**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 实验地点 B402

学生姓名 钟颖谦 学号 2019051091

学院 智能科学与工程 系 专业 信息安全

实验时间 2021 年 09 月 7上午～ 9月 12日上午 温度 ℃湿度

## （一）实验目的

* 1. 熟悉TCP/IP协议的配置；
  2. 熟悉常见网络命令的使用；
  3. 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。
  4. 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。
  5. 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）实验内容和要求

* 1. 以Winodws 或linux系统为例，对TCP/IP协议进行安装和配置；
  2. 利用ipconfig查看主机接口的配置，并理解其含义。
  3. 利用route查看本机路由，并了解其含义。
  4. 利用netstat查看当前主机上网络简介统计信息，了解其含义。
  5. 利用ping对网络故障诊断与分析。用wrireshark分析其工作过程。
  6. 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）主要仪器设备

**仪器：一台具有网络功能的PC机**

**实验环境：wireshark&cmd**

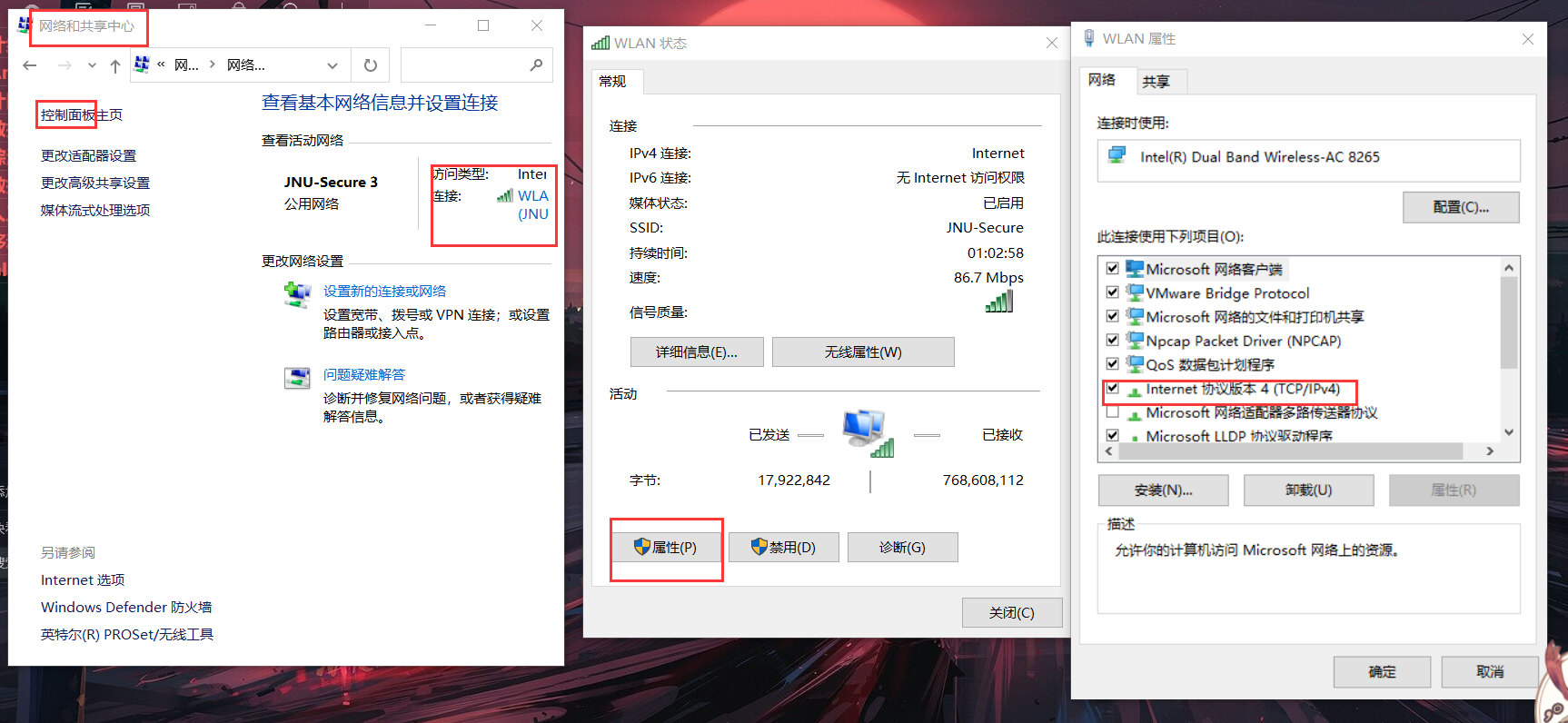
## （四）源程序

写出程序的源程序。

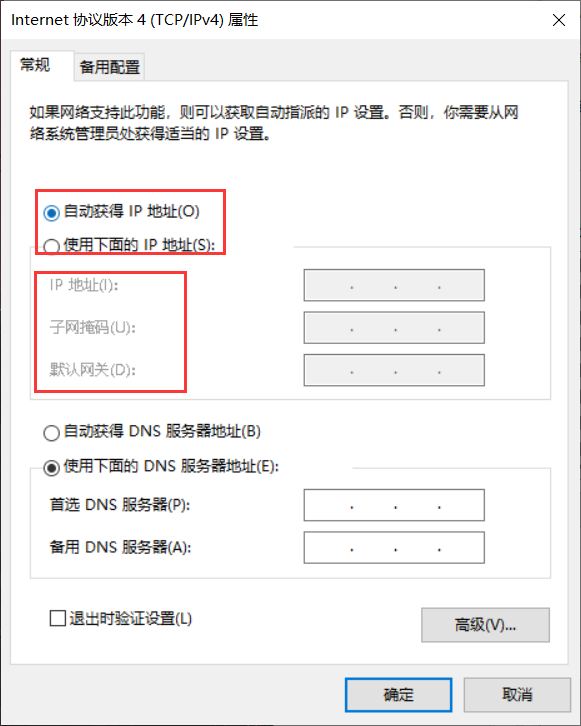
## （五）实验步骤与调试

### TCP/IP协议的安装和配置

通过控制面板找到网络控制中心，查看所连接网络属性，找到TCP/IP协议位于Internet协议出，（IPv4 IPv6）



有两个选项：自动获得IP地址、使用下面的IP地址。如果想自己设置IP地址可以选择“使用下面的IP地址”并自己修改，这里连接的是校园网就直接自动获得IP地址。



#### 相关专业名词释义：

##### IP地址：

IP地址（英语：IP Address，全称Internet Protocol Address），又译为网际协议地址、互联网协议地址。当设备连接网络，设备将被分配一个IP地址，用作标识。通过IP地址，设备间可以互相通讯，如果没有IP地址，我们将无法知道哪个设备是发送方，无法知道哪个是接收方。

IP地址有两个主要功能：标识设备或网络和寻址（英语：location addressing）。

常见的IP地址分为IPv4与IPv6两大类，IP地址由一串数字组成。IPv4 由十进制数字组成，并以点分隔，如：172.16.254.1 ； IPv6 由十六进制数字组成，以冒号分割，如：2001:db8:0:1234:0:567:8:1。

IP地址有两个主要的功能：

1. 标识主机。更具体地说，标识其网络接口，并且提供主机在网络中的位置。

2. 网络寻址，网际协议（缩写：IP）的一个重要机制就是网络寻址（英语：internet address）。该功能的目的是将 数据报 从一个网络模块 送到 目的地。在发送的整个过程，IP地址（address）充当着目的地的位置，域名（name）意味着我们要找什么，路由（route）代表着如何到达目的地的这个过程。每个IP数据包的标头包含了发送主机的IP地址和目的主机的IP地址。

##### 子网掩码：

它是一种用来指明一个IP地址的哪些位标识的是主机所在的网络地址以及哪些位标识的是主机地址的位掩码。

通常情况下，子网掩码的表示方法和地址本身的表示方法是一样的。在IPv4中，就是点分十进制四组表示法（四个取值从0到255的数字由点隔开，比如255.128.0.0）或表示为一个八位十六进制数（如FF.80.00.00，它等同于255.128.0.0），后者用得较少。

另一种更为简短的形式叫做无类别域间路由（CIDR）表示法，它给出的是一个地址加上一个斜杠以及网络掩码的二进制表示法中“1”的位数（即网络号中和网络掩码相关的是哪些位）。例如，192.0.2.96/28表示的是一个前28位被用作网络号的IP地址（和255.255.255.240的意思一样）。

子网掩码是一个32位地址，是与IP地址结合使用的一种技术。它的主要作用有两个，一是用于屏蔽IP地址的一部分以区别网络标识和主机标识，并说明该IP地址是在局域网上，还是在远程网上。二是用于将一个大的IP网络划分为若干小的子网络。

使用子网是为了减少IP的浪费。因为随着互联网的发展，越来越多的网络产生，有的网络多则几百台，有的只有区区几台，这样就浪费了很多IP地址，所以要划分子网。使用子网可以提高网络应用的效率。

通过计算机的子网掩码判断两台计算机是否属于同一网段的方法是，将计算机十进制的IP地址和子网掩码转换为二进制的形式，然后进行二进制“与”(AND)计算（全1则得1，不全1则得0），如果得出的结果是相同的，那么这两台计算机就属于同一网段。

子网掩码的好处就是：不管网络有没有划分子网，只要把子网掩码和IP地址进行逐位的“与”运算（AND）即得出网络地址来。这样在路由器处理到来的分组时就可以采用同样的方法。

##### 默认网关：

默认网关（Default Gateway）是子网与外网连接的设备，通常是一个路由器。当一台计算机发送信息时，根据发送信息的目标地址，通过子网掩码来判定目标主机是否在本地子网中，如果目标主机在本地子网中，则直接发送即可。如果目标不在本地子网中则将该信息送到默认网关/路由器，由路由器将其转发到其他网络中，进一步寻找目标主机。

##### DNS（域名服务器）

DNS（Domain Name Server，域名服务器）是进行域名(domain name)和与之相对应的IP地址 (IP address)转换的服务器。DNS中保存了一张域名(domain name)和与之相对应的IP地址 (IP address)的表，以解析消息的域名。 域名是Internet上某一台计算机或计算机组的名称，用于在数据传输时标识计算机的电子方位（有时也指地理位置）。域名是由一串用点分隔的名字组成的，通常包含组织名，而且始终包括两到三个字母的后缀，以指明组织的类型或该域所在的国家或地区。

**首选DNS服务器&备用DNS服务器：**

DNS服务器的主要作用是把域名例如www.baidu.com解析成IP地址如61.135.169.125供计算机读取。如果没有DNS服务器，则需要在浏览器里输入61.135.169.125才可以打开百度主页。即形象而言，网址是给用户看的，IP地址是给计算机看的。

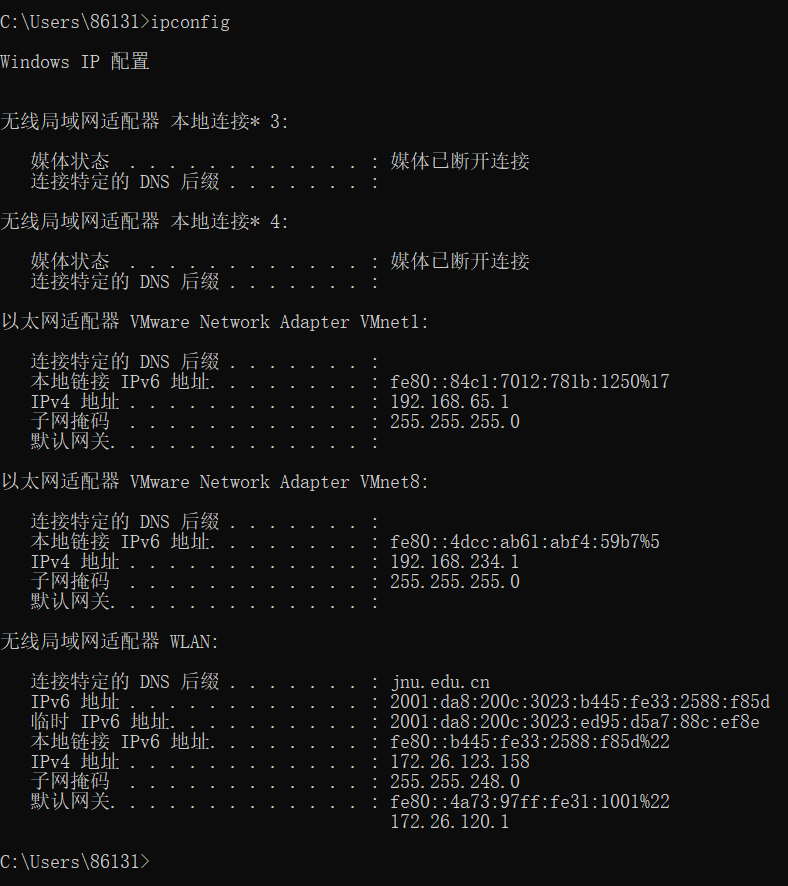
DNS是计算机域名系统 (Domain Name System 或Domain Name Service) 的缩写，它是由域名解析器和域名服务器组成的。

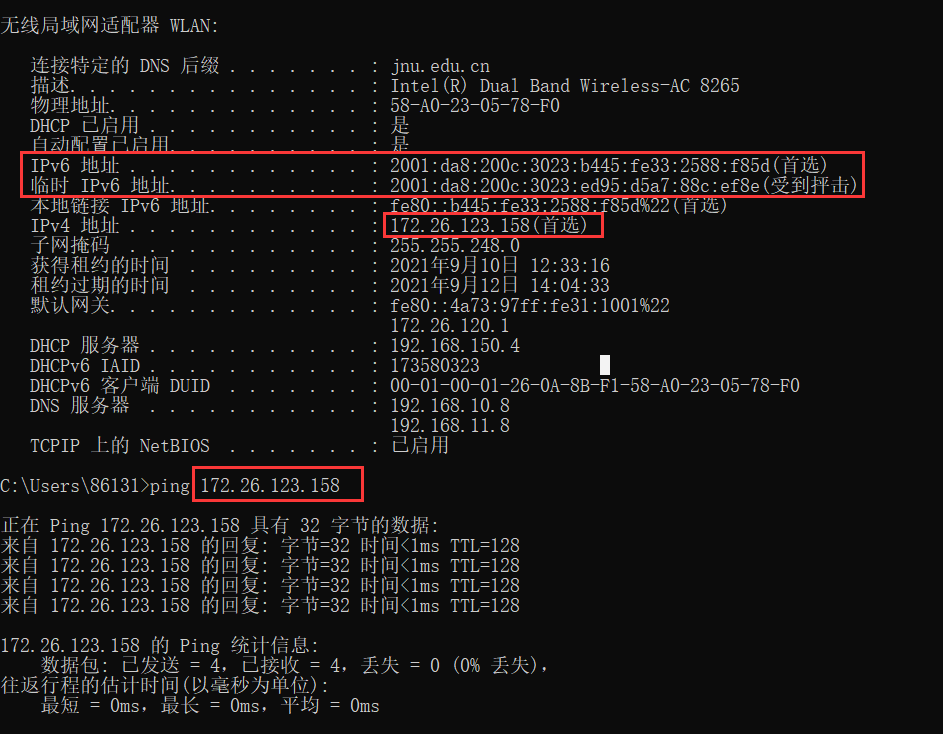
域名服务器是指保存有该网络中所有主机的域名和对应IP地址，并具有将域名转换为IP地址功能的服务器。其中域名必须对应一个IP地址，一个IP地址可以有多个域名，而IP地址不一定有域名。

域名系统采用类似目录树的等级结构。域名服务器通常为客户机/服务器模式中的服务器方，它主要有两种形式：主服务器和转发服务器。将域名映射为IP地址的过程就称为“域名解析”。

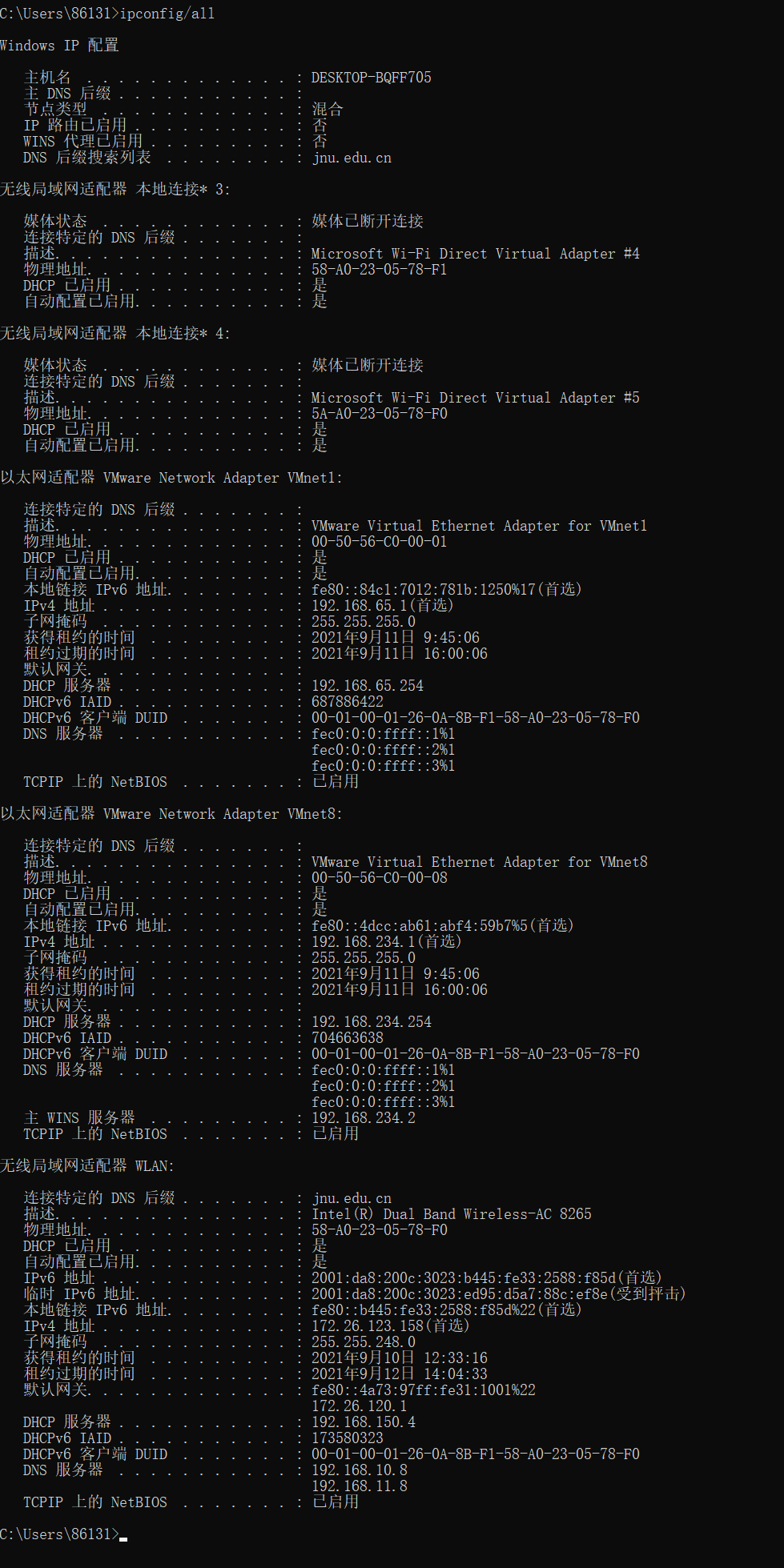
### 2．常见网络命令的使用

#### a.利用ipconfig查看主机接口的配置，并理解其含义

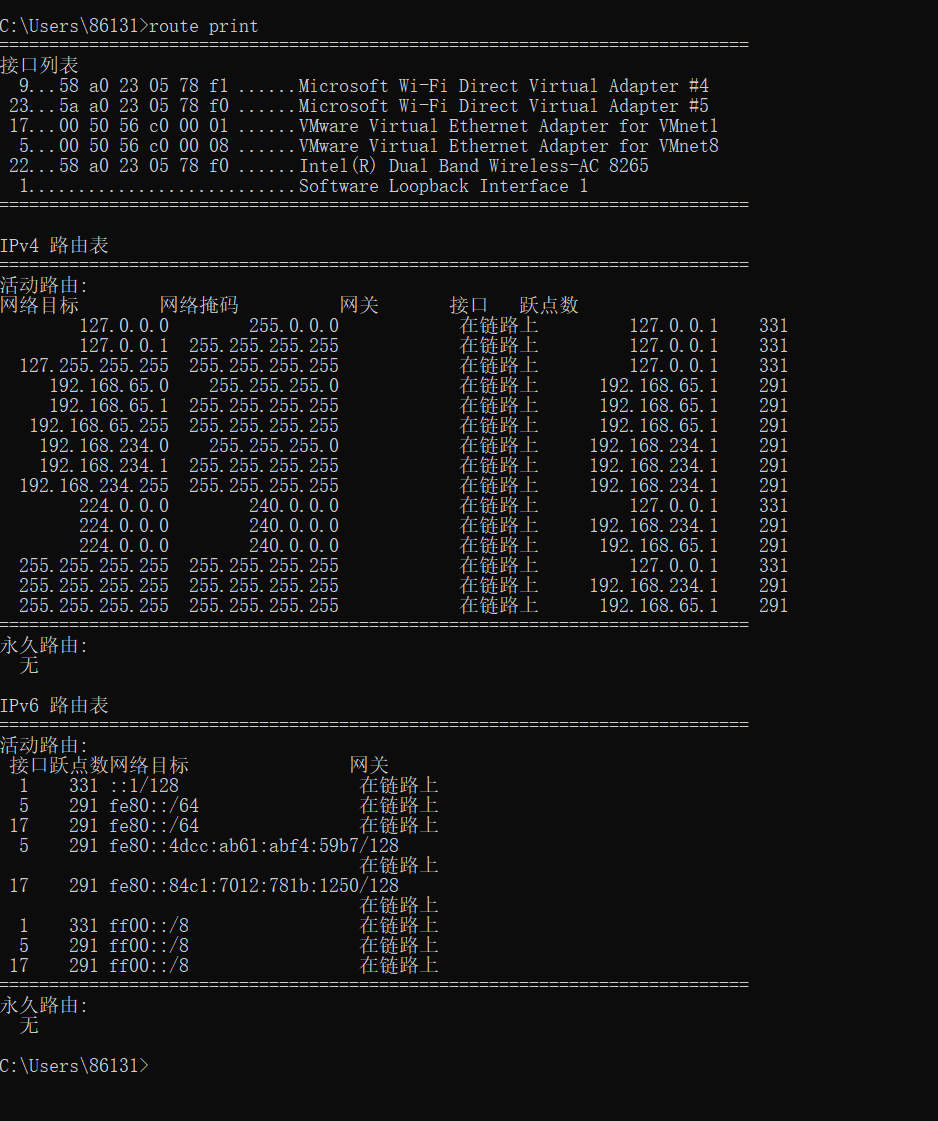




成功看到本机配置的IP地址，ping成功，查看可见IPv6协议的使用。



#### b.利用route查看本机路由，并了解其含义。



##### 专业名词解释：

###### 网关：

又称下一跳路由器。在发送IP数据包时，网关定义了针对特定的网络目的地址，数据包发送到的下一跳服务器。如果是本地计算机直接连接到的网络，网关通常是本地计算机对应的网络接口，但是此时接口必须和网关一致；如果是远程网络或默认路由，网关通常是本地计算机所连接到的网络上的某个服务器或路由器。

接口：

接口定义了针对特定的网络目的地址，本地计算机用于发送数据包的网络接口。网关必须位于和接口相同的子网（默认网关除外），否则造成在使用此路由项时需调用其他路由项，从而可能会导致路由死锁。

###### 跃点数：

跃点数用于指出路由的成本，通常情况下代表到达目标地址所需要经过的跳跃数量，一个跃点数代表经过一个路由器。跃点数越低，代表路由成本越低，优先级越高。

###### 路由表分析：

第一列是网络目标地址，列出了路由器连接的所有的网段。

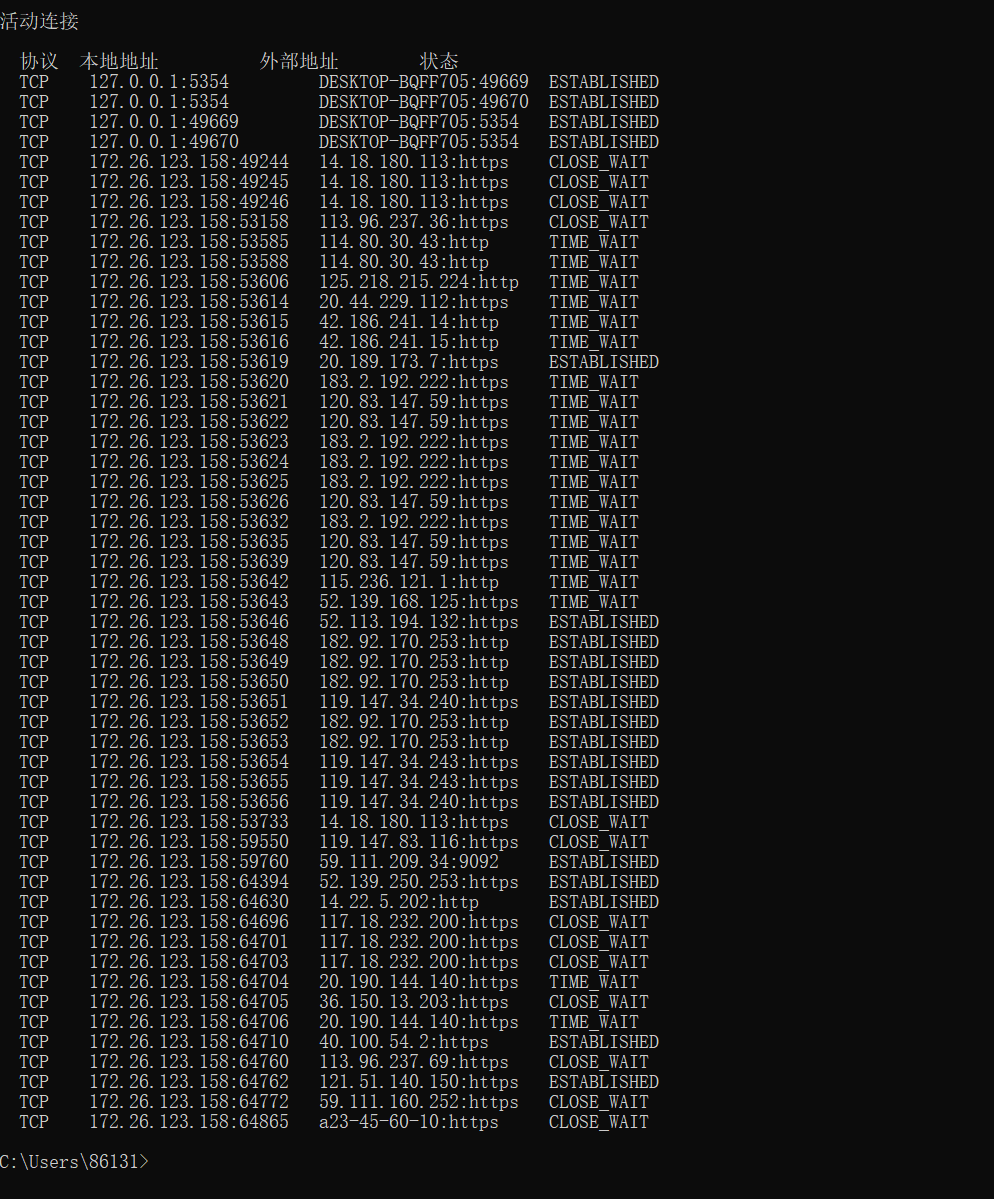
第二列是网络掩码，提供这个网段本身的子网掩码，而不是连接到这个网段的网卡的子网掩码，这基本上能够让路由器确定目的网络的地址类。

第三列是网关，一旦路由器确定它要把这个数据包转发到哪一个目的网络，路由器就要查看网关列表，网关表告诉路由器这个数据包应该转发到哪一个网关IP地址才能达到目的网络。

第四列是接口地址，接口列告诉路由器哪一个网卡连接到了合适的目的网络。从技术上说，接口列仅告诉路由器分配给网卡的IP地址，相应的网卡就把路由器连接到目的网络，然而，路由器很聪明，知道这个地址绑定到哪一个物理网卡。

第五列是跃点数，跃点数用于指出路由的成本，通常情况下代表到达目标地址所需要经过的跃点数量，一个跃点代表经过一个路由器。跃点数越低，代表路由成本越低；跃点数越高，代表路由成本越高。当具有多条到达相同目的网络的路由项时，TCP/IP会选择具有更低跃点数的路由项。

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



##### TCP各状态详解:

###### 1.LISTEN

服务端状态，应用程序打开监听端口，处理来自客户端TCP端口的连接

###### 2.SYN\_SENT

客户端状态，当客户端通过应用程序connect()连接时，客户端TCP发送SYN标记主动建立连接，此时状态为SYN\_SENT

###### 3.SYN\_RECV

服务端状态，当收到客户端SYN封包后，服务端会发送一个SYN及ACK确认到客户端，再等待对方连接确认，这时状态为SYN\_RECV，如果发现有很多SYN\_RCVD状态，可能受到了SYN Flood的Dos攻击

###### 4.ESTABLISHED

当客户端回复正确的ack值后，就建立一个打开的连接，客户端和服务端就都进入ESTABLISHED状态，此时便可以PSH数据

###### 5.FIN\_WAIT1

客户端调用close()关闭连接后，TCP发出FIN标记主动关闭连接，然后进入FIN\_WAIT1状态，等待远程TCP连接中断或者确认

###### 6.CLOSE\_WAIT

被动关闭状态，TCP接收到FIN后，就发送ack回应客户端的FIN标识封包，然后就进入了CLOSE\_WAIT状态

###### 7.FIN\_WAIT2

半关闭状态，主动关闭端(也就是客户端调用close()后)接收到ack确认后，此时进入FIN\_WAIT2状态，该状态下，客户端应用程序依然能接收数据

###### 8.LAST\_ACK

服务端发送确认中断后，也发送FIN关闭，然后进入LAST\_ACK最后确认关闭状态

###### 9.TIME\_WAIT

在主动关闭端接收到FIN后，TCP就发送ACK，并进入TIME-WAIT状态，该状态持保持由内核参数默认等待2MSL，之后主动关闭方也进入CLOSED状态关闭连接

###### 10.CLOSED

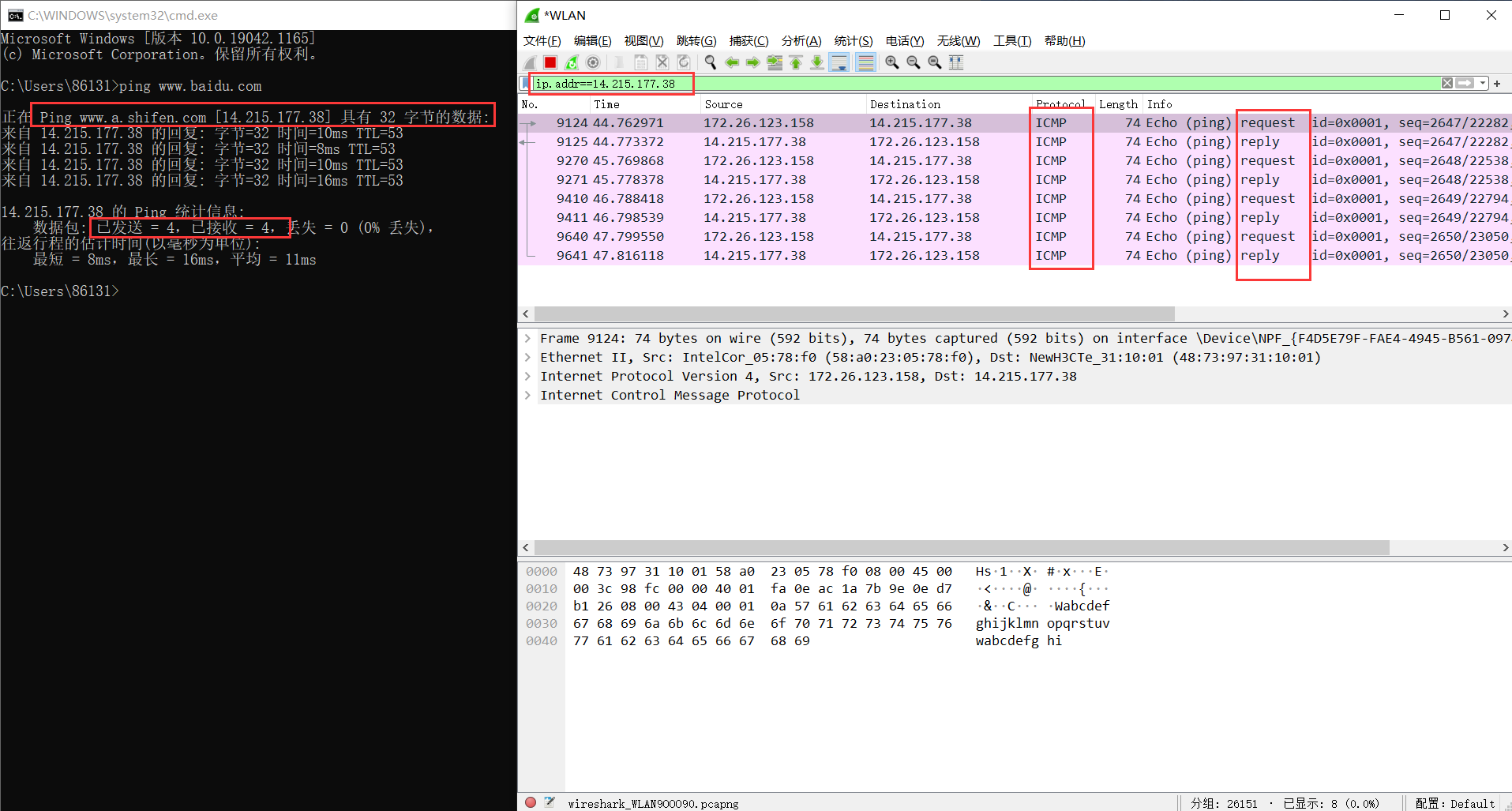
TCP连接关闭，被动关闭端在接收到ack包后，进入CLOSED状态关闭TCP连接

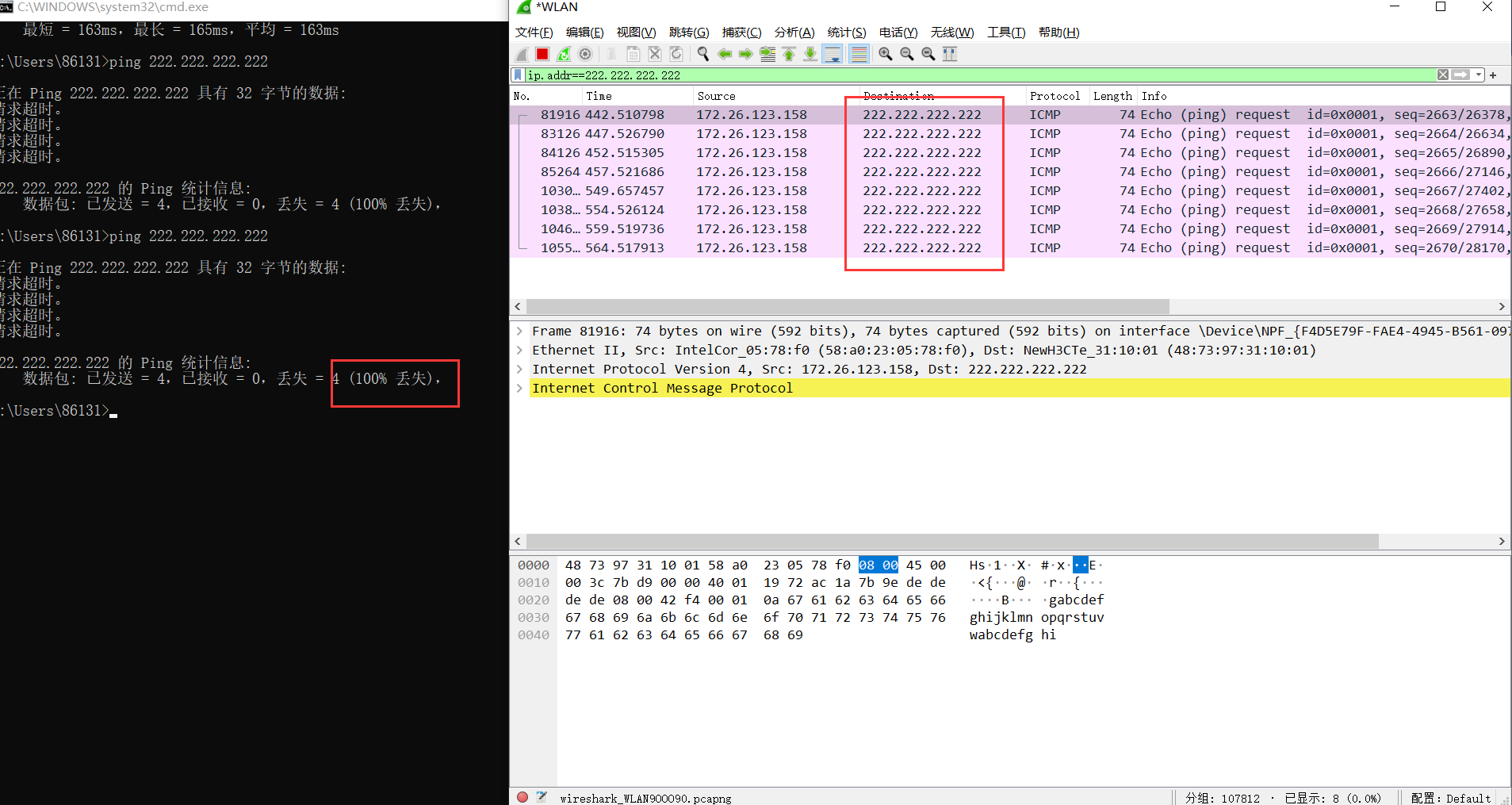
###### 11.CLOSING

CLOSING状态一般较少出现，这种是客户端和服务端同时发起了FIN主动关闭。如客户端发送FIN主动关闭，但是没有收到服务端发来的ACK确认，而是先收到了服务端发来的FIN关闭连接，所以必须是同时

在进入CLOSING状态后，只要收到了对方对自己发送的FIN的ACK，收到FIN的ACK确认就进入TIME\_WAIT状态，因此，如果RTT(Round Trip Time TCP包的往返延时)处在一个可接受的范围内，发出的FIN会很快被ACK从而进入到TIME\_WAIT状态，CLOSING状态持续的时间就特别短，因此很难看到这种状态

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





**Ping命令的工作过程：**

假定主机A的IP地址是192.168.1.1，主机B的IP地址是192.168.1.2，都在同一子网内，则当你在主机A上运行“Ping 192.168.1.2”后，流程如下：

首先，Ping命令会构建一个固定格式的ICMP请求数据包，然后由ICMP协议将这个数据包连同地址“192.168.1.2”一起交给IP层协议，IP层协议将以地址“192.168.1.2”作为目的地址，本机IP地址作为源地址，加上一些其他的控制信息，构建一个IP数据包，并在一个映射表中查找出IP地址192.168.1.2所对应的物理地址（也叫MAC地址），一并交给数据链路层。后者构建一个数据帧，目的地址是IP层传过来的物理地址，源地址则是本机的物理地址，还要附加上一些控制信息，依据以太网的介质访问规则，将它们传送出去。

主机B收到这个数据帧后，先检查它的目的地址，并和本机的物理地址对比，如符合，则接收；否则丢弃。接收后检查该数据帧，将IP数据包从帧中提取出来，交给本机的IP层协议。同样，IP层检查后，将有用的信息提取后交给ICMP协议，后者处理后，马上构建一个ICMP应答包，发送给主机A，其过程和主机A发送ICMP请求包到主机B一模一样。

从Ping的工作过程，我们可以知道，主机A收到了主机B的一个应答包，说明两台主机之间的去、回通路均正常。也就是说，无论从主机A到主机B，还是从主机B到主机A，都是正常的。

**是什么原因引起只能单方向Ping通的呢?**

一、安装了个人防火墙

在共享上网的机器中，出于安全考虑，大部分作为服务器的主机都安装了个人防火墙软件，而其他作为客户机的机器则一般不安装。几乎所有的个人防火墙软件，默认情况下是不允许其他机器Ping本机的。一般的做法是将来自外部的ICMP请求报文滤掉，但它却对本机出去的ICMP请求报文，以及来自外部的ICMP应答报文不加任何限制。这样，从本机Ping其他机器时，如果网络正常，就没有问题。但如果从其他机器Ping这台机器，即使网络一切正常，也会出现“超时无应答”的错误。

大部分的单方向Ping通现象源于此。解决的办法也很简单，根据你自己所用的不同类型的防火墙，调整相应的设置即可。

二、错误设置IP地址

正常情况下，一台主机应该有一个网卡，一个IP地址，或多个网卡，多个IP地址（这些地址一定要处于不同的IP子网）。但对于在公共场所使用的电脑，特别是网吧，人多手杂，其中不泛有“探索者”。曾有一次两台电脑也出现了这种单方向Ping通的情况，经过仔细检查，发现其中一台电脑的“拨号网络适配器”（相当于一块软网卡）的TCP/IP设置中，设置了一个与网卡IP地址处于同一子网的IP地址，这样，在IP层协议看来，这台主机就有两个不同的接口处于同一网段内。当从这台主机Ping其他的机器时，会存在这样的问题：

（1）主机不知道将数据包发到哪个网络接口，因为有两个网络接口都连接在同一网段；

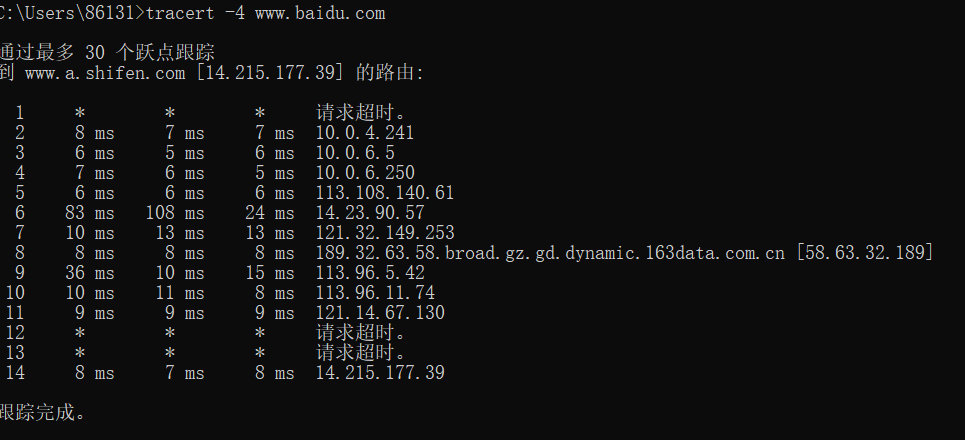
（2）主机不知道用哪个地址作为数据包的源地址。因此，从这台主机去Ping其他机器，IP层协议会无法处理，超时后，Ping就会给出一个“超时无应答”的错误信息提示。但从其他主机Ping这台主机时，请求包从特定的网卡来，ICMP只须简单地将目的、源地址互换，并更改一些标志即可，ICMP应答包能顺利发出，其他主机也就能成功Ping通这台机器了。

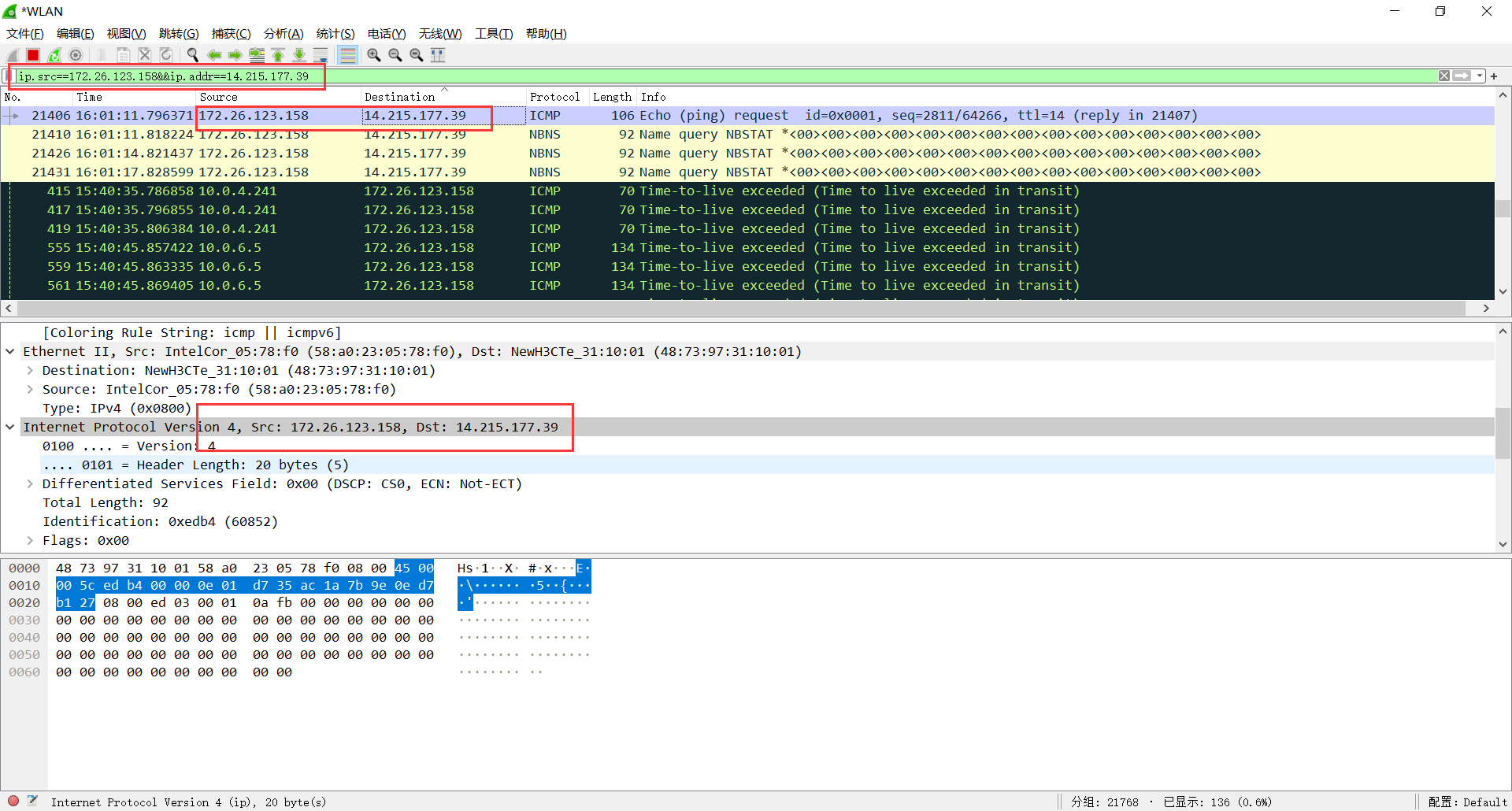
##### ICMP协议:

ICMP（Internet Control Message Protocol）Internet控制报文协议。它是TCP/IP协议簇的一个子协议，用于在IP主机、路由器之间传递控制消息。控制消息是指网络通不通、主机是否可达、路由是否可用等网络本身的消息。这些控制消息虽然并不传输用户数据，但是对于用户数据的传递起着重要的作用。

ICMP使用IP的基本支持，就像它是一个更高级别的协议，但是，ICMP实际上是IP的一个组成部分，必须由每个IP模块实现。

#### e.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





该诊断实用程序将包含不同生存时间(TTL)值的Internet控制消息协议(ICMP)回显数据包发送到目标，以决定到达目标采用的路由。要在转发数据包上的TTL之前至少递减1，必须经过路径上的每个路由器，所以TTL是有效的跃点计数。数据包上的 TTL 到达 0 时，路由器应该将“ICMP已超时”的消息发送回源系统。Tracert先发送TTL为1的回显数据包,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。路由通过检查中级路由器发送回的“ICMP已超时”的消息来确定路由。不过，有些路由器悄悄地下传包含过期TTL值的数据包，而tracert看不到。

## 思考题

### 1、TCP/IP协议配置中的“网关”作用是什么？

答：默认网关（Default Gateway）是子网与外网连接的设备，通常是一个路由器。当一台计算机发送信息时，根据发送信息的目标地址，通过子网掩码来判定目标主机是否在本地子网中，如果目标主机在本地子网中，则直接发送即可。如果目标不在本地子网中则将该信息送到默认网关/路由器，由路由器将其转发到其他网络中，进一步寻找目标主机。

### 2、 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 unreachable”,则意味着什么？“Destination host unreachable”和“Time out”的区别是什么？

**A.用ping命令检测网络中的故障点**

1）ping 127.0.0.1，检测TCP/IP协议栈是否正常。

这个命令检测的是本地回环地址，被送到本地计算机的IP软件，如果未能ping通，则表示TCP/IP的安装或运行存在某些问题。

2)ping本地IP，检测网卡或本地配置是否正常。

这个命令被送到计算机所配置的IP地址，我们的计算机始终都应对该命令作出应答，如果没有，则表示本地配置或安装存在问题。出现此问题时，局域网用户可以断开网线，然后重新发送该命令，如果能ping通，则表示另一台计算机可能配置了相同的IP地址。

3）ping局域网内其他IP，检测网卡、网线等是否正常。

这个命令离开本地计算机，经过网卡及网络电缆到达其他计算机，再返回。收到回送应答表明本地网络中的网卡和载体运行正确。如果没有收到回送应答，那么表示子网掩码不正确（网段不一致），或网卡配置错误，或电缆系统有问题。

4）ping网关IP，检测与网关的连接性。

这个命令如果应答正确，表示局域网中的网关路由器正在运行并能够作出应答。

5）ping远程IP，检测远程连接。

能ping通表示可以成功的访问Internet（但不排除ISP的DNS会有问题）。

6）ping localhost。

检测主机文件localhost是一个保留域名，在Windows系统中，它是127.0.0.1的别名，每台计算机都应能将该名字转换成该地址。如果没有做到这一点，则表示主机文件（/Windows/host）存在问题。

**B.出现“Destination host unreachable”**

出现这种情况，可能的原因有：

①对方与自己不在同一网段内，而自己又未设置默认路由；

②网线故障；③网卡故障。

**C．“Destination host unreachable”和“Time out”的区别**

所经过的路由器的路由表中具有到达目标的路由，而目标因为其它原因不可到达，这时候会出现"Request timed out"；

如果路由表中连到达目标的路由都没有，那就会出现"destination host unreachable"。

## （七）实验小结

通过本次实验，我对TCP/IP协议有了进一步的了解，明白了其并非只是简单的TCP和IP协议，还包括其下的子协议，最重要的是，开启了我对计算机网络的新认知，开拓了我的知识，让我在继续学习安全之路奠定基础，学到基本的所需只是。

同时，在对本次实验的实验操作下，认识了windows下的ping、ipconfig、route、tracert、netstat等命令的操作，对其功能以及使用进行进一步的熟悉，在做实验的过程中让自己感觉到了真正动手掌握网络知识，掌握安全知识的乐趣和满足感，对每一个命令的学习能充分地提升自己对信息安全道路的认识，让自己知道自己能够掌握知识和提升能力的重要性，对于信息安全的道路有了更深的执着。

也通过这次实验学会使用wireshark对网络流量包的获取、分析，通过具体的实践操作，从偏底层原理的角度对网络有了进一步的认识，也对网络安全有了更加底层，基础、全面的了解，相信坚持学习下去，就会让自己的安全意识得到提升和让自己的安全发展前景越发光明。

**暨南大学本科实验报告专用纸(附页)**