**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 2 实验项目类型 验证型 实验地点 实B402

学生姓名 张景曦 学号 2019051098

学院 智能科学与工程学院 系 计算机 专业 信息安全

实验时间 2021 年 9 月 8 日 上 午～ 9 月 12日 上午

温度 27 ℃ 湿度 70%

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。
2. **实验内容和要求**
   * 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
3. **主要仪器设备**
   * 一台具有网络功能的PC 机
4. **实验环境**

计算机网络实验平台（D组）、以及校园网络环境。

1. **实验步骤与调试**

1. **TCP/IP协议的安装和配置**

①打开控制面板，点击网络和Internet进入



②点击进入网络和共享中心



③选择本地连接（WLAN）



④点击属性进入，勾选Internet协议版本4（TCP/Ipv4），再点击安装，选择确定



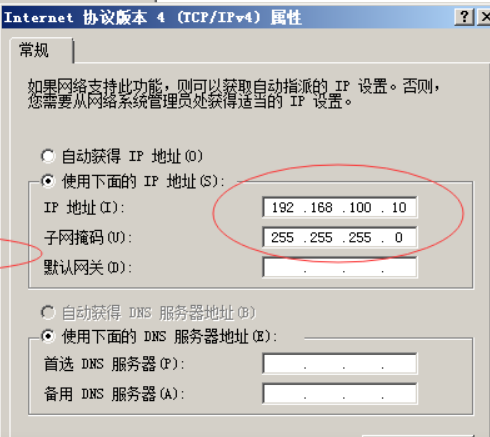
⑤弹出的界面中选择协议，然后点击添加

⑥在界面中点击从磁盘安装，在厂商文件复制来源框中键入“C:\WINDOWS\inf”再点击确定

⑦进入的界面中选择Internet 协议(TCP/IP)，点击确定（IPv6同理）



我的电脑已经自动获得IP地址，若要手动配置，则按如下操作





TCP/IP是指能够在多个不同网络间实现信息传输的协议簇。TCP/IP协议不仅仅指的是TCP 和IP两个协议，而是指一个由FTP、SMTP、TCP、UDP、IP等协议构成的协议簇， 只是因为在TCP/IP协议中TCP协议和IP协议最具代表性，所以被称为TCP/IP协议。

TCP/IP传输协议，即传输控制/网络协议，也叫作网络通讯协议。它是在网络的使用中的最基本的通信协议。TCP/IP传输协议对互联网中各部分进行通信的标准和方法进行了规定。并且，TCP/IP传输协议是保证网络数据信息及时、完整传输的两个重要的协议。TCP/IP传输协议是严格来说是一个四层的体系结构，应用层、传输层、网络层和数据链路层都包含。

TCP/IP协议是Internet最基本的协议,其中应用层的主要协议有Telnet、FTP、SMTP等，是用来接收来自传输层的数据或者按不同应用要求与方式将数据传输至传输层；传输层的主要协议有UDP、TCP，是使用者使用平台和计算机信息网内部数据结合的通道，可以实现数据传输与数据共享；网络层的主要协议有ICMP、IP、IGMP，主要负责网络中数据包的传送等；而网络访问层，也叫网路接口层或数据链路层，主要协议有ARP、RARP，主要功能是提供链路管理错误检测、对不同通信媒介有关信息细节问题进行有效处理等。

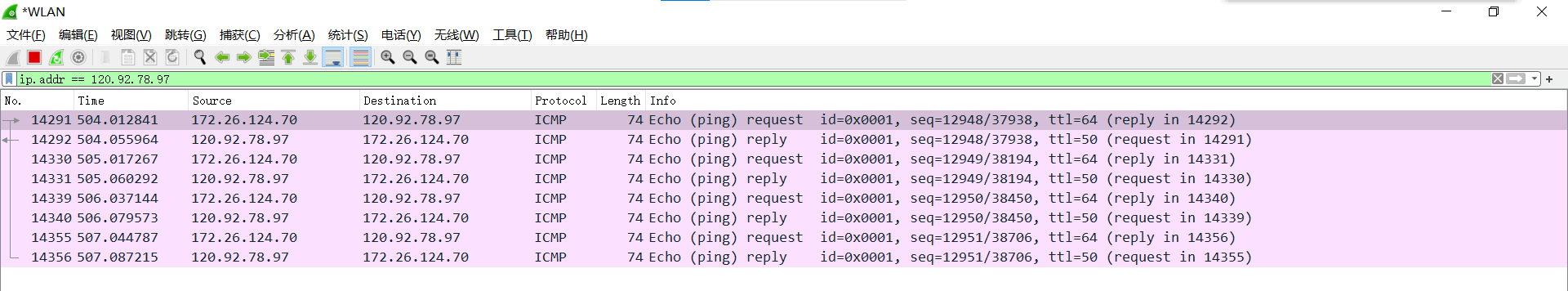
2. **常见网络命令的使用**

（1）Ping

在主机上打开windows命令行窗口；输入ping IP地址或域名 ，观察输出结果，并记录相关信息。**（注意对成功或失败两种情况的测试。熟悉显示的信息。用wireshark捕获相关信息并初步分析ping的工作过程，相关协议ICMP在网络层学习。）**

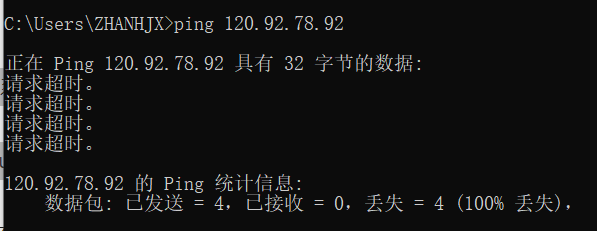
①ping B站

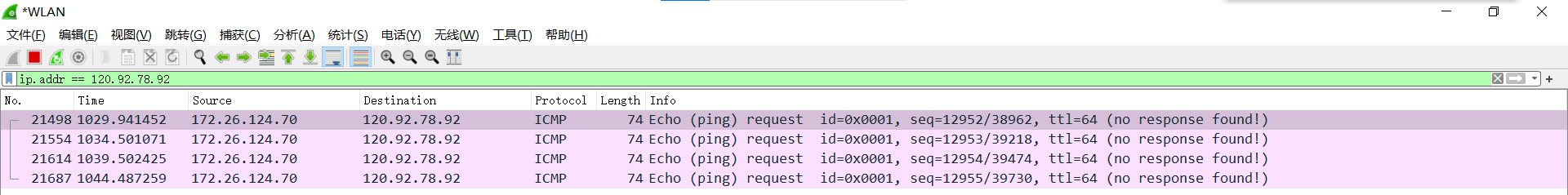




成功ping到了B站（丢包率为0）

②失败的情况，丢包率100%





③每次ping计算机都会向该ip地址发送4个数据包，字节和时间均有记录。成功的话则会收到4条回复，失败则请求超时无回复。

④TTL值：Time To Live,表示DNS记录在DNS服务器上存在的时间，它是IP协议包的一个值，告诉路由器该数据包何时需要被丢弃。可以通过Ping返回的TTL值大小，粗略地判断目标系统类型是Windows系列还是UNIX/Linux系列。

默认情况下，Linux系统的TTL值为64或255，WindowsNT/2000/XP系统的TTL值为128，Windows98系统的TTL值为32，UNIX主机的TTL值为255。

因此一般TTL值：

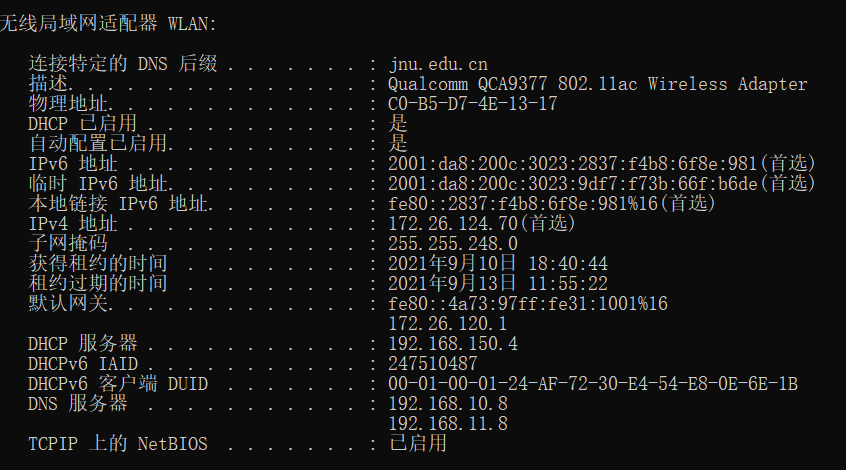
100~130ms之间，Windows系统 ；

240~255ms之间，UNIX/Linux系统。

（2）ipconfig

在主机上打开windows命令行窗口；输入ipconfig/all。观察测试出本地主机的 IP 地址、网卡地址等信息，可以查看配置的情况。（要求能熟悉并理解主要内容，观察是否使用IPV6协议。）

可以看到显示的信息有校园网的IPv4和IPv6的地址、子网掩码、获得租约的时间、租约过期的时间、默认网关等信息。

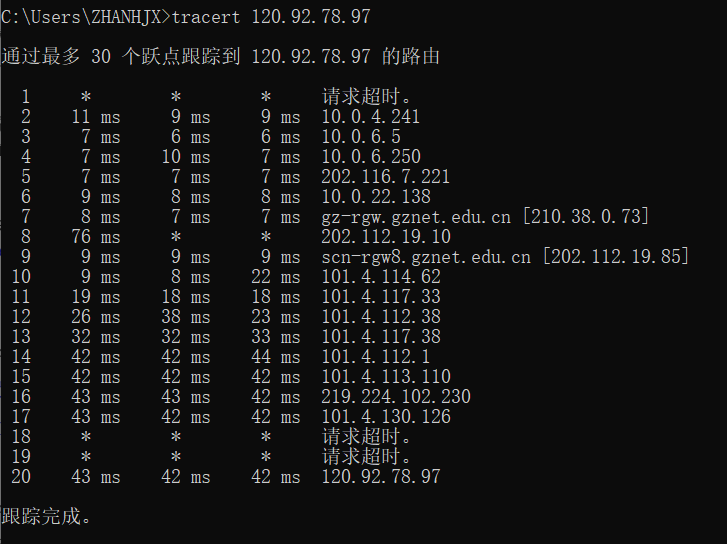


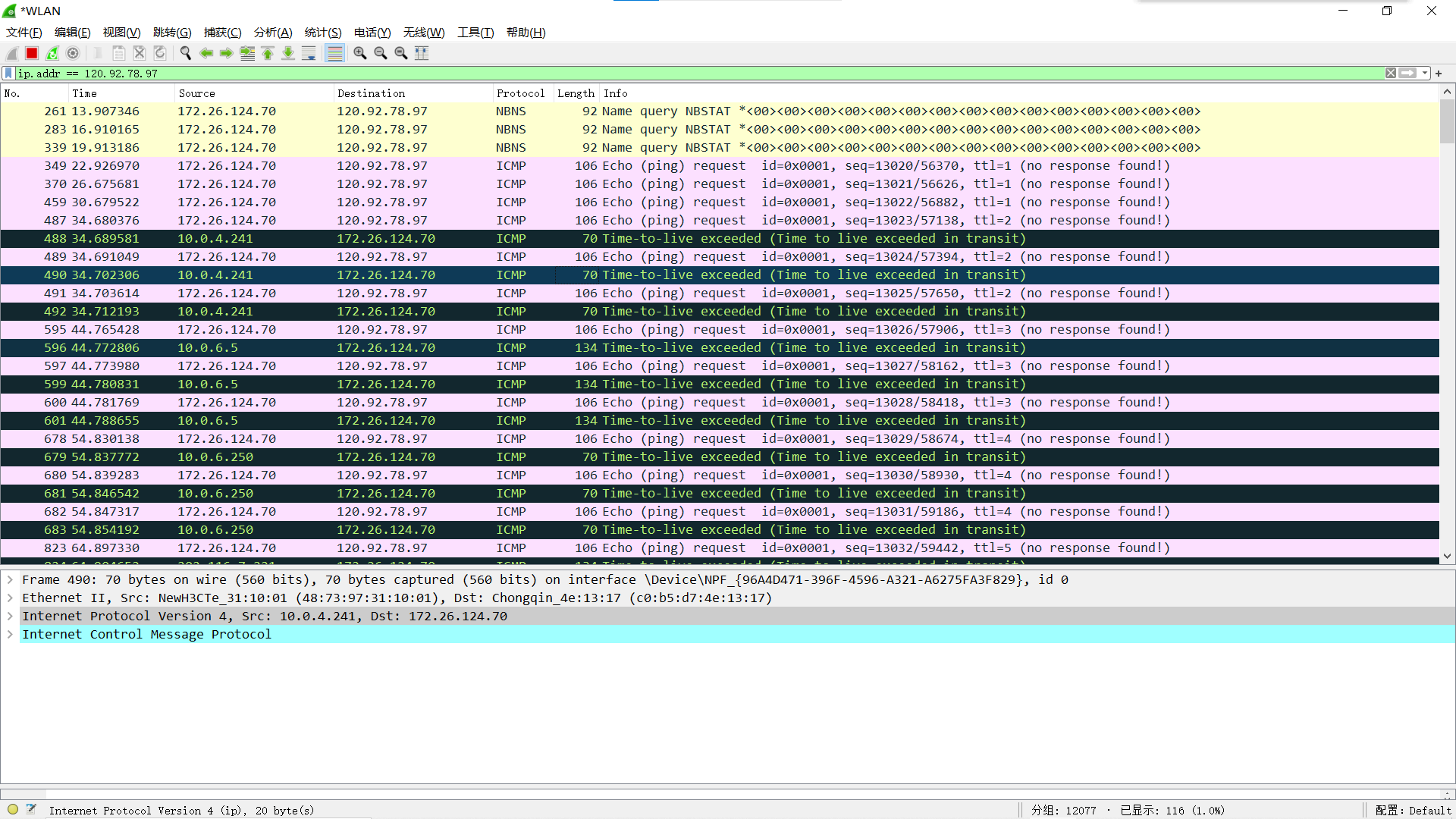
（3）tracert

在主机上打开windows命令行窗口；输入tracert tracert IP地址或主机名,观察用户数据所经过路径上各个路由器的信息，内容包括：每一站的编号、反应时间、站点名称或IP 地址。从中可以查看路由器处理时间的差别。（要求能熟悉显示内容，并用wireshark初步分析该命令的工作过程，其中使用的IP和ICMP协议在网络层学习。）

tracert 是一个简单的网络诊断工具，可以列出分组经过的路由节点，以及它在IP 网络中每一跳的延迟。

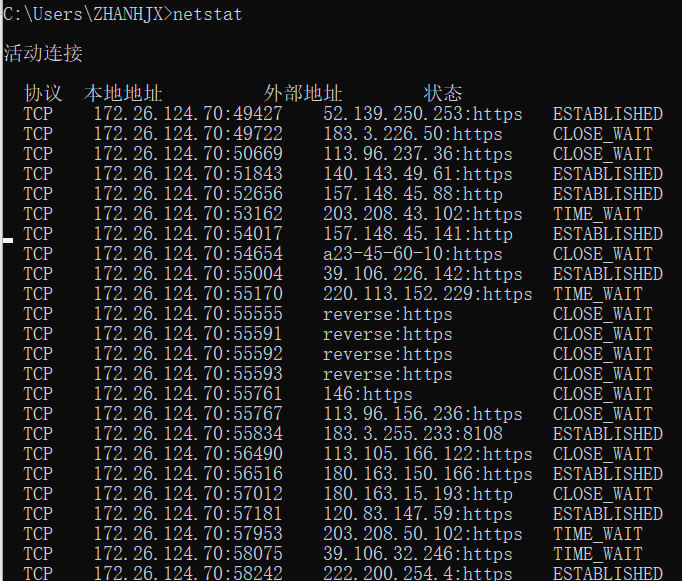
观察B站，第一列是每一站的编号，第二三四列是反应时间，第五列是站点名称或IP 地址。





（4）netstat

在主机上打开windows命令行窗口；输入netstat 。查看网络协议的统计结果、发送和接收数据的大小，连接和侦听端口的状态。例如：netstat （要求上网查询有关TCP状态的含义，初步了解有关概念。与端口和TCP状态相关内容在运输层学习。）



LISTEN：侦听来自远方的TCP端口的连接请求

SYN-SENT：再发送连接请求后等待匹配的连接请求（客户端）

SYN-RECEIVED：再收到和发送一个连接请求后等待对方对连接请求的确认（服务器）

ESTABLISHED：代表一个打开的连接

FIN-WAIT-1：等待远程TCP连接中断请求，或先前的连接中断请求的确认

FIN-WAIT-2：从远程TCP等待连接中断请求

CLOSE-WAIT：等待从本地用户发来的连接中断请求

CLOSING：等待远程TCP对连接中断的确认

LAST-ACK：等待原来的发向远程TCP的连接中断请求的确认

TIME-WAIT：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

CLOSED：没有任何连接状态（初始状态）

一开始，建立连接之前服务器和客户端的状态都为CLOSED。服务器创建socket后开始监听，变为LISTEN状态。客户端请求建立连接，向服务器发送SYN报文，客户端的状态变为SYN\_SENT。服务器收到客户端的报文后向客户端发送ACK和SYN报文，此时服务器的状态变为SYN\_RCVD。然后，客户端收到ACK、SYN，就向服务器发送ACK，客户端状态变为ESTABLISHED，服务器收到客户端的ACK后也变为ESTABLISHED。此时，3次握手完成，连接建立！

由于tcp连接是全双工的，断开连接会比建立连接麻烦一点点。客户端先向服务器发送FIN报文，请求断开连接，其状态变为FIN\_WAIT1。服务器收到FIN后向客户端发生ACK，服务器状态变为CLOSE\_WAIT。客户端收到ACK后就进入FIN\_WAIT2状态。此时连接已经断开了一半了。如果服务器还有数据要发送给客户端，就会继续发送。直到发完了，就发送FIN报文，此时服务器进入LAST\_ACK状态。客户端收到服务器的FIN后，马上发送ACK给服务器，此时客户端进入TIME\_WAIT状态，再过了2MSL长的时间后进入CLOSED状态。服务器收到客户端的ACK就进入CLOSED状态。

至此，还有一个状态没有提及：CLOSING状态。CLOSING状态表示客户端发生了FIN，但没有收到服务器的ACK，却收到了服务器的FIN。这种情况发生在服务器发送的ACK丢包的时候，因为网络传输有时会有意外。

**注明**：（版权声明：上文为CSDN博主「hkhl\_235」的原创文章，遵循CC 4.0 BY-SA版权协议，转载请附上原文出处链接及本声明。）

原文链接：https://blog.csdn.net/hkhl\_235/article/details/79721645

（5）route

在主机上打开windows命令行窗口；输入route print。观察本机路由表情况，并进行说明。例如：route print。（要求在网上查询并熟悉每一项内容。相关内容在网络层学习。）

网络目标：此列显示目的网络IP地址

网络掩码： 此列显示目的网络的子网掩码

网关：此列显示网络连接的路由器地址

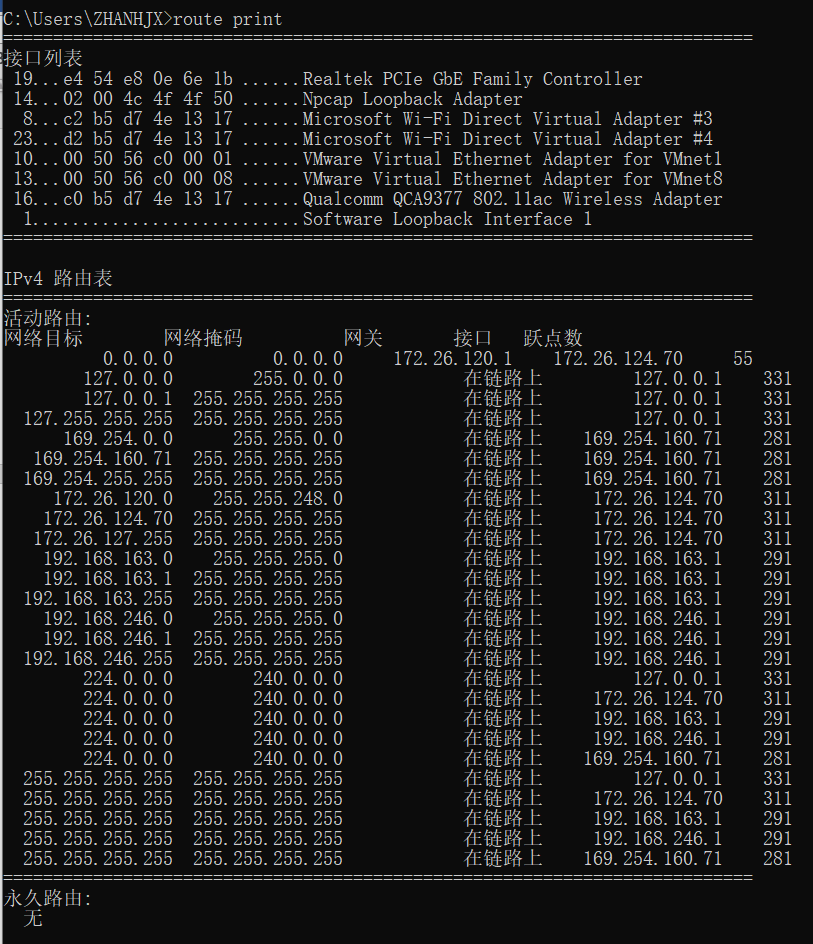
接口：此列显示接受数据的IP地址

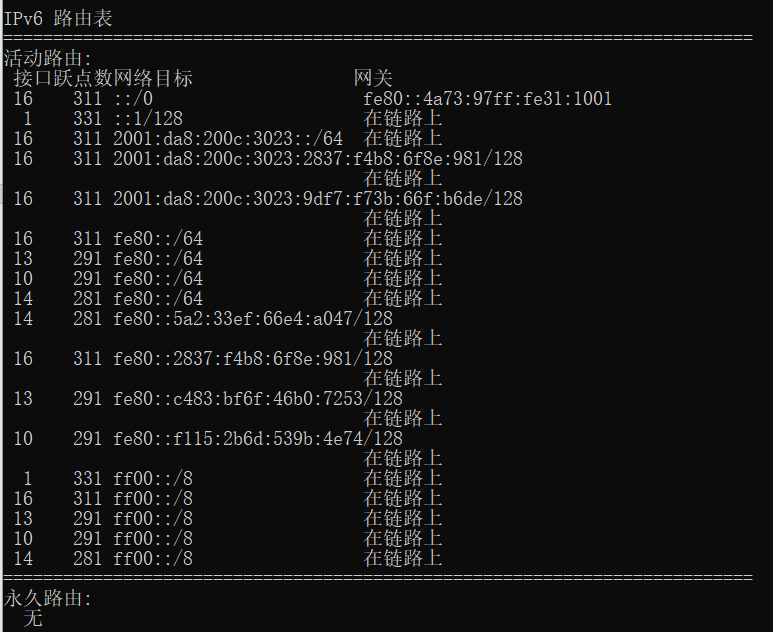
跃点数：此列表示的数据安全程度，越小越安全

网络目标 网络掩码 网关 接口 跃点数

0.0.0.0 0.0.0.0 172.26.120.1 172.26.124.70 55

表示发向任意网络的数据通过本机接口172.26.124.70被送到了一个默认网关172.26.120.1，他的跃点数是55，跃点数越小可信度越高。





1. **实验结果与分析**

【思考题】：

1、TCP/IP协议配置中的“网关”作用是什么？

网关就是一个网络连接到另一个网络的"关口"，实质上是一个网络通向其他网络的IP地址。

它的作用就是对两个网络段中的使用传输协议的数据进行互相的翻译转换，以及对网络和用户应有的保护功能。

2、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？

（1）用ping 检测网络中的故障点

①输入ping 127.0.0.1，检查本地TCP/IP协议是否安装正常，正常响应说明本地TCP/IP网络协议安装是正常的。

②输入命令ipconfig检查本地连接等网络链接的IP地址、子网掩码、默认网关。

③ping 自己的IP地址

④然后Ping一台同网段计算机的IP，不通则表明网络线路出现故障;若网络中还包含有路由器，则应先Ping路由器在本网段端口的IP，不通则此段线路有问题;通则再Ping路由器在目标计算机所在网段的端口IP，不通则是路由出现故障;通则再Ping目的机IP地址。

⑤检查电脑和互联网是否接通

（2）用ping 测试网络连通性时，若出现“Destination host unreahable”,则意味着无法访问主机。

（3）“Destionation host unreachable”和“Time out”的区别：，Destination host unreachable是ping包没有去到目的地的路由，无法与主机正常连接，Timed out是ping包没有返回的路由，导致超时。

**暨南大学本科实验报告专用纸(附页)**