**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 实验地点计算机网络实验室

学生姓名 袁霖 学号 2019051099

学院 智能科学与工程学院/人工智能产业学院 系 专业 信息安全

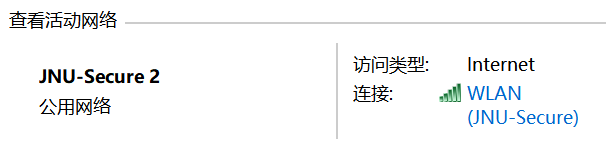
实验时间 2021 年 9 月 6 日 上 午～ 9 月 13 日 下 午

1. **实验目的**
2. 熟悉TCP/IP协议的配置；
3. 熟悉常见网络命令的使用；
4. 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。
5. **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。**
6. **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。**
7. **实验内容和要求**
8. 以Winodws 或linux系统为例，对TCP/IP协议进行安装和配置；
9. 利用**ipconfig**查看主机接口的配置，并理解其含义。
10. 利用**route**查看本机路由，并了解其含义。
11. 利用**netstat**查看当前主机上网络简介统计信息，了解其含义。
12. 利用**ping**对网络故障诊断与分析。**用wrireshark分析其工作过程**。
13. 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**
14. **主要仪器设备**

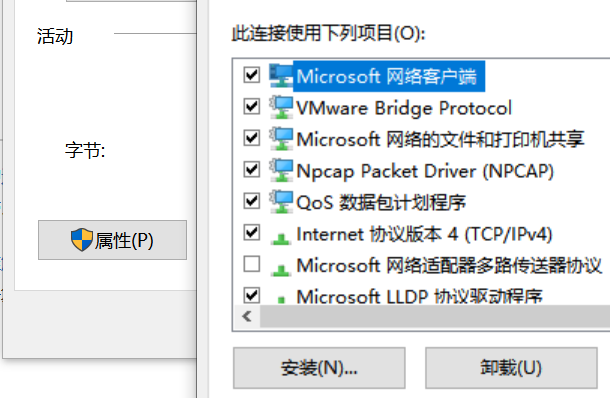
**仪器：一**台具有网络功能的PC 机

**实验环境：**win10,连接校园网

1. **实验步骤与调试**
2. TCP/IP协议的安装和配置
   1. TCP/IP协议的安装
      1. 打开控制面板，进入【网络和共享中心】，点击【连接】



* + 1. 在弹出窗口中点击【属性】，选择TCP/IPV4协议，若没有安装则选择安装即可



* 1. TCP/IP协议的配置
     1. 在【网络和共享中心】中，点击【连接】，在弹出窗口中点击【详细信息】即可查看网络连接的详细信息



* + 1. 在弹出窗口中点击【属性】，双击TCP/IPV4协议，选择【使用下面的IP地址】与【使用下面的DNS服务器地址】，即可手动配置TCP/IP协议



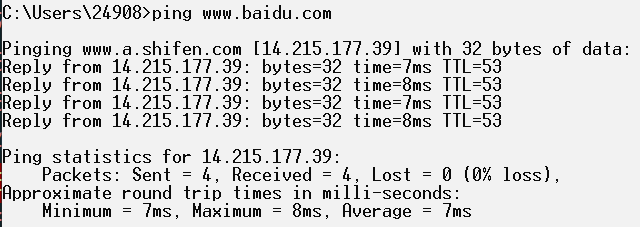
上图将主机的IP地址设置为同学的IP地址，发现两台主机不能同时连接校园网，但接入不同网络后两台主机均能上网。原因：相同的IP地址会在同一网段内发生IP地址冲突，导致两台主机或其中一台的连通性被破坏。

TCP/IP协议属性说明：

1. IP地址：互联网协议地址。IP地址是[IP协议](https://baike.baidu.com/item/IP%E5%8D%8F%E8%AE%AE/131947" \t "https://baike.baidu.com/item/IP%E5%9C%B0%E5%9D%80/_blank)提供的一种统一的[地址格式](https://baike.baidu.com/item/%E5%9C%B0%E5%9D%80%E6%A0%BC%E5%BC%8F/53569124" \t "https://baike.baidu.com/item/IP%E5%9C%B0%E5%9D%80/_blank)，它为互联网上的每一个网络和每一台[主机](https://baike.baidu.com/item/%E4%B8%BB%E6%9C%BA/455151" \t "https://baike.baidu.com/item/IP%E5%9C%B0%E5%9D%80/_blank)分配一个[逻辑地址](https://baike.baidu.com/item/%E9%80%BB%E8%BE%91%E5%9C%B0%E5%9D%80/3283849" \t "https://baike.baidu.com/item/IP%E5%9C%B0%E5%9D%80/_blank)，以此来屏蔽[物理地址](https://baike.baidu.com/item/%E7%89%A9%E7%90%86%E5%9C%B0%E5%9D%80/2901583" \t "https://baike.baidu.com/item/IP%E5%9C%B0%E5%9D%80/_blank)的差异。
2. 子网掩码：能够让路由器确定目的网络的地址类，用以区别网络标识和主机标识的地址，需要结合IP地址才有意义。它提供了网段本身的子网掩码，而不是连接到该网段网卡的子网掩码，这能够让路由器确定目的网络的地址类
3. 默认网关：在路由器将数据包转发到目的网络时，需要查看网关列表，而网关表就是告诉路由器该数据包需要转发到哪一个IP地址才能到达目的网络
4. DNS服务器：域名服务器，能够进行域名及与之相对应的IP地址的转换。
5. 常见网络命令的使用

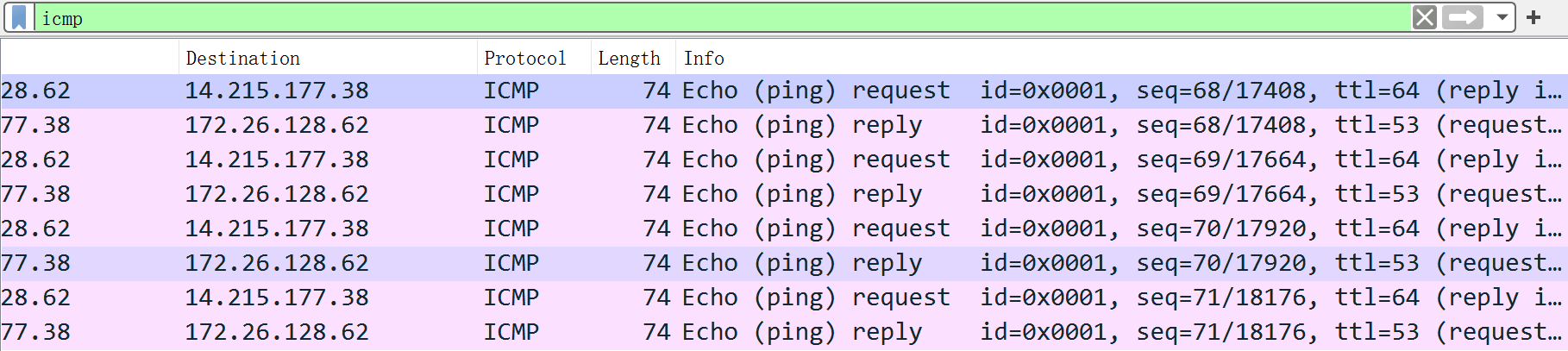
(1)利用**ping**对网络故障诊断与分析。**用wrireshark分析其工作过程**。

* + 1. ping成功情况及分析

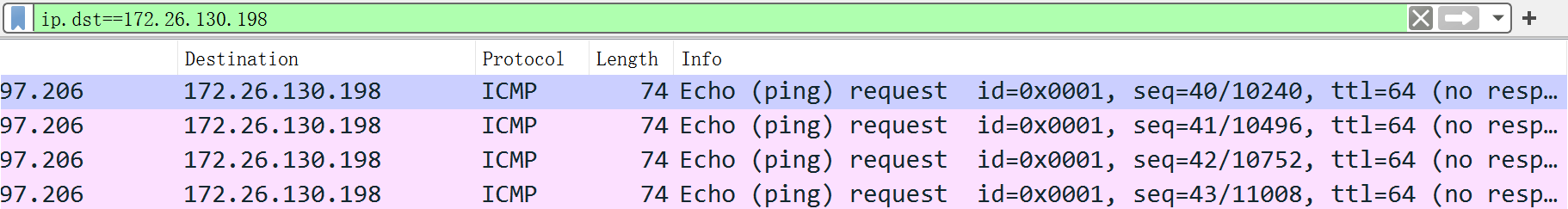


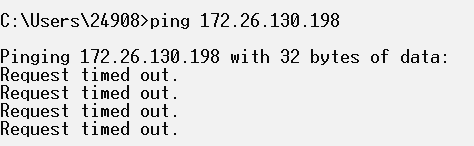
可以看到主机向百度发送了4个32字节的IP数据包，且百度均有回应。说明本机与百度服务器之间已经存在了一条连通的物理路径。并得到百度的IP地址为14.215.177.39。其中，time表示数据包返回时间。而TTL的值可以用来确定数据包经过了多少个路由器过渡段，每当数据包经过一个路由器，TTL的值就相应减一。

现通过Wireshark捕获数据包并观察结果。



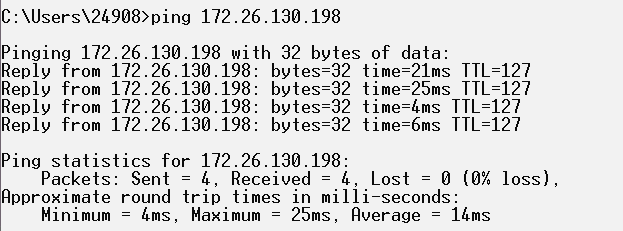
* + 1. ping失败情况及修正

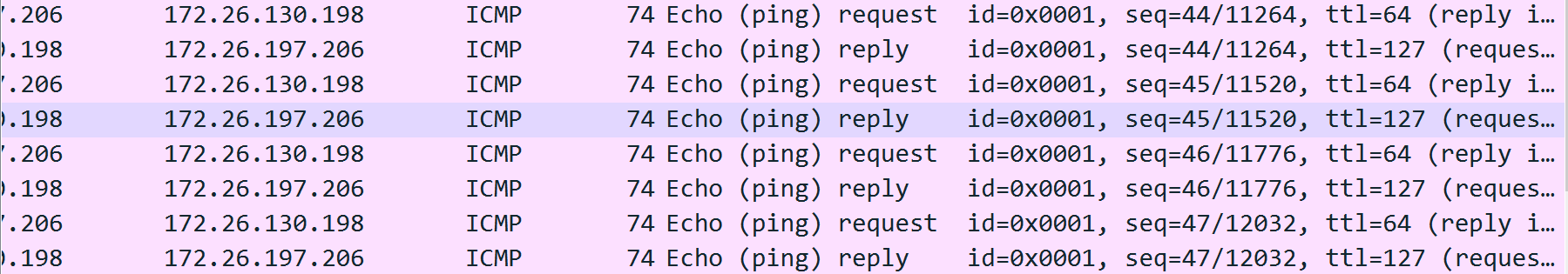




失败原因分析：ping失败会有以下几种情况1. 网线故障 2.网络适配器配置不正确 3.IP地址不正确 4.未关闭防火墙

通过检查网络配置，本次失败情况不存在前三种原因，在对方关闭防火墙以后即可ping成功。

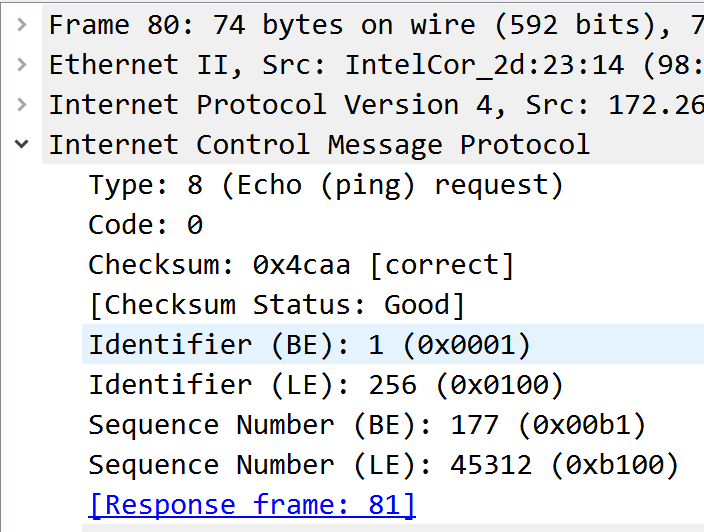




* + 1. 利用Wireshark分析ping命令的工作过程

由Wireshark的抓包结果得知，ping命令是依托于ICMP协议实现的，该协议有利于更高效地转发IP数据包。

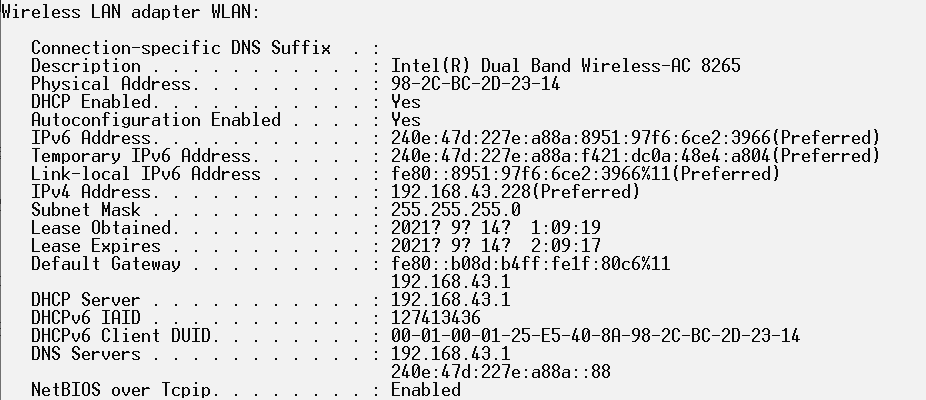
以下是一个request数据包中ICMP协议的具体内容：



可以看到，ICMP类型为8，表示ping的回声请求。由以上截图可知，在执行ping命令时，会连通源地址及目的地址构建一个ICMP请求数据包。而目的主机收到数据包后，会构建一个ICMP应答包发送给源主机。

* 1. ipconfig

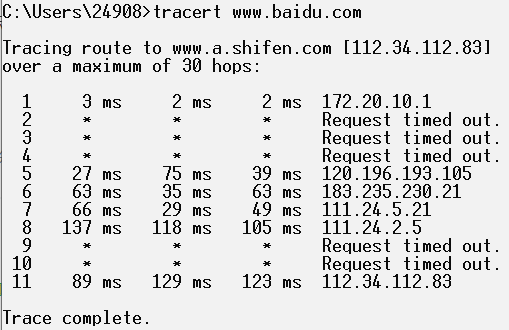
ipconfig 实用程序可以测试出本地主机的 IP 地址、网卡地址等信息，可以查看配置的情况，结果如下：



上图即为网络连接的详细信息，且说明WLAN使用了IPV6协议，分别有：

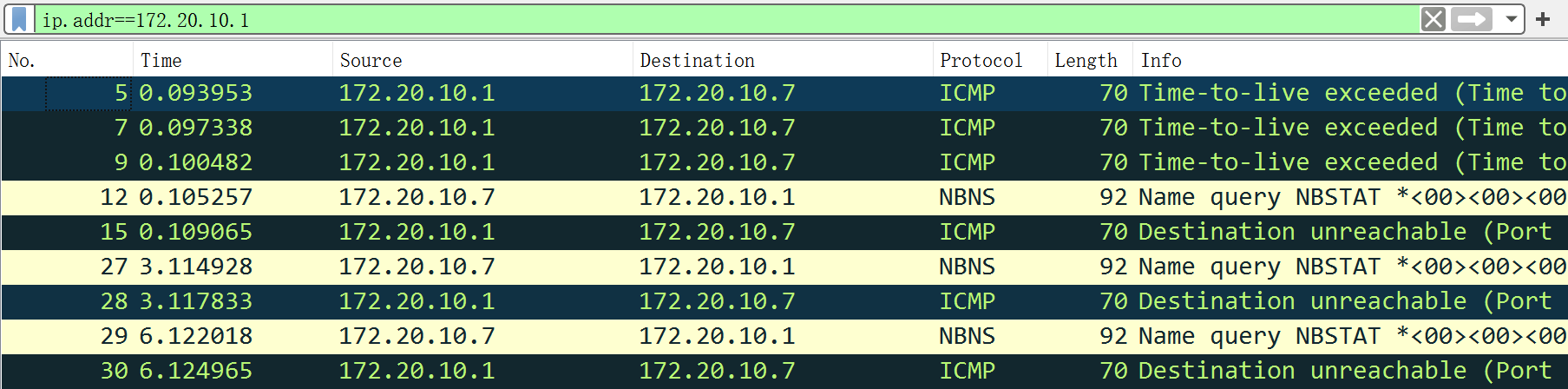
* + 1. Connection-specific DNS Suffix：连接特定的DNS后缀，此处为空
    2. Description：描述，网型号
    3. Physical Address：网卡的物理地址
    4. DHCP Enabled：在自动获取IP时，会启用DHCP协议，它是一个动态分配IP的协议
    5. Autoconfiguration Enabled：自动配置已启用，即已启用自动配置IP功能
    6. IPv6 Address：本地链接的IPv6地址
    7. IPv4 Address：IPv4地址
    8. Subnet Mask：子网掩码，用以区别网络标识和主机标识的地址，需要结合IP地址才有意义
    9. Default Gateway：默认网关，通常是路由器
    10. DNS Servers：进行域名与IP地址转换的服务器
  1. tracert

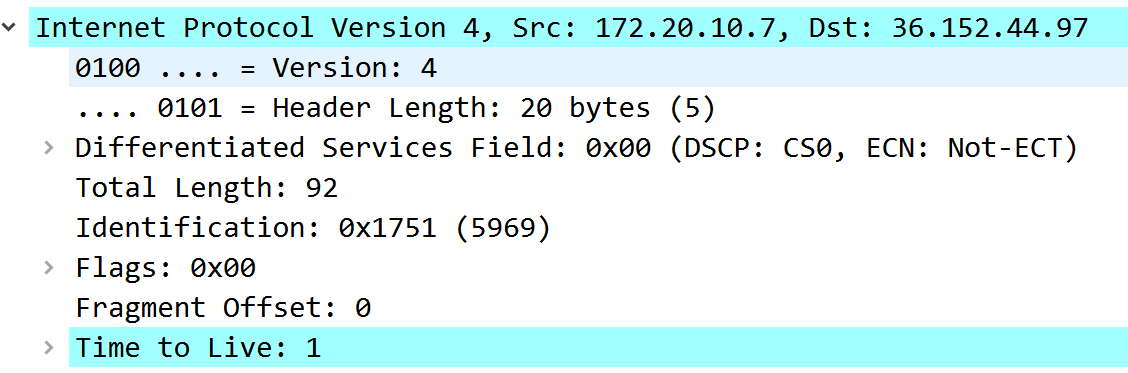
利用tracert跟踪数据包在传输过程中经过的路径，结果如下：



由上图可知，用户数据一共经过了6个路由器。其中，第一列数据表示生存时间，第二列至第四列数据表示三次发送ICMP包的返回时间，第五列表示各途径的路由器的IP地址。出现Request timed out的原因为路由接口禁用了对tracert数据包的响应。

再用Wireshark过滤路由器172.20.10.1的地址，得到：

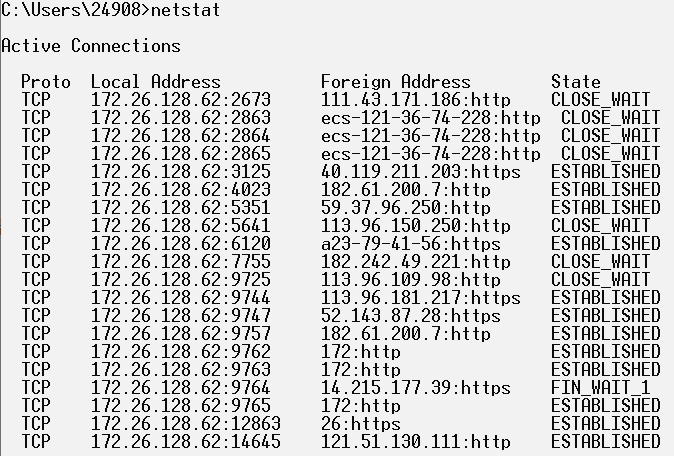




上图为tracert发送的第一个ICMP包的信息，可以看到，tracert会首先发送一个TTL为1IP数据包到目的地址，当路径上的第一个路由器收到该数据包时，TTL变为0，故该路由器会将该数据包丢弃，并送回一个ICMP time exceeded消息，其中包括路由器的IP地址。当tracert接收到该消息时，便知道该路由器在路径上。接着，tracert会发送一个TTL为2的数据包，并以此类推，当主机不再接收到ICMP time exceeded消息时，证明已经达到目的地。

* 1. netstat

利用netstat查看当前主机上网络简介统计信息，得到：



上图即为当前主机上网络简介统计信息，分别有：

* + - 1. Proto：协议名，说明用到的是TCP协议还是UDP协议
      2. Local Address：本地地址
      3. Foreign Address：外部地址，与本机端口通信的外部socket
      4. State：状态,链路状态，一共有12种可能状态，前面11种是按照TCP连接建立的三次握手和TCP连接断开的四次挥手过程来描述的，以下介绍九种TCP状态

a.ESTABLISHED 指TCP连接已建立，双方可以进行方向数据传递

b.CLOSE\_WAIT: 这种状态的含义其实是表示在等待关闭。

c.LISTENING: 指TCP正在监听端口，可以接受链接

d.TIME\_WAIT: 指连接已准备关闭。

e.FIN\_WAIT\_1: 等待对方的FIN报 文。

f.FIN\_WAIT\_2：等待对方的FIN报 文。

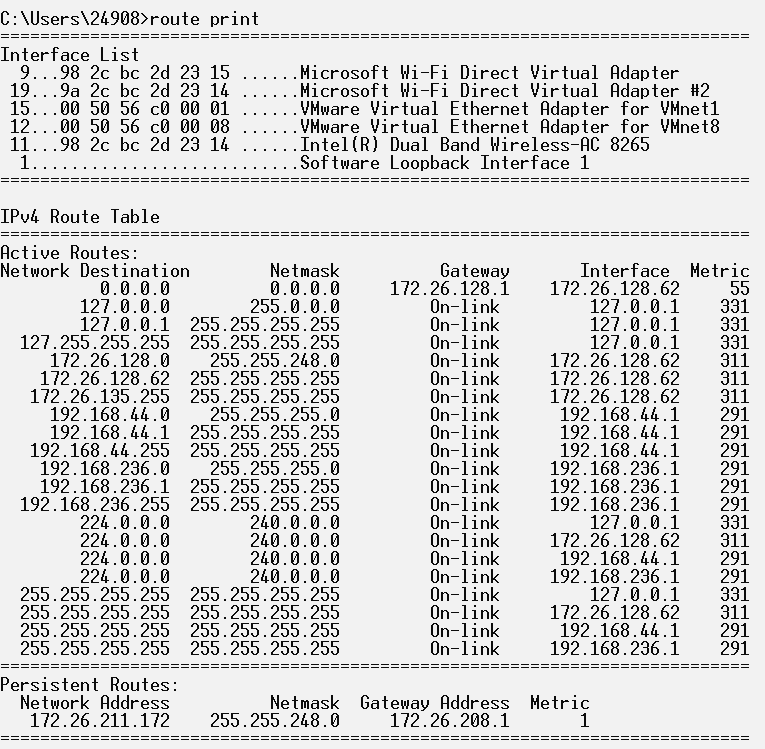
g.LAST\_ACK: 是被动关闭一方在发送FIN报文后，最后等待对方的ACK报文。

h.SYNC\_RECEIVED: 收到对方的连接建立请求

i.SYNC\_SEND: 已经主动发出连接建立请求。

* 1. route

利用route命令查看本机路由，得到：



上图即为本地路由的详细信息，分别有：

* + 1. Network Destination：网络目的地址，即路由器连接的所有网段
    2. Netmask：网段的子网掩码，能够让路由器确定目的网络的地址类，用以区别网络标识和主机标识的地址，需要结合IP地址才有意义。它提供了网段本身的子网掩码，而不是连接到该网段网卡的子网掩码，这能够让路由器确定目的网络的地址类
    3. Gateway：网关，在路由器将数据包转发到目的网络时，需要查看网关列表，而网关表就是告诉路由器该数据包需要转发到哪一个IP地址才能到达目的网络
    4. Interface：接口，这告诉了路由器哪一个网卡连接到了合适的目的网络
    5. Metric：为跃点数，路由指定所需跃点数的整数值(范围是1～9999)，它用来在路由表里的多个路由中选择与转发包中的目标地址最为匹配的路由

1. 思考题
2. TCP/IP协议配置中的“网关”作用是什么？

答：网关是一种网络互联设备，用于在传输层上实现网络互联，通常是一个路由器。它实质上是一个网络通向另一个网络的路由器接口IP地址，是向外发送数据的出口。当不设置网关的情况下，即使两台主机在连接在同一台交换机上，两个网络之间也是不能进行通信的。

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：1.①ping 本地循环地址，若不能ping通则说明主机的TCP/IP协议不能正常工作或网卡损坏②ping 本地ip地址，若ping不通则说明网络适配器出现故障或网卡损坏③ping 同网段的主机ip地址，若ping不通则说明网络线路出现故障或对方防火墙未关闭④ping 路由器在本网段端口ip，若ping不通则说明网络线路出现故障⑤ping 路由器在目标主机所在网段的端口ip,若ping不通则说明路由器出现故障⑥ping 目的主机ip地址，若ping不通则说明对方网络适配器出现故障或防火墙未关闭

1. 意味着无法到达目标主机，可能原因有①源主机与目标主机不再同一网段，源主机未设置默认路由②网线故障③网卡故障
2. 当路由器的路由表中有到达目标的路由，而因其他原因无法到达时，会出现request timed out；当路由表中没有到达目标的路由是，会出现destination host unreachable
3. **实验结果与分析**

通过本次实验，我进一步熟悉了wireshark的使用、TCP/IP协议配置及一些网络实用命令的使用。同时，对利用ping命令进行网络故障诊断有了更深刻的理解。为日后课程的学习打下来基础。

**暨南大学本科实验报告专用纸(附页)**