

本科生实验报告

实验课程:计算机网络实验

专业名称:计算机科学与技术（超算方向）

学生姓名:李钰

学生学号:19335112

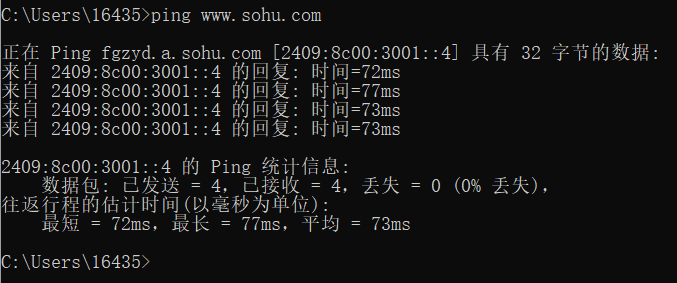
实验成绩:

报告时间:

# 一、实验内容

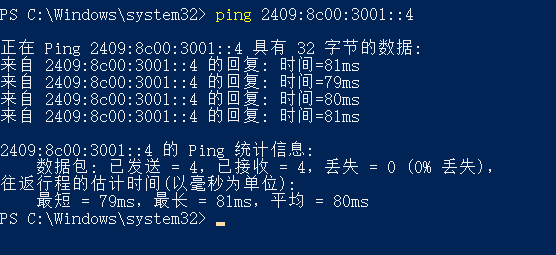
# 实验一 Ping命令

### ping [www.sohu.com](http://www.sohu.com)



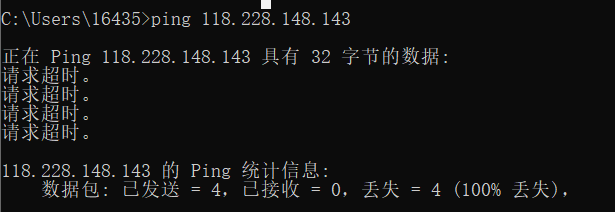
* 结果中可显示域名www.sohu.comIP地址是2409:8c00:3001::4，体现ping 命令从域名中查找对应IP地址的作用.
* 结果显示一共发送了4个数据包，且全部被接收，与对方主机往返一次所用的时间最快为72ms，最长为77ms，平均用时73ms。

### ping 2409:8c00:3001::4



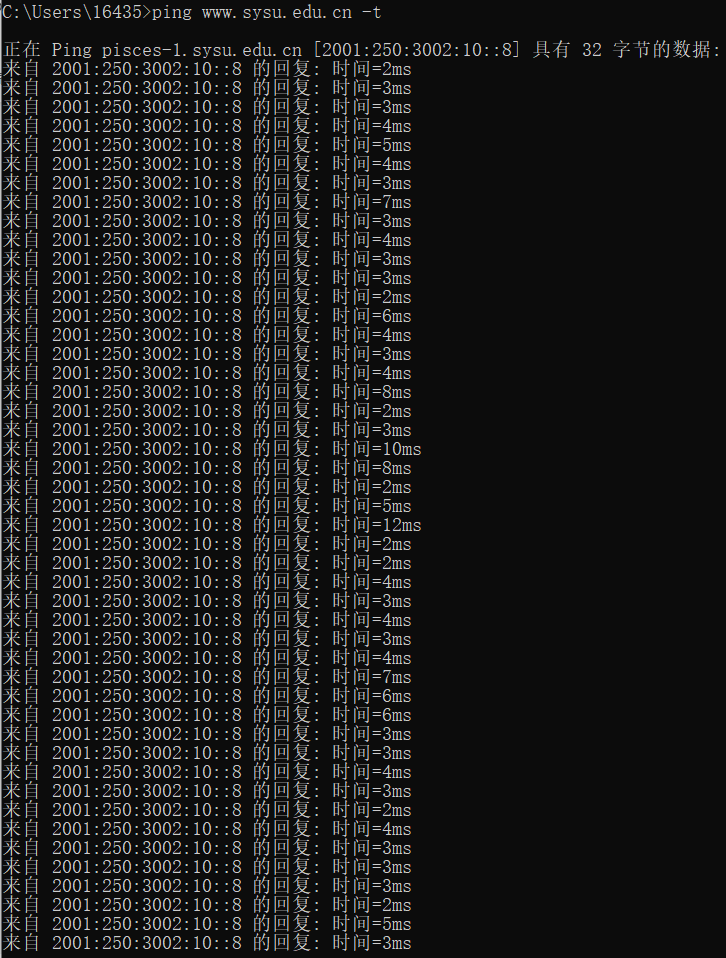
* 利用第一次ping得到的IP地址，更改为ping IP，连通成功。

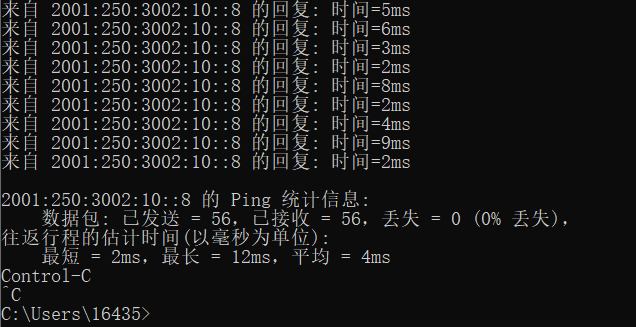
### p**ing 118.228.148.143**



* 由于搜狐的IP地址已作更改，所以此IP地址失效，本机发出的四个数据包全部没有在规定时间(TTL, 生存时间)内被接收，所以显示请求超时，本机与IP地址为118.228.148.143的主机网络连通失败。

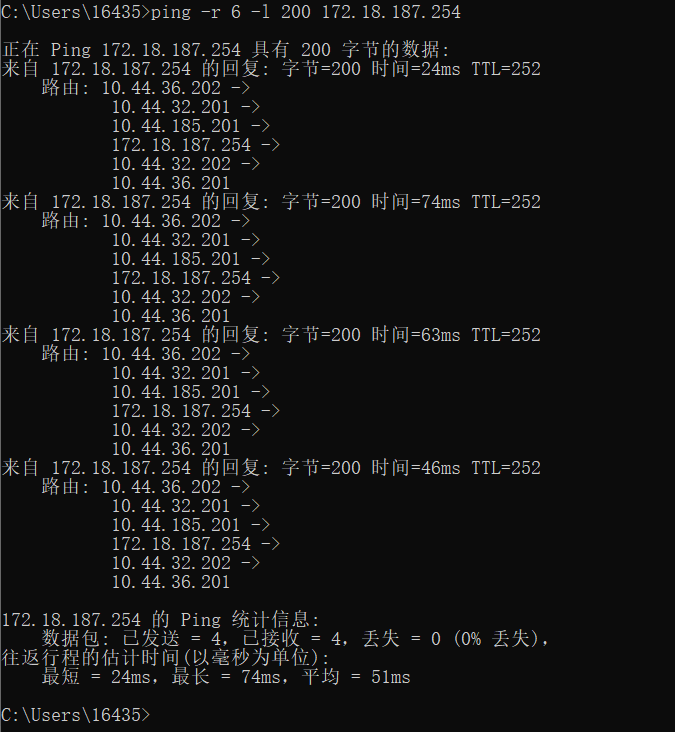
### **ping [www.sysu.edu.cn](http://www.sysu.edu.cn) -t**





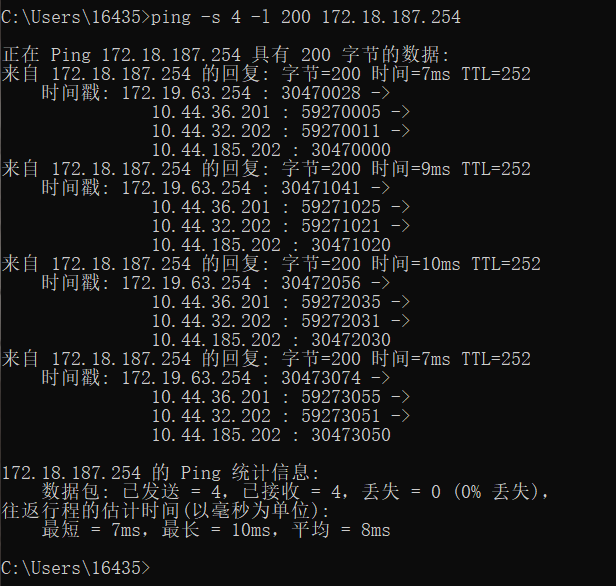
* 该命令表示连续向 [www.sysu.edu.cn](http://www.sysu.edu.cn) 发送ping 测试报文，直至使用ctrl + C键

### **ping -r 6 -l 200 172.18.187.254**



* 该命令记录了向 IP地址为172.18.187.254 发送4个大小为200字节的数据包时，所经历的6个路由

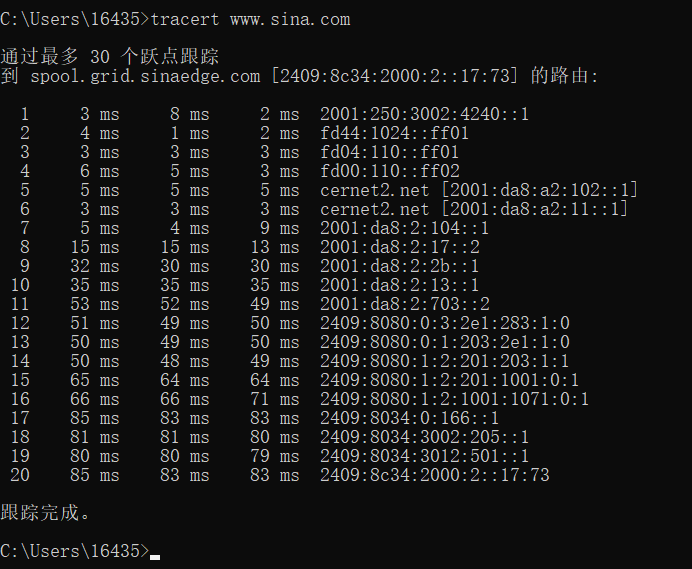
### ping -s 4 -l 200 172.18.187.254



* 该条命令是指设置了4个时间戳，向IP地址为172.18.187.254的主机发送数据包，得到了接受回复。

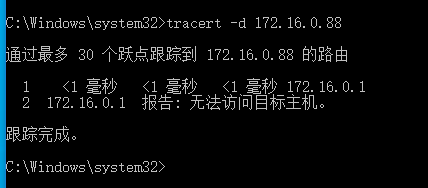
# **实验二 tracert命令**

### **tracert [www.sina.com](http://www.sina.com)**



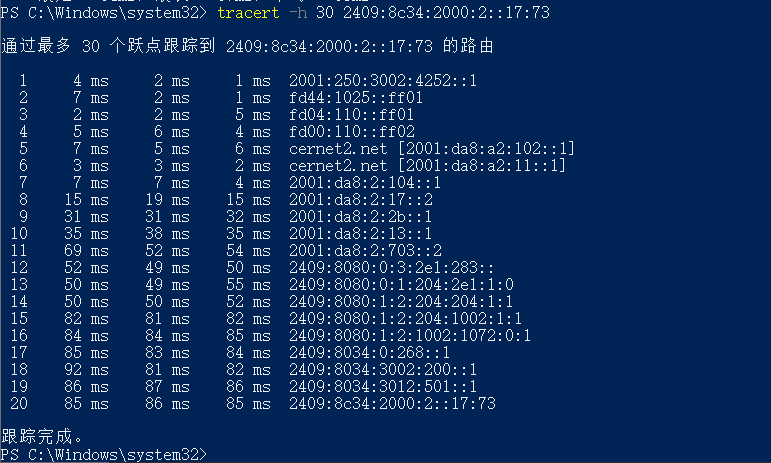
* traert是路由跟踪实用程序，用于获得IP数据报访问目标时从本地计算机到目的主机的路径信息。
* 本条命令，跟踪了www.sina.com路由，结果显示，经过20个路由，最终本机与该网络联通成功。

1. **tracert -d 172.16.0.88**



* 由结果可知，本机与IP地址为172.16.0.88的主机网络连接失败。

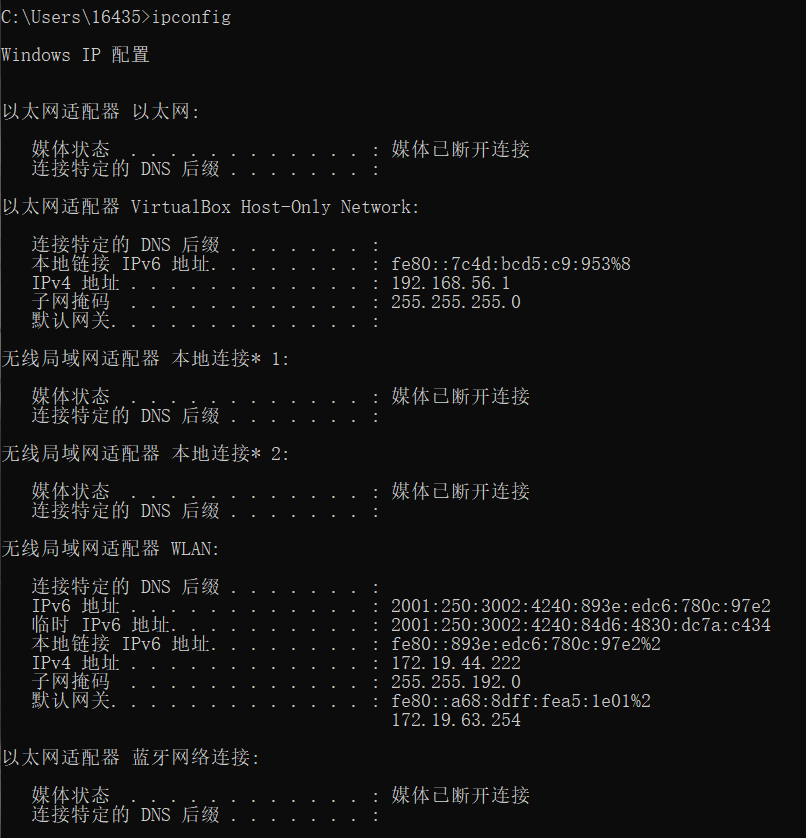
1. **tracert -h 30 2409:8c34:2000:2::17:73**



* 设置搜索目标的路径中存在的跃点最大数为30，实际上通过了20个路由及跟踪到了目的地址。

**实验三 ipconfig**

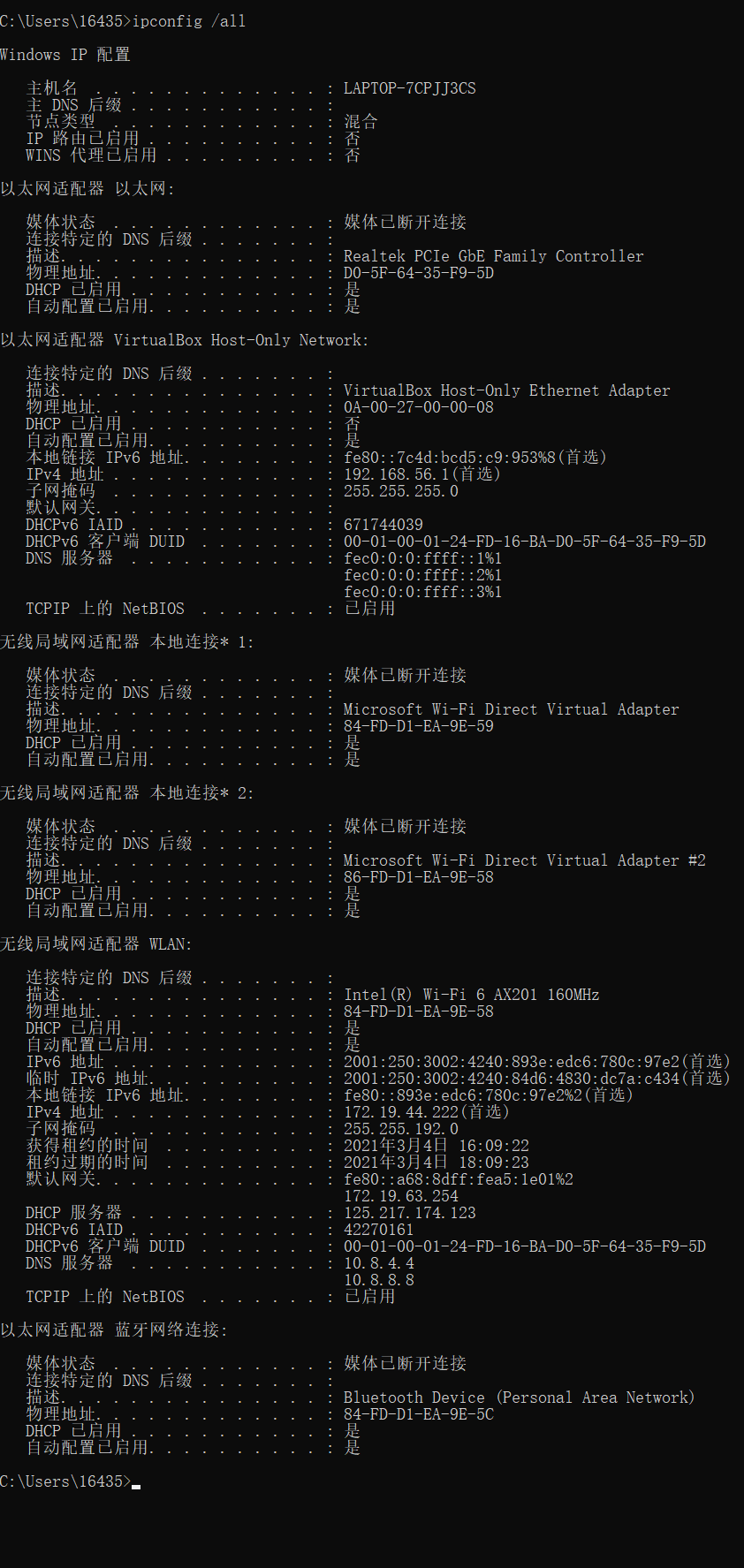
1. **ipconfig**



* 如上图，通过ipconfig命令，显示了本机所有适配器的基本TCP/IP配置

1. **ipconfig /all**

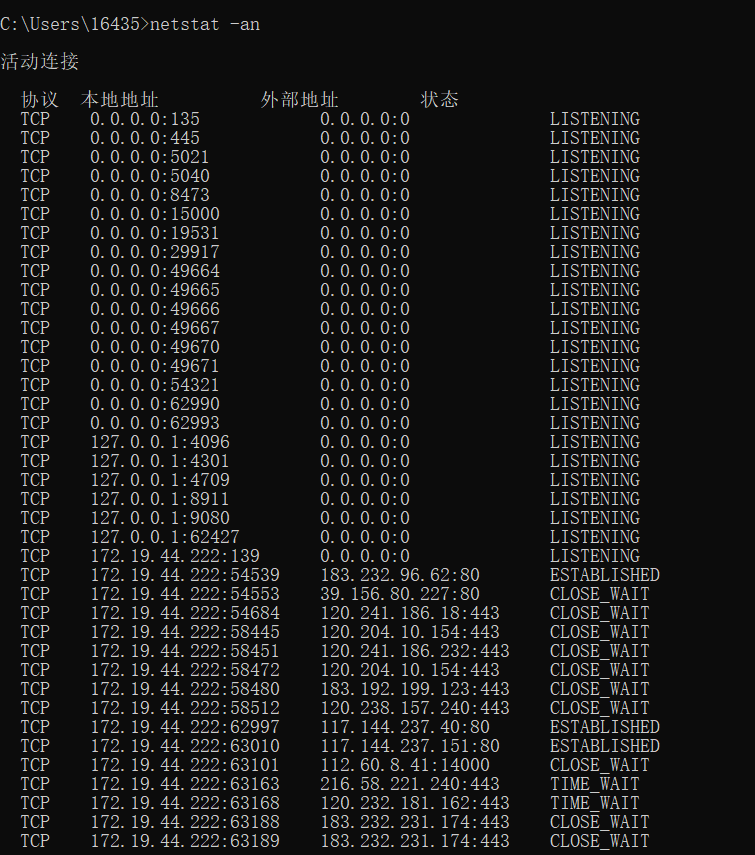
* 如下图，利用 ipconfig /all命令，显示了所有适配器的完整TCP/IP配置

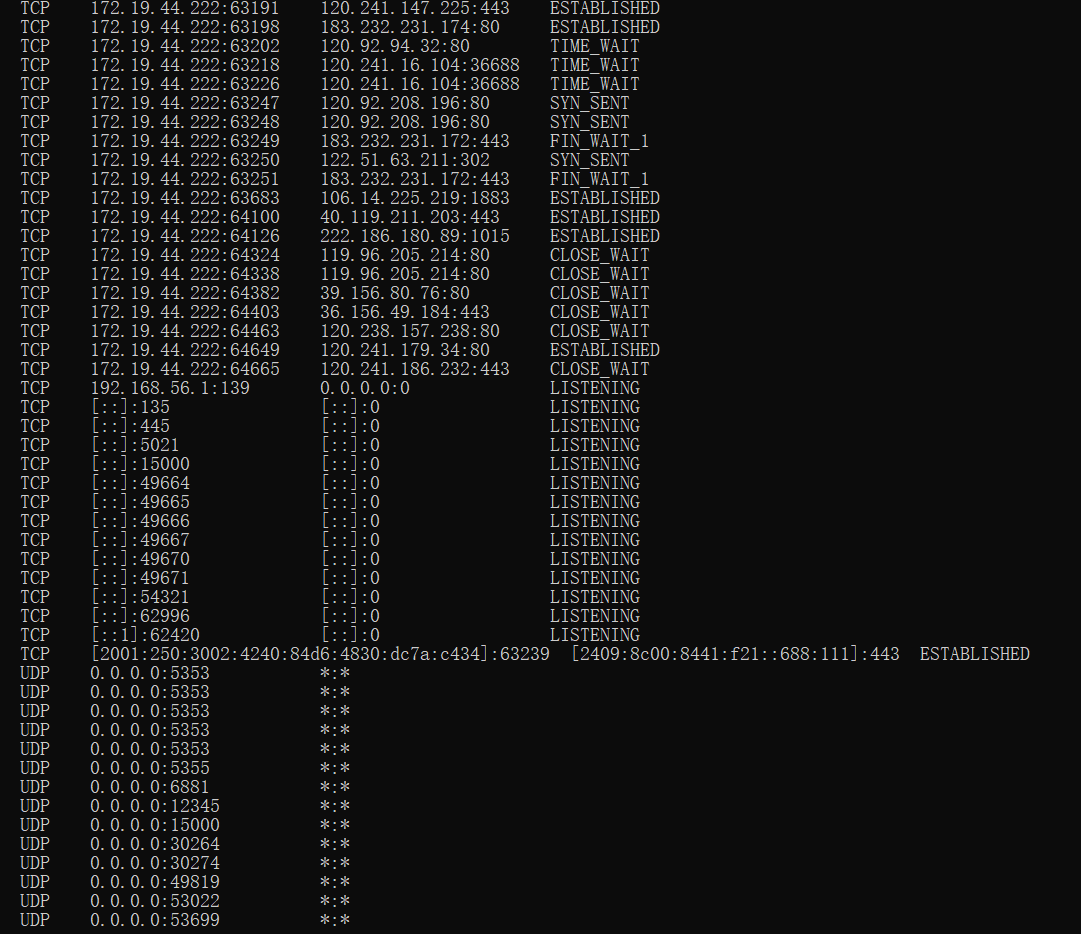


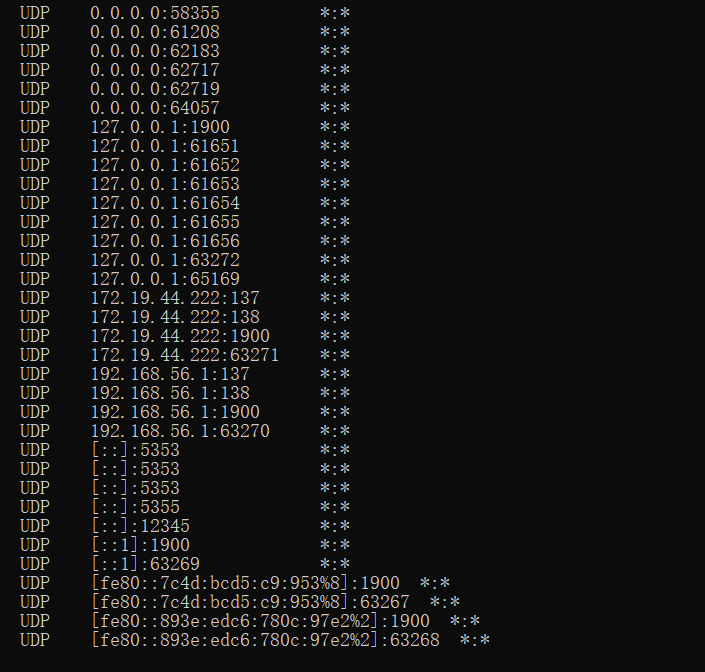
**实验四 netstat命令**

1. **netstat -an**

* 该命令显示了所有活动的TCP链接以及计算机侦听的TCP和UCP端口。



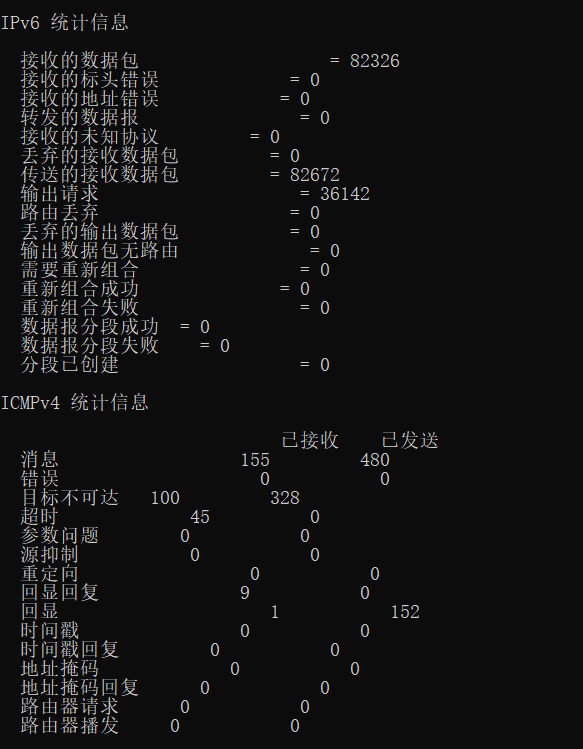


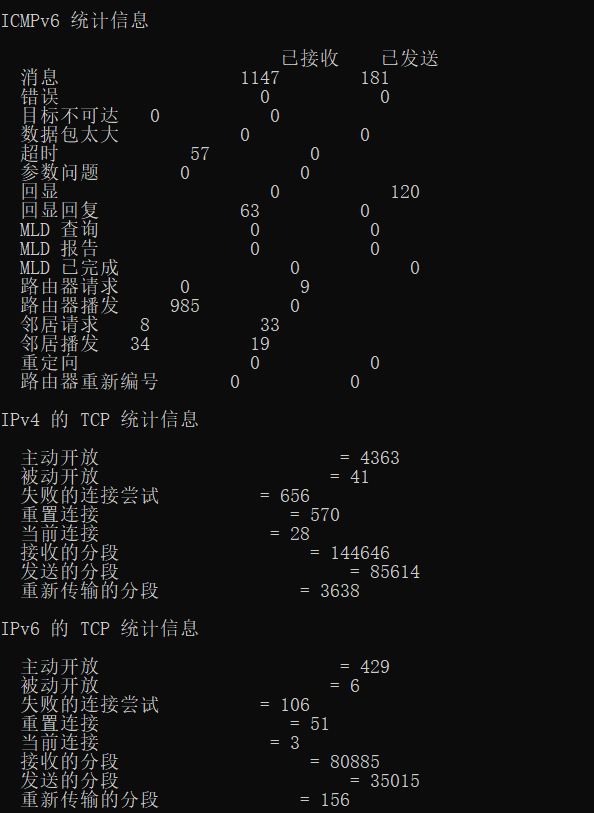


1. **netstat -e -s**

* 该命令，显示了以太网统计信息，例如发送和接收的字节数、数据包数



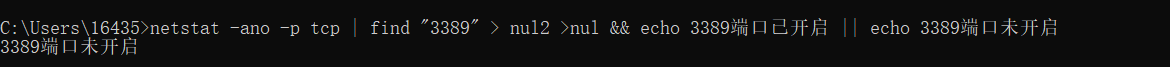






**实验五 netstat命令检测端口是否被开放**

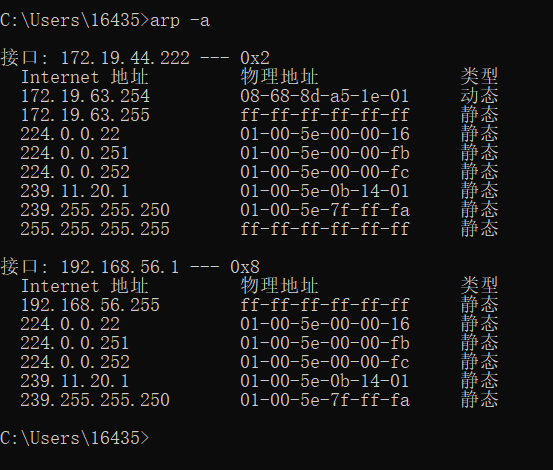
1. **命令：netstat -ano -p tcp | find “3389”>nuk 2>nul &&echo 3389端口已开启 || echo 3389 未开启**



* 图中结果显示：3389端口未开启

**实验六 arp**

1. **arp -a**

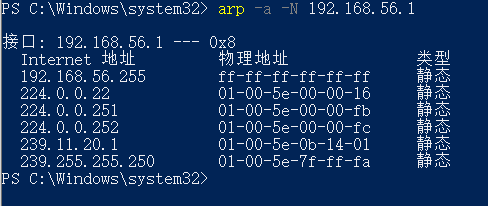


* 该指令显示了所有接口的arp缓存表，其IP地址、物理地址以及类型

1. **arp -a -N 192.168.1.100**

98a0e2554ab8f43de8095171cdb1ed4

* 因为本机无该接口，所以显示错误参数
* 修改命令为arp -a -N 192.168.56.1



* 显示了该接口的ARP缓存表

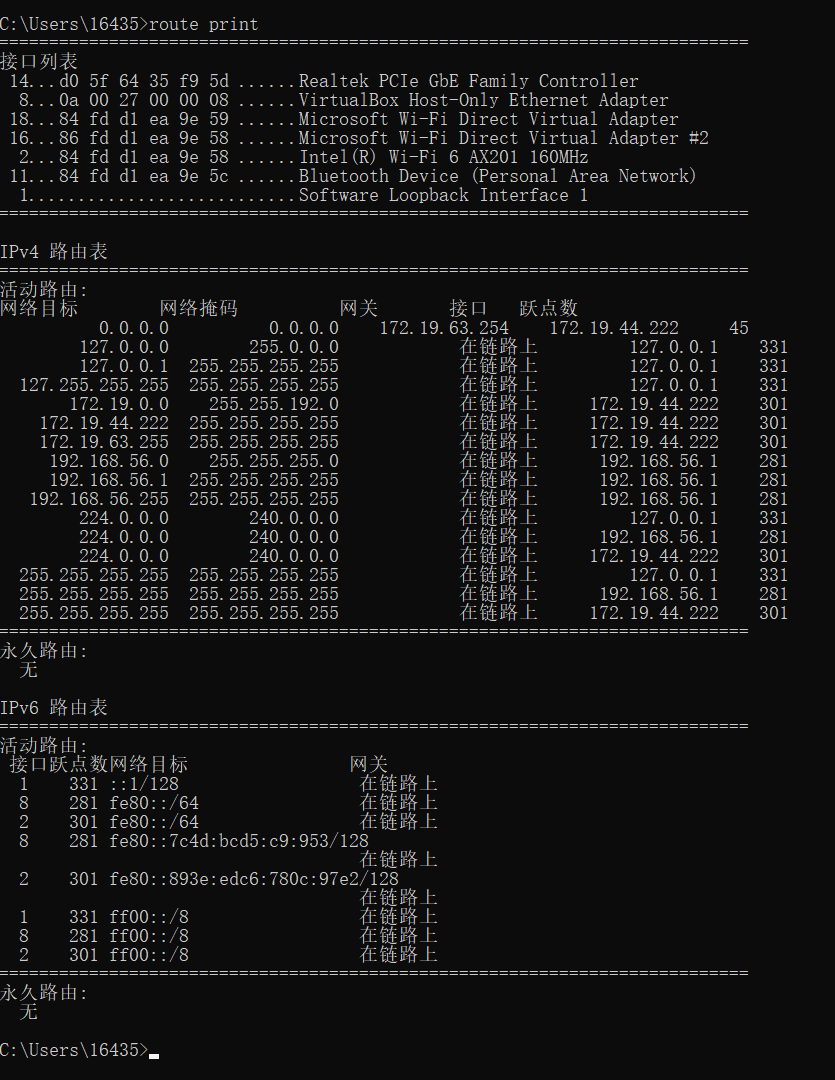
1. **arp -s 192.168.56.1 01-00-5e-00-00-16**



* 该指令将本机IP地址与物理地址01-00-5e-00-00-16绑定,再次查看接口缓存表，对比之前的可以发现多了一条记录

**实验七 route**

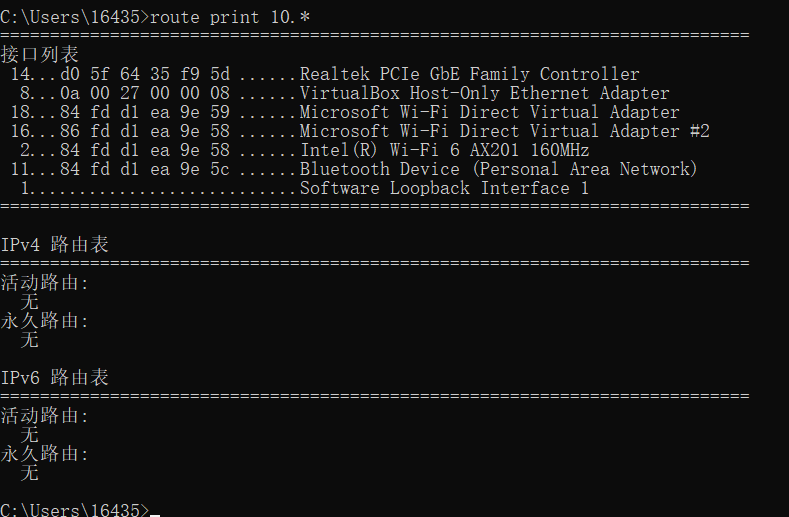
1. **route print**



* 通过该指令，显示了IP路由表的完整内容。

1. **route print 10.\***

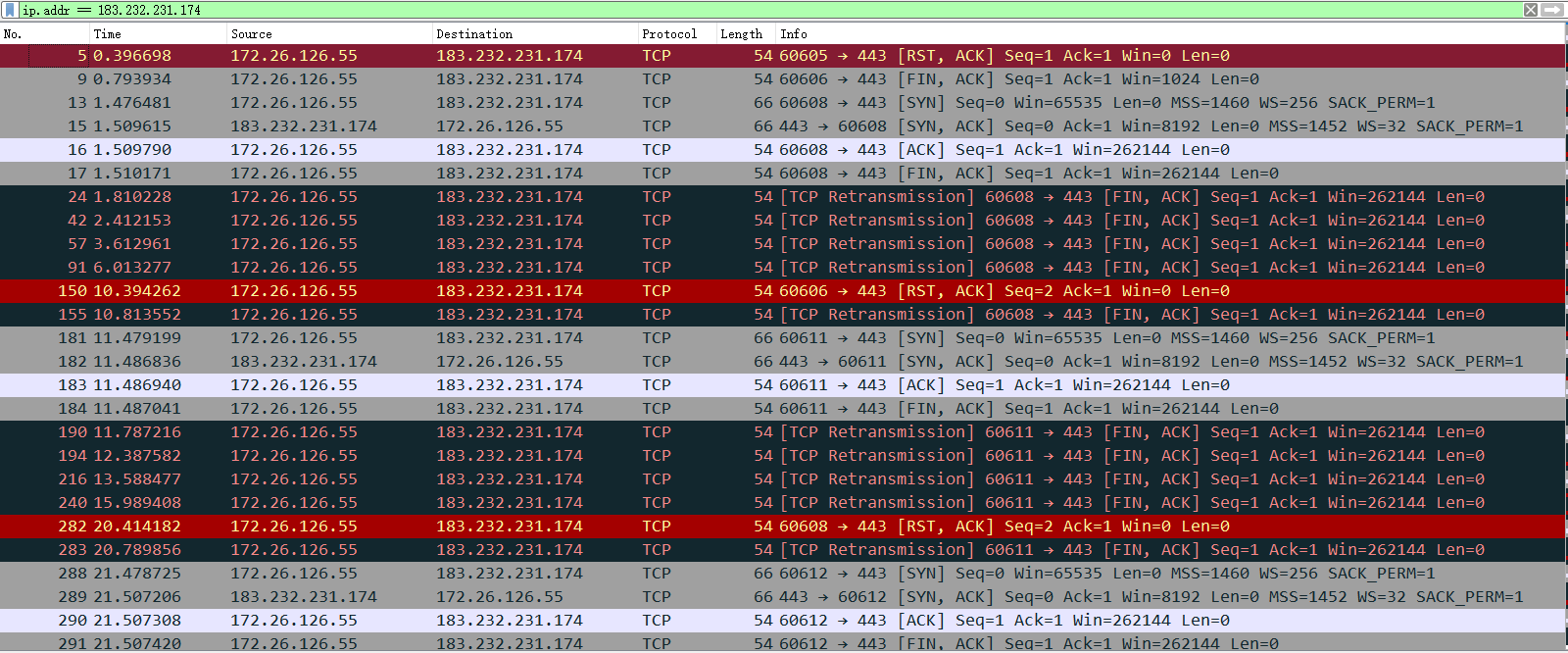
* 通过该指令，显示了IP路由表中以10.开头的路由



**实验八 使用wireshark捕获数据包，设置2至多种不同过滤条件**

1. **ip.addr == 183.232.231.174**

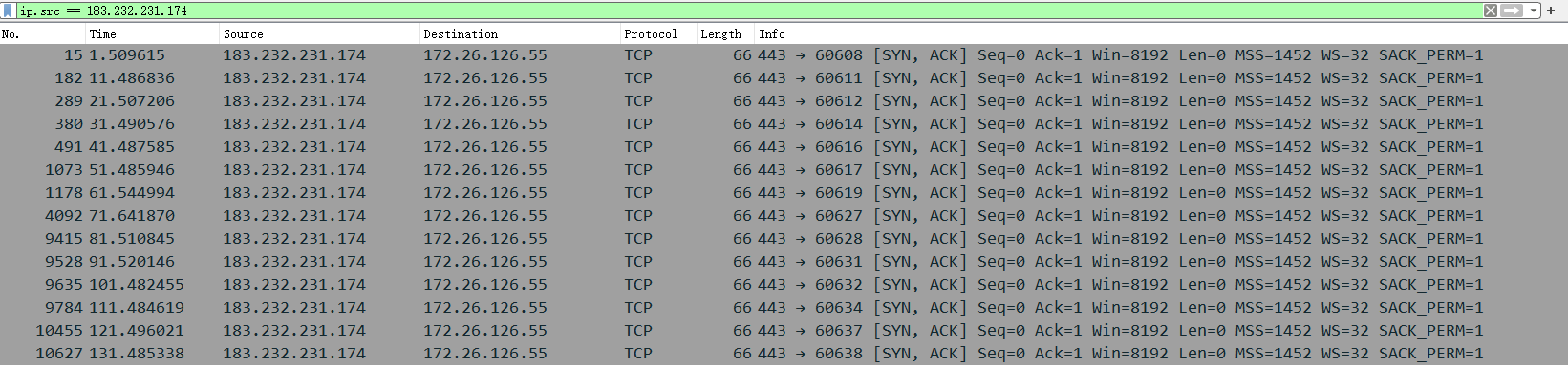
* 第一个过滤条件，仅显示与指定IP地址（183.232.231.174）通信的记录



* 如图，显示的所有记录来源或目的地为183.232.231.174

1. **ip.src == 183.232.231.174**

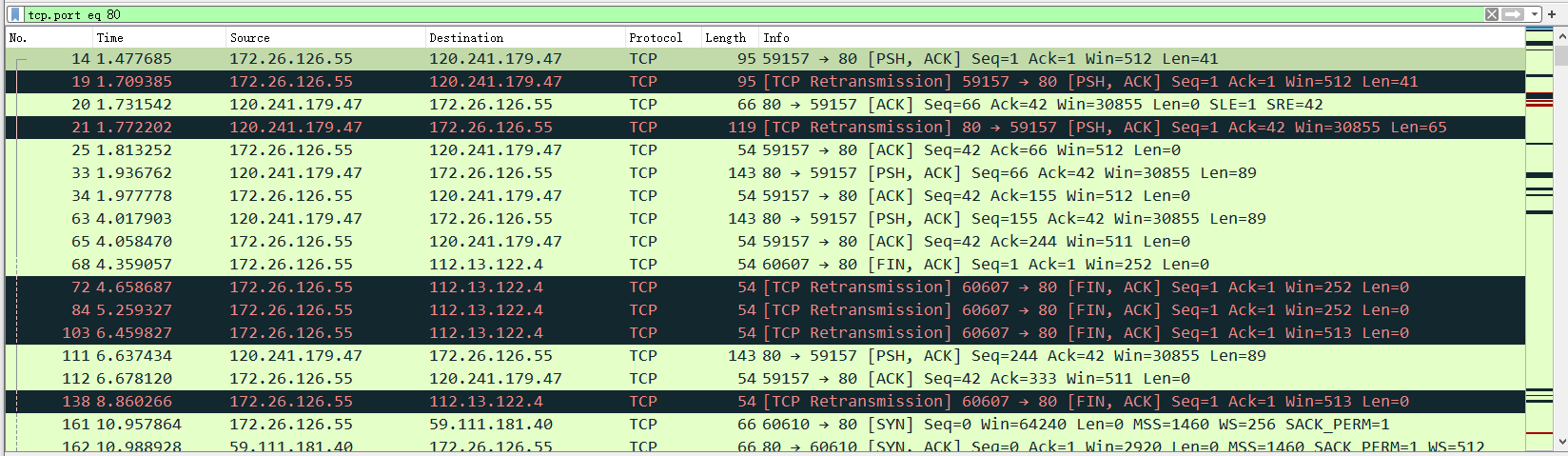
* 如图，将过滤条件设置为ip地址的来源为183.232.231.174



* 图中显示的均是来自183.232.231.174的记录

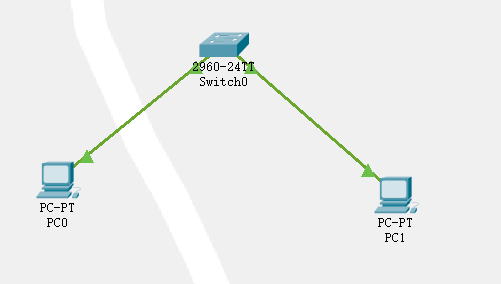
1. **tcp.port eq 80**

* 该过滤条件是按端口过滤的，不管端口是源还是目标的都只显示满足tcp.port == 80条件的包。

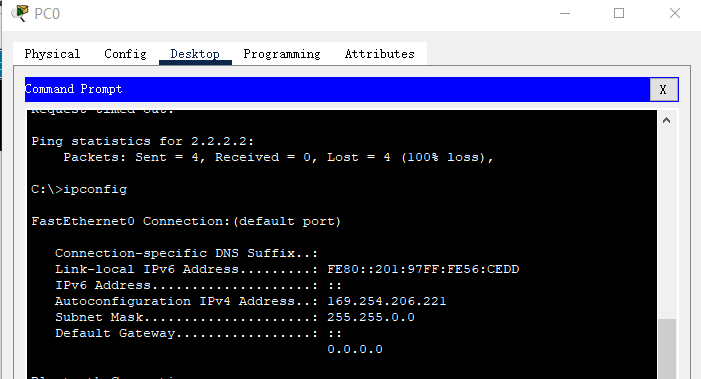


**实验九 使用packet tracer实时、仿真两个操作模式呈现网络的行为**

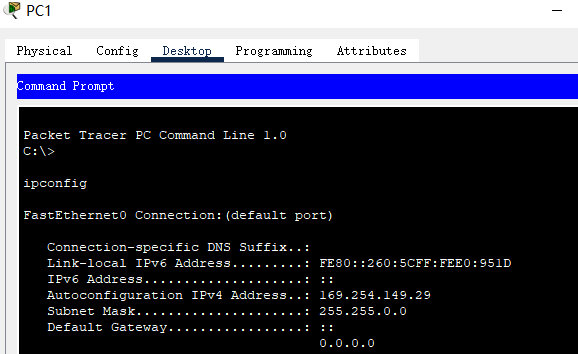
1. **实时模式**



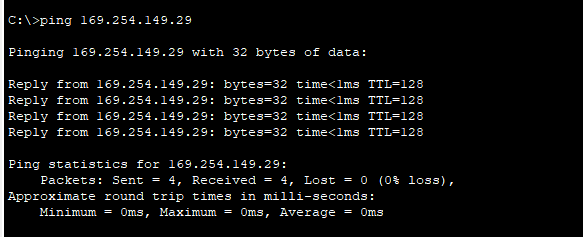
* 通过ipconfig命令，得知PC0的IP地址为169.254.206.221



* 同样，得知PC1 的IP地址为169.254.149.29

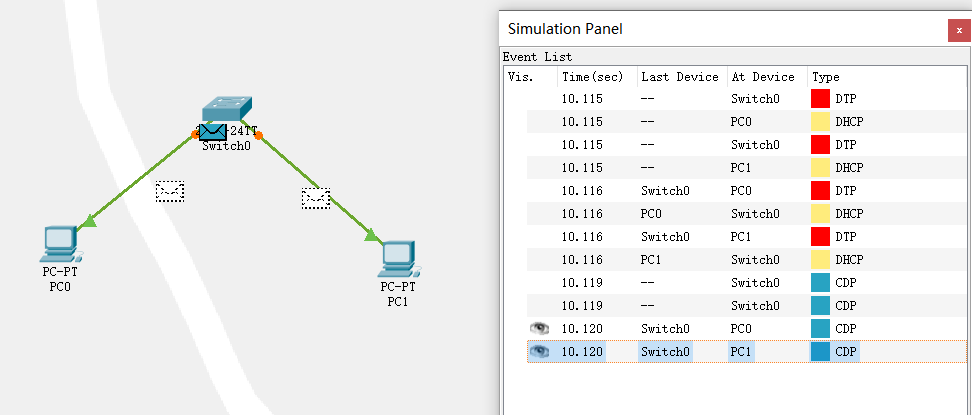


* 在PC0上操作，ping 169.254.149.29，连接成功



* 在实时模式中，网络行为和真实设备一样，对所有网咯行为及时响应。

1. **仿真模式**

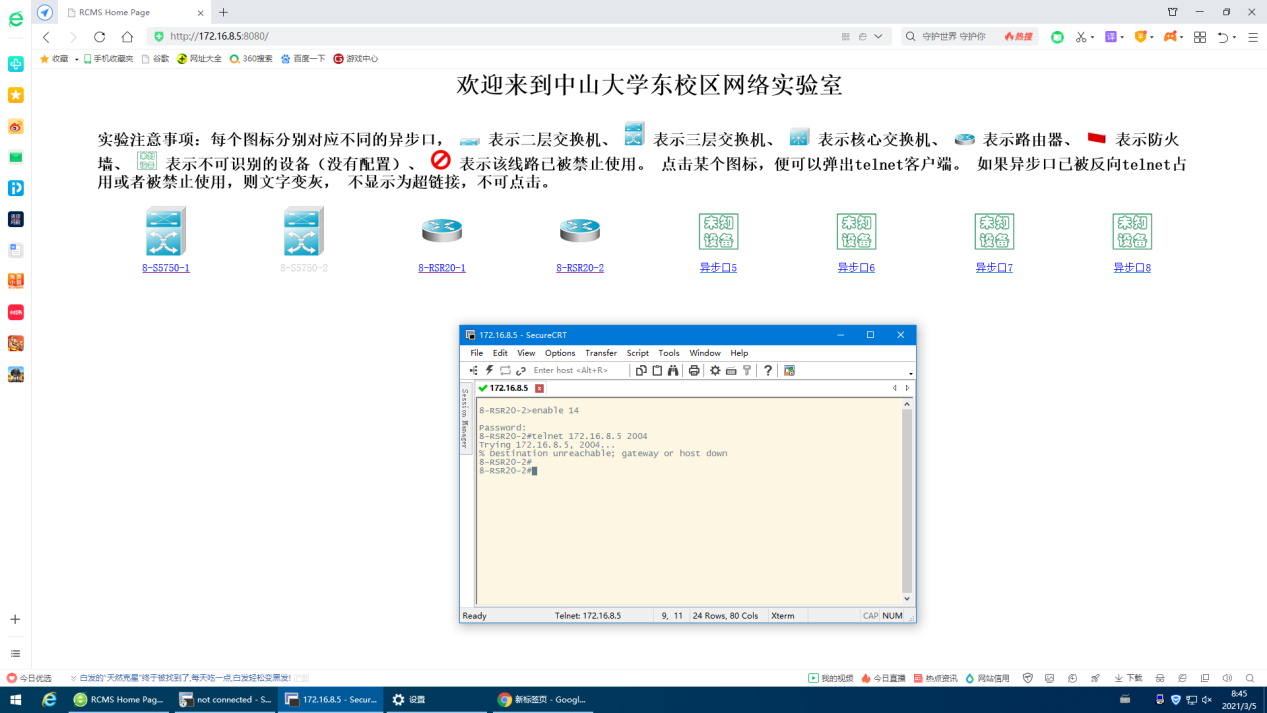


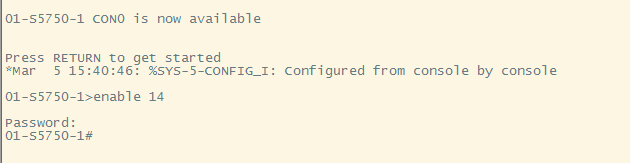
* 在仿真模式中，用户可以看到和控制时间间隔、数据传输的内部流程。

**实验十**

1. **通过web访问RCMS**

* 打开浏览器，输入http://172.16.8.5:8080即可进入
* 选择实验设备
* Enable 14 进入特权模式
* 输入密码b402

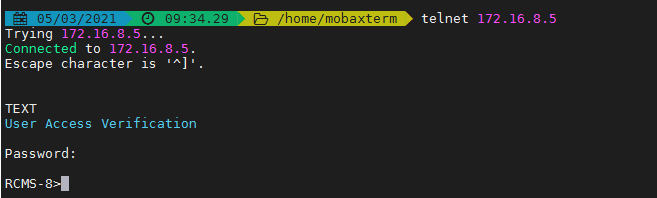




* 进入全局模式



1. **通过telnet访问网络设备**



* 按正确形式输入命令，可见显示已连接

# 二、总结

通过这次实验，我学习到了若干网络命令，对他们的功能、用途、格式，有了一定得了解；其次还学习应用了两个软件wire shark抓包工具以及packet tracer，体会到了在实时和仿真两种模式下不同的网络行为呈现，为后续实验奠定了一定的基础。