**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 02 实验项目类型 验证 实验地点 b402

学生姓名 邓芷灵 学号 2019051115

学院 智能科学与工程学院 系 专业 信息安全

实验时间2021 年9月7日 上 午～9月7日上 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。
* 了解用Wireshark捕获信息，初步理解ping 、tracert命令的工作原理。
* 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。

1. **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tracet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

1. **实验设备**

一台具有网络功能的PC机

1. **实验环境**

JNU校园网

1. **实验步骤**

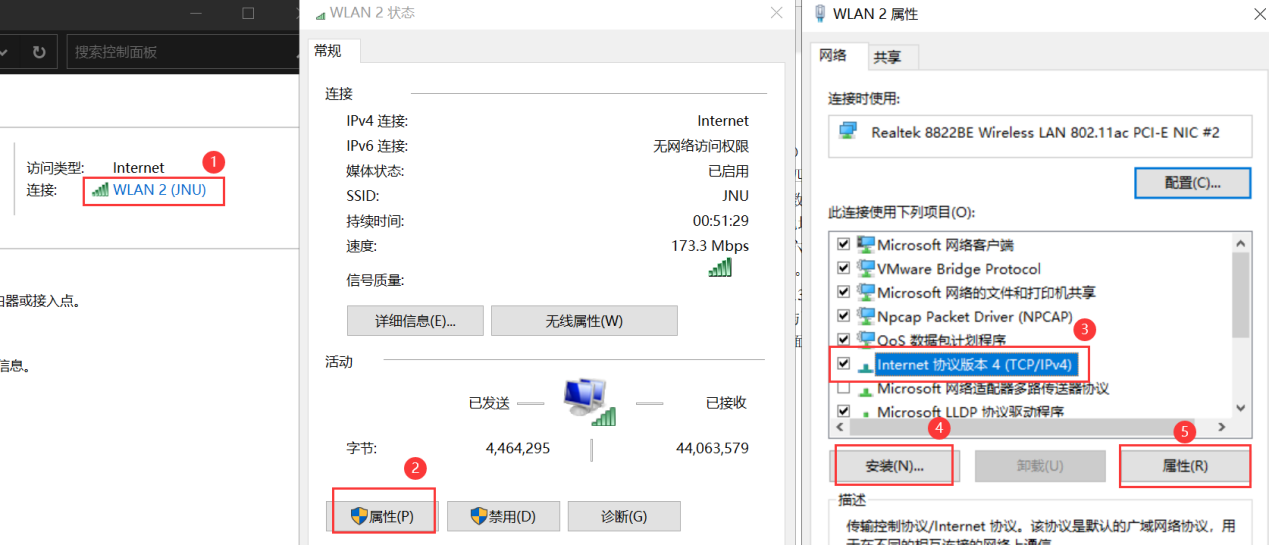
**1.TCP/IP协议的安装和配置**

（1）术语了解

* TCP/IP协议：即互联网协议套件（IPS），为互联网的基础通信架构。TCP（传输控制协议）和IP（网际协议）是该协议家族中最早通过的标准，因此又称为TCP/IP协议。
* IPv4：即网际协议第四版（Internet Protocol version 4），也是该协议第一个被广泛使用的版本。该协议负责数据包的传输，操作在链路层上。该版本采用32位地址，因此地址总数只有232个。地址常用格式为以点分隔的4个十进制字节，如192.0.2.235。
* IPv6：即网际协议第六版（Internet Protocol version 6），设计目的在于取代IPv4。该版本采用128位地址。地址格式为以冒号分隔的8组4位十六进制数，如：2001:0db8:86a3:08d3:1319:8a2e:0370:7344。
* TCP：传输控制协议（Transmission Control Protocol），为传输层通讯协议，在IP层之上。负责建立可靠连接，将上层交付的数据分割成适当长度的报文段并传给IP层。

1. TCP/IP协议的安装与配置

Windows10下，控制面板 > 网络和Internet > 查看网络状态和任务 > 活动网络 > 属性，如图所示：

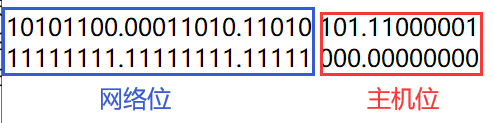


点击安装即可按引导自行从磁盘中安装相应协议。

点击属性可打开配置面板对TCP/IP协议进行配置，如图：



* 图中的“如果网络支持此功能”指的是DHCP（Dynamic Host Configuration Protocol，动态主机设置协议），使网络管理员能够集中管理和自动分配IP网络地址，通常被应用在大型的局域网络环境中。本实验机连接的是JNU校园网，由图中可见是支持DHCP的。
* 子网掩码：用于判断两个IP是否属于同一网段，即用于表明IP中的网络号和主机号分别是什么。如本机IP：172.26.213.193，子网掩码为255.255.248.0，分别转换为二进制数再做与运算，结果与IP相比不变的前若干位即网络位，变为0的后若干位即主机位。两个IP网络位相同即位于同一网段，可以直接通信；不在同一网段则需要经过网关。（子网掩码subnet mask，可以由字面意思理解为遮掩网络位的遮罩）



* 默认网关：为主机提供默认路由以便与远程网络上的其他主机通信。当不存在到目标主机的特定路由时，主机会将数据转发至默认网关。
* DNS服务器：将域名解析为IP地址。

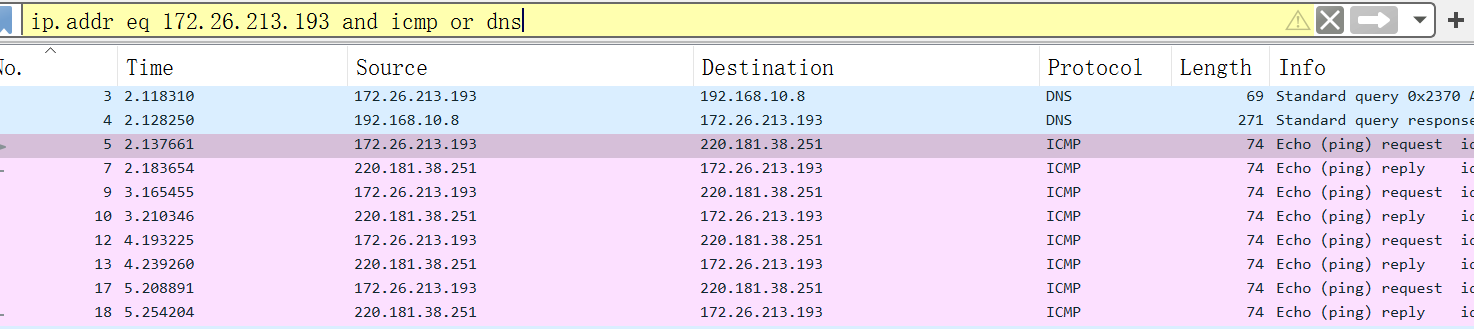
1. **常见网络命令的使用**
2. Ping

Ping baidu.com 并用wireshark捕获：



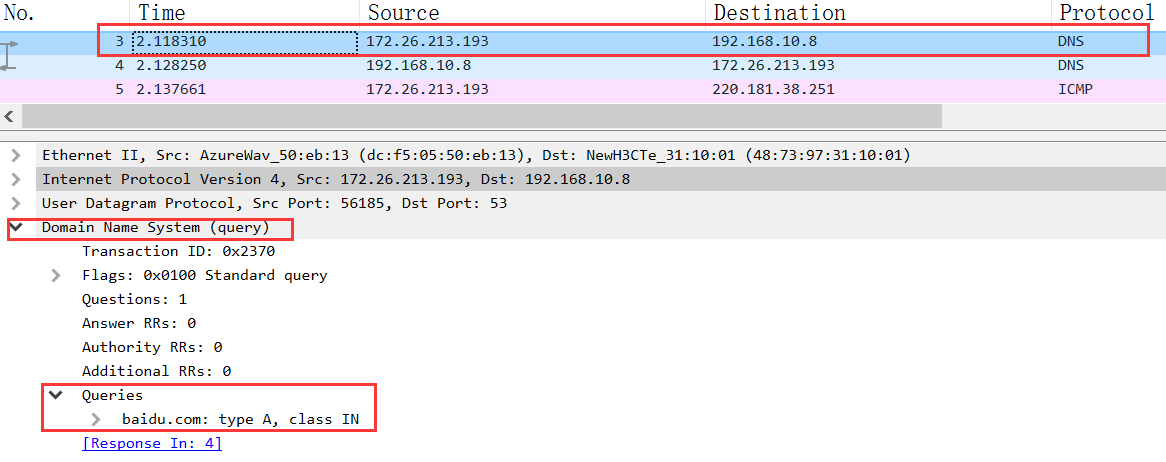
* ping命令默认向目标主机发送4个32字节的数据包，并等待接收回应数据包。
* TTL是数据包被允许转发的最大次数，避免其在网络中的无限循环和收发。
* 220.181.38.251是域名baidu.com解析到的IP地址。

wireshark捕获信息如图：

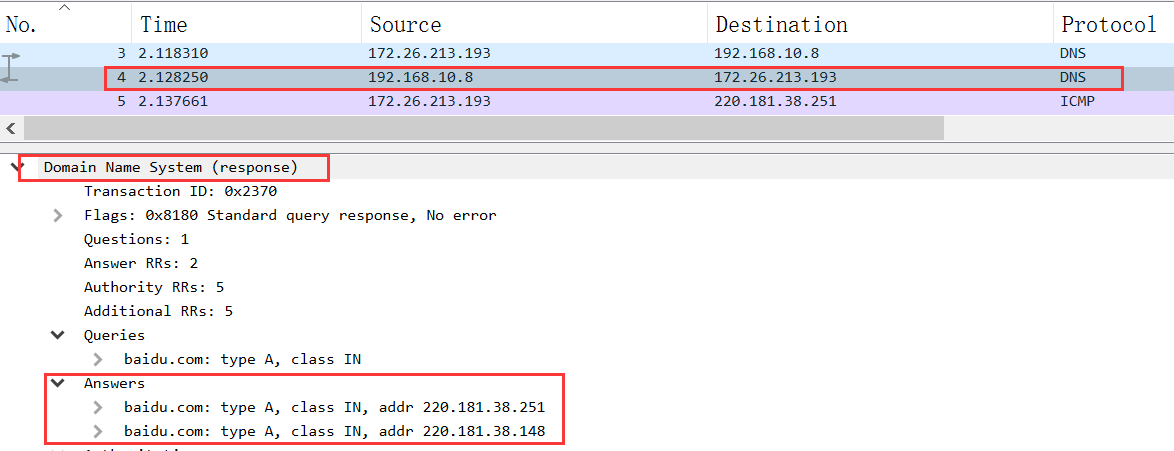


初步分析Ping工作过程如下：

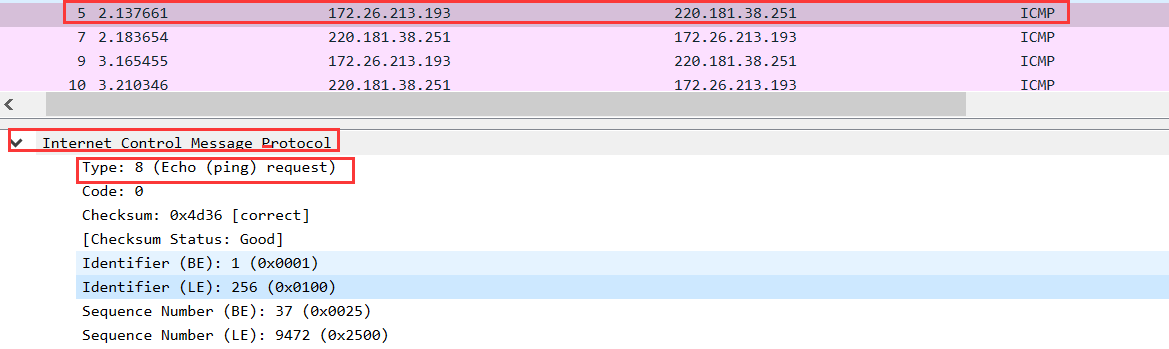
1. 首先转发至DNS服务器192.168.10.8（这是校园网自动配置的），查询A记录，如图。



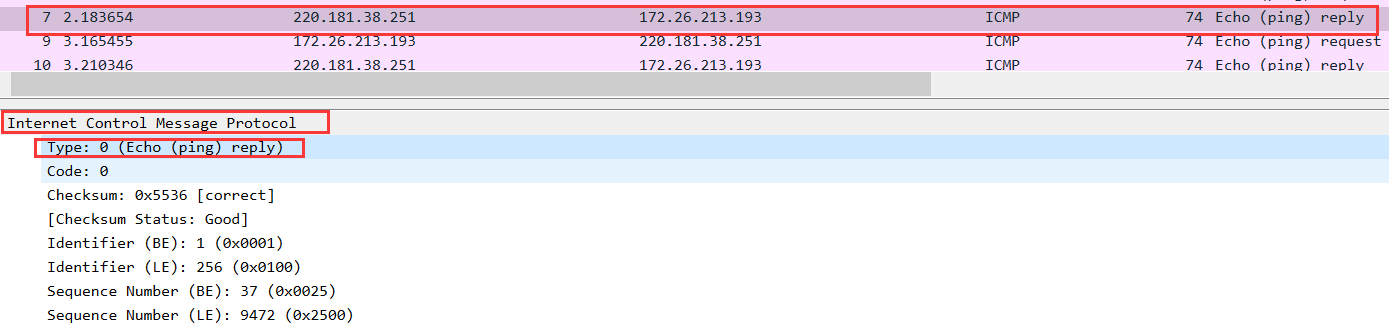
1. 本机收到回应，得到目标主机IP，如图。



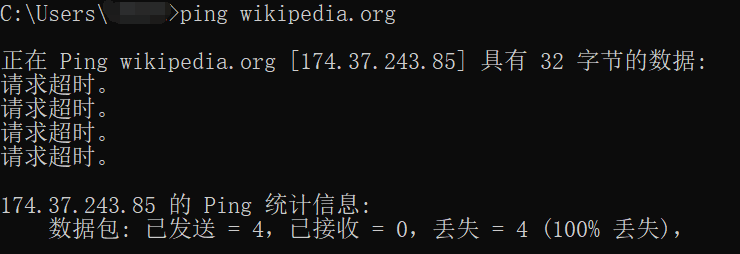
1. 本机向目标主机IP通过ICMP发送请求回显数据包（Echo Request）。



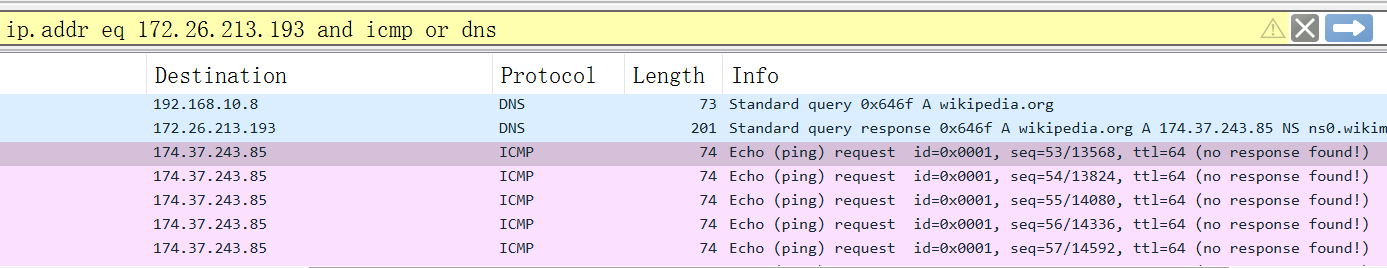
1. 本机接收回显相应数据包（Echo Reply）。



以上是成功的ping，下面是请求超时的情况：



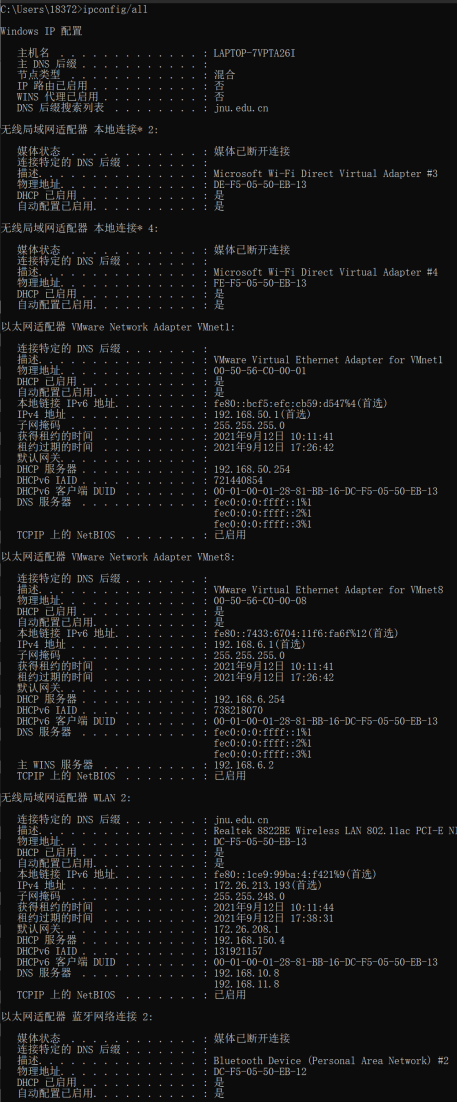
Wireshark捕获相关信息显示如下：



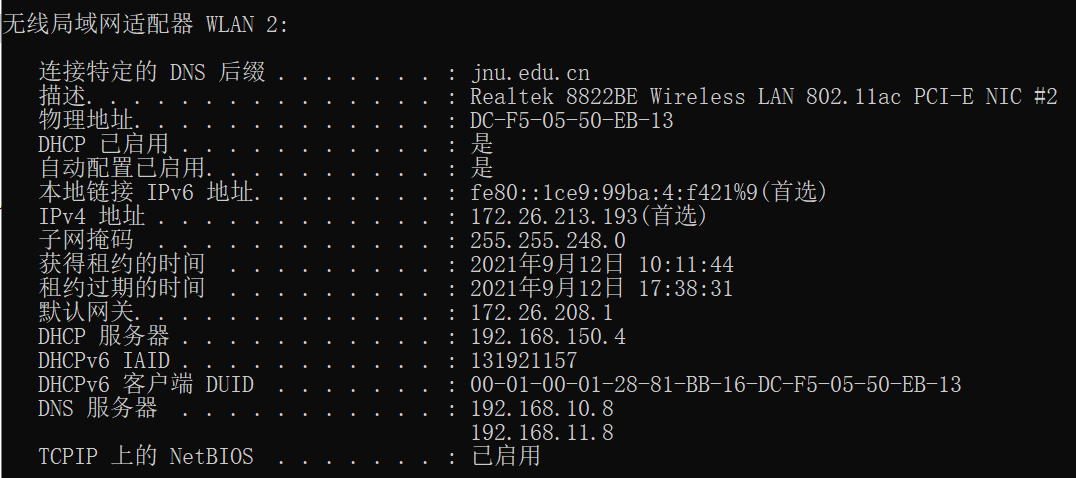
表明DNS可将域名解析为IP 174.37.243.85，并且本机可以发送回显请求，但收不到回显数据包。

1. ipconfig

在命令行窗口输入ipconfig/all，结果如下图：



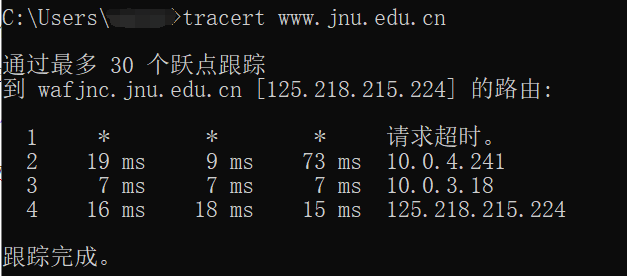
本机主机相关信息主要在“无线局域网适配器WLAN2”部分，如图：



* IP地址（IPv4地址）：172.26.213.193，本机的IP地址。
* 子网掩码：255.255.248.0，具体作用已在前文说明。
* 默认网关：172.26.208.1，向位于外网的目标主机发送信息时进行转发默认网关IP地址。
* 物理地址（MAC地址）：DC-F5-05-50-EB-13，固化在网卡中的地址，用于标记主机。
* 已启用DHCP及自动配置：通过DHCP自动获取IP地址等TCP/IP配置。
* 未使用IPv6协议。因为没有显示IPv6相关信息，只有本地链接IPv6地址，它与DHCP自动分配地址有关。
* 租约：DHCP指定的本机所分配IP地址的使用时长。若在过期时本机仍在工作，会自动续约。
* DNS服务器：用于将域名解析到对应IP地址的服务器，如当本机通过域名访问网页时会通过它。图中有两个DNS服务器的IP地址，分别为首选DNS服务器和备用DNS服务器。

1. tracert

在命令行窗口输入tracert www.jnu.edu.cn，结果如下：



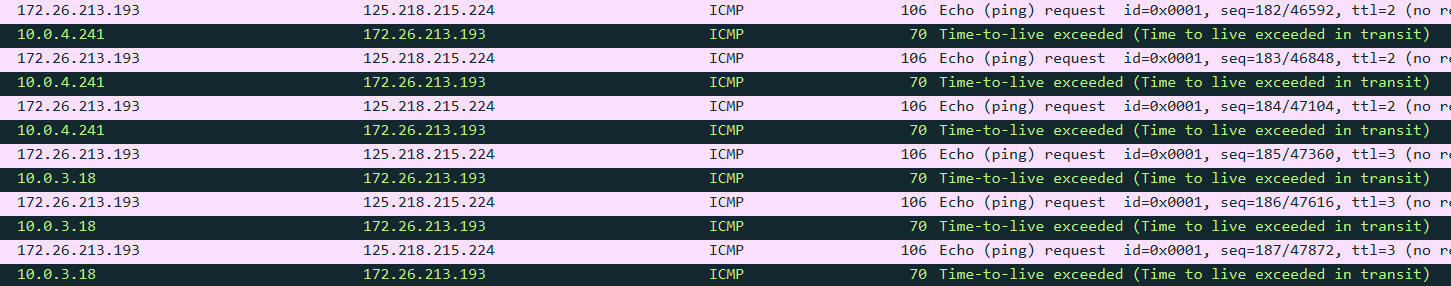
从左到右的5条信息分别代表了“生存时间”（每途经一个路由器结点自增1）、“三次发送的ICMP包返回时间”（共计3个，单位为毫秒ms）和“途经路由器的IP地址”（如果有主机名，还会包含主机名）。

初步分析tracert工作过程如下：

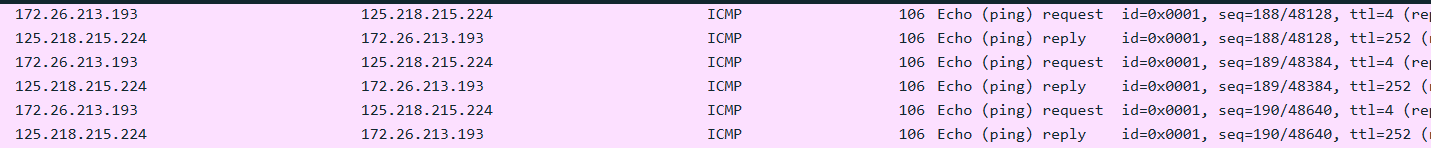
①初始时，本机向目标主机发送1个回显请求数据包，并将该数据包TTL设置为1。

②到达路由器时，TTL减1。

③当TTL为0时，数据包被丢弃。最后一个经手的路由器向源主机发送一个Time-to-live exceeded的ICMP信息。



④重复①-③，每次重复时初始TTL加1。直到目标主机收到数据包并发送响应数据包。

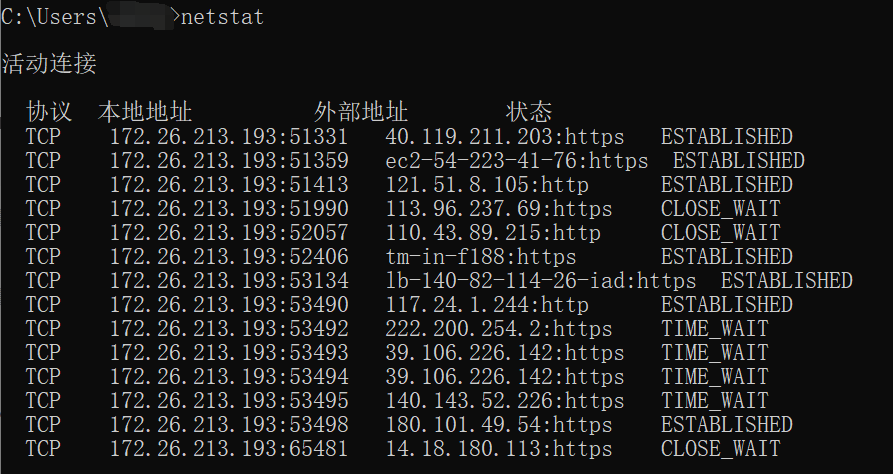


⑤本机收到相应数据包，tracert结束。

总结：tracert命令通过递增地设置数据包的TTL时间，利用路由器丢弃数据包时会向源主机发送ICMP信息这一机制，间接获得数据包转发路径上的路由器信息。在实验中，当TTL为1,时，第一个经手的路由器没有在给定的时间内发出ICMP信息，因此打印\*号并说明超时，然后继续进行。由ICMP信息发送者可知后续经手的路由器分别为10.0.4.241和10.0.3.18。在TTL=4时，数据包最终转发到了目的主机。

1. Netstat

在命令行窗口输入netstat，结果如下：



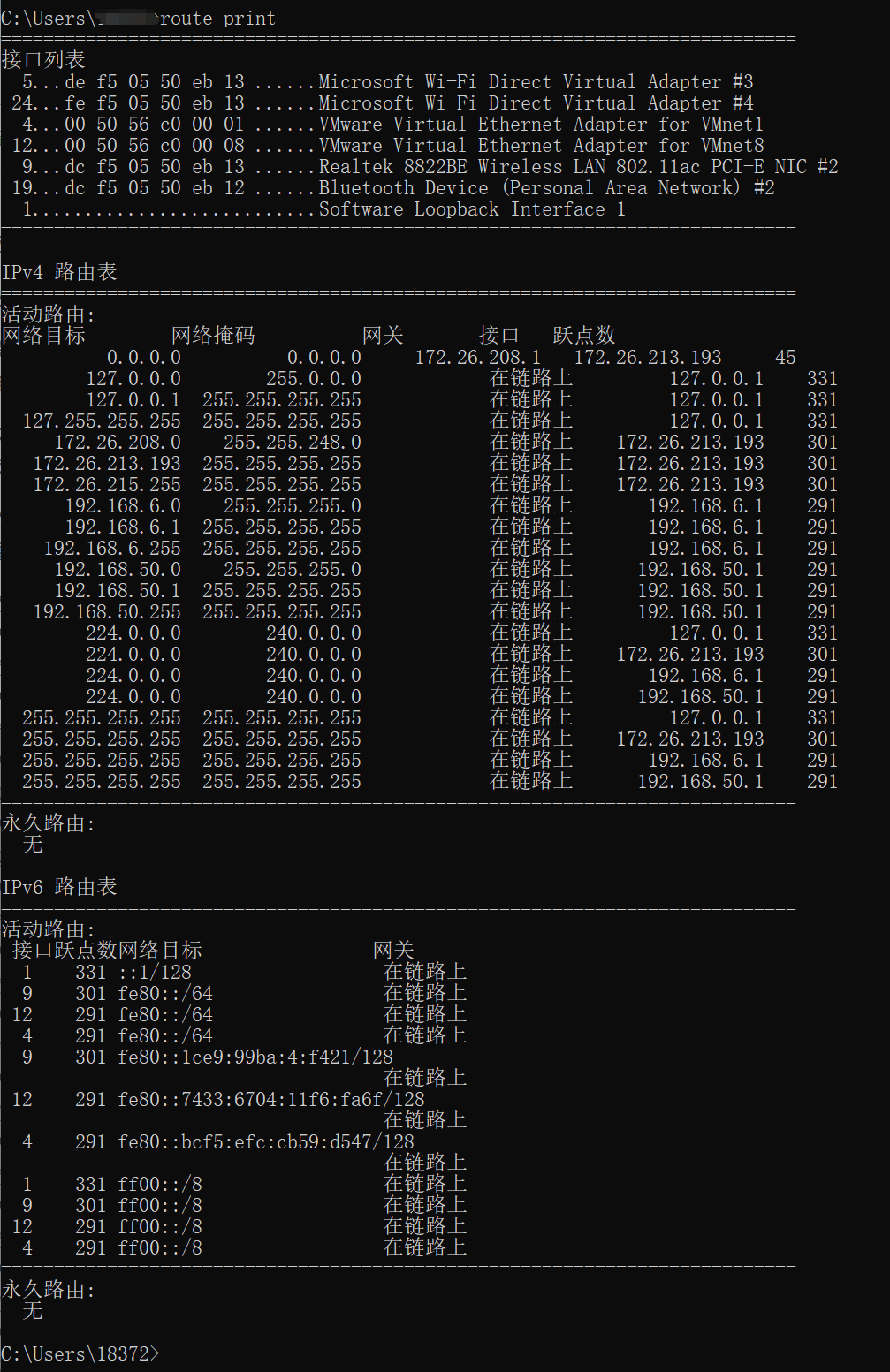
* 本地地址：本地计算机的IP地址和正在使用的端口号
* 外部地址：远程计算机的IP地址和正在使用的端口号
* 状态：TCP的连接状态，列表如下：

|  |  |
| --- | --- |
| CLOSED | 初始状态，表示TCP连接关闭 |
| CLOSE\_WAIT | 正在等待关闭，下一步动作是关闭自己到对方的连接 |
| ESTABLISHED | TCP连接已经成功建立 |
| LISTEN | 正在监听连接请求 |
| SYNC\_RCVD | 接收到了对方请求连接的报文 |
| SYN\_SENT | 发送了连接请求 |
| FIN\_WAIT\_1 | 处于ESTABLISHED状态时向对方发送FIN报文主动关闭连接后转入该状态 |
| FIN\_WAIT\_2 | 接上，接收到ACK报文后从FIN\_WAIT\_1转入该状态 |
| TIME\_WAIT | 表示收到了对方的FIN报文，并发送出了ACK报文。 |
| CLOSING | 处于FIN\_WAIT\_1状态，期望收到ACK报文但收到了FIN报文时转入该状态，表示双方都发出了关闭连接请求 |
| LAST\_ACK | 被动关闭连接的一方发送FIN报文后转入该状态 |

* ACK：回执。接收方在接受到发送方发送的报文后，向发送方发送ACK报文确认收到。
* FIN：发送该报文，表示主动终止自己到对方的连接。
* SYN：同步序列编号，是TCP/IP建立连接时使用的握手信号。
* 三次握手：TCP连接建立的过程。①客户端向服务器发送SYN包，并进入SYN\_SENT状态；②服务器收到SYN包并确认，再向客户端发送SYN+ACK包，并进入SYN\_RECV状态；③客户端收到SYN+ACK包，再向服务器发送ACK包，客户端和服务器都进入ESTABLISHED状态，TCP连接成功建立。
* 四次挥手：TCP连接终止协议。①客户端向服务器发送FIN包，主动关闭客户端到服务器的连接。②服务器收到FIN包，再向客户端发送ACK包。③服务器关闭到客户端的连接，并向客户端发送FIN。④客户端收到FIN，向服务器发送ACK确认。

1. route

在命令行窗口输入route print，结果如下：



* 网络目标：路由器连接的所有网段
* 网络掩码：提供这个网段本身的子网掩码
* 网关：表示下一跳的IP地址
* 接口：表示连接到了合适的目的网络的网卡
* 跃点数：所经过的路由器数量

1. **思考题**
2. TCP/IP协议配置中的“网关”作用是什么？

答：用于子网与外网连接。对于同在本地子网中的主机，可以直接发送信息；但如果目标主机不在本地子网中，则需要将信息送至网关，由网关转发到其他网络，进一步寻找目标主机。

1. 如何用ping 检测网络中的故障点？用ping 测试网络连通性时，若出现“Destination host unreahable”，则意味着什么？“Destionation host unreachable”和“Time out”的区别是什么？

答：用ping检测网络故障点有以下四个方面：①ping 127.0.0.1，即ping本主机，用于确定本机TCP/IP能否正常工作；②ping 本机IP，用于确定网络适配器是否正常工作；③ping 网关IP，用于确定数据包是否正常到达网关；④ping 网址，用于确定DNS服务器是否能正常解析域名。

“Destionation host unreachable”表示目标主机不可达，即不存在能到达目标主机的路由，可能是因为物理连接等存在问题。与“Time out”的区别在于，后者表示连接超时，但存在能到达目标主机的路由。

1. **实验总结**

一开始做实验时对TCP/IP协议族并没有多少概念，但在搜索术语解释的过程中逐渐将TCP、IPv4、IPv6与之前已有的对网络结构的概念关联起来，如TCP在传输层提供可靠的数据流端对端传输，其实就像是将下面网络层IP的工作做了个“封装”，比起直接面对网络层的数据包传输，在传输层的TCP提供了更完整的服务。

配置TCP/IP协议时其实已经被自动配置了，由此去了解了背后的协议——DHCP，通过它可以更方便地管理和分配大型局域网的IP地址。在了解子网掩码时搜索到各类比喻，但总的来说其实只是一个用于判断IP地址网络位和主机位的工具，让IP地址与它做个与运算即可。

在熟悉网络常用命令的过程中没有遇到太大困难，Wireshark很清楚地列出了各类信息，可以很直观地初步分析ping、tracert等命令的工作过程。tracert命令稍微有点复杂，但分析后发现只是在利用TTL的设置及路由器丢包时通知源主机的机制，间接获取转发路径上的路由器信息。

通过搜索Netstat命令显示出的各种TCP状态，间接了解到了三次握手和四次挥手，各TCP状态大多数在这两个过程中有体现，将各个状态融入到这两个过程中进行理解会更好。

最实用的还是学会了用ping并且结合目前学到的网络知识排查网络故障，家里网络出现问题的时候不会一头雾水了，至少可以知道一下原因。