/IP协议的配置；
   * 熟悉常见网络命令的使用；
   * 加深对TCP/IP协议的认识并对简单网络故障诊断和网络分析。
   * **进一步熟悉使用Wireshark捕获信息，初步了解ping 、tracert命令的工作过程。**
   * **培养使用wireshark对网络工作过程进行跟踪分析的习惯，为计算机网络（和网络安全）课程的学习打下基础。**

**二、实验内容**

* + 以Winodws 或linux系统为例，对TCP/IP协议进行安装和配置；
  + 利用**ipconfig**查看主机接口的配置，并理解其含义。
  + 利用**route**查看本机路由，并了解其含义。
  + 利用**netstat**查看当前主机上网络简介统计信息，了解其含义。
  + 利用**ping**对网络故障诊断与分析。**用wrireshark分析其工作过程**。
  + 利用**tracert**跟踪数据包在传输过程中经过的路径。**用wrireshark分析其工作过程**

**三、实验步骤**

**1.安装TCP/IP协议：**

①打开“网络和共享中心”：



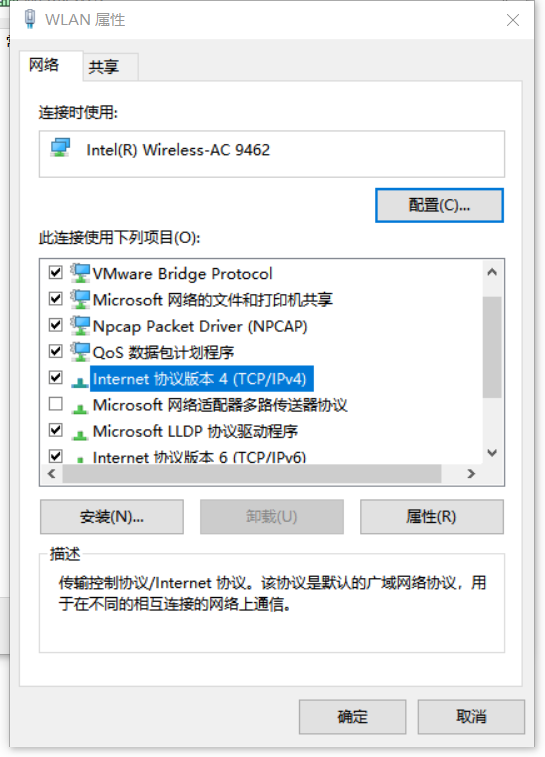
②选择本地连接：



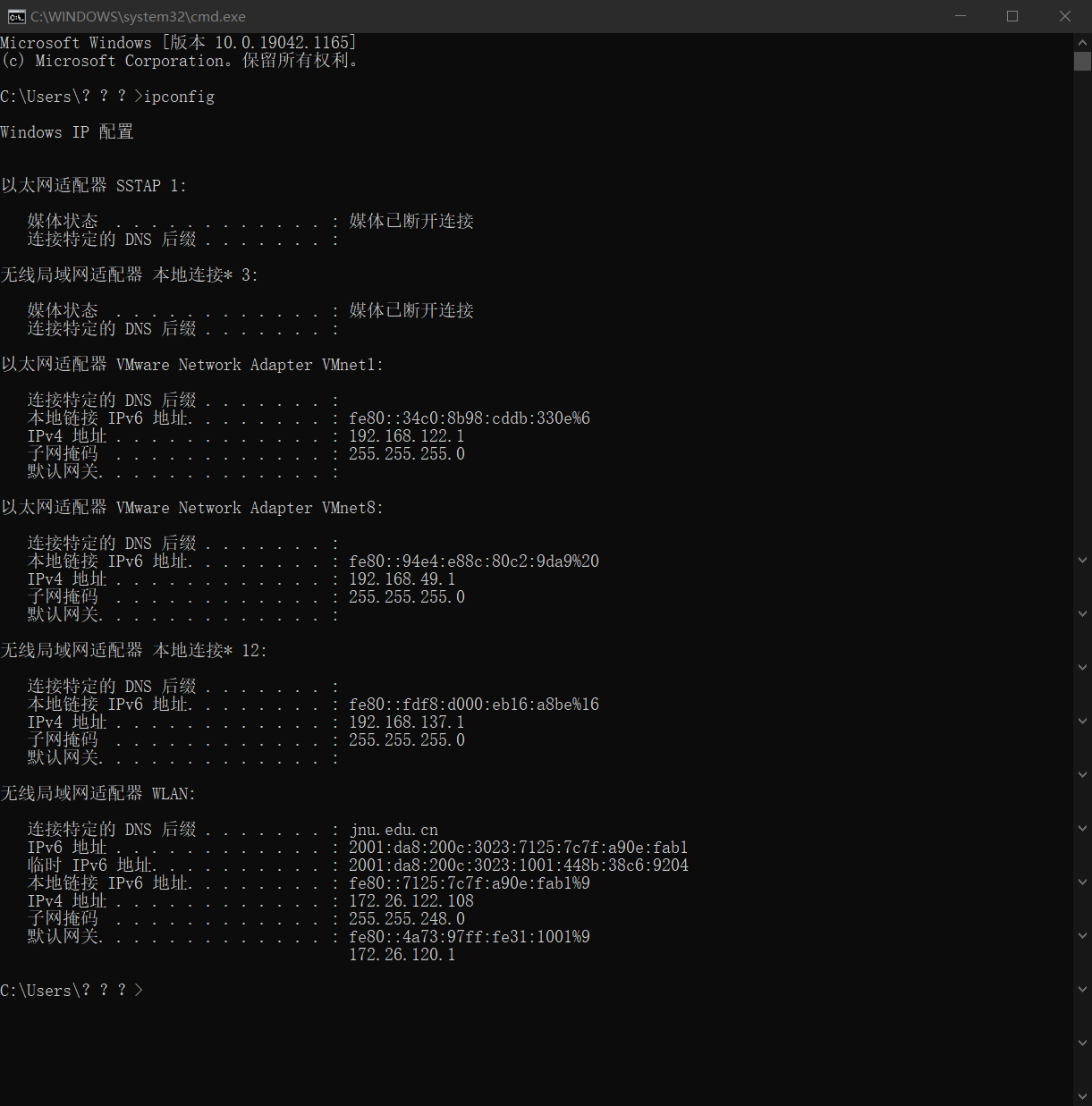
③点击属性：



④选择TCP/IPv4，点击安装，选择协议，选择安装包所在路径即可。



1. **利用ipconfig查看主机接口的配置，并理解其含义。**



**①以太网适配器：计算机与外界局域网连接是通过主机箱插入一块网络接口板（或者是在笔记本电脑中插入PCMCIA卡）。网络接口板又称通信适配器，或网络适配器，或网络接口卡NIC，简单的名称为“网卡”。**

**②DNS：DNS英文全称为：Domain Name System，域名系统。万维网上作为域名和IP地址相互映射的一个分布式数据库，能够使用户更方便的访问互联网。**

**③本地连接IPV4：IPv4是互联网协议的第四版，第一个被广泛使用，是互联网技术的基础协议。IPv4地址格式：IPv4规定格式地址长度为32（按TCP/IP参考模型划分）即有2^32-1个地址。一般的书写法为4个用小数点分开的十进制数。也有人把4位数字化成一个十进制长整数，但这种标示法并不常见。**

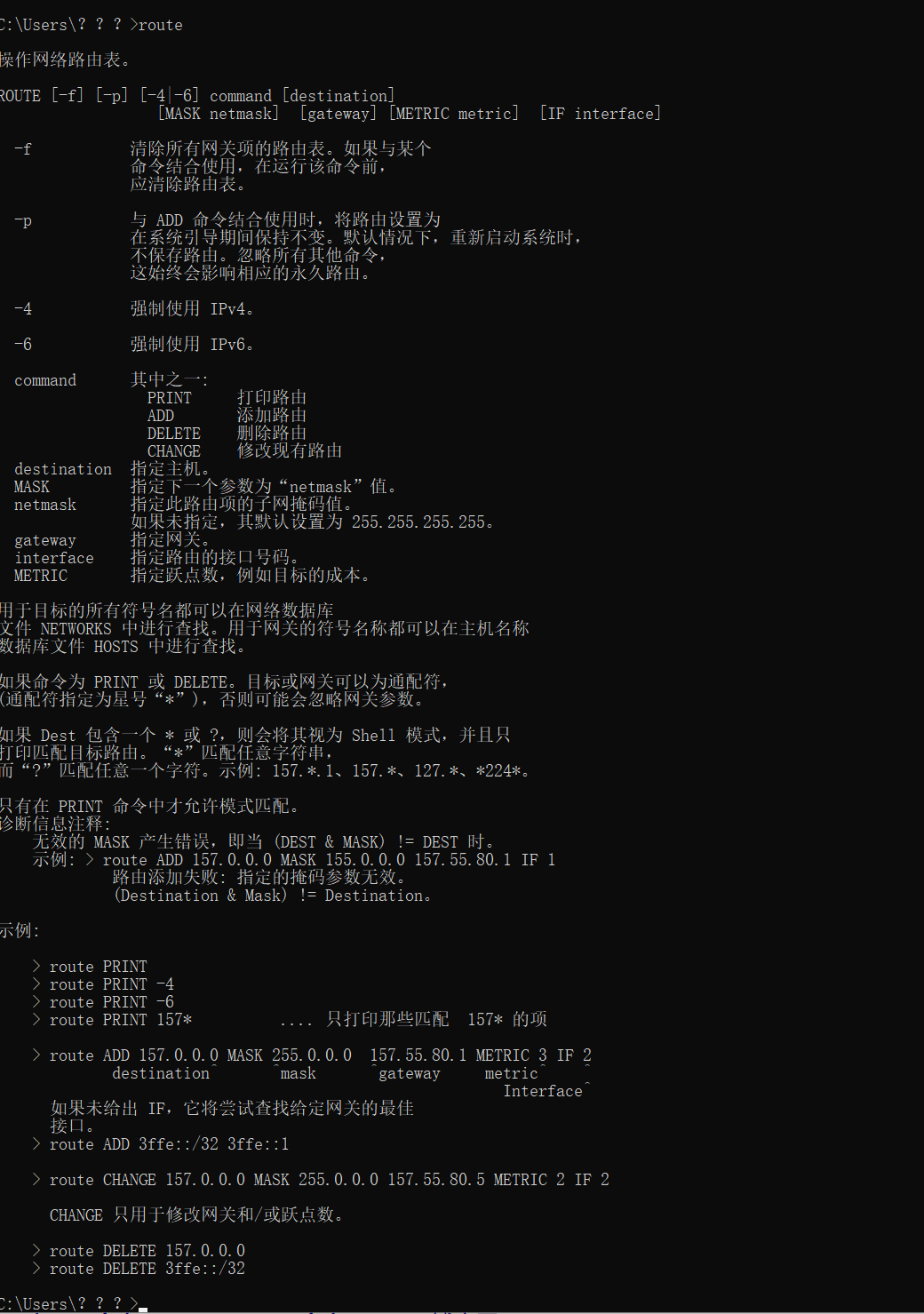
**④本地连接IPv6：IPv6是Internet Protocol Version 6的缩写，其中Internet Protocol译为“互联网协议”。IPv6是用于替代现行版本IP（IPv4）的下一代IP协议，号称可以为全世界每一粒沙子编上一个网址。IPv6 的表示方法：IPv6的地址长度为128b，是IPv4地址长度的4倍，IPv4点分十进制格式不再适用，采用十六进制表示。**

**⑤子网掩码：子关掩码与IP地址都是由4个数段组成，每个数段的取值范围是0-255（供256个值，2的8次方）。比如我们在搭建局域网时通常用到的IP地址192.168.1.1，子关掩码255.255.255.0，当然十进制是为了方便人的理解。转换成机器能识别的2进制后，每个数段有8个0或1组成的序列。一个完整的IP地址或子网掩码就转换成32个0或1的组成序列。子网掩码和IP地址是组合使用的，IP地址是计算机网络内唯一标识，而子网掩码顾名思义是用于划分子网的。**

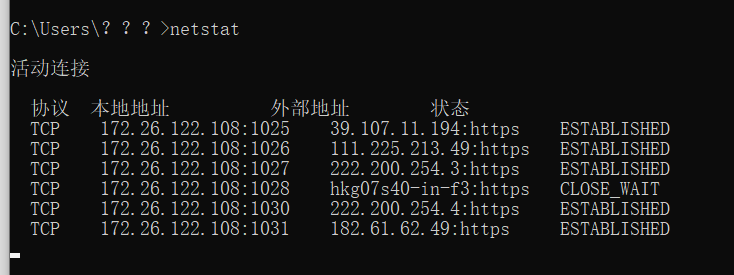
**⑥默认网关：网关（Gateway），又称网间连接器、协议转换器。网关在传输层上以实现网关互联，是最复杂的网络互联设备，仅用于两个高层协议不同的网络互联。网关既可以用于广域网互联，也可以用于局域网互联。网关是一种充当转换重任的计算机系统或设备。在使用不同的通信协议、数据格式或语言甚至体系结构完全不同的两种系统之间，网关是一个翻译器。与网桥仅仅简单的传达信息不同，网关对收到的信息要重新打包，以适应目的系统的需求。同时网关也提供过滤和安全功能。**

**默认网关：就好像一个房间有多扇门，一个主机也可以有多个网关，默认网关的意思就是，一台主机如果找不到可以用的网关，就把数据包转发给默认制定的网关，由这个网关来处理数据包。现在主机使用的网关，一般指的是默认网关。这就是为什么我们在路由器上网的时候，必须要把计算机中默认网关地址设置成路由器LAN接口地址的原因，因为路由器的LAN接口就是你所在的网络的网关，你的电脑要上网，数据必须经过网关转发出去。在一般的路由器网络中，默认网关192.168.1.1和192.168.0.1，也就是路由器LAN接口的默认IP地址。当然，也有一些智能路由器会使用其它IP地址作为默认网关，这个主要是路由器厂商出厂前设定的。**

1. **利用route查看本机路由，并了解其含义。**



1. **利用netstat查看当前主机上网络简介统计信息，了解其含义。**



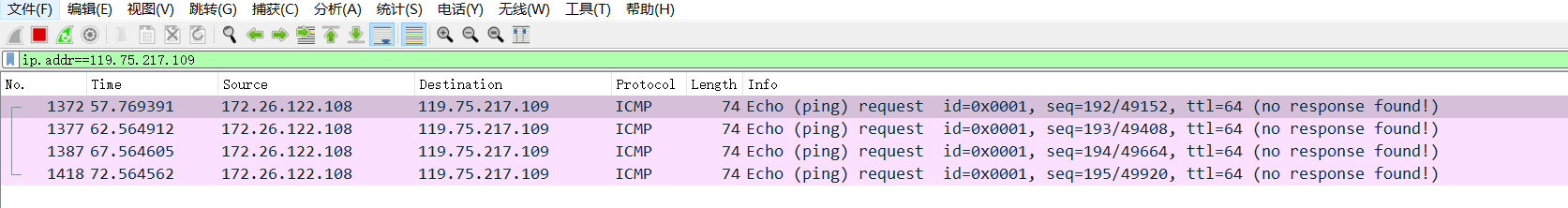
**链路状态（共12种）：**

|  |  |
| --- | --- |
| LISTEN | 首先服务端需要打开一个socket进行监听，状态为LISTEN./\* The socket is listening for incoming connections. 侦听来自远方TCP端口的连接请求 \*/ |
| SYN\_SENT | 客户端通过应用程序调用connect进行active open.于是客户端tcp发送一个SYN以请求建立一个连接.之后状态置为SYN\_SENT./\*The socket is actively attempting to establish a connection. 在发送连接请求后等待匹配的连接请求 \*/ |
| SYN\_RECV | 服务端应发出ACK确认客户端的 SYN,同时自己向客户端发送一个SYN. 之后状态置为SYN\_RECV/\* A connection request has been received from the network. 在收到和发送一个连接请求后等待对连接请求的确认 \*/ |
| ESTABLISHED | 代表一个打开的连接，双方可以进行或已经在数据交互了。/\* The socket has an established connection. 代表一个打开的连接，数据可以传送给用户 \*/ |
| FIN\_WAIT1 | 主动关闭(active close)端应用程序调用close，于是其TCP发出FIN请求主动关闭连接，之后进入FIN\_WAIT1状态./\* The socket is closed, and the connection is shutting down. 等待远程TCP的连接中断请求，或先前的连接中断请求的确认 \*/ |
| CLOSE\_WAIT | 被动关闭(passive close)端TCP接到FIN后，就发出ACK以回应FIN请求(它的接收也作为文件结束符传递给上层应用程序),并进入CLOSE\_WAIT./\* The remote end has shut down, waiting for the socket to close. 等待从本地用户发来的连接中断请求 \*/ |
| FIN\_WAIT2 | 主动关闭端接到ACK后，就进入了 FIN-WAIT-2 ./\* Connection is closed, and the socket is waiting for a shutdown from the remote end. 从远程TCP等待连接中断请求 \*/ |
| LAST\_ACK | 被动关闭端一段时间后，接收到文件结束符的应用程 序将调用CLOSE关闭连接。这导致它的TCP也发送一个 FIN,等待对方的ACK.就进入了LAST-ACK ./\* The remote end has shut down, and the socket is closed. Waiting for acknowledgement. 等待原来发向远程TCP的连接中断请求的确认 \*/ |
| TIME\_WAIT | 在主动关闭端接收到FIN后，TCP 就发送ACK包，并进入TIME-WAIT状态。/\* The socket is waiting after close to handle packets still in the network.等待足够的时间以确保远程TCP接收到连接中断请求的确认 \*/ |
| CLOSING | 比较少见./\* Both sockets are shut down but we still don’t have all our data sent. 等待远程TCP对连接中断的确认 \*/ |
| CLOSED | 被动关闭端在接受到ACK包后，就进入了closed的状态。连接结束./\* The socket is not being used. 没有任何连接状态 \*/ |
| UNKNOWN | 未知的Socket状态。/\* The state of the socket is unknown. \*/ |

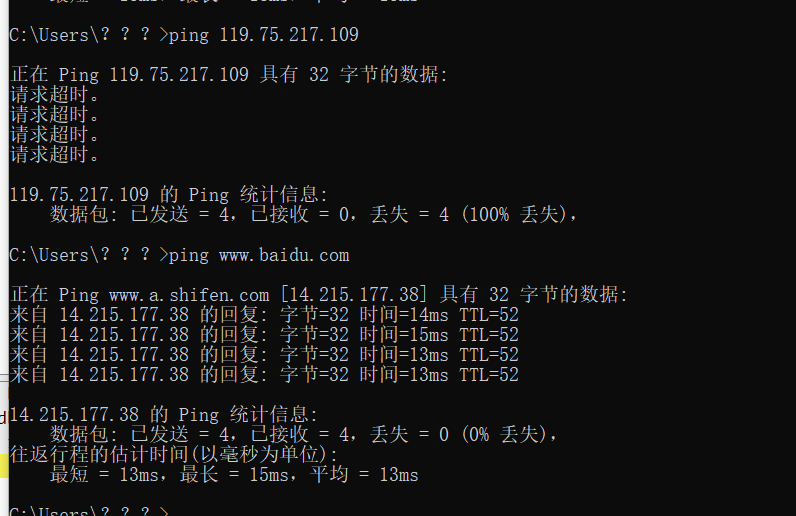
**netstat是在内核中访问网络相关信息的程序，它能够提供TCP连接、TCP和UDP监听、进程内存管理的状态。netstat也是一种控制台命令，是一个监控TCP/IP网络的非常有用的工具，他可以显示路由表、实际网络连接以及每一个网络接口设备的状态信息。使用netstat可以让用户知道有哪些网络连接正在运作，使用时如果不带参数，netstat显示活动的TCP连接。**

1. **利用ping对网络故障诊断与分析。用wrireshark分析其工作过程。**

**Ping的原理：向指定的网络地址发送一定长度的数据包，按照约定，若指定网络地址存在的话，会返回同样大小的数据包，当然，若在特定时间内没有返回，就是“超时”，会被认为指定的网络地址不存在。**

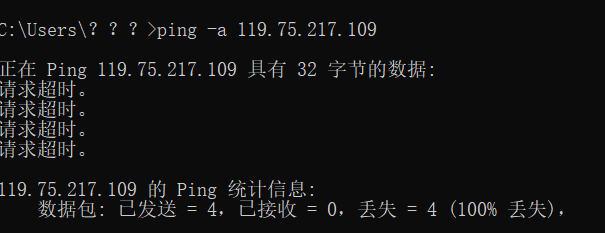


命令行ping 19.75.217.109 没有数据包返回，没有收到回应



Request Timeout的原因：a.对方已关机，或者网络上根本没有这个地址：比如在上图中主机A中PING 192.168.0.7 ,或者主机B关机了，在主机A中PING 192.168.0.5 都会得到超时的信息。b.对方与自己不在同一网段内，通过路由也无法找到对方，但有时对方确实是存在的，当然不存在也是返回超时的信息。　　c.对方确实存在，但设置了ICMP数据包过滤（比如防火墙设置）

使用了 -a参数的ping命令发现还是Timeout 判断119.75.217.109这个IP地址不存在。

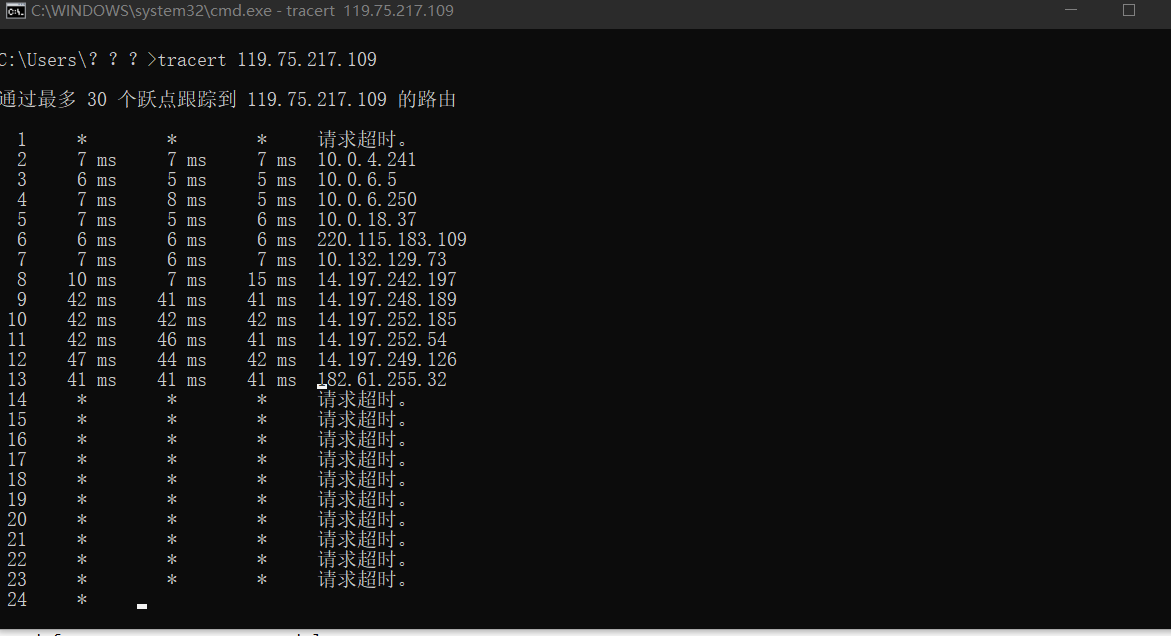


1. **利用tracert跟踪数据包在传输过程中经过的路径。用wrireshark分析其工作过程**

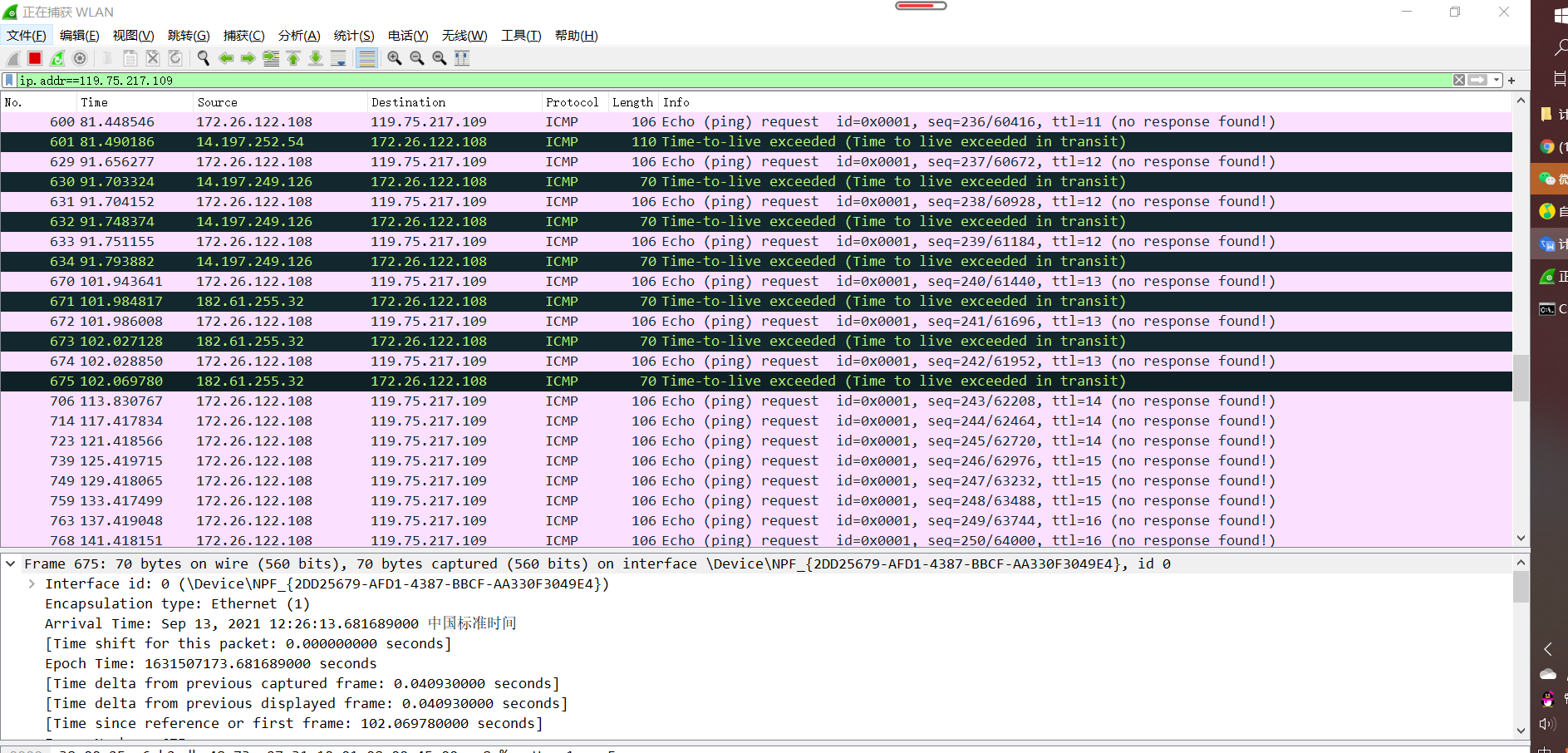
**Tracert是路由跟踪程序，用于确定 IP 数据报访问目标所经过的路径。Tracert 命令用 IP 生存时间 (TTL) 字段和 ICMP 错误消息来确定从一个主机到网络上其他主机的路由。 在工作环境中有多条链路出口时，可以通过该命令查询数据是经过的哪一条链路出口。**

**Tracert一般用来检测故障的位置，我们可以使用用tracert IP命令确定数据包在网络上的停止位置，来判断在哪个环节上出了问题，虽然还是没有确定是什么问题，但它已经告诉了我们问题所在的地方，方便检测网络中存在的问题。**

**tracert命令跟踪主机与119.75.217.109的数据包的发送路由。**



**Wireshark抓包跟踪路由过程：**



**通过向目标发送不同 IP 生存时间 (TTL) 值的“Internet 控制消息协议 (ICMP)”回应数据包，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 TTL 递减 1。数据包上的 TTL 减为 0 时，路由器应该将“ICMP 已超时”的消息发回源系统。**

**Tracert 先发送 TTL 为 1 的回应数据包，并在随后的每次发送过程将 TTL 递增 1，直到目标响应或 TTL 达到最大值，从而确定路由。通过检查中间路由器发回的“ICMP 已超时”的消息确定路由。某些路由器不经询问直接丢弃 TTL 过期的数据包，这在 Tracert 实用程序中看不到。**

**四、实验总结**

**本实验熟悉了TCP/IP协议的配置、 熟悉了ping、ipconfig、route、tracert和netstat命令的使用，以及通过wireshark 分析了它们的工作过程，更加清晰地理解了命令的工作过程和原理，而不是简单的会使用而已。也更加熟悉了wireshark这个软件的使用，学会初步分析wireshark抓到的数据包的各项信息，如时间、目的IP、源IP以及数据包所包含的额外信息等。简单地使用了wireshark的过滤数据包功能，在实验过程中使用到了几次过滤筛选IP地址为“119.75.217.109”的数据包，帮助我们更加清晰地分析包的状态，对特定的包还可以观察到帧数、字节数等，还有使用的协议，具体内容等。**