**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 宿舍

学生姓名 赖智聪 学号 2019051118

学院 智能科学与工程 系 专业 信息安全

实验时间 2021 年 9 月 12 日 上 午～ 9 月 12 日 上 午

|  |
| --- |
| **一、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。** |

|  |
| --- |
| **二、实验环境**  宿舍个人电脑 |
|  |
| **三、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** |

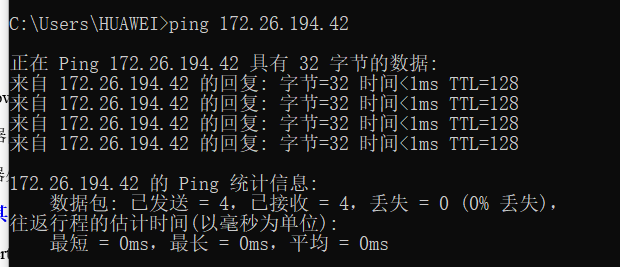
**四、实验及分析**

1 tcp/ip协议由windows默认安装并配置

2

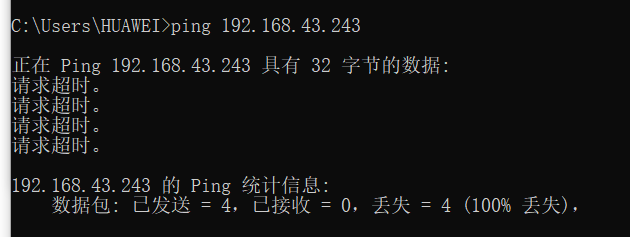
1 ping

当ping自己的网络时，可见成功：



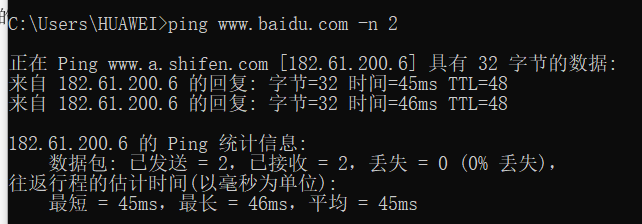
其中TTL表示Time to live，即该包还可以经过的路由器数量。

当ping一个不存在的网络时，失败：

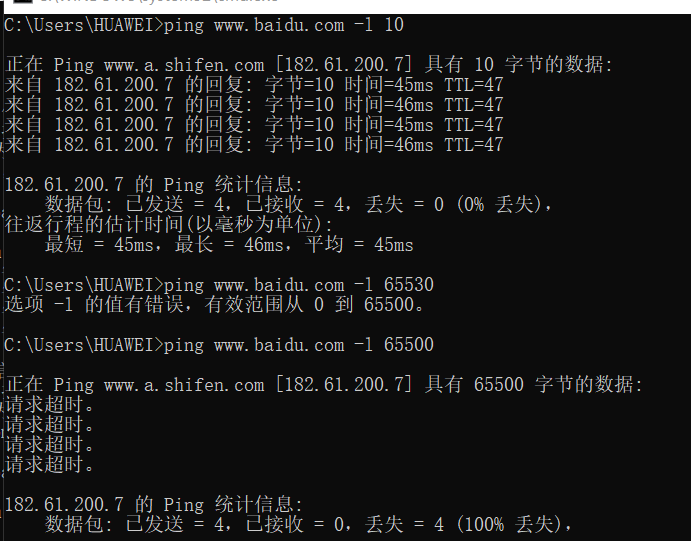


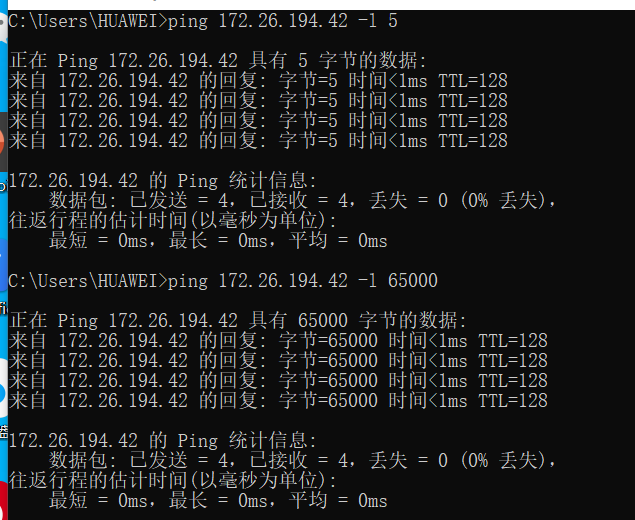
参数测试：

-n测试如下，当使用-t时则一直发送数据。当组合使用两者时，出现在更后面的一项有效。

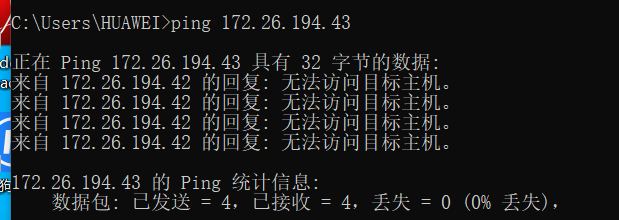


-l： 当指定的数值过大时提示错误，而当数值较大时丢失概率也很大从而导致超时。而当ping自己时，当数值在有效范围，几乎总能成功。

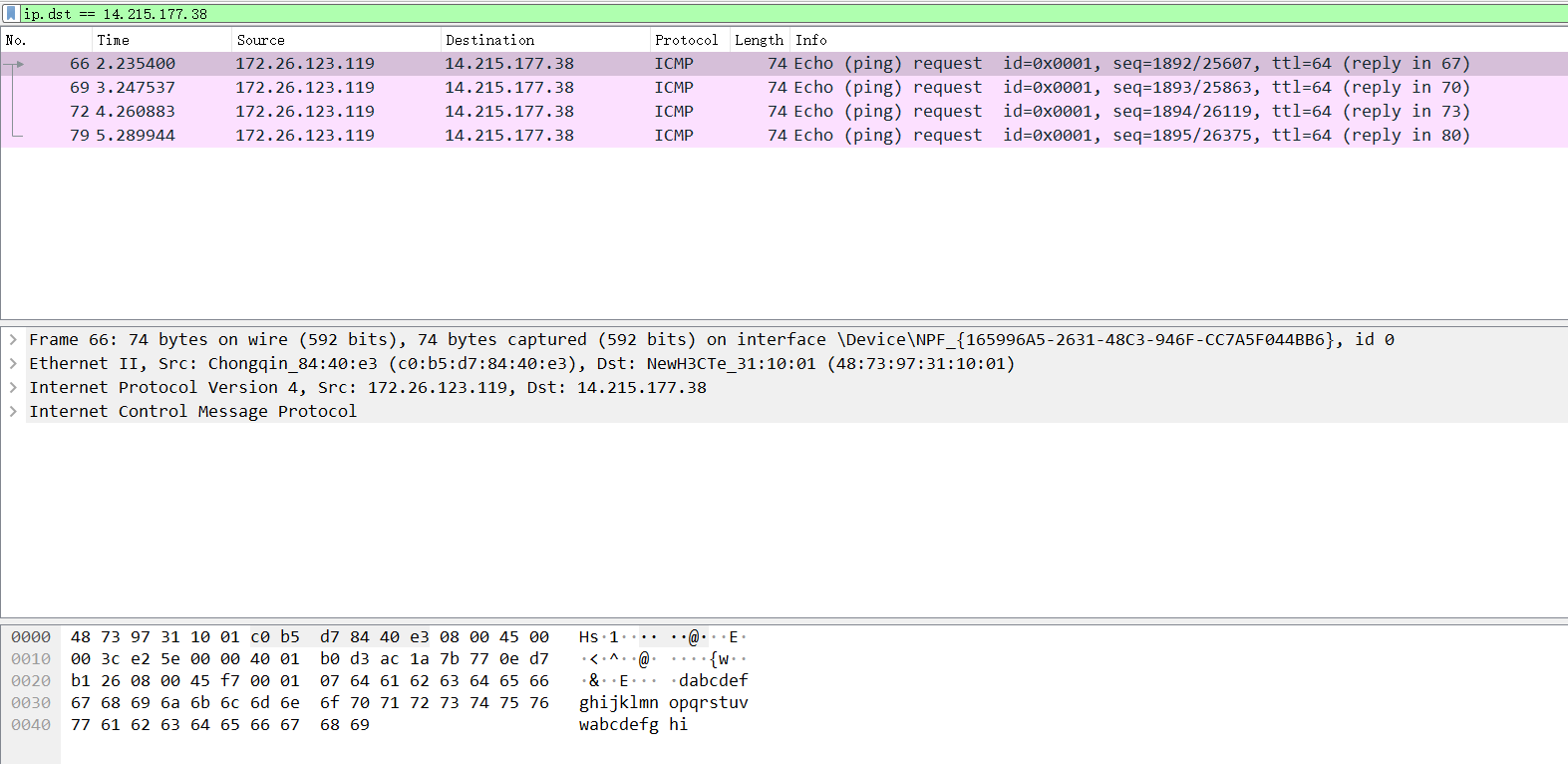




测试-r和-a参数失败，均没有达到预期效果。使用-r时发生超时，使用-a时发现和没有-a时没有区别，无法显示-a的作用。当仅仅修改最后一个数字时：



当ping百度时，使用wireshark得到的结果：

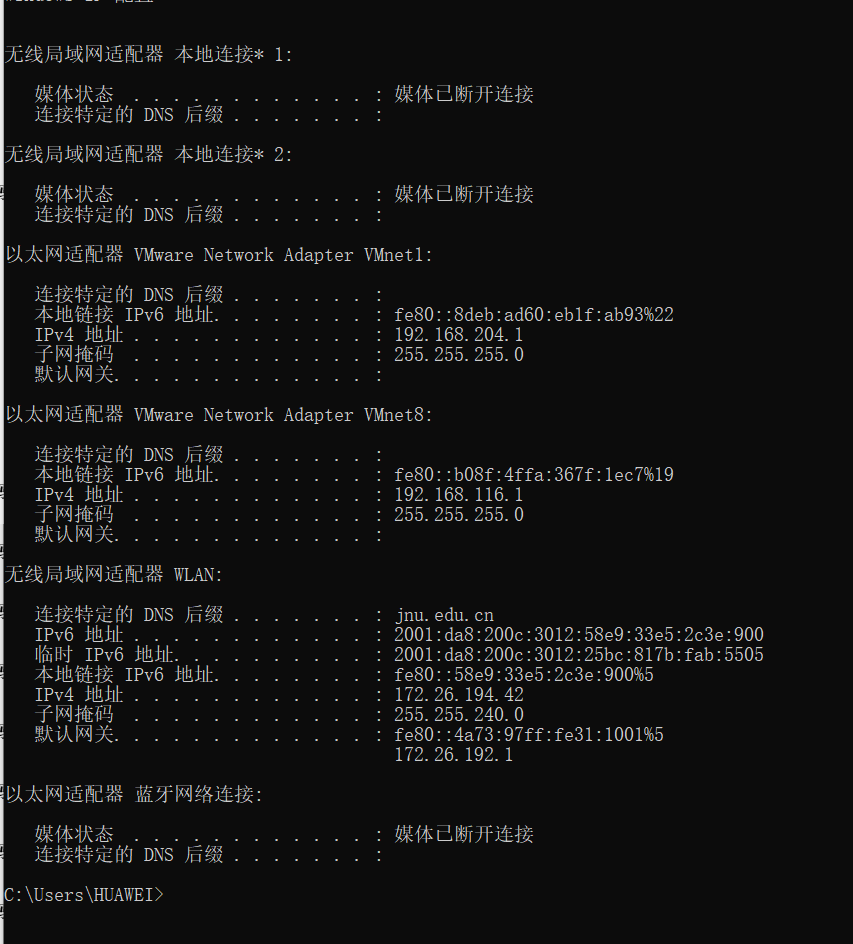


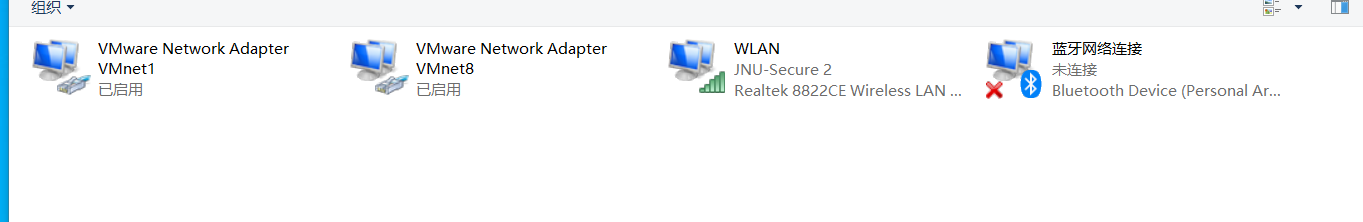
由ping知，其会发送36字节的数据，而在该图中数据的长度都大于36，可以猜想发送时会对数据做一定程度的封装，而根据下半部分的二进制及其ASCII字符，可以猜想发送的信息是abc…uvw，然后再重复abc…uvw。

当ping时，可能发生超时，此时可能是没有该网址，或对方设置了ICMP数据包过滤，或设置了错误的IP等。

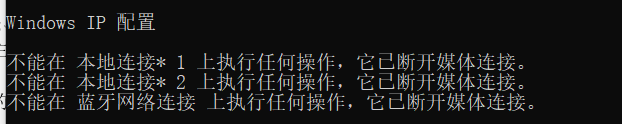
ipconfig

如图，可见后四个和从控制面板中得到的四个是一致的，并且使用了ipv6协议。

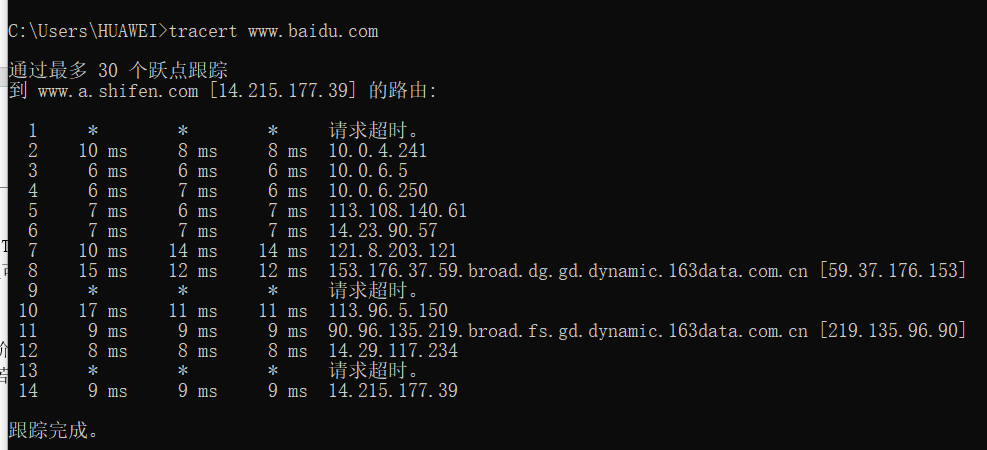




当使用 /release 或 /renew 时，显示的前部多了如下信息



tracert:



当使用wireshark捕捉相应的过程时，可见source列出现了上表中最右列的数字，即经过了相应的结点。

-h：只跟踪指定数目个路由。

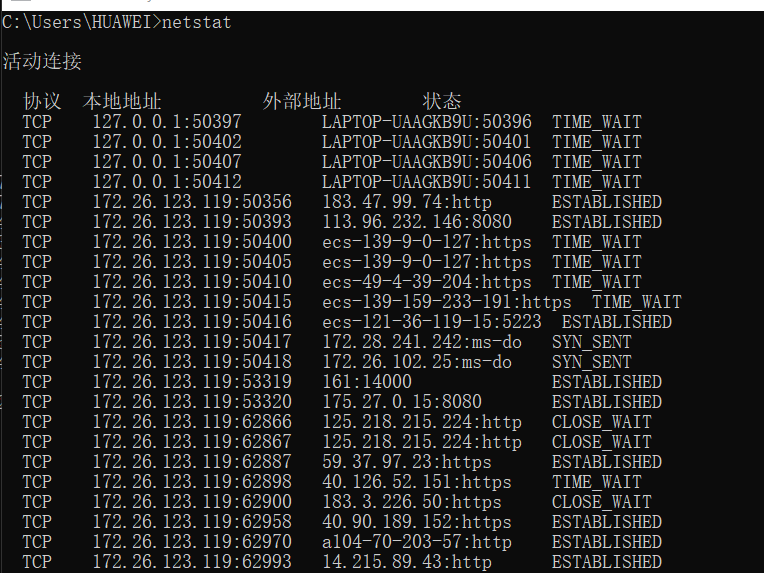


-w：当使用 -w 2时，和不使用-w相比，可见在超时项上前者明显更快。

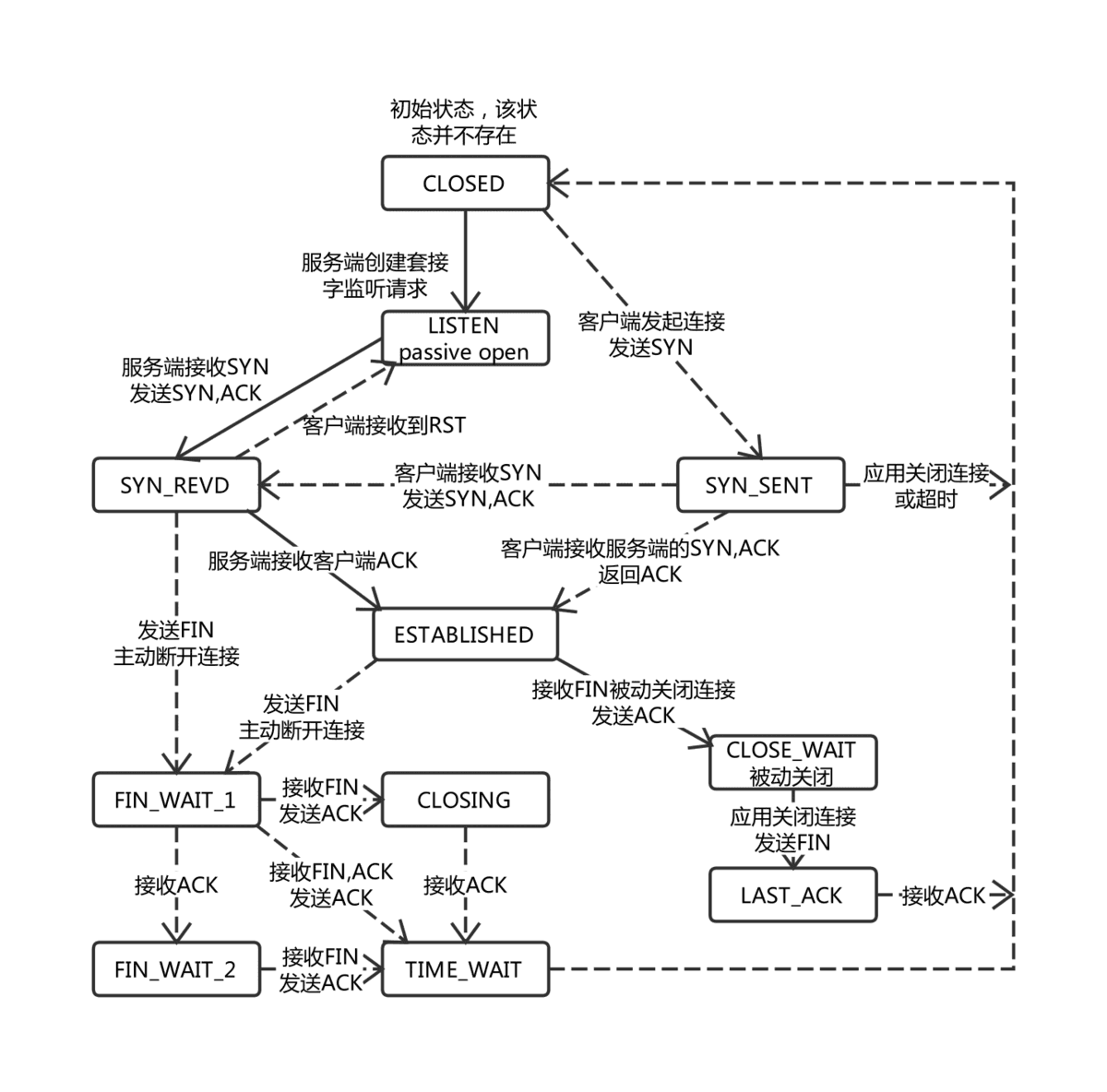
-d：



netstat:

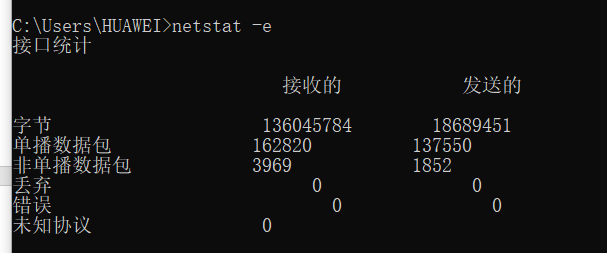


其中各种状态的含义如图所示：



参数测试：

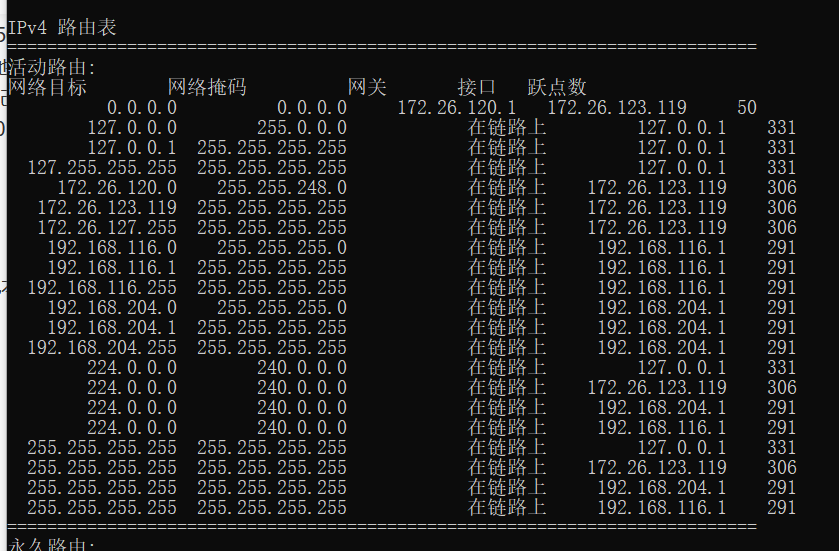
-e



-s：可以显示各种协议的统计信息。

route:

主要部分如下图。第一列是该路由器连接的所有网段。最后一列的数值越少，则可信度越高。第一行的含义是：发向任意网段的数据会通过172.26.123.119被发向172.26.120.1。其余各行类似。



**思考题：**

1. 网关的作用和现实世界中海关的作用类似，充当网络的入口和出口，还可以将具有不同传输协议的两个网络连接在一起。
2. Ping相应的地址，观察发生的情况，依据相应的情况进行处置，比如，如果发生超时，则要考虑检查线路是否接通、地址是否有效等；意味着对方主机不存在或没有与对方建立连接；如果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time 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。

**五、实验总结**

学习了一些和网络相关命令的使用，并且应该学会在恰当的情况使用相关命令进行错误排查，或防止命令被滥用（如实施攻击），初步了解了使用wireshark抓包并进行简单分析。