**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 实验项目类型 实验地点

学生姓名 张强 学号 2019053448

学院 智科院 系 信息安全 专业

实验时间 年 月 日 午～ 月 日 午 温度 ℃湿度

1. **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. 了解用Wireshark捕获信息，初步理解ping 、tracert命令的工作原理。
   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。
2. **实验内容**
   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ping对网络故障诊断与分析。**用**wrireshark分析其工作过程。
   4. 利用route查看本机路由。
   5. 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
   6. 利用netstat查看当前主机上网络简介统计信息。
3. **仪器设备**

**仪器：**可以联网的PC一台

**实验环境：**自备Windows10笔记本

1. **技术原理**

TCP/IP协议windows安装时的默认安装，配置TCP/IP协议是保证主机与网络正常连接的基础。Windows提供的一组网络使用命令，能够网络信息的统计与网络故障的判断。这些实用程序均可以在命令标识后加斜线和问号，得到该命令的功能、参数和使用说明的帮助信息，下面介绍主要命令。

1. Ping

Ping是测试网络联接状况以及信息包发送和接收状况非常有用的工具。Ping向目标主机(地址)发送一个32 字节的IP 数据报到目标站点的主机上，记录下主机的响应时间。从而判断网络的响应时间和本机是否与目标主机(地址)连通。

　　如果执行Ping不成功，则可以预测故障出现在以下几个方面:网线故障，网络适配器配置不正确，IP地址不正确。如果执行Ping成功而网络仍无法使用，那么问题很可能出在网络系统的软件配置方面，Ping成功只能保证本机与目标主机间存在一条连通的物理路径。

命令格式：ping IP地址或主机名 [-t] [-a] [-n count] [-l size]  
　　参数含义:  
　　-t不停地向目标主机发送数据;  
　　-a 以IP地址格式来显示目标主机的网络地址 ;  
　　-n count 指定要Ping多少次，具体次数由count来指定 ;  
　　-l size 指定发送到目标主机的数据包的大小。

-r count 记录节点跳跃的路由

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。

命令格式如下：ipconfig [/? | /all | /release [adapter] | /renew [adapter]]   
其中的参数说明如下：   
使用不带参数的ipconfig命令可以得到以下信息：IP地址、子网掩码、默认网关。  
/? 显示ipconfig的格式和参数的英文说明；   
/all 显示所有的配置信息；   
/release 为指定的适配器（或全部适配器）释放IP地址（只适用于DHCP）；   
/renew 为指定的适配器（或全部适配器）更新IP地址（只适用于DHCP）。   
/all，则可以得到更多的信息：主机名、DNS服务器、节点类型、网络适配器的物理地址、主机的IP地址、子网掩码以及默认网关等。

1. tracert

tracert 实用程序显示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。

命令格式为：　tracert IP地址或主机名 [-d][-h maximumhops][-j host\_list] [-w timeout]

其中的参数说明如下：  
　　-d 不解析目标主机的名字;  
　　-h maximum\_hops 指定搜索到目标地址的最大跳跃数;  
　　-j host\_list 按照主机列表中的地址释放源路由;  
　　-w timeout 指定超时时间间隔，程序默认的时间单位是毫秒。

1. netstat

**netstat 为网络协议统计命令，可以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。（各状态的含义属于TCP协议内容，可以通过网络查询相关信息）**

命令格式为：netstat –参数。一共有7个参数,说明如下：

-a 显示所有的TCP 连接、所有侦听的TCP 和 UDP 端口。

-e 显示 Ethernet 统计，可以和 /s 参数一起使用。

-n 显示以数字形式表示的地址和端口号。

-p proto 显示由协议参数proto 指定的协议的连接，协议可以是TCP、UDP、TCPv6、

UDPv6。与参数 /s 一起使用，会按协议显示统计信息，此时的协议可以是TCP、

UDP、IP、ICMP、TCP v6、UDP v6、IP v6ICMP v6。

-s 按协议显示统计信息。

-r 显示IP 路由表的内容。该参数的作用与route print 命令等价。

-t 指定再次自动统计、显示统计信息的时间间隔，t 数值为秒。若没有指定，会显

示当前统计信息后退出。

(5) route

Route用来显示、添加、删除和修改路由表项目。命令格式：Route print：用来显示路由表中的当前项目。在单个路由器网段上的输出结果与netstat –r命令输出相同。

1. **实验步骤与调试**

**TCP/IP协议的安装和配置**

**TCP/IP协议位于网络连接-Internet协议处，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。**



**名词解释：**

**IP地址：**

IP协议是为计算机网络相互连接进行通信而设计的协议。在因特网中，它是能使连接到网上的所有计算机网络实现相互通信的一套规则，规定了计算机在因特网上进行通信时应当遵守的规则。任何厂家生产的计算机系统，只要遵守IP协议就可以与因特网互连互通。各个厂家生产的网络系统和设备，如以太网、分组交换网等，它们相互之间不能互通，不能互通的主要原因是因为它们所传送数据的基本单元（技术上称之为“帧”）的格式不同。IP协议实际上是一套由软件程序组成的协议软件，它把各种不同“帧”统一转换成“IP数据报”格式，这种转换是因特网的一个最重要的特点，使所有各种计算机都能在因特网上实现互通，即具有“开放性”的特点。正是因为有了IP协议，因特网才得以迅速发展成为世界上最大的、开放的计算机通信网络。因此，IP协议也可以叫做“因特网协议”。

**默认网关：**

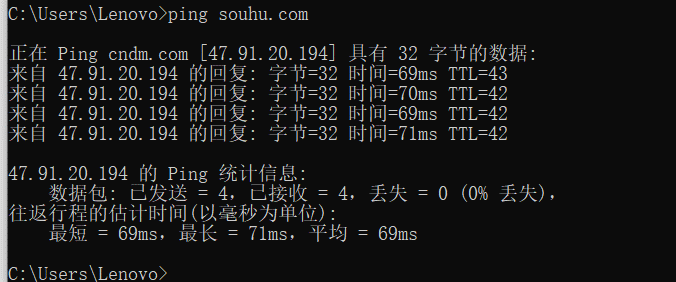
默认网关（Default Gateway）子网与外网连接的设备，通常是一个路由器。当一台计算机发送信息时，根据发送信息的目标地址，通过子网掩码来判定目标主机是否在本地子网中，如果目标主机在本地子网中，则直接发送即可。如果目标不在本地子网中则将该信息送到默认网关/路由器，由路由器将其转发到其他网络中，进一步寻找目标主机。

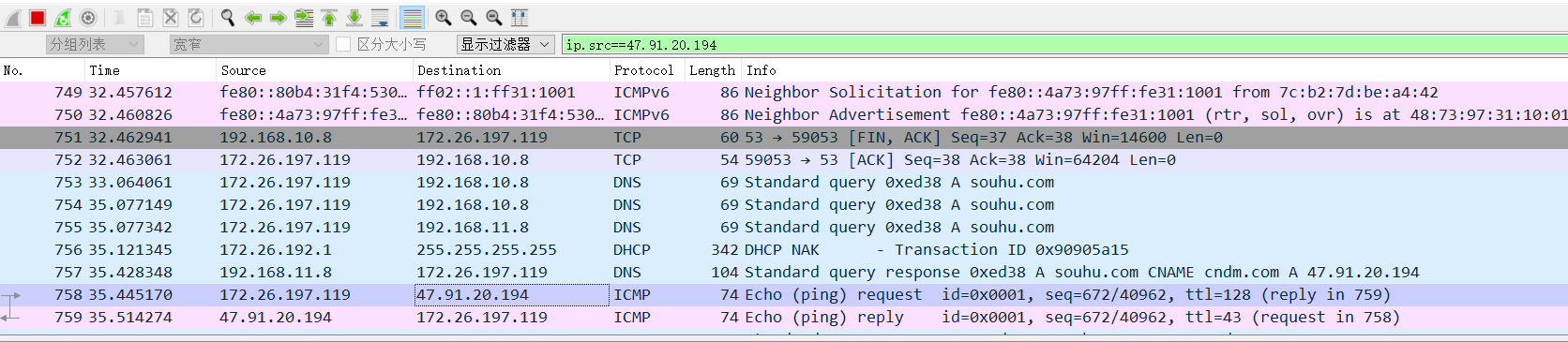
**DNS服务器**

即Domain Name System（域名系统）。DNS提供了很多功能，其中最主要的功能就是进行域名与IP之间的解析。例如www.baidu.com解析出来的IP地址为182.61.200.6。解析成IP地址之后就可以通过对应的规则进行网络通信。

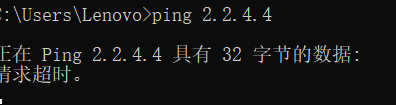
**1.使用ping命令**

**A：ping成功**



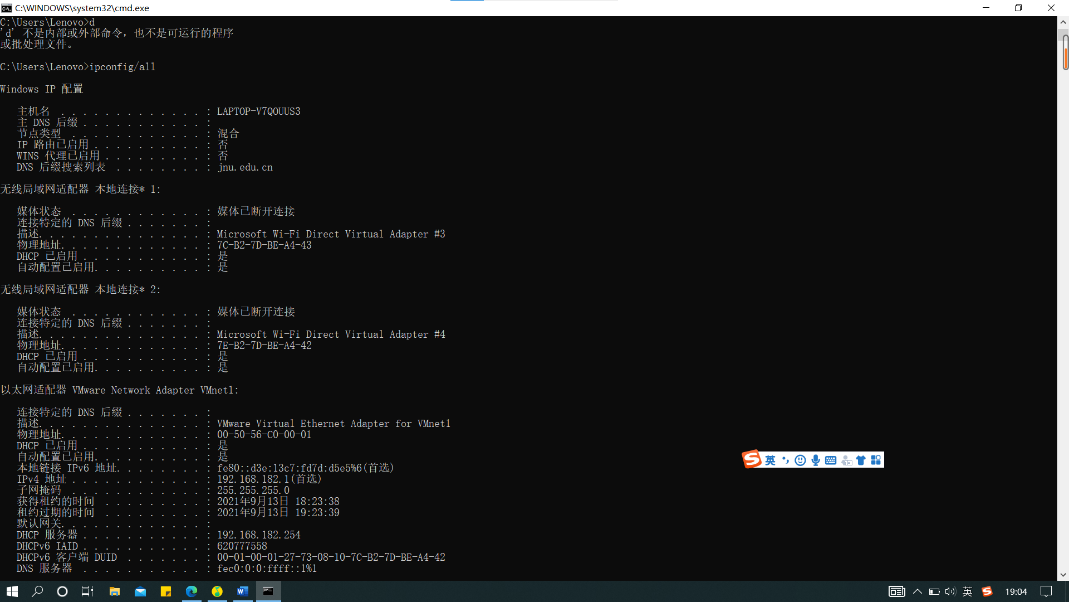
****

**B：ping失败**

****

**2.使用ipconfig命令**

用ipconfig命令查看IP，发现已经修改成功。使用ping命令查看网络连通性



**从上到下分别是 IP地址、子网掩码、默认网关**

ipconfig常用命令操作：

1、ipconfig /all：显示本机TCP/IP配置的详细信息

2、ipconfig /release：DHCP客户端手工释放IP地址

3、ipconfig /renew：DHCP客户端手工向服务器刷新请求

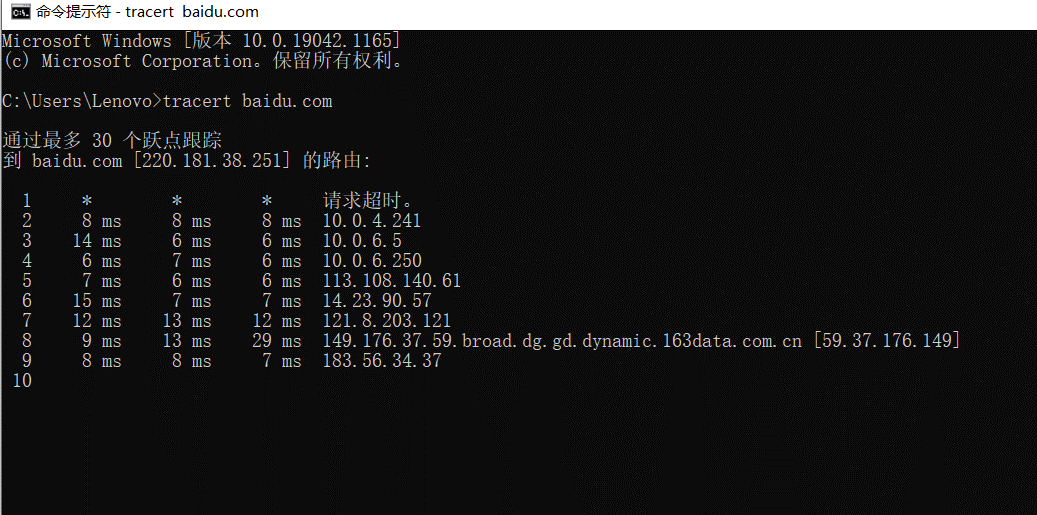
4、ipconfig /flushdns：清除本地DNS缓存内容

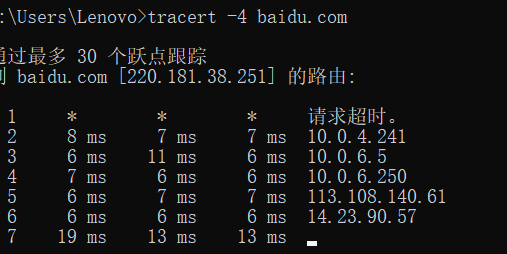
5、ipconfig /displaydns：显示本地DNS内容

6、ipconfig /registerdns：DNS客户端手工向服务器进行注册

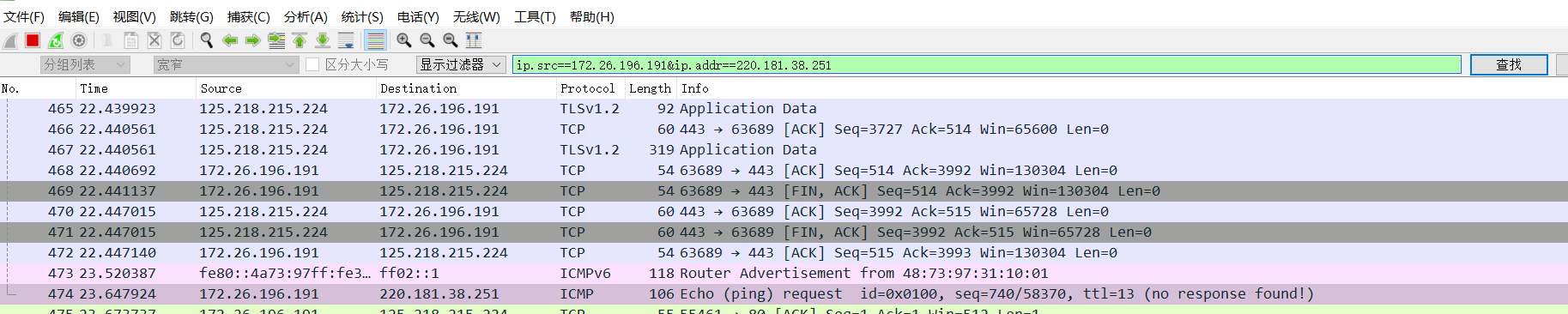
7、ipconfig /showclassid：显示网络适配器的DHCP类别信息

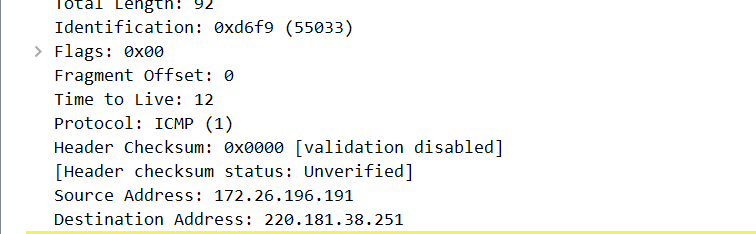
**3.使用tracert命令**





使用wireshark分析





**4.使用netstat命令**

****

.l SYN\_SENT ：这个状态与SYN\_RCVD 状态相呼应，当客户端SOCKET执行connect()进行连接时，它首先发送SYN报文，然后随即进入到SYN\_SENT 状态，并等待服务端的发送三次握手中的第2个报文。SYN\_SENT 状态表示客户端已发送SYN报文。

2.l LISTEN ：表示服务器端的某个SOCKET处于监听状态，可以接受客户端的连接。

3.l SYN\_RCVD ：表示服务器接收到了来自客户端请求连接的SYN报文。在正常情况下，这个状态是服务器端的SOCKET在建立TCP连接时的三次握手会话过程中的一个中间状态，很短暂，基本上用netstat很难看到这种状态，除非故意写一个监测程序，将三次TCP握手过程中最后一个ACK报文不予发送。当TCP连接处于此状态时，再收到客户端的ACK报文，它就会进入到ESTABLISHED 状态。

4.l ESTABLISHED ：表示TCP连接已经成功建立。

5.l FIN\_WAIT\_1 ：这个状态得好好解释一下，其实FIN\_WAIT\_1 和FIN\_WAIT\_2 两种状态的真正含义都是表示等待对方的FIN报文。而这两种状态的区别是：FIN\_WAIT\_1状态实际上是当SOCKET在ESTABLISHED状态时，它想主动关闭连接，向对方发送了FIN报文，此时该SOCKET进入到FIN\_WAIT\_1 状态。而当对方回应ACK报文后，则进入到FIN\_WAIT\_2 状态。当然在实际的正常情况下，无论对方处于任何种情况下，都应该马上回应ACK报文，所以FIN\_WAIT\_1 状态一般是比较难见到的，而FIN\_WAIT\_2 状态有时仍可以用netstat看到。

6.l FIN\_WAIT\_2 ：上面已经解释了这种状态的由来，实际上FIN\_WAIT\_2状态下的SOCKET表示半连接，即有一方调用close()主动要求关闭连接。注意：FIN\_WAIT\_2 是没有超时的（不像TIME\_WAIT 状态），这种状态下如果对方不关闭（不配合完成4次挥手过程），那这个 FIN\_WAIT\_2 状态将一直保持到系统重启，越来越多的FIN\_WAIT\_2 状态会导致内核crash。

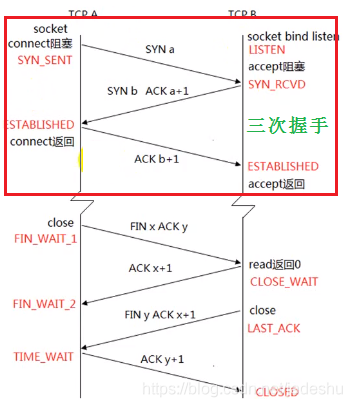
7.l TIME\_WAIT ：表示收到了对方的FIN报文，并发送出了ACK报文。 TIME\_WAIT状态下的TCP连接会等待2\*MSL（Max Segment Lifetime，最大分段生存期，指一个TCP报文在Internet上的最长生存时间。每个具体的TCP协议实现都必须选择一个确定的MSL值，RFC 1122建议是2分钟，但BSD传统实现采用了30秒，Linux可以cat /proc/sys/net/ipv4/tcp\_fin\_timeout看到本机的这个值），然后即可回到CLOSED 可用状态了。如果FIN\_WAIT\_1状态下，收到了对方同时带FIN标志和ACK标志的报文时，可以直接进入到TIME\_WAIT状态，而无须经过FIN\_WAIT\_2状态。（这种情况应该就是四次挥手变成三次挥手的那种情况）

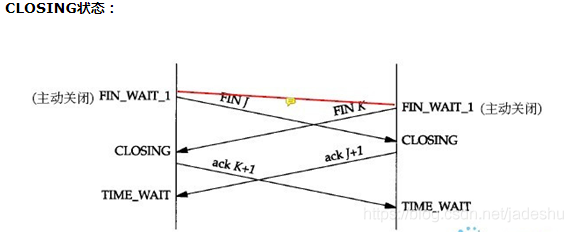
8.l CLOSING ：这种状态在实际情况中应该很少见，属于一种比较罕见的例外状态。正常情况下，当一方发送FIN报文后，按理来说是应该先收到（或同时收到）对方的ACK报文，再收到对方的FIN报文。但是CLOSING 状态表示一方发送FIN报文后，并没有收到对方的ACK报文，反而却也收到了对方的FIN报文。什么情况下会出现此种情况呢？那就是当双方几乎在同时close()一个SOCKET的话，就出现了双方同时发送FIN报文的情况，这是就会出现CLOSING 状态，表示双方都正在关闭SOCKET连接。

9.l CLOSE\_WAIT ：表示正在等待关闭。怎么理解呢？当对方close()一个SOCKET后发送FIN报文给自己，你的系统毫无疑问地将会回应一个ACK报文给对方，此时TCP连接则进入到CLOSE\_WAIT状态。接下来呢，你需要检查自己是否还有数据要发送给对方，如果没有的话，那你也就可以close()这个SOCKET并发送FIN报文给对方，即关闭自己到对方这个方向的连接。有数据的话则看程序的策略，继续发送或丢弃。简单地说，当你处于CLOSE\_WAIT 状态下，需要完成的事情是等待你去关闭连接。

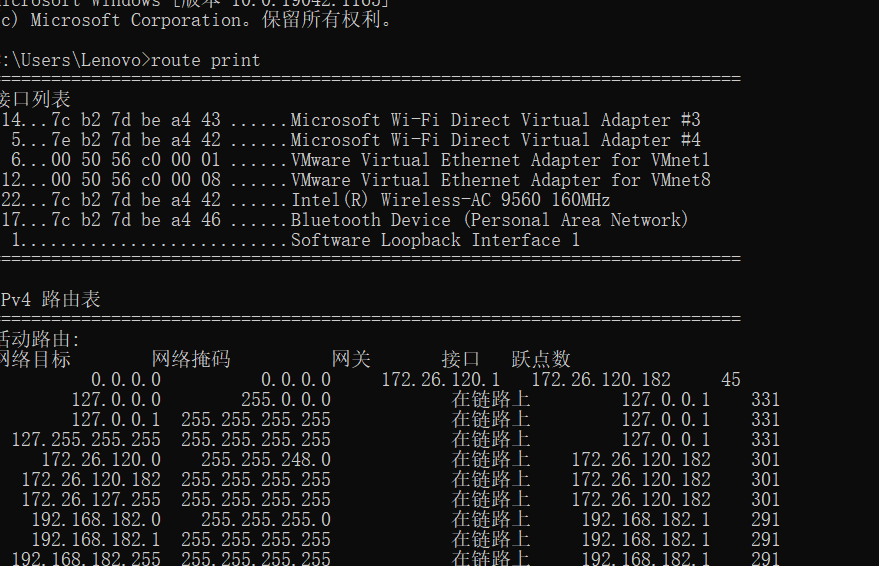
10.l LAST\_ACK ：当被动关闭的一方在发送FIN报文后，等待对方的ACK报文的时候，就处于LAST\_ACK 状态。当收到对方的ACK报文后，也就可以进入到CLOSED 可用状态了。

11.l CLOSED：初始状态，表示TCP连接是“关闭着的”或“未打开的”。





**5.使用route命令**

****

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。

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。

**Windows路由表操作：**

windows路由表的设置主要通过route命令，ROUTE命令格式如下：

ROUTE [-f] [-p] [command [destination] [MASK netmask] [gateway] [METRIC metric] [IF interface]

其中 –f 参数用于清除路由表，-p参数用于永久保留某条路由（即在系统重启时不会丢失路由）。

Command主要有PRINT（打印）、ADD（添加）、DELETE（删除）、CHANGE（修改）共4个命令。

Destination代表所要达到的目标IP地址。

MASK是子网掩码的关键字。Netmask代表具体的子网掩码，如果不加说明，默认是255.255.255.255（单机IP地址）。如果代表全部出口子网掩码可用0.0.0.0。

Gateway代表出口网关。

其他interface和metric分别代表特殊路由的接口数目和到达目标地址的跃点数，一般默认。

**【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。

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？

1.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。

2.出现“Destination host unreahable”

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。

3．“Destionation 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"。

1. **实验小结**

通过本次实验，我对TCP/IP协议有了更深入的了解，对windows下的ping、tracert、netstat等操作的使用更加熟悉，并熟悉和理解其内容，学会使用wireshark对网络流量包的获取、分析。

**暨南大学本科实验报告专用纸(附页)**