廣東工業大學

《计算机网络》实验报告

学　　院　先进制造学院

专　　业　计算机科学与技术

年级班别　22 级计科 8 班

学　　号　3122008883

学生姓名　陈煜祺

指导教师　梁路

成　　绩

广东工业大学

实验题目 Windows 下常用的网络命令

一、 实验目的

学习在 Windows 系统中进行网络配置、用 ping ipconfig/winipcfg 命令工具来进行网络测试、使用 tracert 路由跟踪命令、使用 netstat、arp、nslookup 命令查看网络状态。

本实验在于使学生更好地理解计算机网络设置的基本操作，掌握计算机网络配置的基本监测技术。

二、 实验内容和要求

1、使用 Ping 工具测试本机 TCP/IP 协议的工作情况，记录下相关信息。

2、使用 IPconfig 工具测试本机 TCP/IP 网络配置，记录下相关信息。

3、使用 netsh 工具测试本机 TCP/IP 网络配置，记录下相关信息。

4、使用 Tracert 工具测试本机到 www.sohu.com 所经过的路由数，记录下相关信息。

5、使用 Netstat 工具，记录下相关信息。

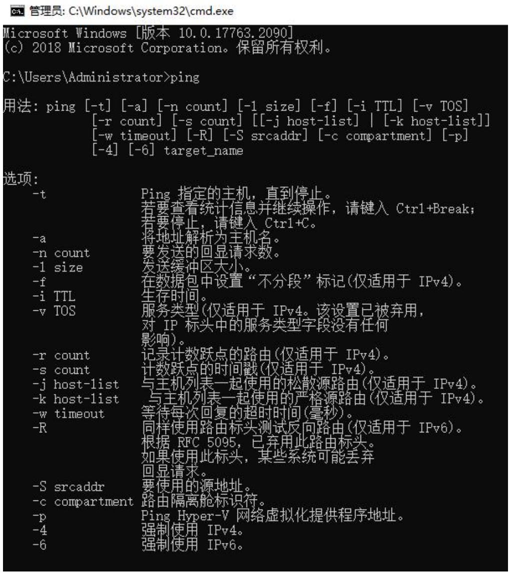
6、使用 Arp 工具，记录下相关信息。

7、使用 Nslookup 工具，记录下相关信息。

三、 实验结果 （截图和说明）

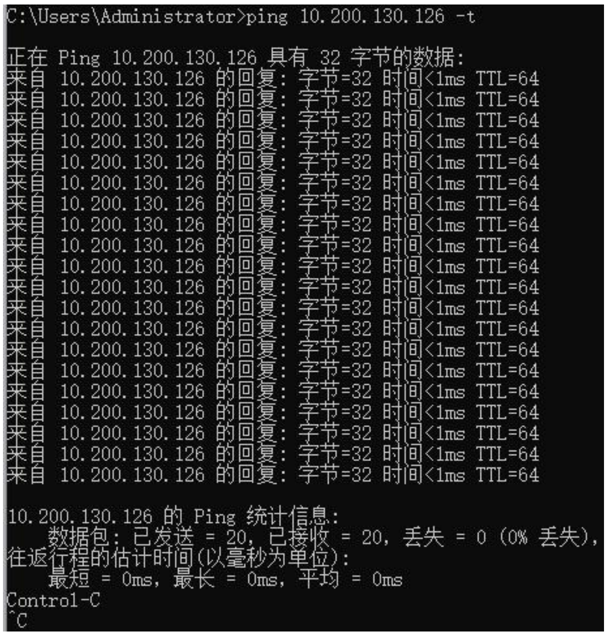
3.1 使用 Ping 工具测试本机 TCP/IP 协议的工作情况，记录下相关信息。

3.1.1 ping 命令格式



如图，显示出了 ping 命令的用法和选项格式。

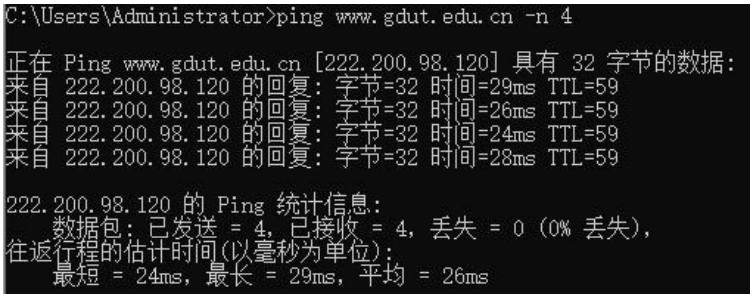
3.1.2 ping –t 的使用



如图，ping 机房中本机的网关显示可以正常访问。

然后使用键盘 Ctrl+C 终止了 ping 行为。

3.1.3　ping –n 的使用



如图，使用 ping [域名] –n 4 向广工官网进行了四次 ping 操作，可以正常访问。

3.1.4　ping -l 的使用

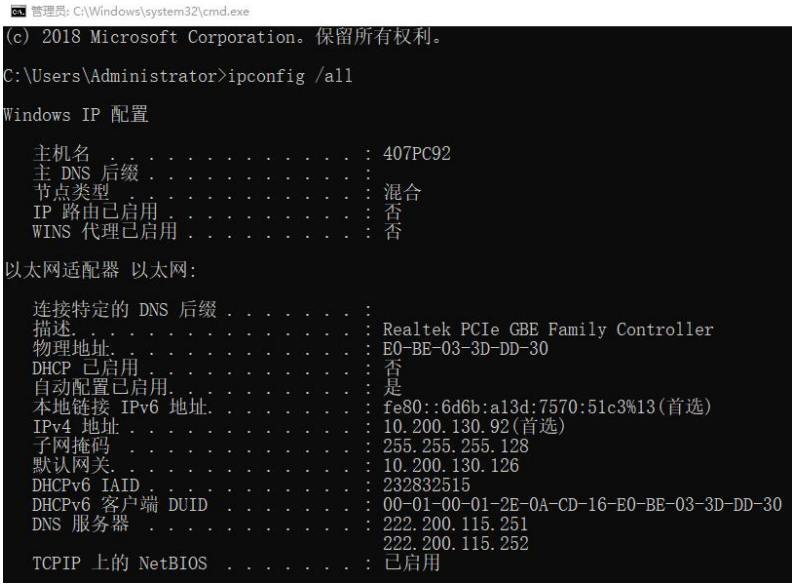
如图，使用 ping –l 向百度官网进行了 ping 操作，发送长度为 1024B。

3.1.5　ping -l -t 的组合使用

如图，使用 ping -t -l 向新浪官网进行了连续 ping 操作，发送长度为 128B。

然后使用键盘 Ctrl+C 终止了 ping 行为。

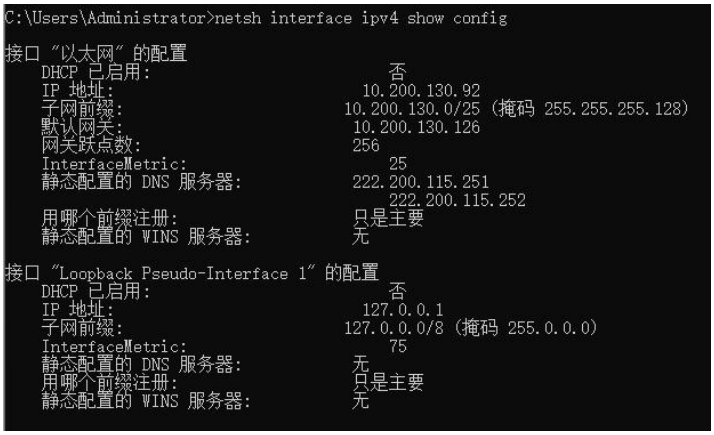
3.2　使用 IPconfig 工具测试本机 TCP/IP 网络配置，记录下相关信息。



如图，为本机的 TCP/IP 网络配置信息。

3.3 使用 netsh 工具测试本机 TCP/IP 网络配置，记录下相关信息。

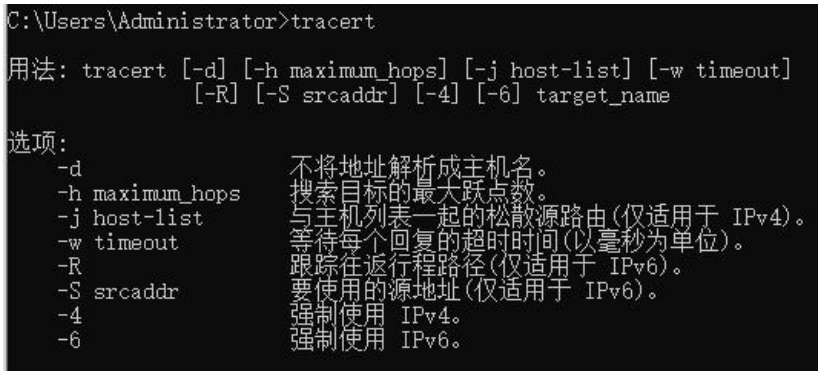
如图，通过 netsh 工具显示了 TCP 的全局参数。



如图，通过 netsh 工具显示了 IPv4 的配置信息。

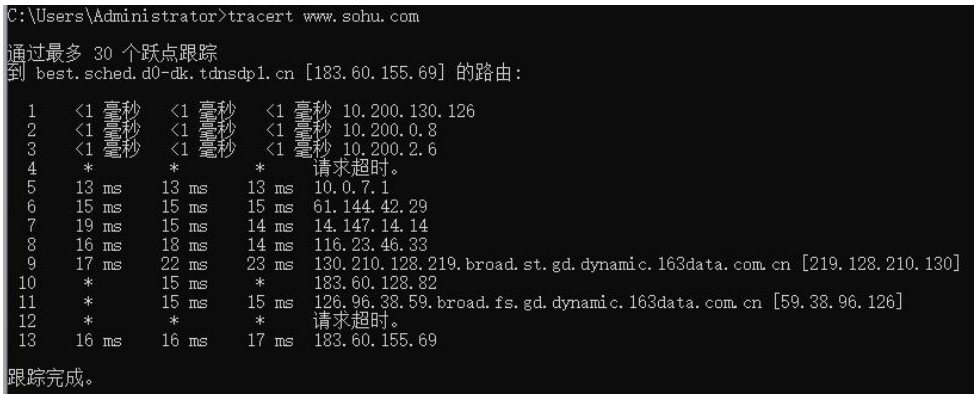
3.4 使用 Tracert 工具测试本机到 www.sohu.com 所经过的路由数，记录下相关信息。

3.4.1 tracert 命令的格式



如图，显示了 tracert 命令的格式和用法。

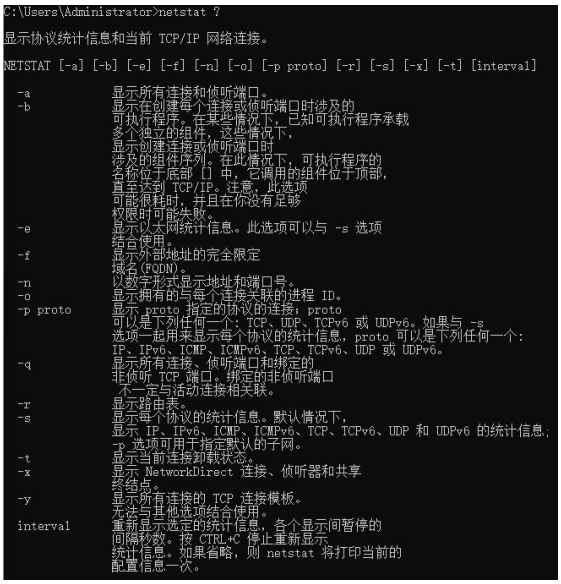
3.4.2 使用 tracert 跟踪搜狐官网



如图，显示了本机到搜狐官网的路由跟踪过程，共经过了 13 个路由。

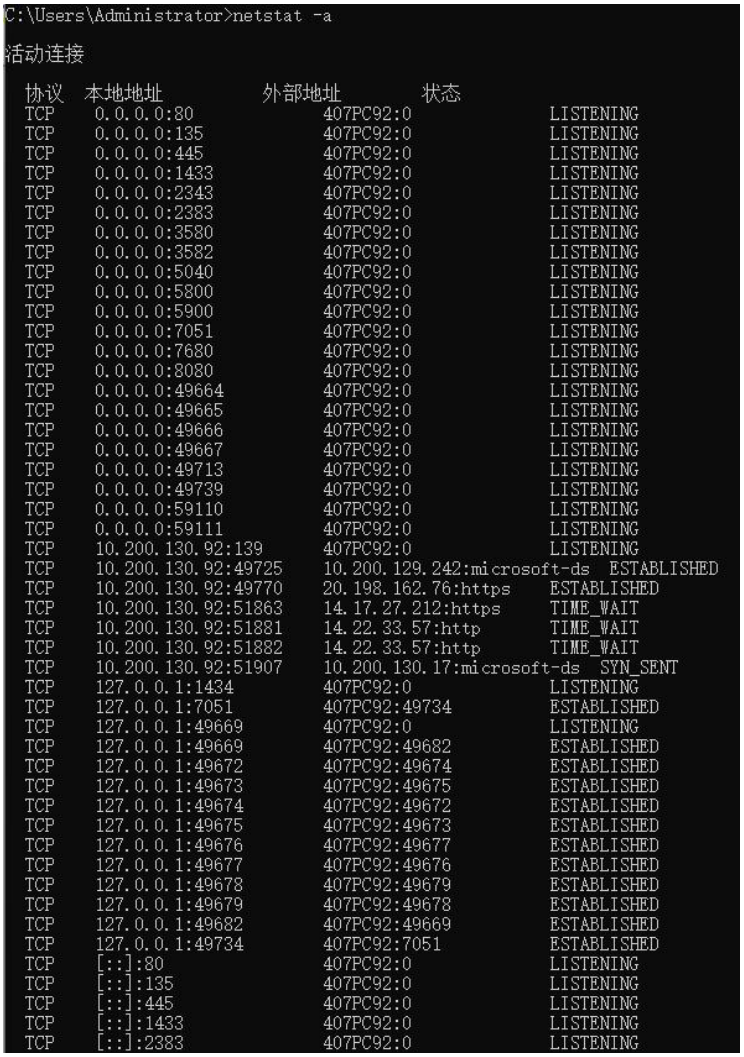
3.5 使用 netstat 工具测试本机 TCP/IP 网络配置，记录下相关信息。

3.5.1 netstat 命令格式



如图，输入 netstat ?后显示了该命令的用法格式。

3.5.2 netstat –a 的使用



如图，显示了正在活动的连接。后半部分已省略。

3.5.3　netstat –e 的使用

```
C:\Users\Administrator>netstat -e
接口统计

                           接收的            发送的

字节                    3916296520        81094504
单播数据包                 158188          151848
非单播数据包              4950632           34024
丢弃                           0                 0
错误                           0                 0
未知协议                       0
```

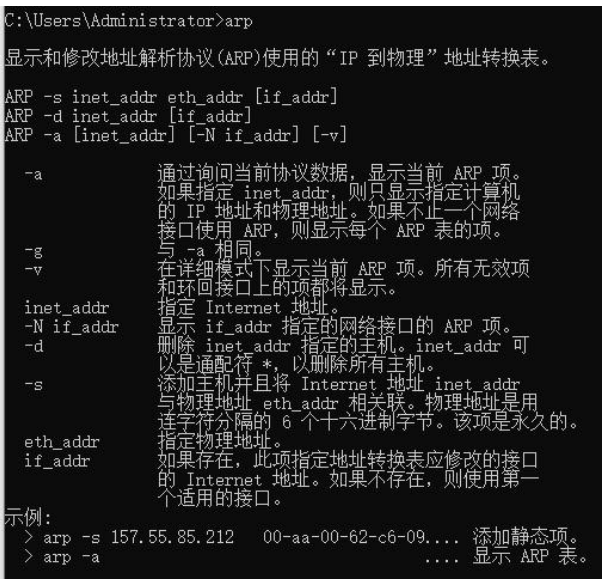
如图，显示了接收和发送数据量的统计信息。

3.5.4　netstat –n 的使用

```
C:\Users\Administrator>netstat -n

活动连接

  协议  本地地址          外部地址        状态
  TCP    10.200.130.92:49725    10.200.129.242:445     ESTABLISHED
  TCP    10.200.130.92:49770    20.198.162.76:443      ESTABLISHED
  TCP    10.200.130.92:51970    52.177.176.186:443     ESTABLISHED
  TCP    10.200.130.92:51971    14.22.7.190:80         TIME_WAIT
  TCP    127.0.0.1:7051         127.0.0.1:49734        ESTABLISHED
  TCP    127.0.0.1:49669        127.0.0.1:49682        ESTABLISHED
  TCP    127.0.0.1:49672        127.0.0.1:49674        ESTABLISHED
  TCP    127.0.0.1:49673        127.0.0.1:49675        ESTABLISHED
  TCP    127.0.0.1:49674        127.0.0.1:49672        ESTABLISHED
  TCP    127.0.0.1:49675        127.0.0.1:49673        ESTABLISHED
  TCP    127.0.0.1:49676        127.0.0.1:49677        ESTABLISHED
  TCP    127.0.0.1:49677        127.0.0.1:49676        ESTABLISHED
  TCP    127.0.0.1:49678        127.0.0.1:49679        ESTABLISHED
  TCP    127.0.0.1:49679        127.0.0.1:49678        ESTABLISHED
  TCP    127.0.0.1:49682        127.0.0.1:49669        ESTABLISHED
  TCP    127.0.0.1:49734        127.0.0.1:7051         ESTABLISHED
```

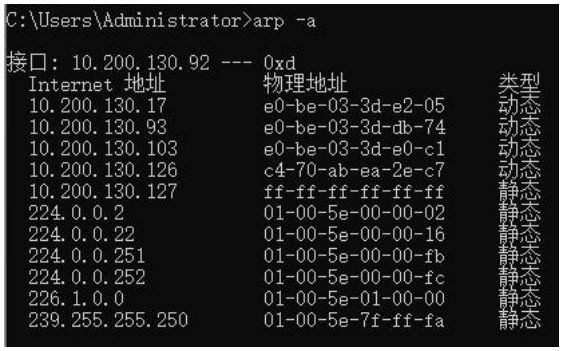
3.6 使用 Arp 工具，记录下相关信息。

3.6.1 arp 命令的格式和用法



如图，显示了 arp 命令的格式和用法。

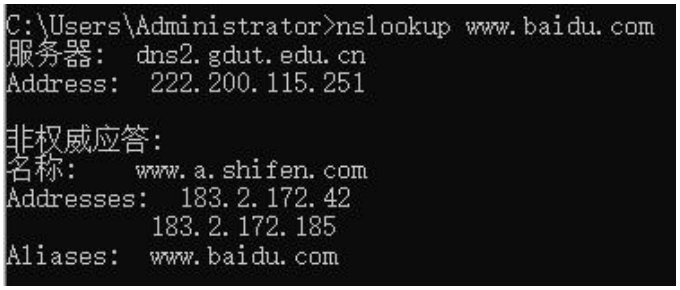
3.6.2 使用 arp 命令显示 ARP 表



如图，通过 arp –a 命令显示出了当前的 ARP 表。

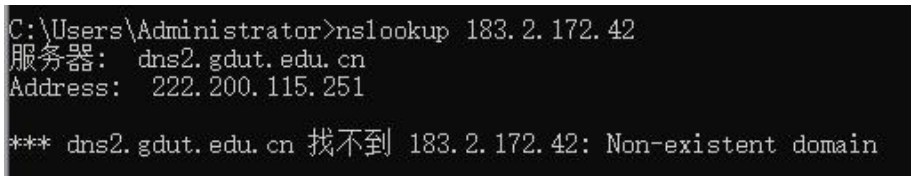
3.7 使用 Nslookup 工具，记录下相关信息。

3.7.1 查询百度域名信息



以上结果显示，正在工作的 DNS 服务器的主机名为 dns2.gdut.edu.cn，它的 IP 地址是 222.200.115.251。域名 www.baidu.com 的 IP 地址是 183.2.172.42。

3.7.2. 将 IP 地址反向解析



如图所示，通过 IP 地址无法解析。

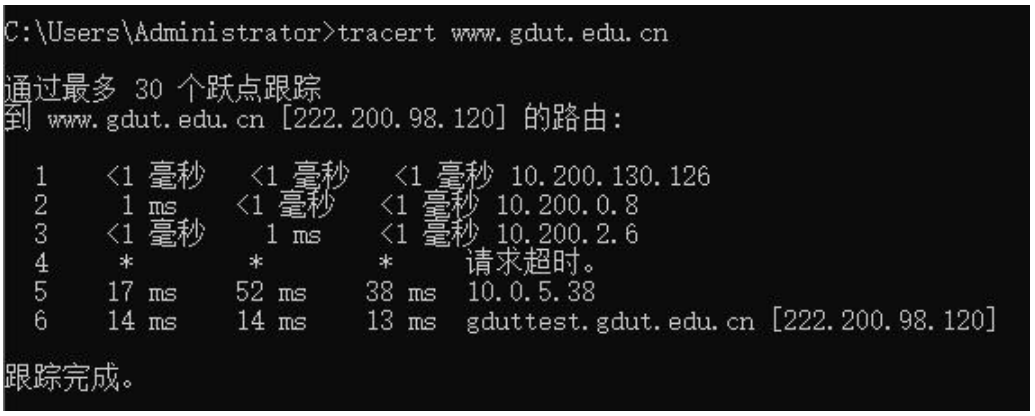
四、 问题与讨论

1. 如何测试你的主机到特定网址的连接是否有故障？如果有故障，如何进一步分析故障的原因?

答：使用 ping 命令可以测试主机到特定网址的连接是否有故障；如果有故障，可以尝试使用 tracert 命令来跟踪路由情况，进而得知在哪一跳出现了问题。也可以尝试 ping 网关来检查主机是否能与网关正常连接。此外，也可以通过 ipconfig 等命令来查看本机网络配置，检查是否配置有误。

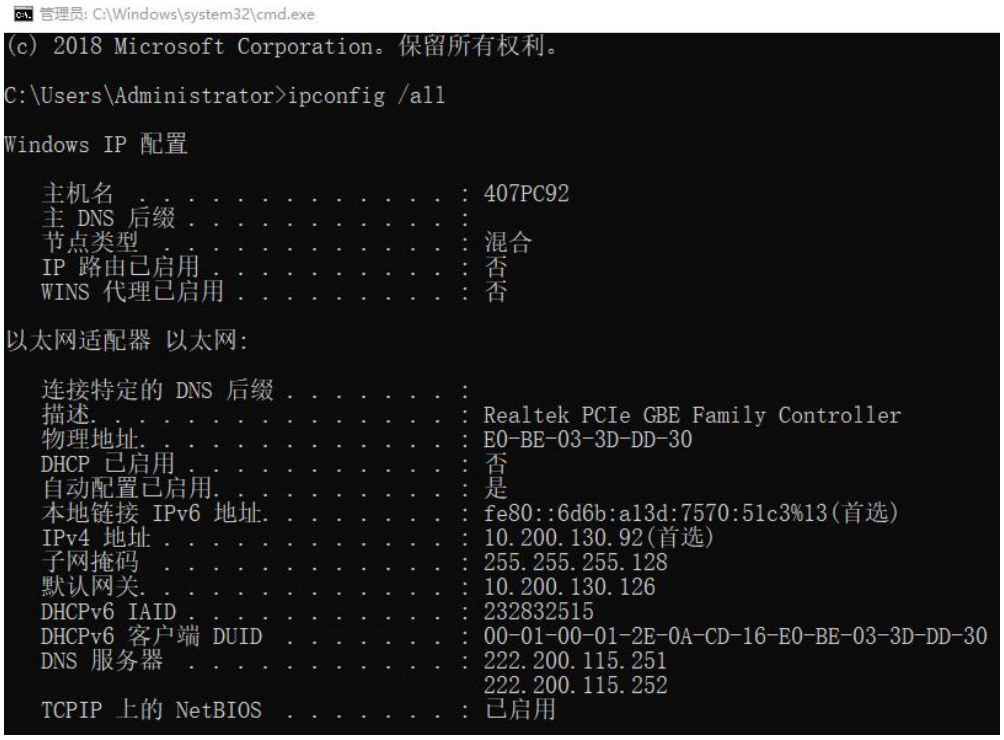
2. 记录结果：Tracert www.gdut.edu.cn

答：结果如下图所示。



3． 你的主机的 48 位以太网地址(MAC 地址)是多少？

答：通过 ipconfig 命令可以查询到本机的以太网地址。如下图所示，为 e0:be:03:3d:dd:30。



广东工业大学

实验题目 协议分析软件基础

一、 实验目的

1．掌握如何利用协议分析工具分析 IP 数据报报文格式，体会数据报发送、转发的过程。在学习的过程中可以直观地看到数据的具体传输过程。

通过分析截获TCP报文首部信息，理解首部中的序号、确认号等字段是TCP可靠连接的基础。通过分析Wireshark连接的三次握手建立和释放过程，理解TCP连接建立和释放机制。

2．利用Wireshark（Ethereal）抓包。

3．对抓取到的包进行分析，通过分析巩固对Ethernet II 封包、ARP 分组及IP、ICMP 数据包的认识。

二、 实验内容和要求

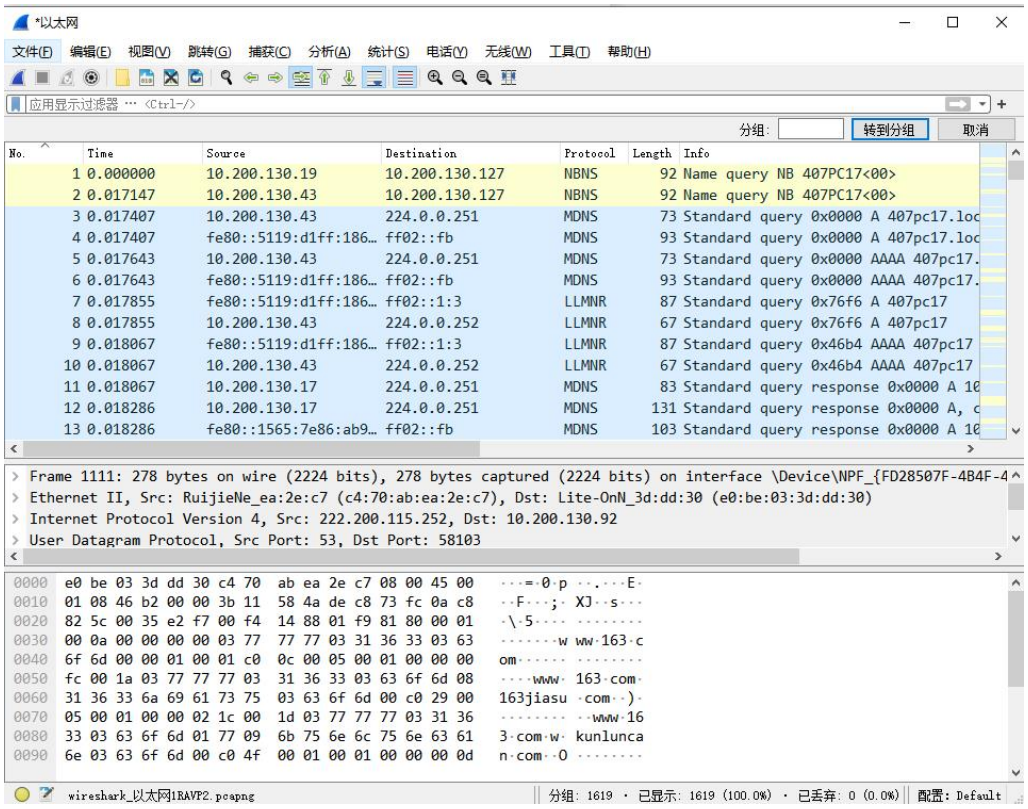
1) 学习协议分析工具 Wireshark 的基本使用方法；
2) 对抓到的任一个 IP 包，分析其 IP 包的起始地址与终止地址，以及对应的 MAC 帧的起始地址与终止地址，TTL 的值、协议字段内容，并分析其意义。
3) 利用 Wireshark 监听 ICMP 包，分析 ping 程序和 tracert 程序的主要功能。对抓到的任一个 ICMP 包，分析其 MAC 帧、IP 包、ICMP 包间的相互关系。
4) 利用 Wireshark 监听 arp 包，分析 arp 请求包与应答包的内容。

三、 实验结果 （截图和说明）

3.1 使用 WireShark 进行网络抓包

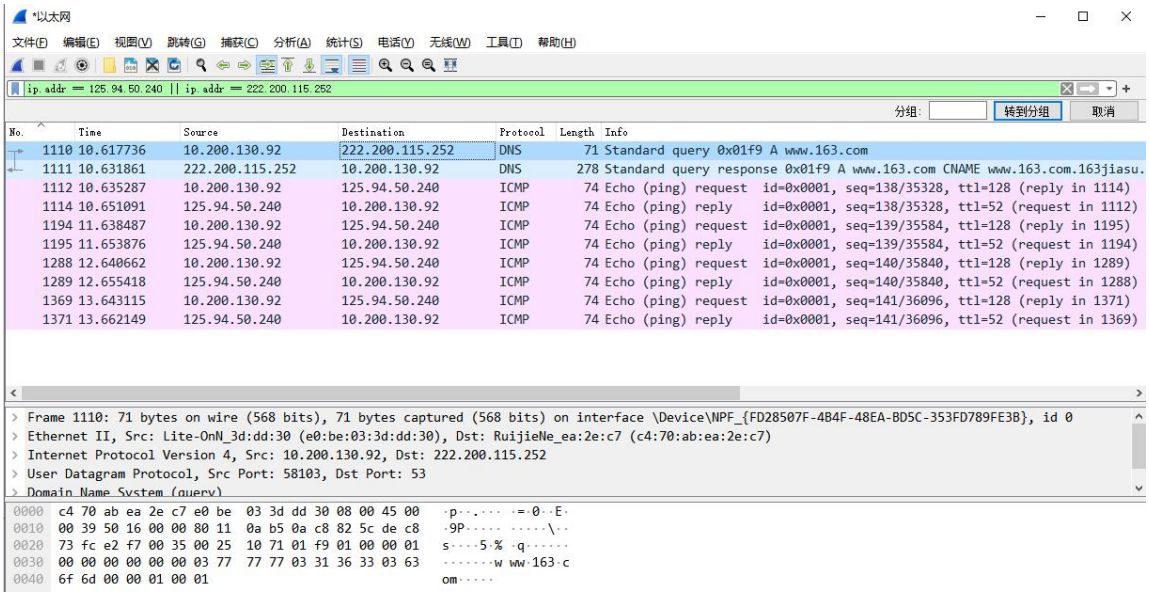
3.1.1 对 163 网站进行 ping 操作

3.1.2 ping 163 网站的同时使用 WireShark 抓包结果



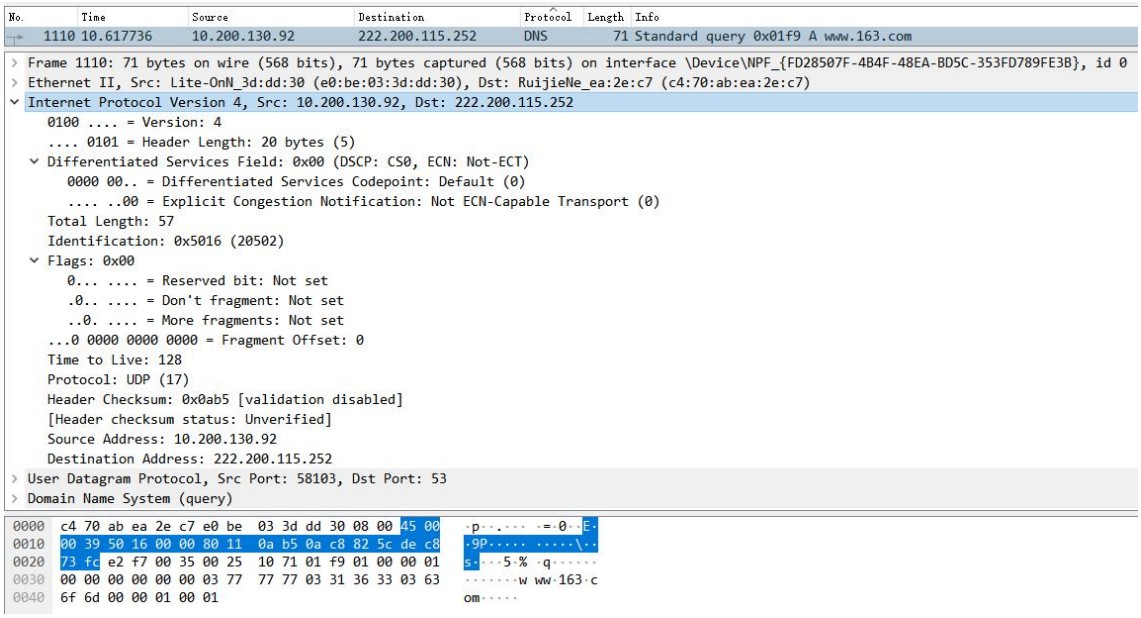
如图为 ping 过程中使用软件抓到的所有包。

3.1.3 使用条件进行过滤



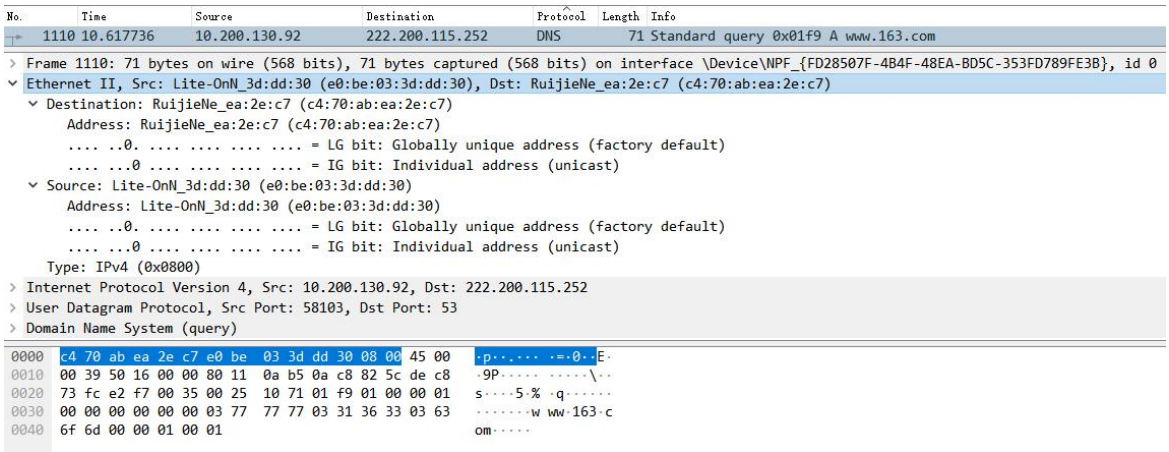
在刚才使用的 ping 命令中主要使用到了两种数据包：DNS、ICMP。通过“ip.addr == 125.94.50.240 || ip.addr == 222.200.115.252”条件进行过滤，可以看到 ping 命令产生的 2 个 DNS 数据包和 8 个 ICMP 数据包。其中 125.94.50.240 为 163 网站的 IP 地址，222.200.115.252 为广工的 DNS 服务器的 IP 地址。

3.2 对抓到的 IP 包进行分析



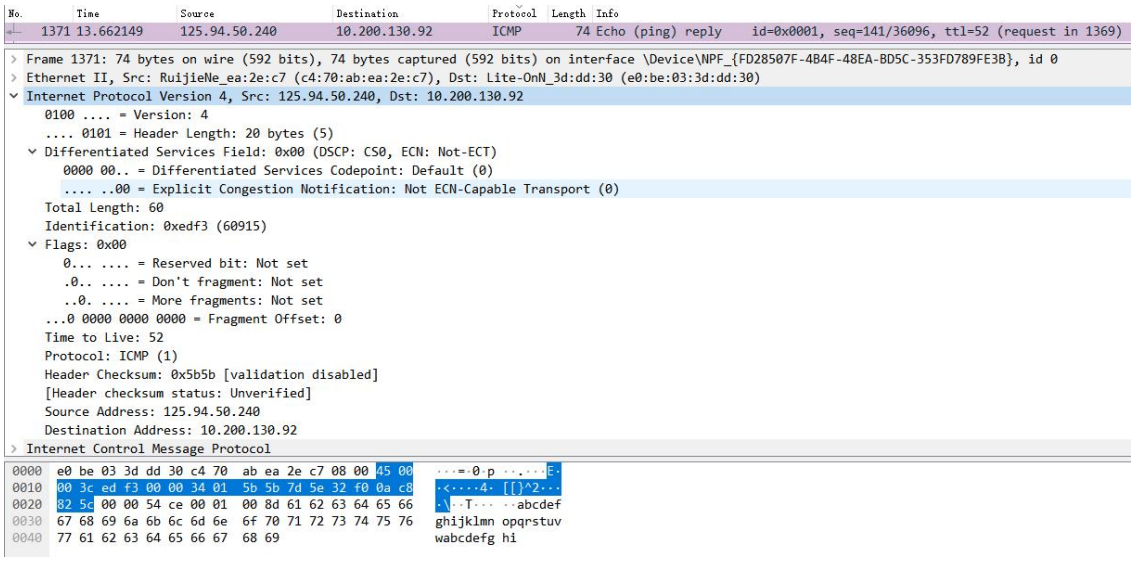
如图，对抓到的包进行分析，其中选中的部分为 IP 数据报。可见其起始地址为 10.200.130.92，目的地址为 222.200.115.252。TTL 值为 128。IP 协议版本为

4。协议字段内容为 17，即表示使用 UDP 协议。此外还可以见到其 DF 位、MF 位、片偏移字段均为 0，首部检验和为 0x0ab5 等。



如图，对抓到的包进行分析，其中选中的部分为以太网 MAC 帧的内容。可见其 MAC 起始地址为 e0:be:03:3d:dd:30，目的地址为 c4:70:ab:ea:2e:c7。

3.3 对抓到的 ICMP 包进行分析



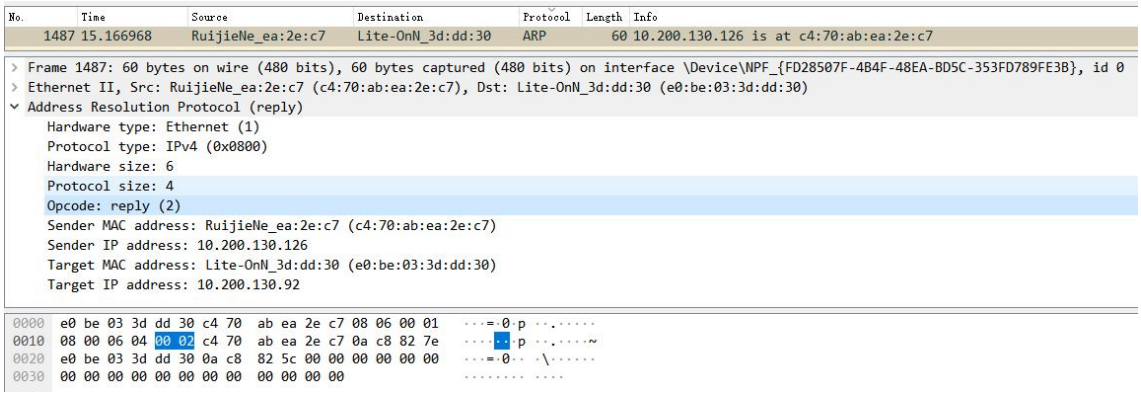
如图所示，起始地址为 125.94.50.240，目的地址为 10.200.130.92。TTL 值为 52。IP 协议版本为 4，协议字段内容为 1，表示使用 ICMP 协议。MAC 帧的起始地址为 c4:70:ab:ea:2e:c7，目的地址为 e0:be:03:3d:dd:30。

回答问题：ping 命令主要用于测试网络是否连通，目的 IP 是否可以访问。Tracert 命令主要用于跟踪路由通路，记录通过的路由及与目的地址之间的跳数。

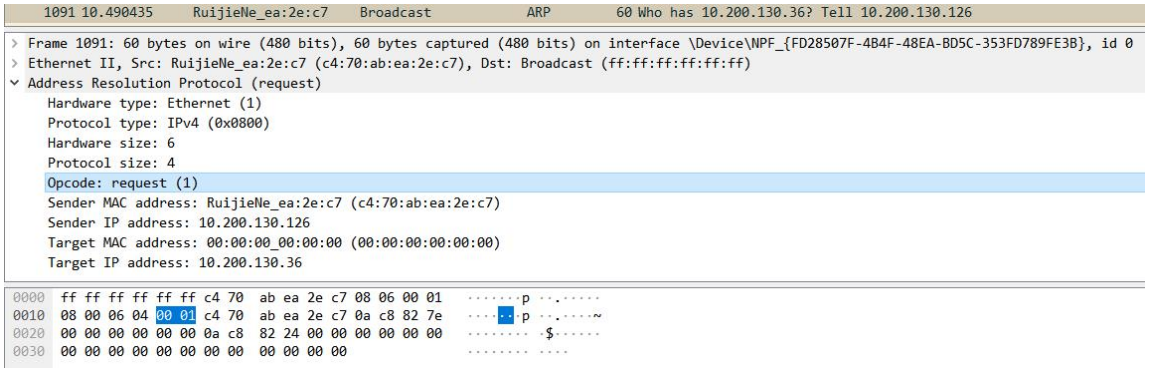
报文首先根据协议字段 1（即 ICMP 协议）封装成 ICMP 报文后，交付给网

络层，然后再根据 IPv4 协议封装成 IP 数据报，最后向下交付给数据链路层封装成为 MAC 帧。所以在抓取到的包中可以同时看到 MAC 帧的地址和 IP 层的地址，其中 MAC 地址位于较前处，作为 MAC 帧的一部分存在。

3.4 对抓到的 ARP 包进行分析



如图所示，对抓到的 ARP 包进行分析，其 OP 字段的值为 2（见图中选中部分），表示这个 ARP 报文为应答报文。是主机 10.200.130.126（c4:70:ab:ea:2e:c7）收到请求，把自己的 MAC 地址发回给发起请求的主机 10.200.130.92（e0:be:03:3d:dd:30）。



如图所示，对抓到的 ARP 包进行分析，其 OP 字段的值为 1（见图中选中部分），表示这个 ARP 报文为请求报文。是主机 10.200.130.126（c4:70:ab:ea:2e:c7）向局域网发起广播，向其他主机询问主机 10.200.130.26 的 MAC 地址。

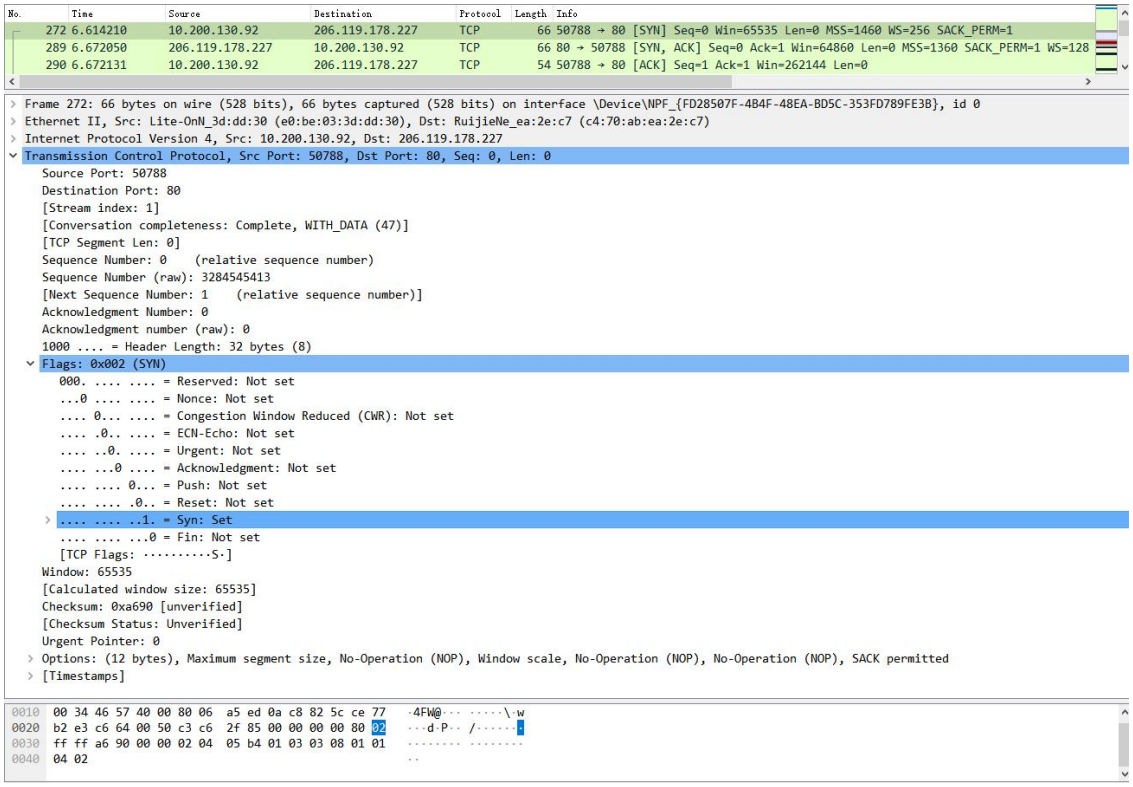
四、 思考题

1）在学校机房做实验的同学，尝试抓一下目标 IP 地址是隔壁设备的 TCP 数据包，能抓到吗？为什么？

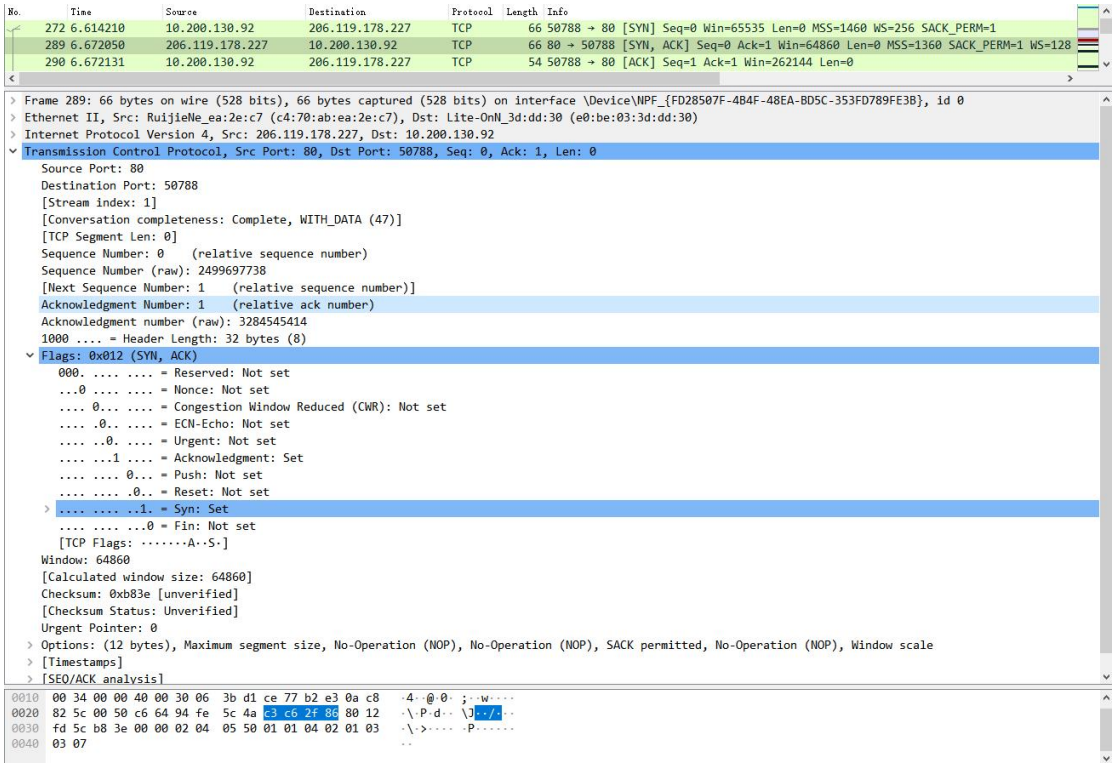
答：不能抓到邻机设备的数据报。因为两台主机虽然在同一个局域网中，但主机的 IP 地址以及 MAC 地址都是不同的。数据包只会送到其对应的地址，如果数据包的目的地不是本机本网段的地址，网卡将不会接收。并且 Wireshark 只能抓本机网卡的包，所以不能抓到隔壁主机的数据包。

2）不在学校机房做本实验的同学，有条件的可以利用自己家庭的路由器组建一个小的局域网，包括台式机、笔记本、手机等，先获取各个设备的局域网物理地址和 IP 地址，互相 Ping 测试连通性。再做思考题第一题。

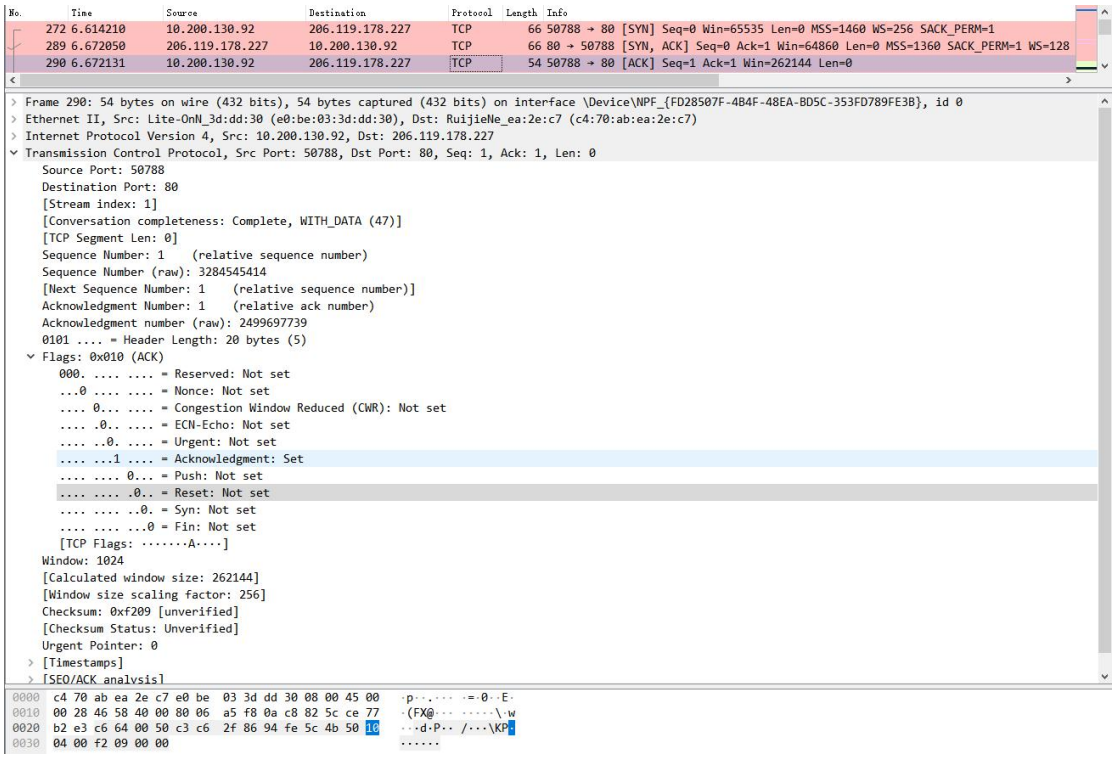
3）利用 Wireshark 监听 HTTP 的访问过程，找出 TCP 建立连接的三次握手的相关 IP 数据报文，并解析 TCP 建立连接的三次握手的过程，及 IP 数据报文的变化情况。



如上图所示为第一次握手的报文，该报文中 SYN=1，ACK=0。



如上图所示为第二次握手的报文，该报文中 SYN=1，ACK=1。



如上图所示为第三次握手的报文，该报文中 SYN=0，ACK=1。

广东工业大学

实验题目 交换机的基本配置

一、实验目的

了解交换机网络硬件设备，初步掌握交换机的常用配置。

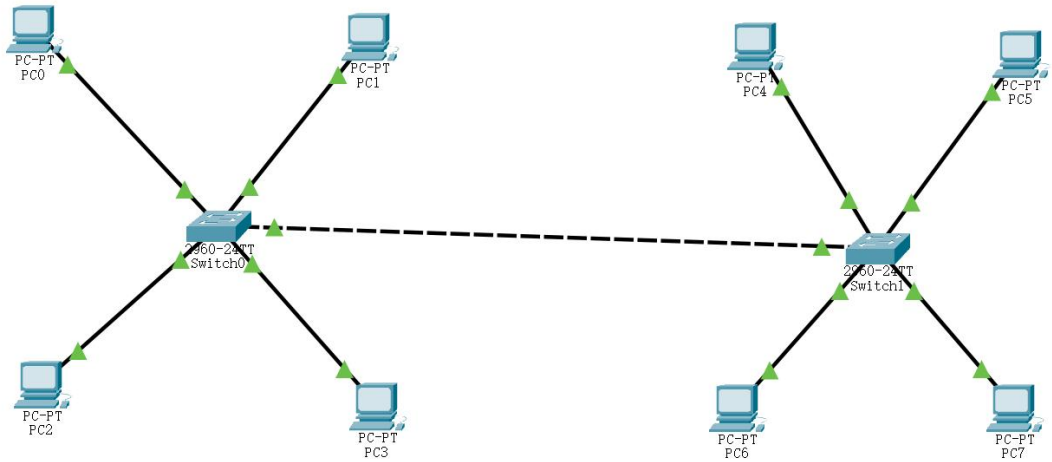
二、实验要求

熟悉 Cisco IOS 命令，理解交换机的工作原理，通过 Packet Tracer 软件能对交换机进行仿真配置，完成 Vlan。可根据情况进一步完成 VTP，STP 等配置并测试。

三、实验结果 （截图和说明）

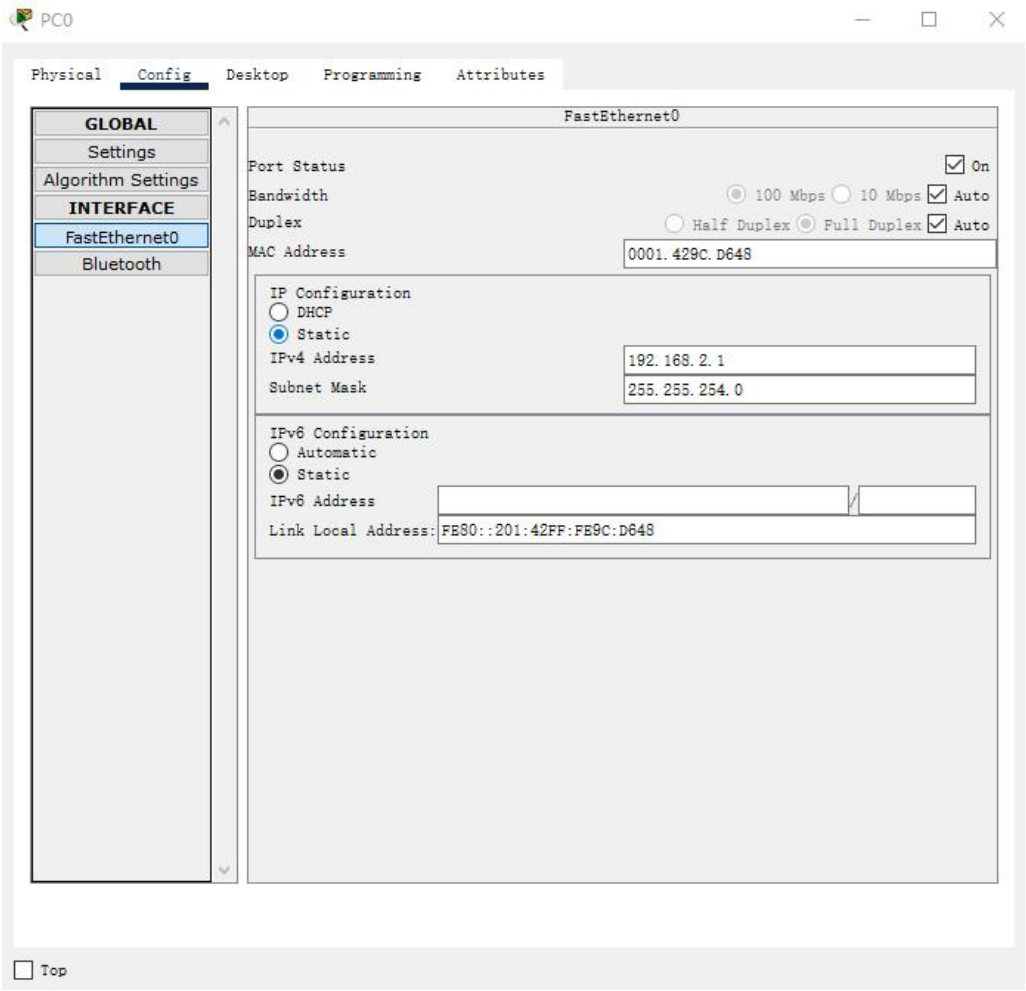
3.1 网络拓扑图

实验所配置的交换机网络拓扑图如下所示。



3.2 主机设置

将各主机的 IP 获取方式设置为静态，配置它们的 IP 地址与子网掩码。



如上图为配置主机 0 时的界面，其余主机的配置界面略去不表。

最终各主机配置如下：

PC0: 192.168.2.1　　255.255.254.0

PC1: 192.168.2.2　　255.255.254.0

PC4: 192.168.2.3　　255.255.254.0

PC5: 192.168.2.4　　255.255.254.0

PC2: 192.168.3.1　　255.255.254.0

PC3: 192.168.3.2　　255.255.254.0

PC6: 192.168.3.3　　255.255.254.0

PC7: 192.168.3.4　　255.255.254.0

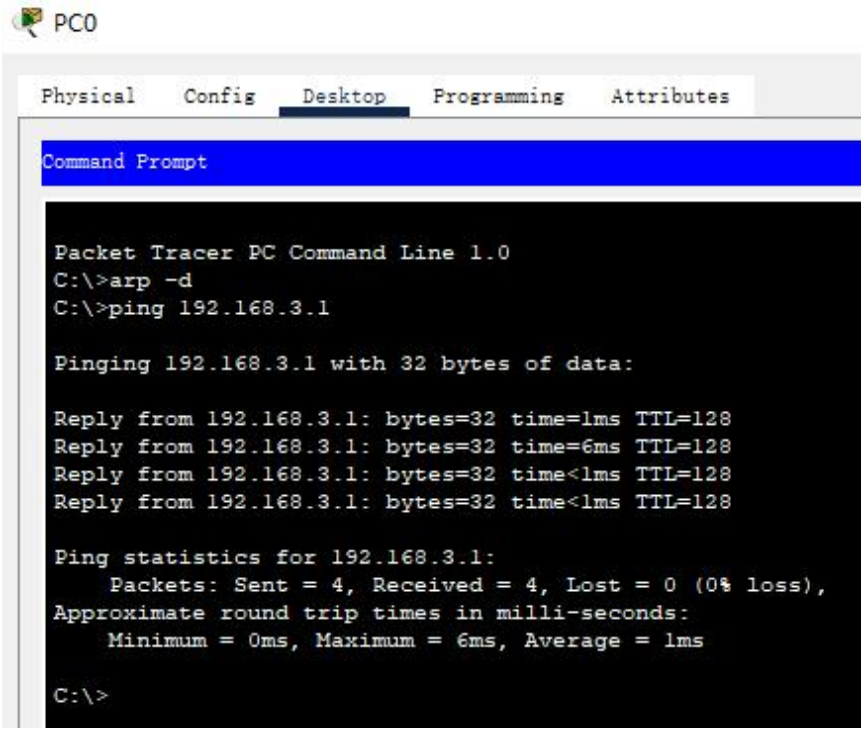
各主机均不设置缺省网关。

3.3 用 PC0 和 PC2 做子网划分实验

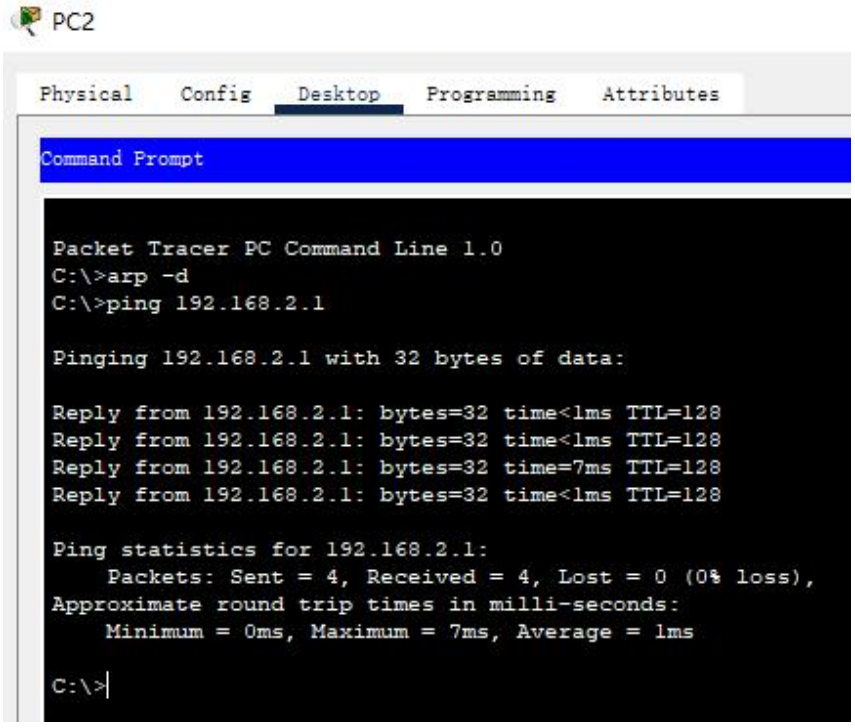
3.3.1 测试 1

1）用 arp -d 命令清除 PC0 和 PC2 两台主机上的 ARP 表，然后在 PC0 与 PC2 上分别用 ping 命令与对方通信，观察并记录结果，并分析原因。

在 PC0 上 ping PC2 的结果如下图所示。



在 PC2 上 ping PC0 的结果如下图所示。



因为将 PC0 与 PC2 各自的 IP 地址与子网掩码进行 AND 运算后的结果相同，即它们在同一网段，所以它们能够互相 ping 通。

2）在两台 PC 上分别执行 arp -a 命令，观察并记录结果，并分析原因。

```
C:\>arp -a
  Internet Address      Physical Address      Type
  192.168.3.1           0007.ec76.2c88        dynamic
```

如上图所示为在 PC0 上执行 arp -a 命令后的结果，可见 ARP 表中显示了 PC2 的 IP 地址和它的 MAC 地址。

```
C:\>arp -a
  Internet Address      Physical Address      Type
  192.168.2.1           0001.429c.d648        dynamic
```

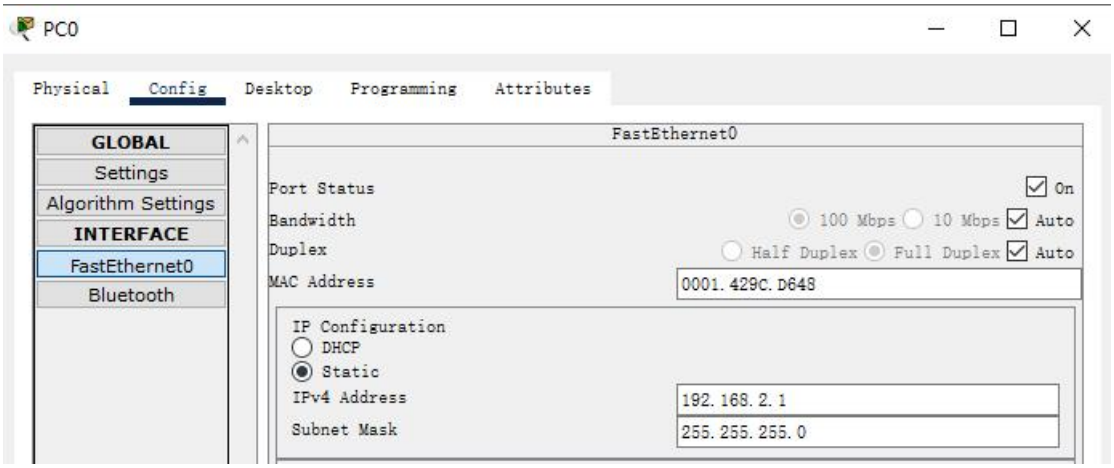
如上图所示为在 PC2 上执行 arp -a 命令后的结果，可见 ARP 表中显示了 PC0 的 IP 地址和它的 MAC 地址。

3）分析 PC0 和 PC1 在不在同一网段？如何判断？同一网段是什么情况？不同网段又是什么情况？按此思路去分析。

答：PC0 和 PC1 在同一网段。通过它们的 PC 地址与子网掩码进行 AND 运算后的结果可以判断。在同一网段中可以互相 ping 通，由于只设置了交换机，没有设置路由器，故不在同一网段中时不能 ping 通。

3.3.2 测试 2

1）将 PC0 的子网掩码改为：255.255.255.0，其他设置保持不变。



2）在两台 PC 上分别执行 arp -d 命令清除两台主机上的 ARP 表。然后在 PC0 上"ping"PC2，观察并记录结果。

```
C:\>arp -d
C:\>ping 192.168.3.1

Pinging 192.168.3.1 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.3.1:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

如上图为在 PC0 上 ping PC2 的结果，显示无法 ping 通。

3）在两台 PC 上分别执行 arp -a 命令，观察并记录结果，并分析原因。

```
C:\>arp -d
C:\>ping 192.168.3.1

Pinging 192.168.3.1 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.3.1:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>arp -a
No ARP Entries Found
C:\>
```

如上图所示为在 PC0 上执行 arp -a 命令后的结果，可见 ARP 表中无内容。

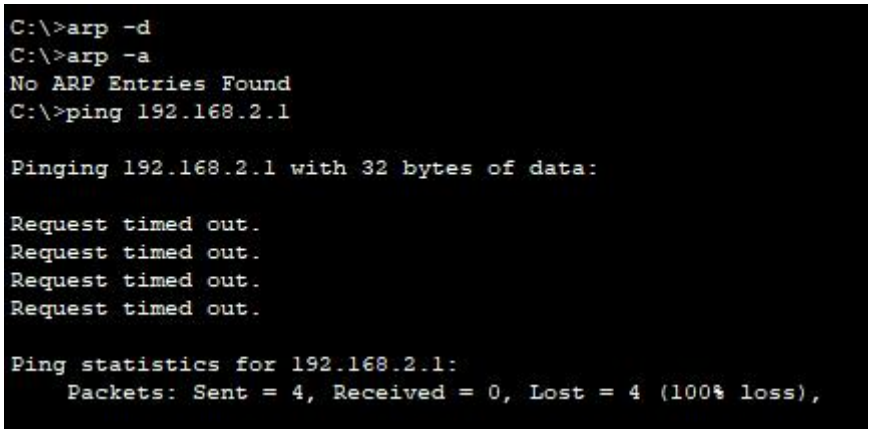
```
C:\>arp -a
No ARP Entries Found
```

如上图所示为在 PC2 上执行 arp -a 命令后的结果，可见 ARP 表中也无内容。

出现该结果的原因为：PC0 将目标设备的 IP 地址（192.168.3.1）和自己的子网掩码（255.255.255.0）进行 AND 运算得 192.168.3.0，和自己不在同一网段（PC0 所在网段为：192.168.2.0），则 PC0 必须将该 IP 分组首先发向缺省网关，无法直接 ping 通，故 ARP 表也就没有更新，显示无内容。

3.3.3 测试 3

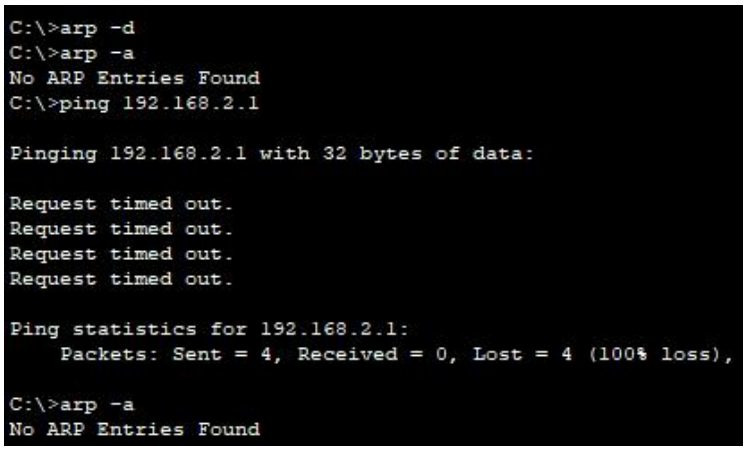
1）按照测试 2 的配置，接着在 PC2 上"ping"PC0，观察并记录结果，并分析原因。



如上图为在 PC2 上 ping PC0 的结果，显示无法 ping 通。

出现该结果的原因是：PC2 将目标设备的 IP 地址（192.168.2.1）和自己的子网掩码（255.255.254.0）进行 AND 运算后得到 192.168.2.0，发现目标主机与自己位于同一网段。因此，PC2 尝试通过 ARP 协议获得 PC0 的 MAC 地址，并可以正确地在广播中向 PC0 发送 ARP Request 报文。但由于 PC0 不能向 PC2 正确地发回 ARP Reply 报文（原因参见测试 2 中分析），故 PC2 上显示 ping 的结果为"请求超时"。

2）在 PC2 上执行 arp -a 命令，观察并记录结果，并分析原因。



如上图所示为在 PC2 上执行 arp -a 命令后的结果，可见 ARP 表中仍然无内容。

出现该结果的原因是：PC2 向本网段中发送 ARP Request 报文后，因为 PC0 不能正确发回 ARP Reply 报文，故 PC2 无法通过 ARP 协议获得 PC0 的 MAC 地址，也就没有更新其 ARP 表。

3.4 设置 VLAN 实验

3.4.0 配置 VLAN

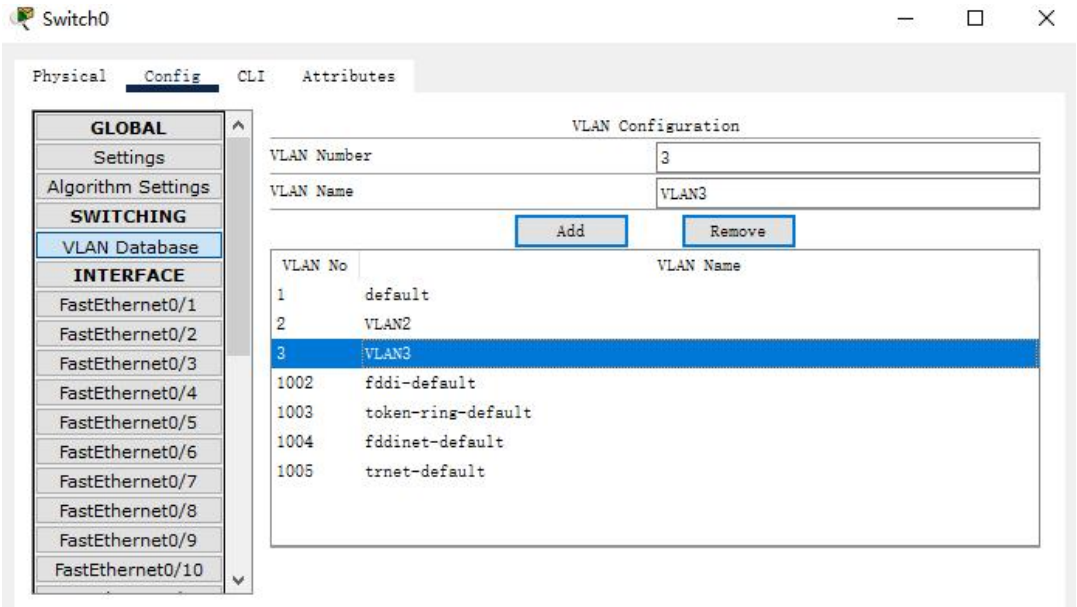
在两台交换机上分别添加 2、3 号的 VLAN：命名为 VLAN2、VLAN3。

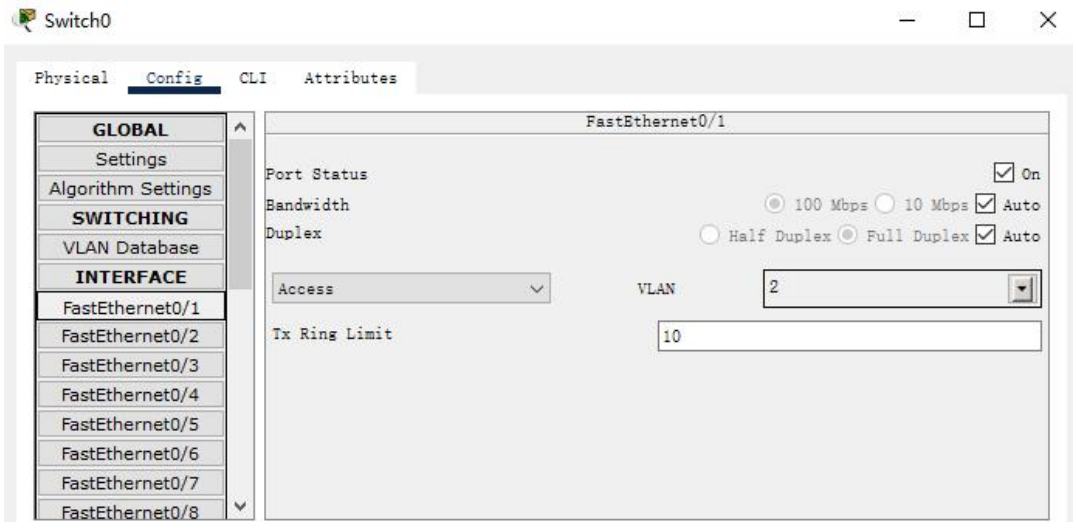
设置交换机连接各主机的接口，分别设置其 VLAN 号如下：

上面的 PC0，PC1，PC4，PC5 都属于 VLAN 2

下面的 PC2，PC3，PC6，PC7 都属于 VLAN 3

如下图所示为配置交换机 0 时的部分截图。



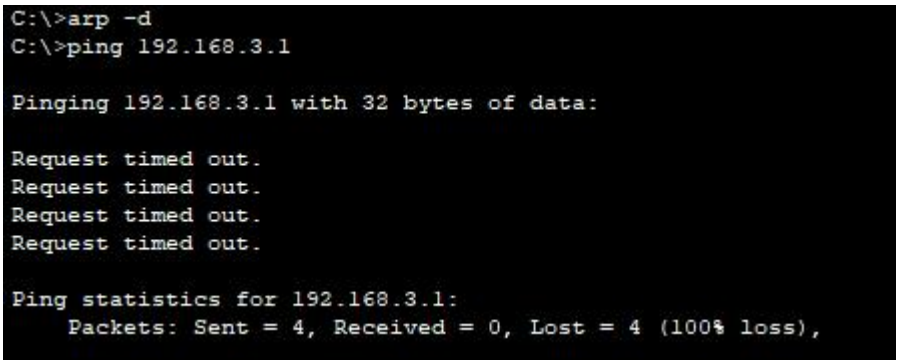


3.4.1 测试 1

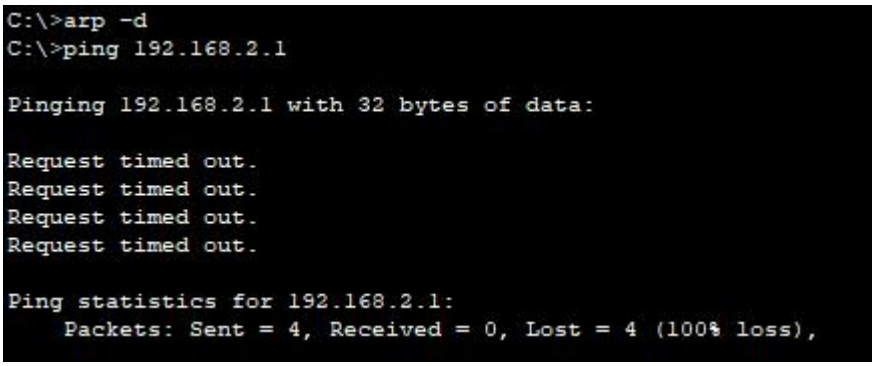
PC0: 192.168.2.1　　255.255.254.0　VLAN 2

PC2: 192.168.3.1　　255.255.254.0　VLAN 3

1）用 arp -d 命令清除 PC0 和 PC2 两台主机上的 ARP 表，然后在 PC0 与 PC2 上分别用 ping 命令与对方通信，观察并记录结果，并分析原因。



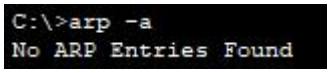
如上图所示，为在 PC0 上 ping PC2 的结果，显示无法 ping 通。



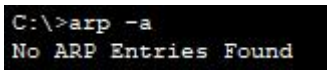
如上图所示为，在 PC2 上 ping PC0 的结果，也显示无法 ping 通。

出现该结果的原因为：PC2 将通信目标 PC0 的 IP 地址与自己的子网掩码进行 AND 运算后，发现目标主机与自己均位于同一网段（192.168.2.0），因此将数据包发往本网络。但是由于交换机只向相同的 VLAN 接口发送数据包，PC0 接口不属于 PC2 接口的 VLAN，故数据包在到达交换机后，实际并未发往 PC0，相应地，也就未能获得对方的 MAC 地址。故 PC2 无法 ping 通 PC0。PC0 无法 ping 通 PC2 的原因也与此同理。

2）在两台 PC 上分别执行 arp -a 命令，观察并记录结果，并分析原因。



如上图所示为在 PC0 上执行 arp -a 命令后的结果，可见 ARP 表中无内容。



如上图所示为在 PC2 上执行 arp -a 命令后的结果，可见 ARP 表中也无内容。

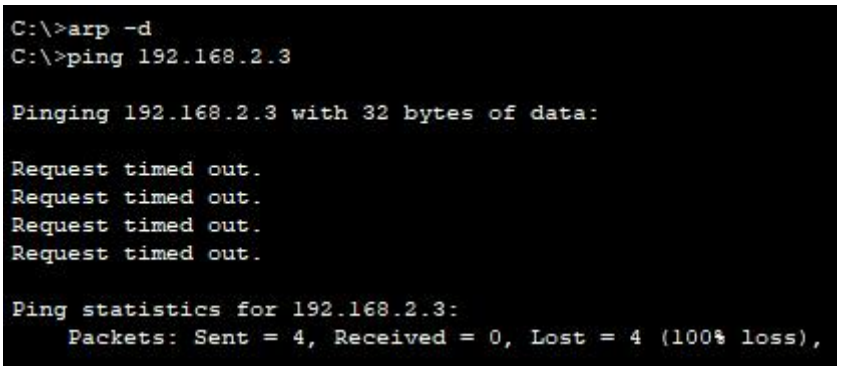
出现该结果的原因为：PC2 将通信目标 PC0 的 IP 地址与自己的子网掩码进行 AND 运算后，发现目标主机与自己均位于同一网段（192.168.2.0），因此将数据包发往本网络。但是由于交换机只向相同的 VLAN 接口发送数据包，PC0 接口不属于 PC2 接口的 VLAN，故数据包在到达交换机后，实际并未发往 PC0，相应地，也就未能获得对方的 MAC 地址。故 PC2 的 ARP 表无法更新，仍未无内容状态。

3.4.2 测试 2

PC0: 192.168.2.1　　255.255.254.0　VLAN 2

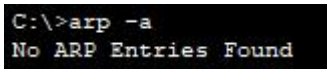
PC4: 192.168.2.3　　255.255.254.0　VLAN 2

1）在两台 PC 上分别执行 arp -d 命令清除两台主机上的 ARP 表。然后在 PC0 上 "ping" PC4，观察并记录结果。

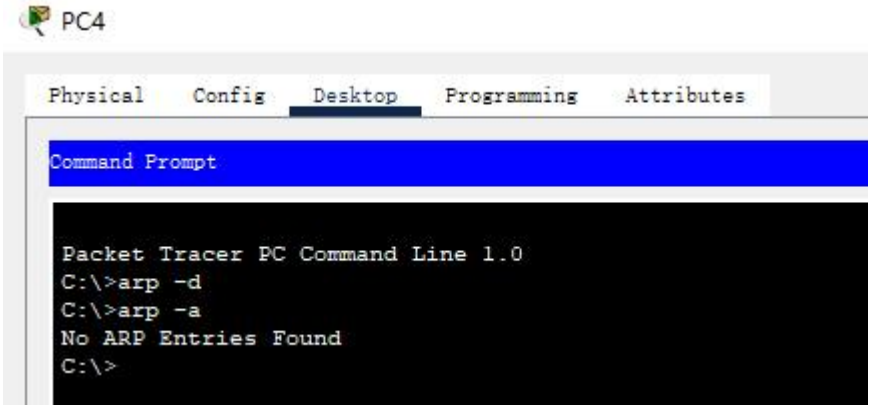


如上图所示，为在 PC0 上 ping PC4 的结果，显示无法 ping 通。

2）在两台 PC 上分别执行 arp -a 命令，观察并记录结果，并分析原因。



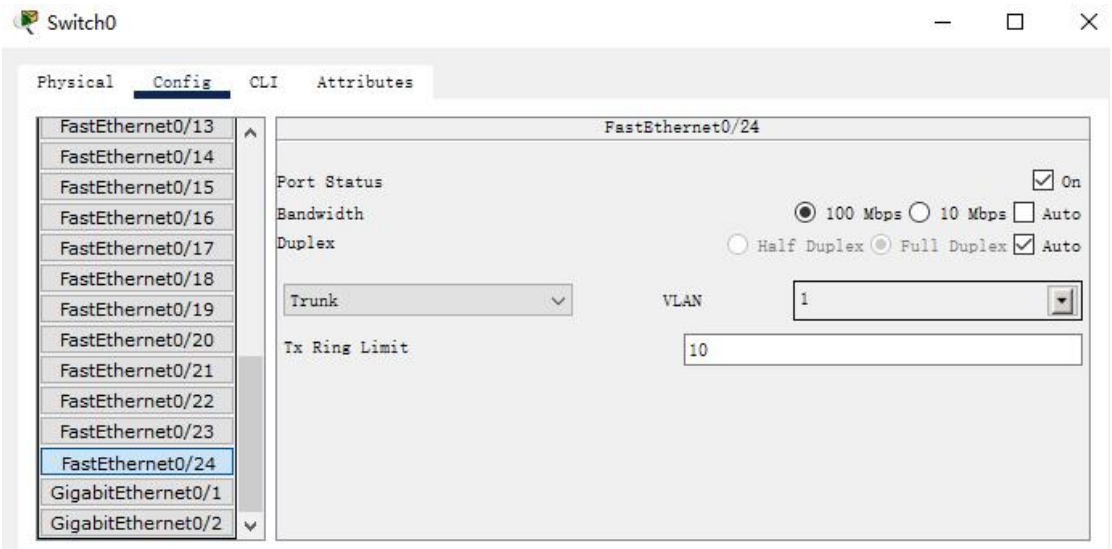
如上图所示为在 PC0 上执行 arp -a 命令后的结果，可见 ARP 表中无内容。



如上图所示为在 PC4 上执行 arp -a 命令后的结果，可见 ARP 表中无内容。

出现该结果的原因为：PC0 将目标设备 PC4 的 IP 地址（192.168.2.3）和自己的子网掩码（255.255.254.0）进行 AND 运算后得 192.168.2.0，和自己在同一网段，则 PC0 将该 IP 分组发向本网段。但由于两台交换机之间的连接接口与 PC0 处于不同的 VLAN，故第二个交换机收不到任何数据包，也就无法发往 PC4。所以无法 ping 通，也无法获取其 MAC 地址来更新 ARP 表，ARP 表仍为空。

改进：设置两台交换机直接相连的接口为 Trunk，如下所示。



此时再次用 PC0 ping PC4 即可 ping 通，但 ping 不通所有其它 VLAN 号的主机。

```
C:\>ping 192.168.2.3

Pinging 192.168.2.3 with 32 bytes of data:

Reply from 192.168.2.3: bytes=32 time<1ms TTL=128
Reply from 192.168.2.3: bytes=32 time<1ms TTL=128
Reply from 192.168.2.3: bytes=32 time<1ms TTL=128
Reply from 192.168.2.3: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.2.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

四、实验思考题

1．简述实验过程中出现的问题及解决方法。

2．子网掩码与 VLAN 都可以进行网络划分，二者的区别是什么？

答：子网掩码是为了合理安排 IP 地址资源而设立，而 VLAN 则是因方便网络管理的需要而设立。基于子网掩码实现的网络划分工作在网络层，需要与主机 IP 地址进行配合，来实现隔离不同网段之间通信的功能；而基于交换机的 VLAN 功能实现的网络划分工作在数据链路层，在交换机处直接将流量进行隔离。

3. 交叉线与直通线的区别是什么？

答：网线两头线序一致为直通线，网线两头线序不同为交叉线。直通线用于连接不同功能的设备，如计算机与交换机之间的连接；而交叉线则用于连接相同功能的设备，如交换机之间的直连。

4．（选做）课后练习，单台交换机上配置VLAN，实现交换机端口隔离。实验用到的拓扑图如图3.1所示，交换机的端口分配及IP地址分配如表3.1所示。

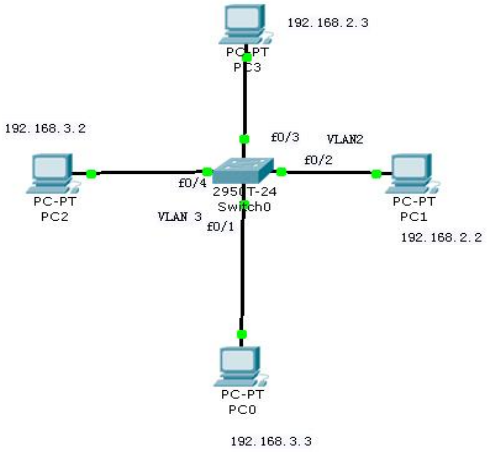


图 3.1 VLAN 基础配置拓扑图

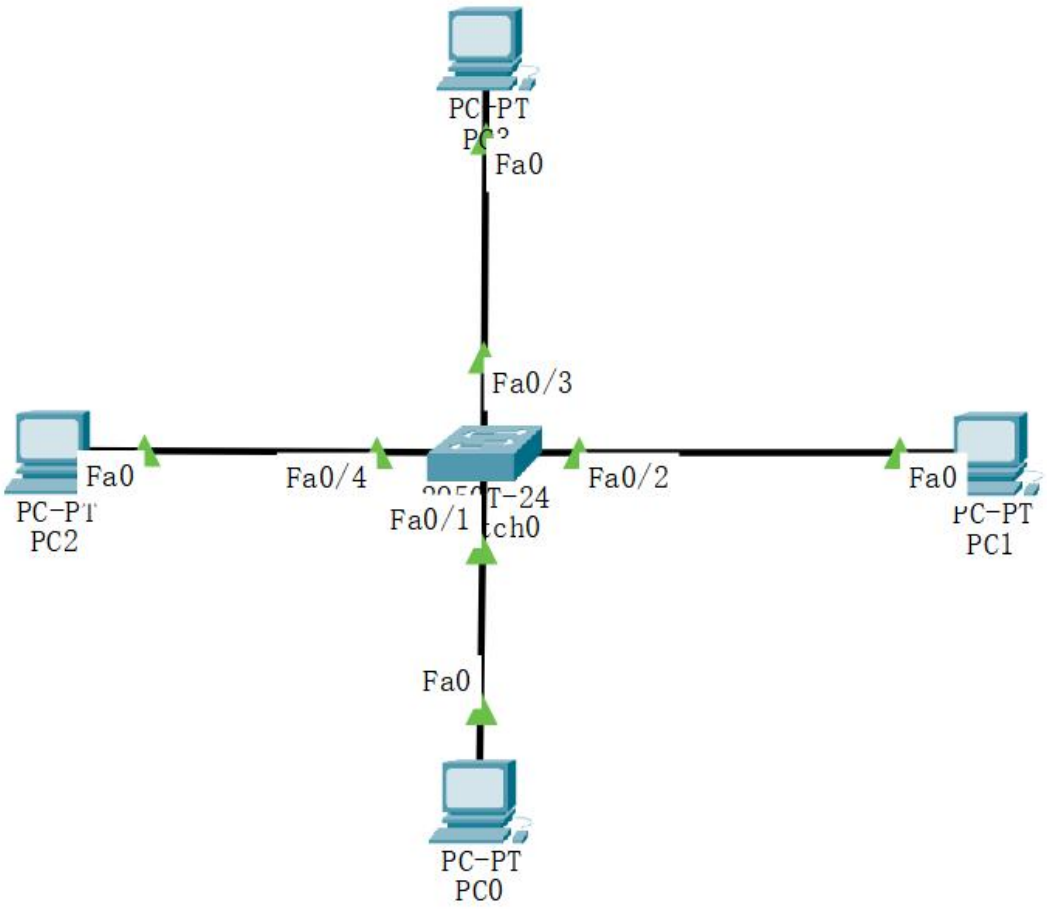
表 3.1 IP 地址分配表

设备名称	接口	IP 地址	子网掩码	默认网关
F0/1	VLAN 3			无
F0/2	VLAN 2			无
F0/3	VLAN 2			无
F0/4	VLAN 3			无
PC0	NIC	192.168.3.3	255.255.255.0	无
PC1	NIC	192.168.2.2	255.255.255.0	无
PC2	NIC	192.168.3.2	255.255.255.0	无
PC3	NIC	192.168.2.3	255.255.255.0	无

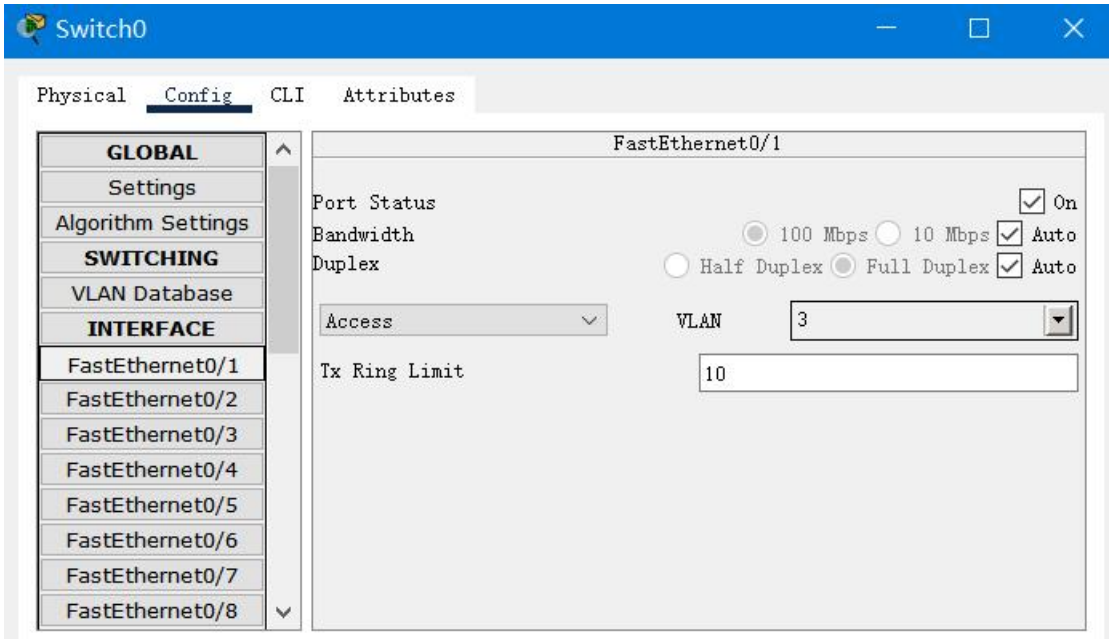
做到交换机端口隔离验证，PC0和PC2、PC1和PC3能互相ping通，其余则不行。

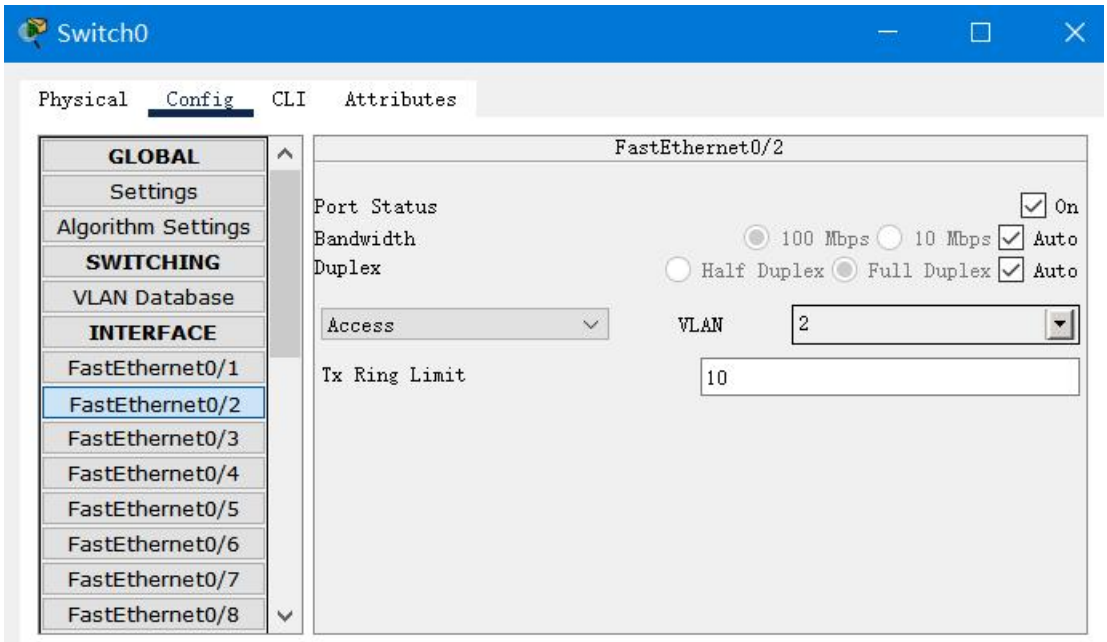
答：

网络拓扑复现如下图所示。

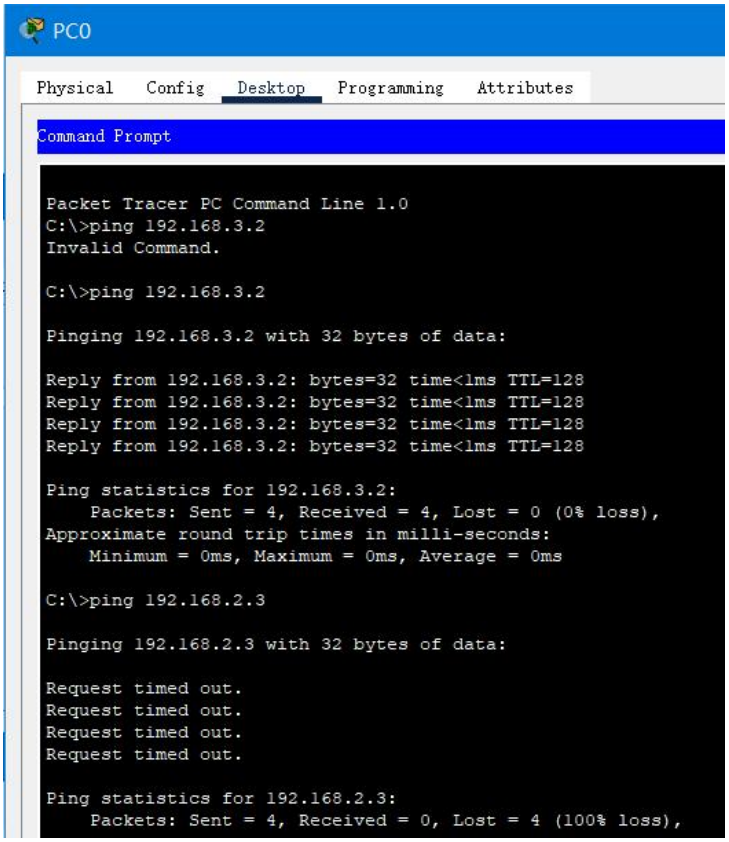


配置 VLAN 时的部分截图如下。

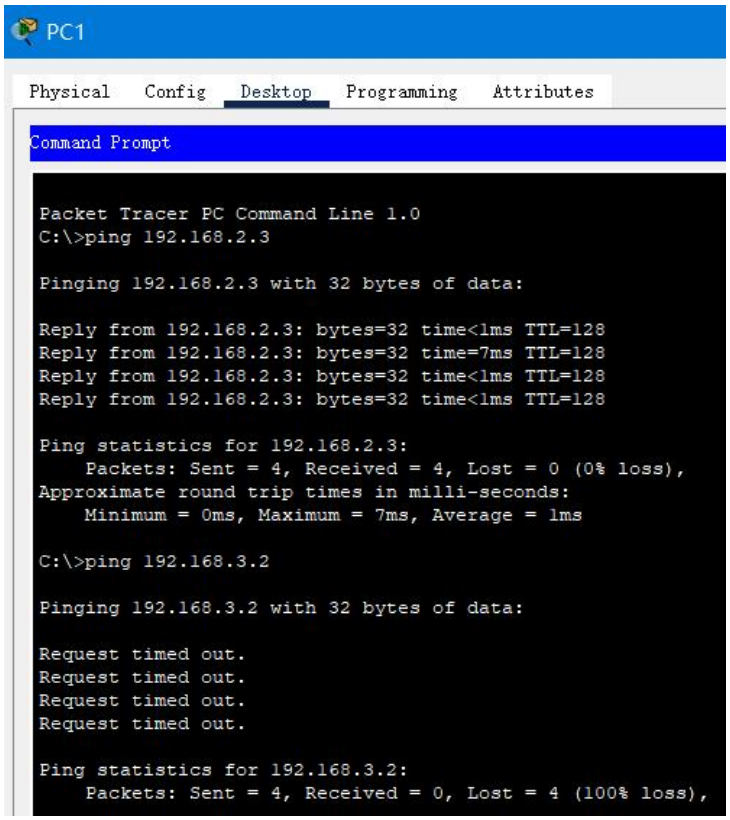




通过在单台交换机上配置 VLAN，实现了交换端口隔离，PC0 和 PC2、PC1 和 PC3 能互相 ping 通，其余则不行。下面通过 ping 命令验证配置结果。



如上图所示，PC0 能 ping 通 PC2，但无法 ping 通其他主机。



如上图所示，PC1 能 ping 通 PC3，但无法 ping 通其他主机。

广东工业大学

实验题目 路由器的基本配置

一、实验目的

了解路由器网络硬件设备，初步掌握路由器的常用配置。

二、实验工具

交换机，路由器，PC，Packet Tracer 软件等。

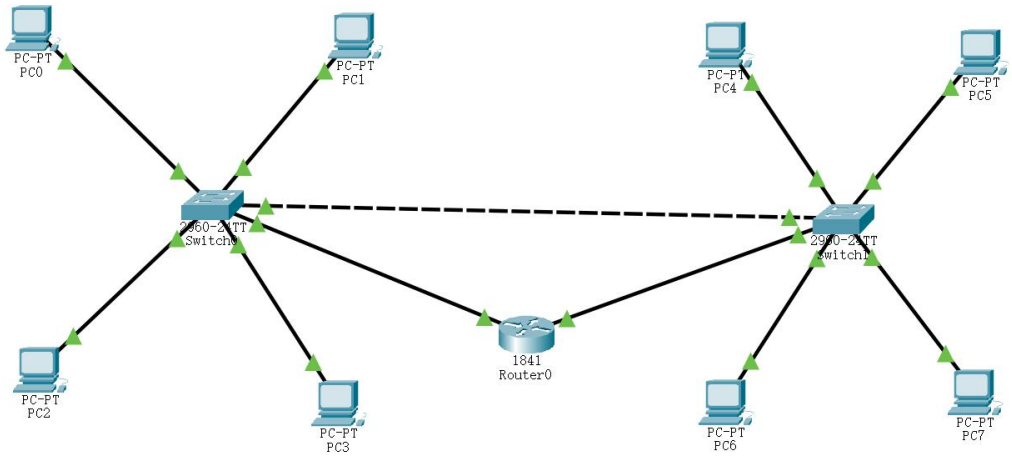
三、实验要求

熟悉Cisco IOS命令，理解路由器的工作原理，通过Packet Tracer软件能对路由器进行基本配置，也可进一步完成RIP配置并测试。

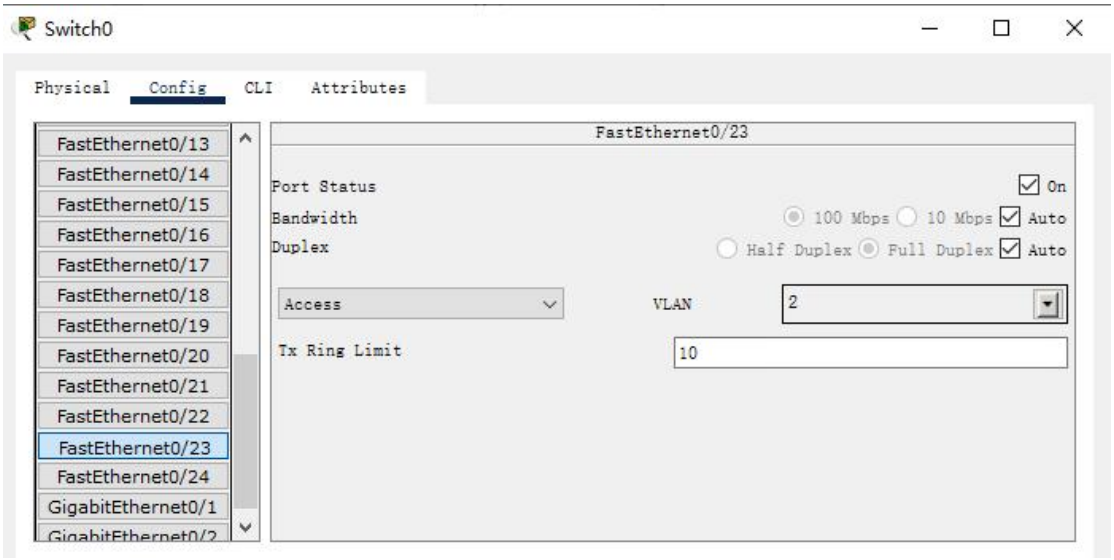
四、实验结果 （截图和说明）

4.1 交换机和路由器配置拓扑图

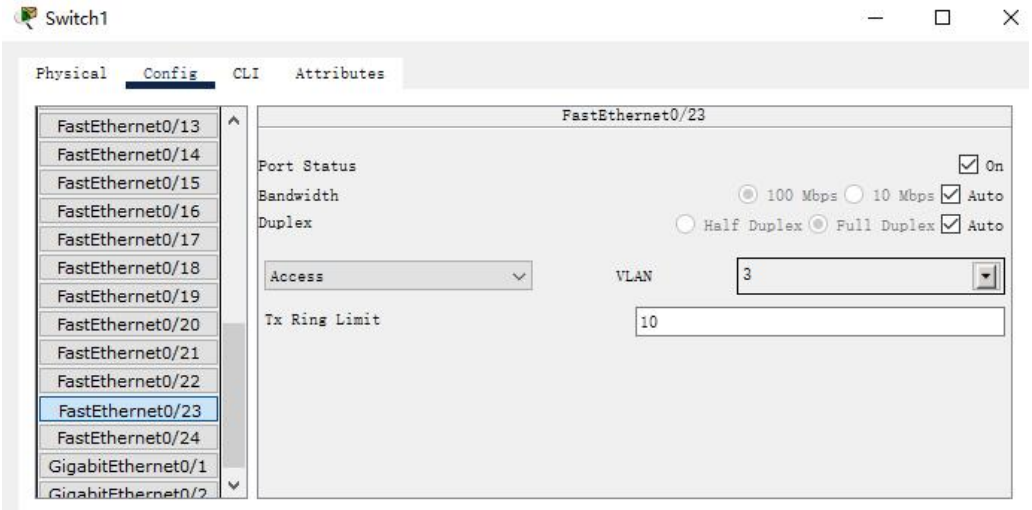
实验所配置的交换机和路由器网络拓扑图如下所示。



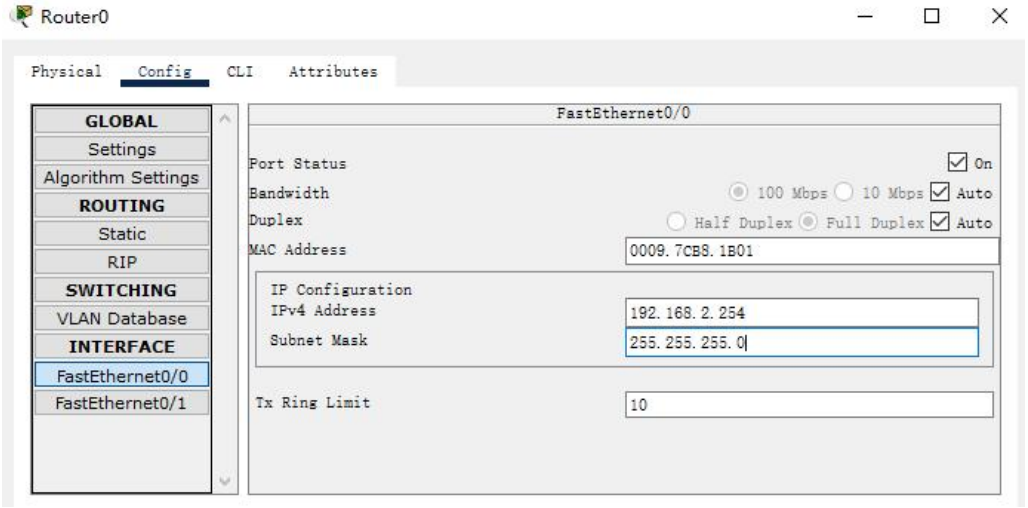
4.2 与路由器左边相连的交换机对应的端口的 VLAN 设置为 VLAN2



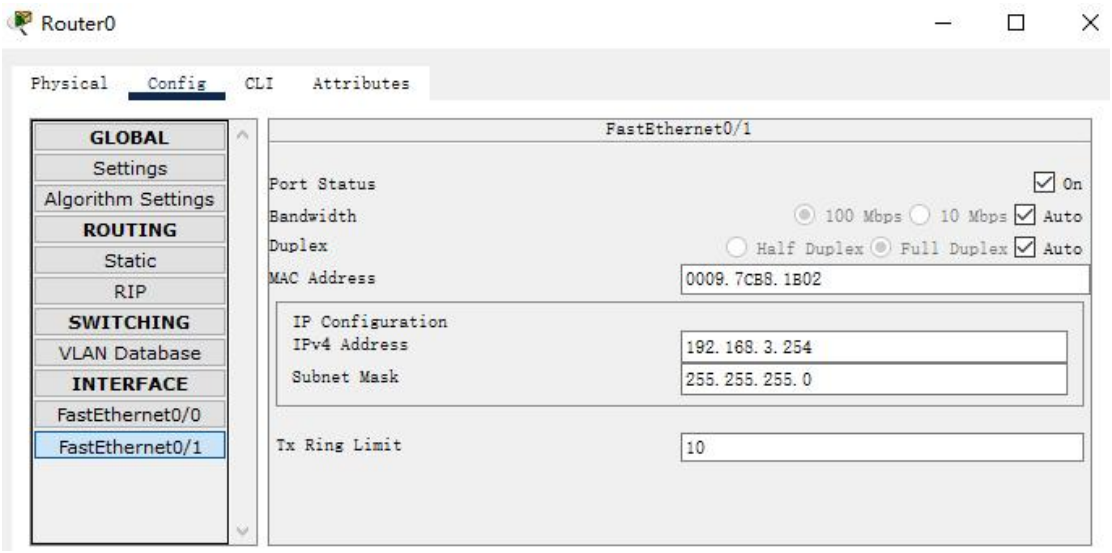
4.3 与路由器右边相连的交换机对应的端口的 VLAN 设置为 VLAN3



4.4 将路由器左边的连线端口的 IP 设置为与 VLAN2 有关的 192.168.2.254



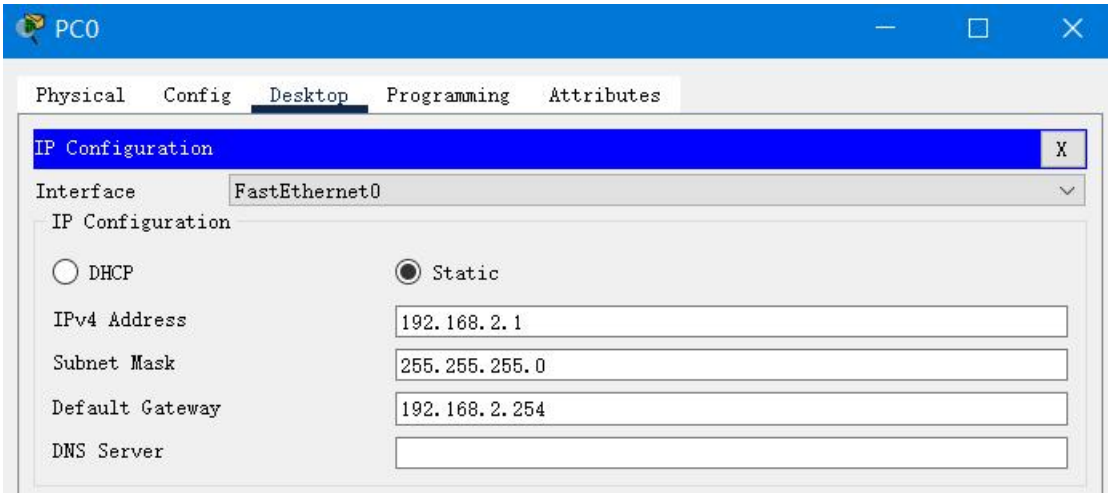
4.5 将路由器右边的连线端口的 IP 设置为与 VLAN3 有关的 192.168.3.254

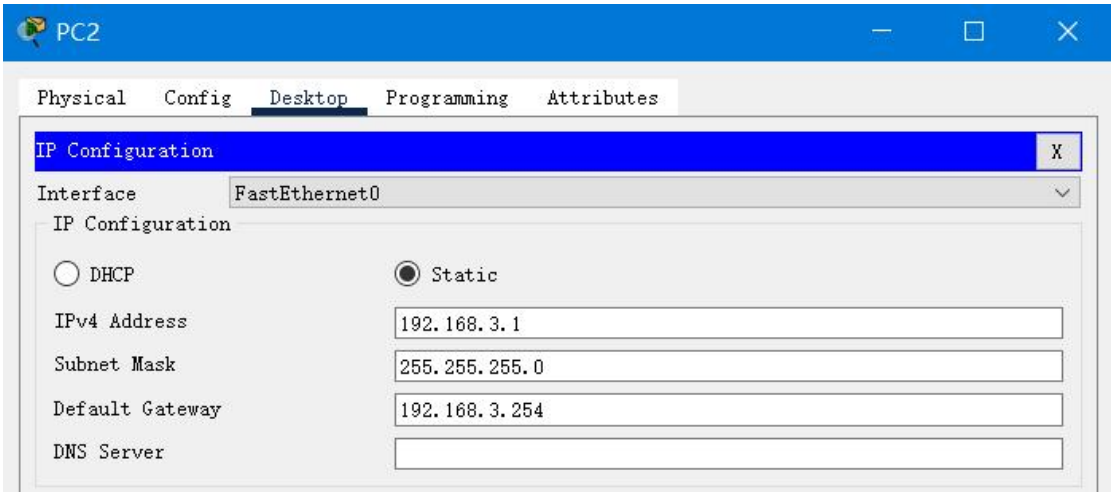


4.6 进行各主机的 IP 地址与默认网关配置

设备名称	IP	默认网关
PC0	192.168.2.1	192.168.2.254
PC1	192.168.2.2	192.168.2.254
PC2	192.168.3.1	192.168.3.254
PC3	192.168.3.2	192.168.3.254
PC4	192.168.2.3	192.168.2.254
PC5	192.168.2.4	192.168.2.254
PC6	192.168.3.3	192.168.3.254
PC7	192.168.3.4	192.168.3.254

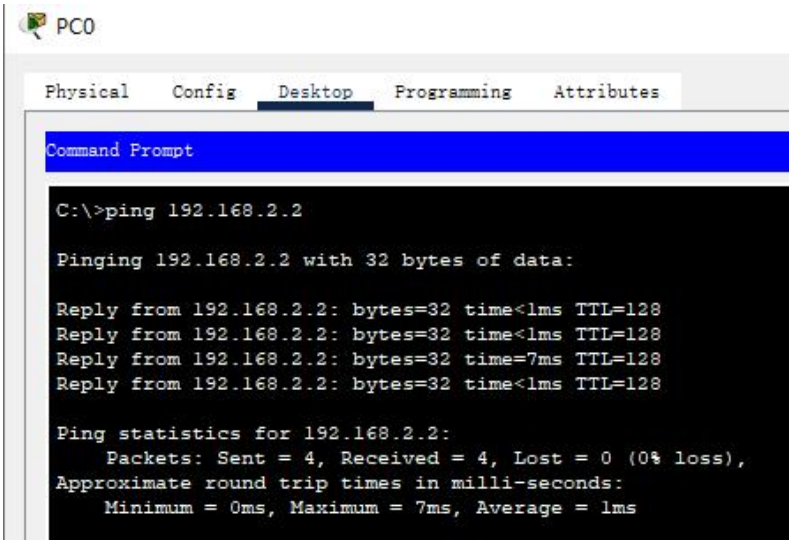
如下图所示为 PC0 与 PC2 的 IP 地址、子网掩码与默认网关配置截图，其余截图省略。



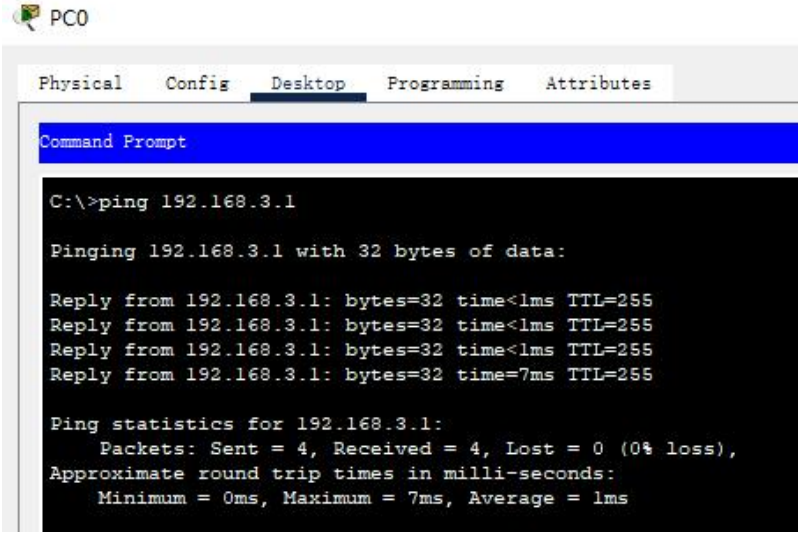


4.7 结果测试

如下图所示为 PC0　ping　PC1 的结果。



如下图所示为 PC0　ping　PC2 的结果。



如下图所示为 PC0　ping　PC3 的结果。

```
C:\>ping 192.168.3.2

Pinging 192.168.3.2 with 32 bytes of data:

Request timed out.
Reply from 192.168.3.2: bytes=32 time<1ms TTL=127
Reply from 192.168.3.2: bytes=32 time<1ms TTL=127
Reply from 192.168.3.2: bytes=32 time<1ms TTL=127

Ping statistics for 192.168.3.2:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

如下图所示为 PC0　ping　PC4 的结果。

```
C:\>ping 192.168.2.3

Pinging 192.168.2.3 with 32 bytes of data:

Reply from 192.168.2.3: bytes=32 time<1ms TTL=128
Reply from 192.168.2.3: bytes=32 time<1ms TTL=128
Reply from 192.168.2.3: bytes=32 time<1ms TTL=128
Reply from 192.168.2.3: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.2.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

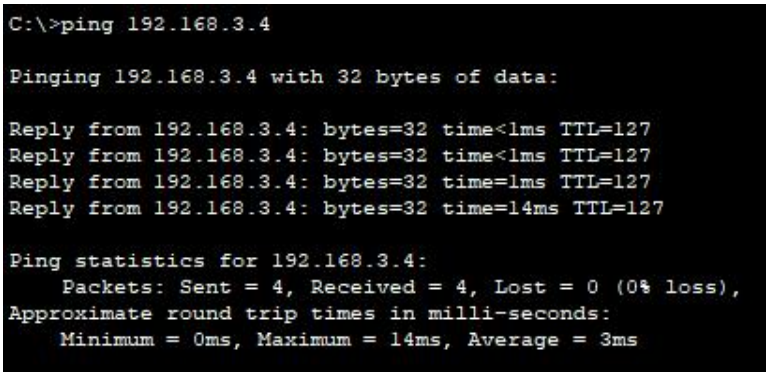
如下图所示为 PC0　ping　PC5 的结果。

```
C:\>ping 192.168.2.4

Pinging 192.168.2.4 with 32 bytes of data:

Reply from 192.168.2.4: bytes=32 time<1ms TTL=128
Reply from 192.168.2.4: bytes=32 time<1ms TTL=128
Reply from 192.168.2.4: bytes=32 time<1ms TTL=128
Reply from 192.168.2.4: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.2.4:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

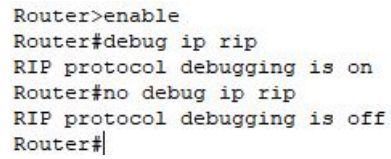
如下图所示为 PC0　ping　PC6 的结果。

```
C:\>ping 192.168.3.3

Pinging 192.168.3.3 with 32 bytes of data:

Reply from 192.168.3.3: bytes=32 time<1ms TTL=127
Reply from 192.168.3.3: bytes=32 time=8ms TTL=127
Reply from 192.168.3.3: bytes=32 time<1ms TTL=127
Reply from 192.168.3.3: bytes=32 time<1ms TTL=127

Ping statistics for 192.168.3.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 8ms, Average = 2ms
```

如下图所示为 PC0　ping　PC7 的结果。



综上可见，任何两台主机，无论是否属于同一 VLAN，都能 ping 通。可见合理配置后，路由器发挥了其作用，实现了不同 VLAN 间的通信。



如上图为在 CLI 界面通过命令来开启和关闭 RIP 诊断的截图。

五、　实验思考题　（选做）

1. 路由器的配置可以通过哪几种方式？

答：有用户模式、特权模式全局设配置模式和接口配置模式四种。

2. 怎样进入特权模式(Privileged Exec Mode)？

答：在用户模式的 router>提示符后输入 enable 并回车，交换机就可以进入特权命令模式。

3. 怎样进入全局配置模式(Global Configuration Mode)？

答：在特权模式的 router#提示符下输入 configure terminal 命令，出现提示符 router(config)#，此时交换机处于全局设置模式，可以设置交换机的全局参数。

4. 在什么模式下哪个命令可以配置路由器某个接口(interface)的 IP 地址？

答：在接口配置模式下的 ip address [IP 地址] [子网掩码] 命令可以配置该端口的 IP 地址和对应的子网掩码。

5. 根据你的理解，比较 RIP 与 OSPF 协议。

答：RIP 是一种简单、易于实现的路由选择协议，但功能有限、收敛速度相对较慢，并且有最大跳数限制，所以更适合小型网络。OSPF 是一种更复杂、功能更强大的协议，但因其收敛相对较快，适合大型和动态变化的网络环境。此外，RIP 使用跳数作为路由度量，这意味着所有类型的链路都被视为等价的；而 OSPF 使用成本值作为路由度量，可以根据链路的带宽、延迟或价格等其他因素来分配不同的成本值。