廣東工業大學

《计算网络 A》实验报告

学　　院___计算机学院　_____ _

专　　业___计算机科学与技术_____

年级班别___19（1）班_____

学　　号___3119004760_____

学生姓名___叶嘉轩_____

指导教师___彭重嘉　_____ __

成　　绩 _____

广东工业大学

计算机　学院　计算机科学与技术　业 19 (1)　班、学号 3119004760

姓名　叶嘉轩　　教师评定_____

实验题目　一. 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。

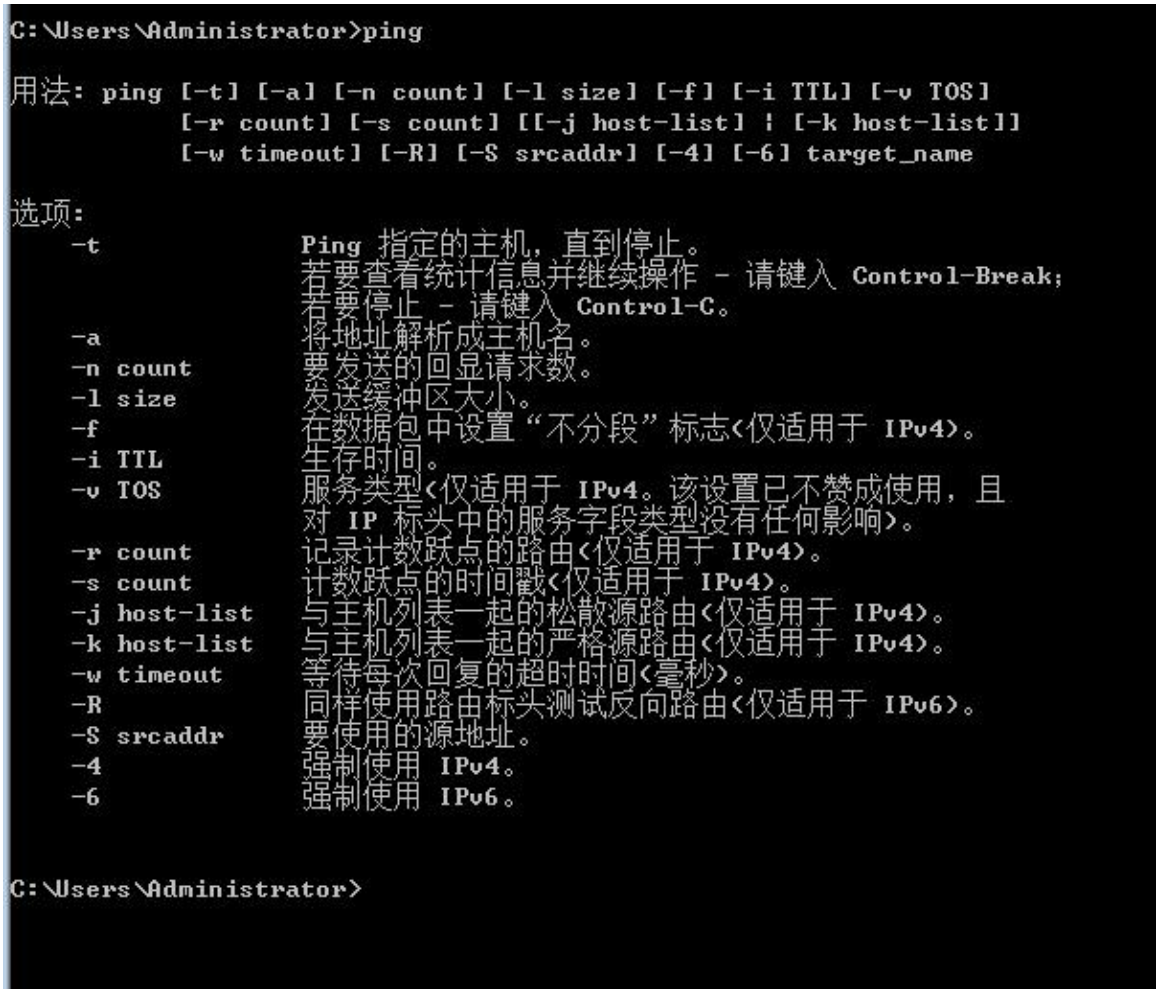
5、使用 Netstat 工具，记录下相关信息。

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

1.使用 ping 工具


C:\Users\Administrator>ping
用法: ping [-t] [-a] [-n count] [-l size] [-f] [-i TTL] [-v TOS]
[-r count] [-s count] [[-j host-list] | [-k host-list]]
[-w timeout] [-R] [-S srcaddr] [-4] [-6] target_name
选项:
-t Ping 指定的主机，直到停止。
若要查看统计信息并继续操作 - 请键入 Control-Break;
若要停止 - 请键入 Control-C。
-a 将地址解析成主机名。
-n count 要发送的回显请求数。
-l size 发送缓冲区大小。
-f 在数据包中设置“不分段”标志(仅适用于 IPv4)。
-i TTL 生存时间。
-v TOS 服务类型(仅适用于 IPv4。该设置已不赞成使用，且
对 IP 标头中的服务字段类型没有任何影响)。
-r count 记录计数跃点的路由(仅适用于 IPv4)。
-s count 计数跃点的时间戳(仅适用于 IPv4)。
-j host-list 与主机列表一起的松散源路由(仅适用于 IPv4)。
-k host-list 与主机列表一起的严格源路由(仅适用于 IPv4)。
-w timeout 等待每次回复的超时时间(毫秒)。
-R 同样使用路由标头测试反向路由(仅适用于 IPv6)。
-S srcaddr 要使用的源地址。
-4 强制使用 IPv4。
-6 强制使用 IPv6。
C:\Users\Administrator>

举例 ping –t 的使用：

```
C:\Users\Administrator>ping 10.21.9.54 -t

正在 Ping 10.21.9.54 具有 32 字节的数据:
来自 10.21.9.54 的回复: 字节=32 时间<1ms TTL=64
来自 10.21.9.54 的回复: 字节=32 时间<1ms TTL=64
来自 10.21.9.54 的回复: 字节=32 时间<1ms TTL=64
来自 10.21.9.54 的回复: 字节=32 时间<1ms TTL=64
来自 10.21.9.54 的回复: 字节=32 时间<1ms TTL=64
来自 10.21.9.54 的回复: 字节=32 时间<1ms TTL=64
来自 10.21.9.54 的回复: 字节=32 时间<1ms TTL=64
来自 10.21.9.54 的回复: 字节=32 时间<1ms TTL=64
来自 10.21.9.54 的回复: 字节=32 时间<1ms TTL=64
来自 10.21.9.54 的回复: 字节=32 时间<1ms TTL=64
来自 10.21.9.54 的回复: 字节=32 时间<1ms TTL=64
来自 10.21.9.54 的回复: 字节=32 时间<1ms TTL=64
来自 10.21.9.54 的回复: 字节=32 时间<1ms TTL=64
来自 10.21.9.54 的回复: 字节=32 时间<1ms TTL=64
来自 10.21.9.54 的回复: 字节=32 时间<1ms TTL=64
来自 10.21.9.54 的回复: 字节=32 时间<1ms TTL=64
来自 10.21.9.54 的回复: 字节=32 时间<1ms TTL=64
来自 10.21.9.54 的回复: 字节=32 时间<1ms TTL=64
来自 10.21.9.54 的回复: 字节=32 时间<1ms TTL=64
来自 10.21.9.54 的回复: 字节=32 时间<1ms TTL=64
来自 10.21.9.54 的回复: 字节=32 时间<1ms TTL=64
来自 10.21.9.54 的回复: 字节=32 时间<1ms TTL=64
来自 10.21.9.54 的回复: 字节=32 时间<1ms TTL=64
来自 10.21.9.54 的回复: 字节=32 时间<1ms TTL=64

10.21.9.54 的 Ping 统计信息:
    数据包: 已发送 = 24, 已接收 = 24, 丢失 = 0 (0% 丢失),
往返行程的估计时间(以毫秒为单位):
    最短 = 0ms, 最长 = 0ms, 平均 = 0ms
Control-C
^C
```

出现上面这些就显示可以正常访问 Internet。

2.使用 ipconfig/all 检测查看网络参数情况

3. Netsh 是命令行脚本实用工具，它允许从本地或远程显示或修改当前正在运行的计算机的网络配置。

```
C:\Users\Administrator>netsh ?

用法: netsh [-a AliasFile] [-c Context] [-r RemoteMachine] [-u [DomainName\]User
Name] [-p Password | *]
            [Command | -f ScriptFile]

下列指令有效:

此上下文中的命令:
?               - 显示命令列表。
add             - 在项目列表上添加一个配置项目。
advfirewall     - 更改到 'netsh advfirewall' 上下文。
branchcache     - 更改到 'netsh branchcache' 上下文。
bridge          - 更改到 'netsh bridge' 上下文。
delete          - 在项目列表上删除一个配置项目。
dhcpclient      - 更改到 'netsh dhcpclient' 上下文。
dnsclient       - 更改到 'netsh dnsclient' 上下文。
dump            - 显示一个配置脚本。
exec            - 运行一个脚本文件。
firewall        - 更改到 'netsh firewall' 上下文。
help            - 显示命令列表。
http            - 更改到 'netsh http' 上下文。
interface       - 更改到 'netsh interface' 上下文。
ipsec           - 更改到 'netsh ipsec' 上下文。
lan             - 更改到 'netsh lan' 上下文。
```

4.使用 Tracert 工具测试本机到 www.baidu.com 所经过的路由数

```
C:\Users\Administrator>tracert www.baidu.com

通过最多 30 个跃点跟踪
到 www.baidu.com [14.215.177.39] 的路由:

  1     6 ms     2 ms     1 ms  10.21.9.1
  2     3 ms     1 ms     1 ms  172.16.255.5
  3    <1 毫秒   <1 毫秒   <1 毫秒 222.200.126.241
  4    <1 毫秒   <1 毫秒   <1 毫秒 10.0.7.1
  5    30 ms     1 ms    <1 毫秒 61.144.42.29
  6     2 ms     2 ms     2 ms  58.61.243.241
  7     2 ms     2 ms     *     117.176.37.59.broad.dg.gd.dynamic.163data.com.c
[59.37.176.117]
  8     5 ms     5 ms     5 ms  245.32.63.58.broad.gz.gd.dynamic.163data.com.cn
[58.63.32.245]
  9     *        5 ms     *     113.96.5.94
 10     6 ms    23 ms     6 ms  113.96.11.78
 11     6 ms     6 ms     6 ms  14.215.32.130
 12     *        *        *     请求超时。
 13     *        *        *     请求超时。
 14     5 ms     5 ms     5 ms  14.215.177.39

跟踪完成。
```

5.netstat 的使用

用 netstat –a 测试本机：

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

活动连接

  协议  本地地址          外部地址        状态
  TCP    0.0.0.0:135            A54:0                  LISTENING
  TCP    0.0.0.0:445            A54:0                  LISTENING
  TCP    0.0.0.0:1025           A54:0                  LISTENING
  TCP    0.0.0.0:1026           A54:0                  LISTENING
  TCP    0.0.0.0:1027           A54:0                  LISTENING
  TCP    0.0.0.0:1028           A54:0                  LISTENING
  TCP    0.0.0.0:1029           A54:0                  LISTENING
  TCP    0.0.0.0:1031           A54:0                  LISTENING
  TCP    10.21.9.54:139         A54:0                  LISTENING
  TCP    10.21.9.54:1088        a184-31-170-80:https   CLOSE_WAIT
  TCP    10.21.9.54:1090        a23-55-248-23:https    ESTABLISHED
  TCP    [::]:135               A54:0                  LISTENING
  TCP    [::]:445               A54:0                  LISTENING
  TCP    [::]:1025              A54:0                  LISTENING
  TCP    [::]:1026              A54:0                  LISTENING
  TCP    [::]:1027              A54:0                  LISTENING
  TCP    [::]:1028              A54:0                  LISTENING
  TCP    [::]:1029              A54:0                  LISTENING
  TCP    [::]:1031              A54:0                  LISTENING
  TCP    [::1]:1055             A54:0                  LISTENING
  UDP    0.0.0.0:500            *:*
  UDP    0.0.0.0:4500           *:*
  UDP    0.0.0.0:4703           *:*
  UDP    0.0.0.0:4704           *:*
  UDP    0.0.0.0:4705           *:*
  UDP    0.0.0.0:4706           *:*
  UDP    0.0.0.0:5355           *:*
  UDP    10.21.9.54:137         *:*
  UDP    10.21.9.54:138         *:*
  UDP    10.21.9.54:1900        *:*
  UDP    10.21.9.54:6660        *:*
  UDP    10.21.9.54:9101        *:*
  UDP    10.21.9.54:59043       *:*
```

```
  UDP    127.0.0.1:1900         *:*
  UDP    127.0.0.1:57771        *:*
  UDP    127.0.0.1:59044        *:*
  UDP    [::]:500               *:*
  UDP    [::]:4500              *:*
  UDP    [::]:5355              *:*
  UDP    [::1]:1900             *:*
  UDP    [::1]:59042            *:*
  UDP    [fe80::1906:8d4b:76bf:1ca5%12]:1900  *:*
  UDP    [fe80::1906:8d4b:76bf:1ca5%12]:59041  *:*
```

Netstat –e 的使用：

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

                           接收的            发送的

字节                     56611896         2790064
单播数据包               16524            7613
非单播数据包             400713           8868
丢弃                     0                0
错误                     0                0
未知协议                 0
```

6.使用 Arp 工具，记录下相关信息。

```
macbookpro@MacBookdeMacBook-Pro ~ % arp
usage: arp [-n] [-i interface] hostname
       arp [-n] [-i interface] [-l] -a
       arp -d hostname [pub] [ifscope interface]
       arp -d [-i interface] -a
       arp -s hostname ether_addr [temp] [reject] [blackhole] [pub [only]] [ifsc
ope interface]
       arp -S hostname ether_addr [temp] [reject] [blackhole] [pub [only]] [ifsc
ope interface]
```

Arp –a 的测试:

```
macbookpro@MacBookdeMacBook-Pro ~ % arp -a
? (10.33.80.1) at 34:a2:a2:89:bd:f on en0 ifscope [ethernet]
? (10.33.81.74) at 40:98:ad:4d:56:2f on en0 ifscope [ethernet]
? (10.33.82.196) at 14:4f:8a:96:a3:57 on en0 ifscope [ethernet]
? (10.33.82.219) at 8:5b:d6:60:ed:a7 on en0 ifscope [ethernet]
? (10.33.85.210) at d8:f2:ca:c:49:9b on en0 ifscope [ethernet]
? (10.33.86.60) at a:ca:e1:fd:83:99 on en0 ifscope [ethernet]
? (10.33.88.117) at d0:d7:83:1c:ce:e8 on en0 ifscope [ethernet]
? (10.33.89.46) at a4:c3:f0:90:ee:80 on en0 ifscope [ethernet]
? (10.33.89.66) at f8:ff:c2:4b:c2:d on en0 ifscope [ethernet]
? (10.33.91.96) at 9c:b6:d0:4:5f:79 on en0 ifscope [ethernet]
? (10.33.91.205) at 94:d9:b3:d6:c4:28 on en0 ifscope [ethernet]
? (10.33.93.5) at 2c:6e:85:68:84:4 on en0 ifscope [ethernet]
? (10.33.94.105) at 34:42:62:10:10:0 on en0 ifscope [ethernet]
? (10.33.94.181) at 60:8b:e:97:4:64 on en0 ifscope [ethernet]
? (10.33.95.195) at 2c:d9:74:7:15:46 on en0 ifscope [ethernet]
? (10.33.95.223) at c0:3c:59:ab:87:ea on en0 ifscope [ethernet]
? (10.33.95.255) at ff:ff:ff:ff:ff:ff on en0 ifscope [ethernet]
? (224.0.0.251) at 1:0:5e:0:0:fb on en0 ifscope permanent [ethernet]
? (239.255.255.250) at 1:0:5e:7f:ff:fa on en0 ifscope permanent [ethernet]
macbookpro@MacBookdeMacBook-Pro ~ %
```

7.使用 Nslookup 工具，记录下相关信息。

Nslookup 必须要安装了 TCP/IP 协议的网络环境之后才能使用。 Ns.lookup 必须要安装了 TCP/IP 协议的网络环境之后才能使用。

```
C:\Documents and Settings\Administrator>nslookup www.baidu.com
Server:  cache-a.guangzhou.gd.cn
Address:  202.96.128.86

Non-authoritative answer:
Name:    www.a.shifen.com
Addresses:  115.239.210.27, 115.239.210.26
Aliases:  www.baidu.com
```

以上结果显示，正在工作的 DNS 服务器的主机名为 cache-a.guangzhou.gd.cn,它的 IP 地址是 202.96.128.86。

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故障的原因?
   答：使用 Ping dns，检查是否正常。

2. 记录结果：Tracert www.baidu.com

```
C:\Users\Administrator>tracert www.baidu.com

通过最多 30 个跃点跟踪
到 www.baidu.com [14.215.177.39] 的路由:

  1     6 ms     2 ms     1 ms  10.21.9.1
  2     3 ms     1 ms     1 ms  172.16.255.5
  3    <1 毫秒   <1 毫秒   <1 毫秒 222.200.126.241
  4    <1 毫秒   <1 毫秒   <1 毫秒 10.0.7.1
  5    30 ms     1 ms    <1 毫秒 61.144.42.29
  6     2 ms     2 ms     2 ms  58.61.243.241
  7     2 ms     2 ms     *     117.176.37.59.broad.dg.gd.dynamic.163data.com.c
[59.37.176.117]
  8     5 ms     5 ms     5 ms  245.32.63.58.broad.gz.gd.dynamic.163data.com.cn
[58.63.32.245]
  9     *        5 ms     *     113.96.5.94
 10     6 ms    23 ms     6 ms  113.96.11.78
 11     6 ms     6 ms     6 ms  14.215.32.130
 12     *        *        *     请求超时。
 13     *        *        *     请求超时。
 14     5 ms     5 ms     5 ms  14.215.177.39

跟踪完成。
```

3. 你的主机的 48 位以太网地址(MAC 地址)是多少?
   答：C0-3F-D5-4E-85-74

广东工业大学

计算机　学院　计算机科学与技术　业 19(1) 班、学号 3119004760

姓名　叶嘉轩　　教师评定_____

实验题目　二. 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。. 进一步熟悉IRIS软件的使用方法；

2．利用Wireshark （Ethereal）抓包；

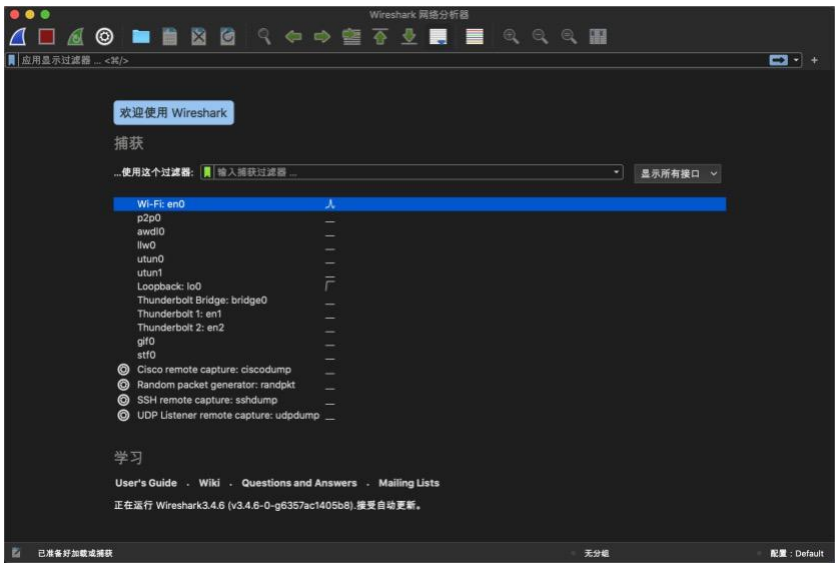
3．对抓取到的包进行分析，通过分析巩固对Ethernet II 封包、ARP 分组及IP、ICMP 数据包的认识。

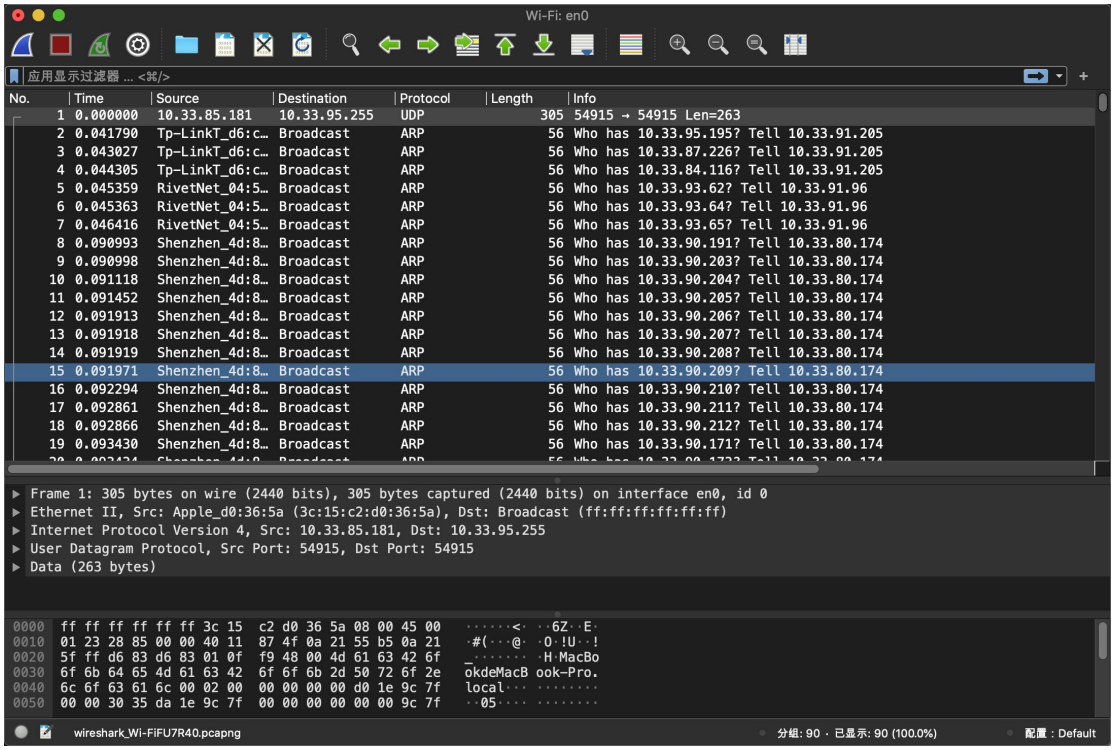
二、　实验内容和要求

1) 学习协议分析工具 Wireshark 的基本使用方法；
2) 利用 Wireshark 进行 IP 数据报报文的抓取；
3) 对抓取到的数据报文进行分析，体会数据报发送、转发的过程。
4) 对抓取到的包进行分析, 通过分析 TCP 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。

三、　实验结果

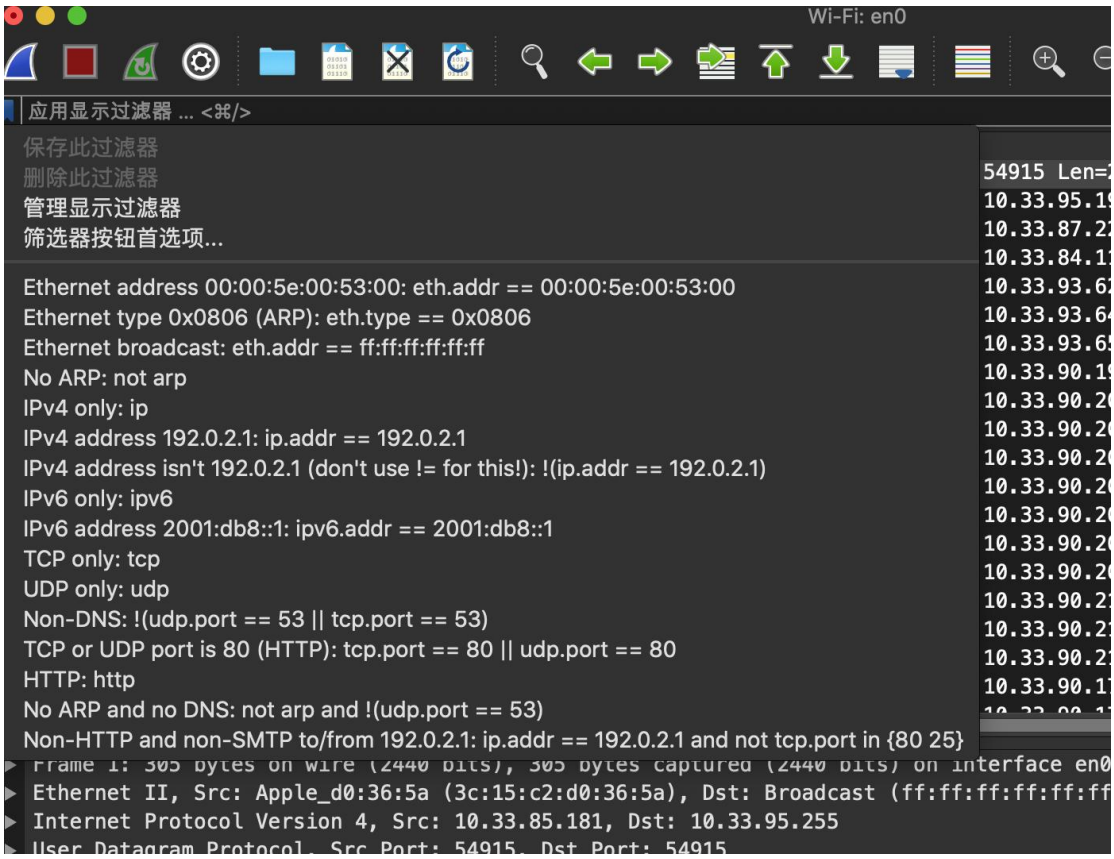
1. 使用方法：选择第一个为本地连接，双击开始抓包





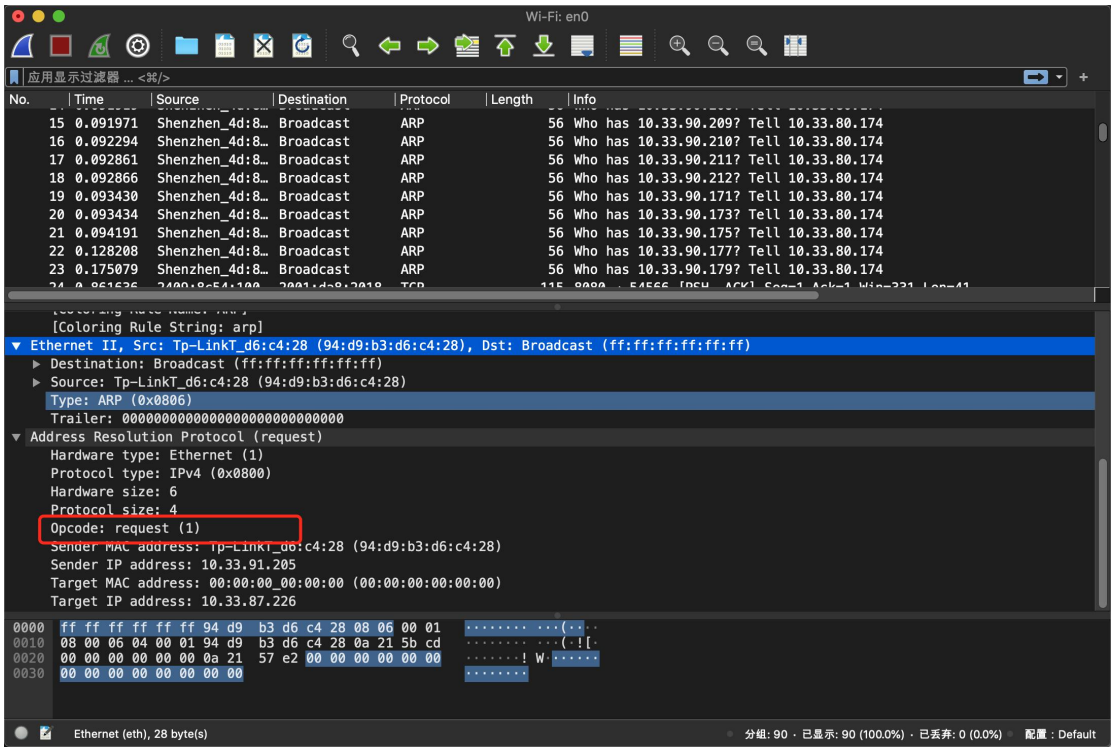
界面主要分为 3 部分，上部分是各个包，中部是包中的组成部件，下部是各部件的二进制码！中部可进行查看包的组成结构。

2. 菜单栏的最左边点击可以选择过滤的内容，或者直接在搜索栏搜索



3. 下图为抓包（arp）

根据 arp 包的组成结构，可以看出是 arp 请求还是应答如下图中 opcode 若是 0001 则是请求，0002 则是应答



四、 思考题

1. 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。

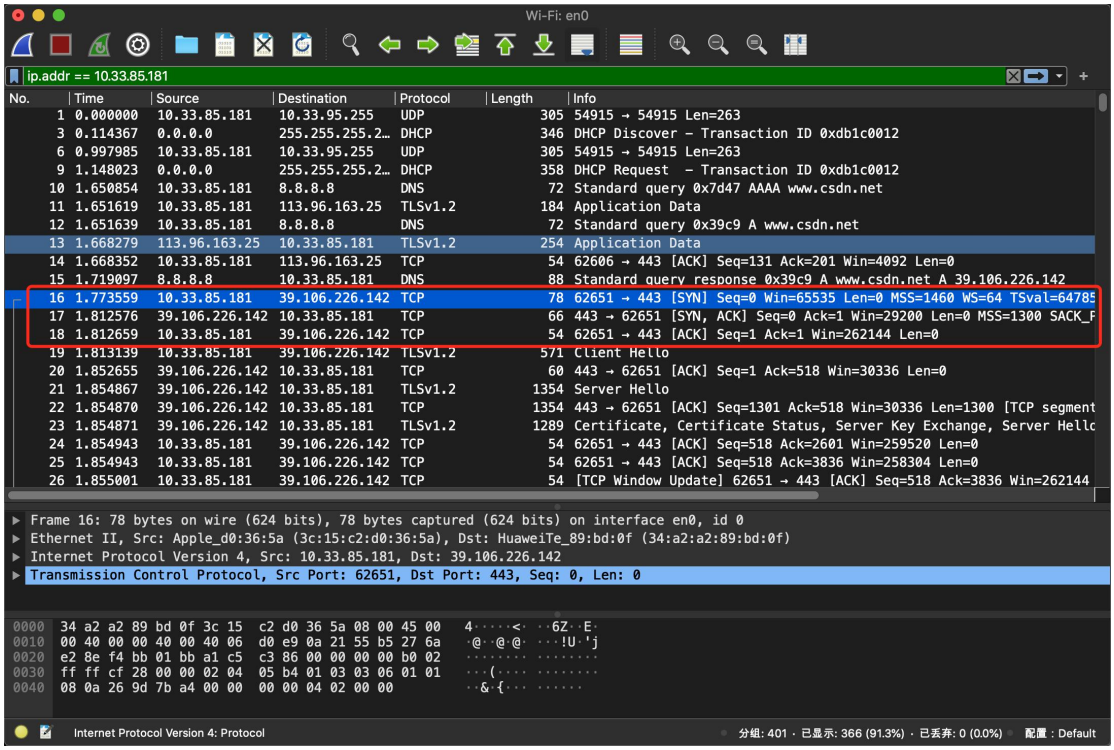
从下图的红框中可以看到，本机的 IP 地址是 10.33.85.181，访问的网站的 IP 地址是 39.106.226.142.

三次握手过程：

1.第一次：本主机向 IP 地址 39.106.226.142 发送了一个 SYN 连接请求

2.第二次：IP 地址 39.106.226.142 向本主机发送了一个 SYN 确认请求以及一个 ACK 确认报

3.第三次：本主机向 IP 地址 39.106.226.142 发送一个 ACK 确认报，表明自己知道已经确认好连接



广东工业大学

计算机　学院　计算机科学与技术　业 19 (1)　班、学号 3119004760

姓名　叶嘉轩　　教师评定_____

实验题目　　三.　交换机的基本配置　　

一、实验目的

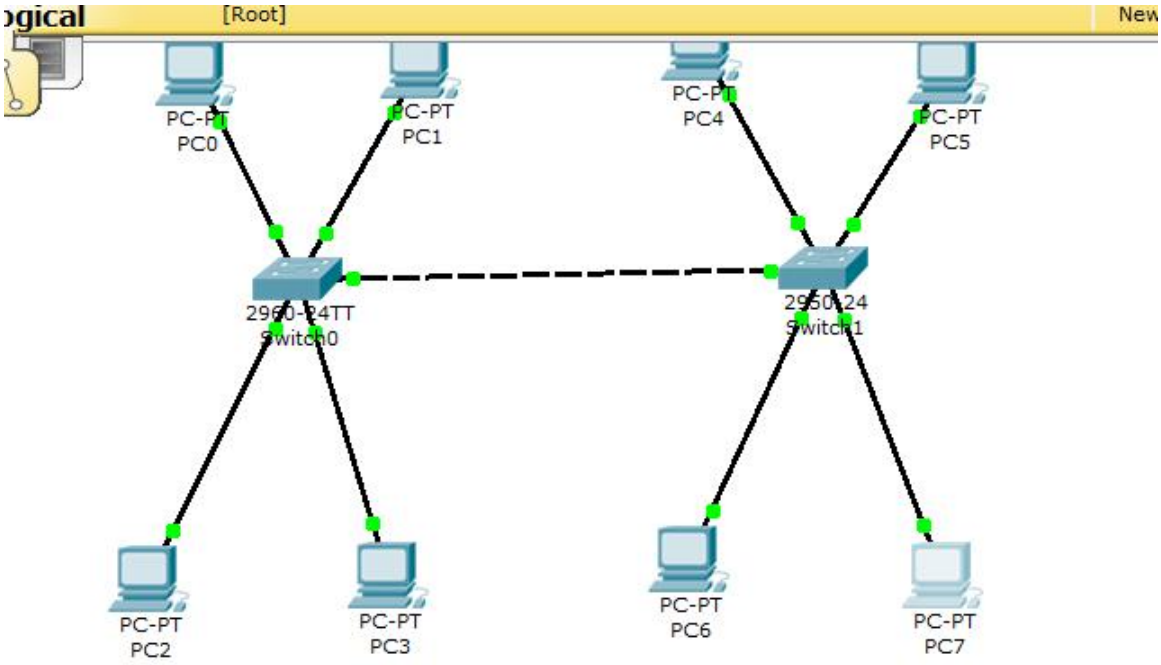
了解交换机网络硬件设备，初步掌握交换机的常用配置。

二、**实验要求**

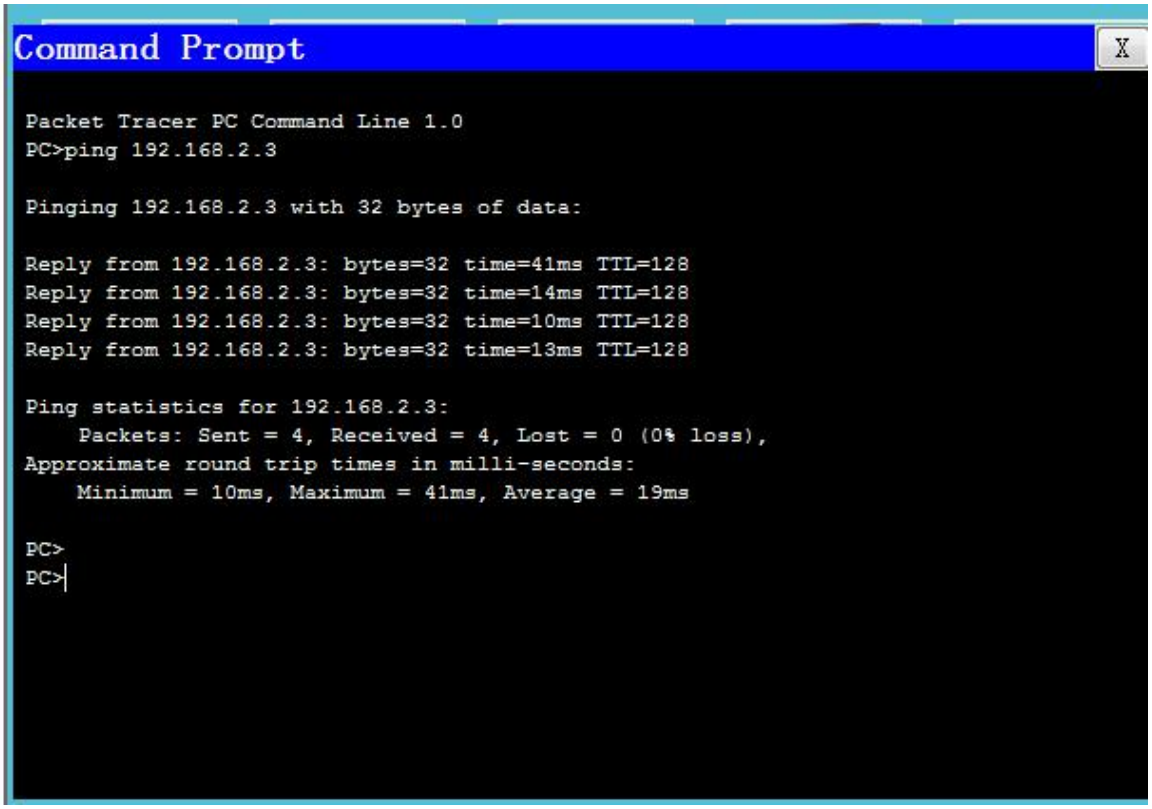
熟悉 Cisco IOS 命令，理解交换机的工作原理，通过 Packet Tracer 软件能对交换机进行仿真配置，完成 Vlan。可根据情况进一步完成 VTP，STP 等配置并测试。

三 、**实验结果**

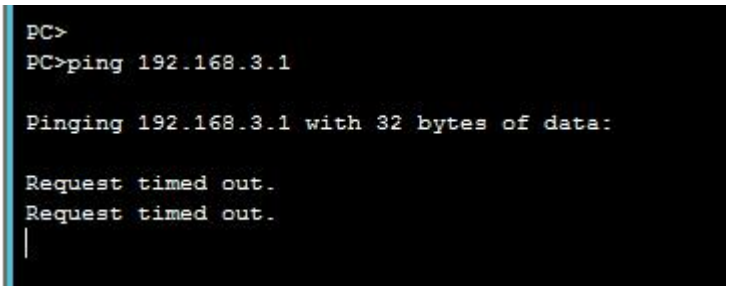
实验图如图所示：



其中 PC0，PC1，PC4，PC5 属于同 VLAN2，PC2，PC3，PC6，PC7 属于同 VLAN3。用 PC0 可以 ping 到 PC4：



而 PC0 不能 ping 到不同 VLAN3 的 PC2：



四、实验思考题

1. 简述实验过程中出现的问题及解决方法。

答：问题：如何建立两个 vlan，和如何将不同的计算机分配于不同的 vlan 之中。
方法：点击交换机，然后在 Config 里设置 switch，将 Vlan2 和 Vlan3 添加进去，两个交换机添加完之后，对连接在交换下的 pc 端设置所属于的 VLan。

2. 交换机的配置可以通过哪几种方式?

答:一种为在命令输入行中输入相关命令，一种是根据软件特点使用其中的便捷按键!

3. 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。

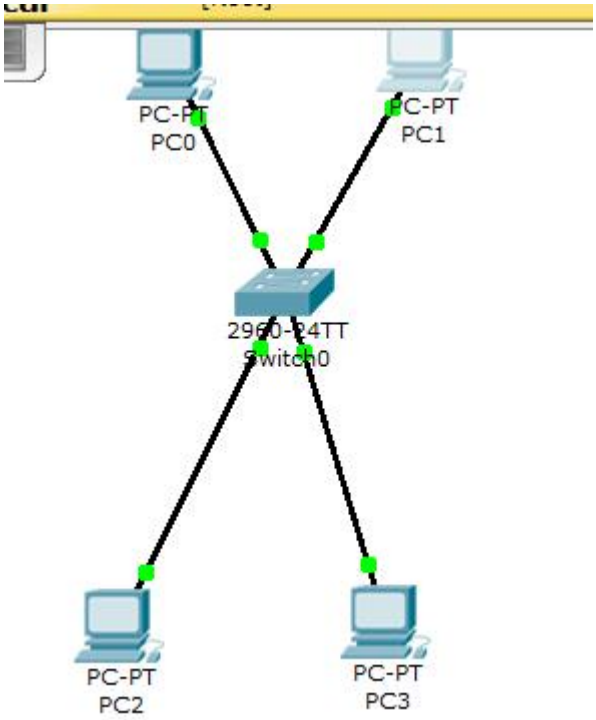


图 3.1 vlan 基础配置拓扑图

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 2			无
F0/2	VLAN 2			无
F0/3	VLAN 3			无
F0/4	VLAN 3			无
PC0	NIC	192.168.2.1		
PC1	NIC	192.168.2.2		
PC2	NIC	192.168.3.1		
PC3	NIC	192.168.3.2		

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

PC0 和 PC1 可以ping通

```
PC>ping 192.168.2.2

Pinging 192.168.2.2 with 32 bytes of data:

Reply from 192.168.2.2: bytes=32 time=18ms TTL=128
Reply from 192.168.2.2: bytes=32 time=6ms TTL=128
Reply from 192.168.2.2: bytes=32 time=9ms TTL=128
Reply from 192.168.2.2: bytes=32 time=8ms TTL=128

Ping statistics for 192.168.2.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 6ms, Maximum = 18ms, Average = 10ms

PC>
PC>
```

PC0 和 PC2ping 不通

```
PC>
PC>ping 192.168.3.1

Pinging 192.168.3.1 with 32 bytes of data:

Request timed out.

Ping statistics for 192.168.3.1:
    Packets: Sent = 2, Received = 0, Lost = 2 (100% loss),

Control-C
^C
PC>
```

广东工业大学

计算机　学院　计算机科学与技术　业 19(1) 班、学号 3119004760

姓名　叶嘉轩　　教师评定_____

实验题目　四．　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

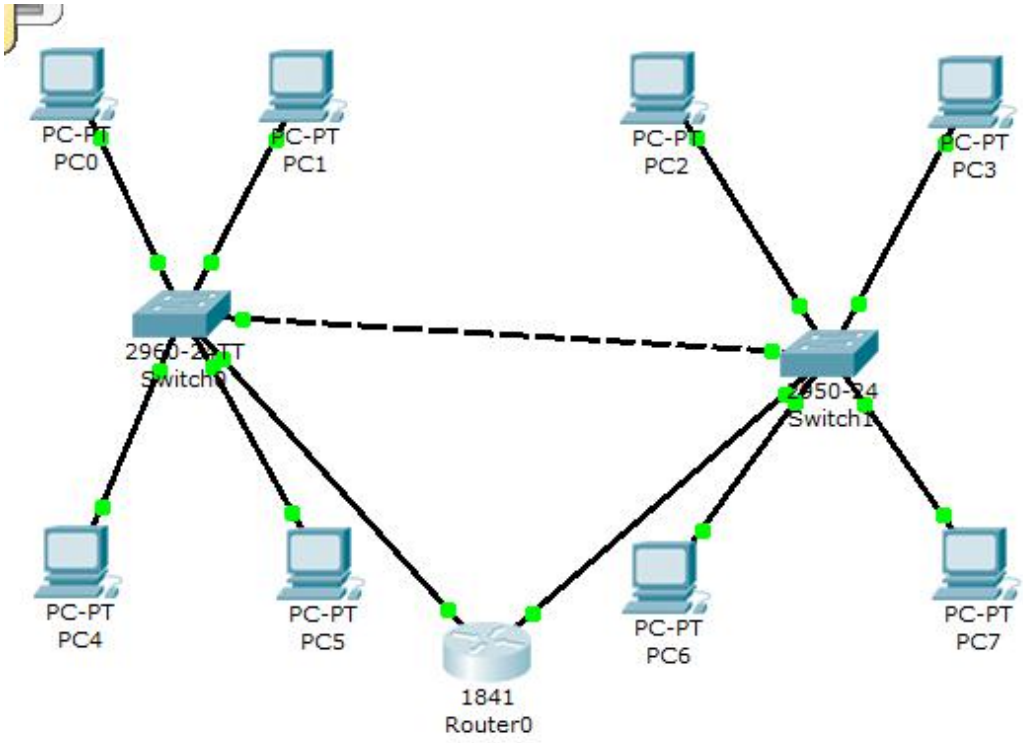
交换机，路由器，PC，Packet Tracer 软件等。

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。

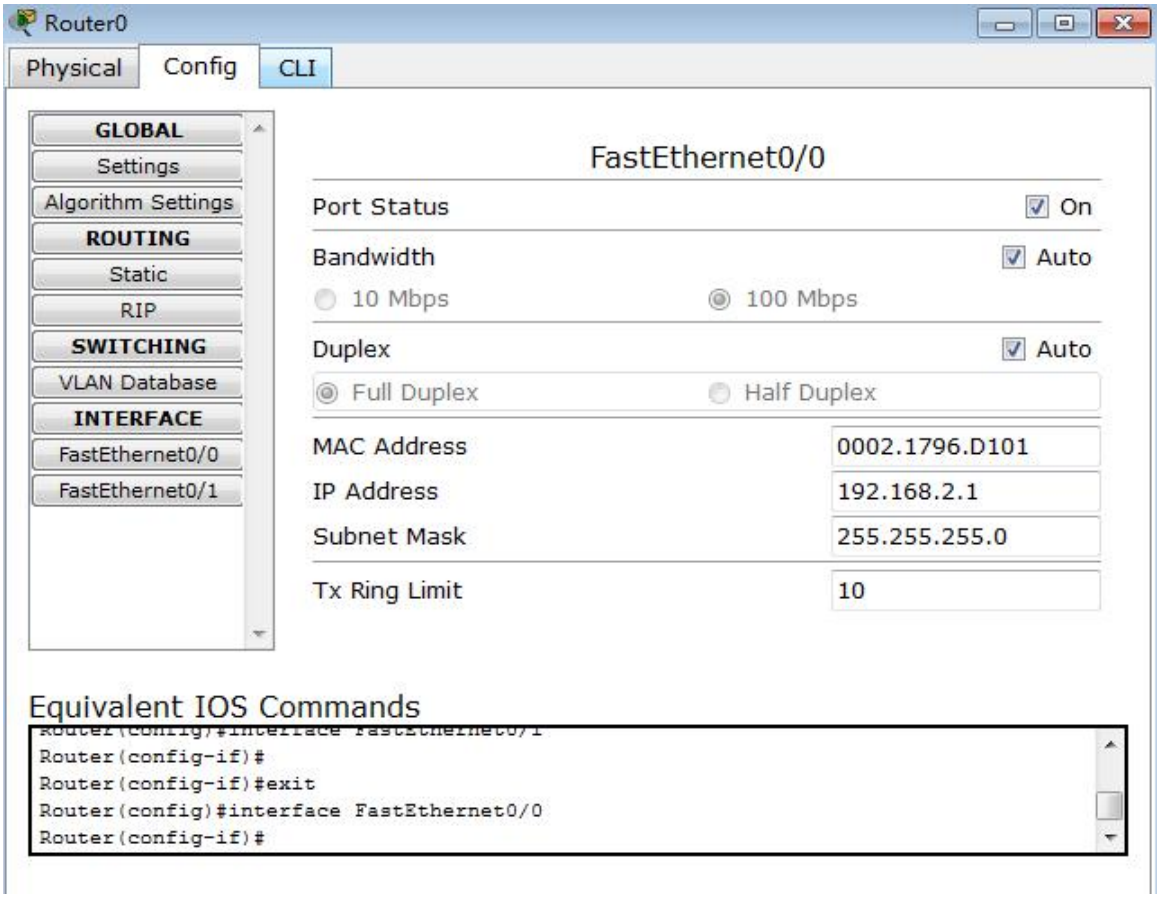
四、实验结果

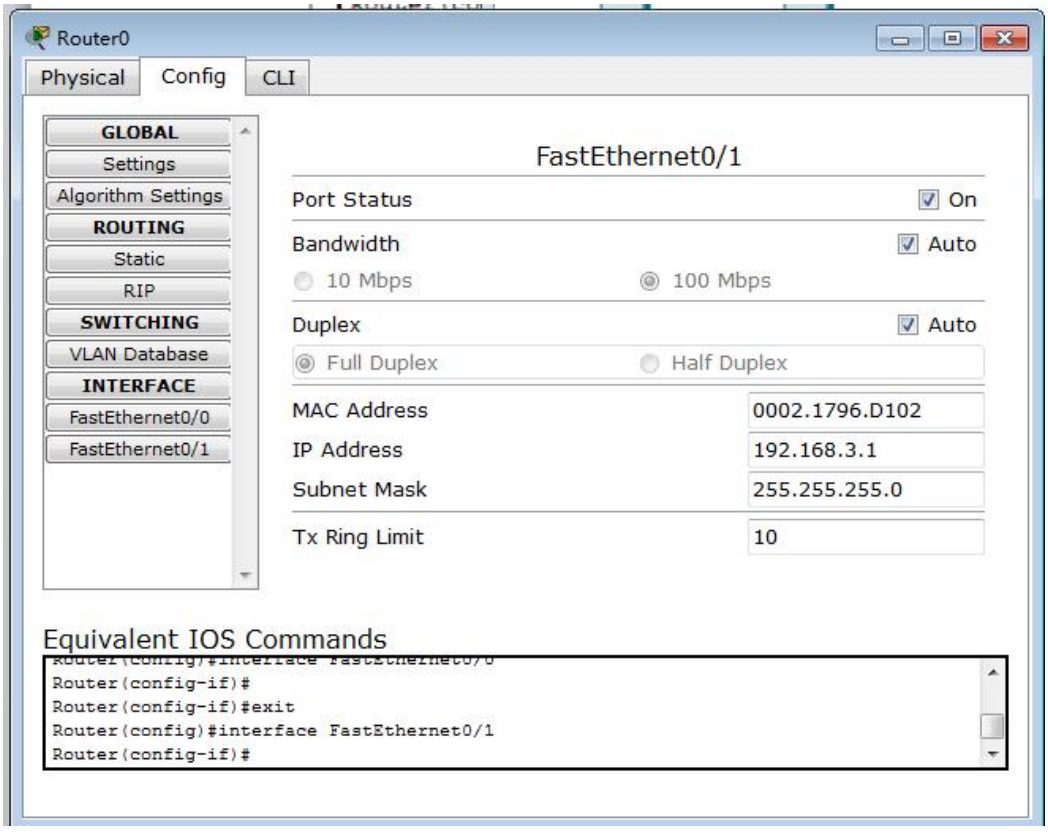
1:实验环境搭建



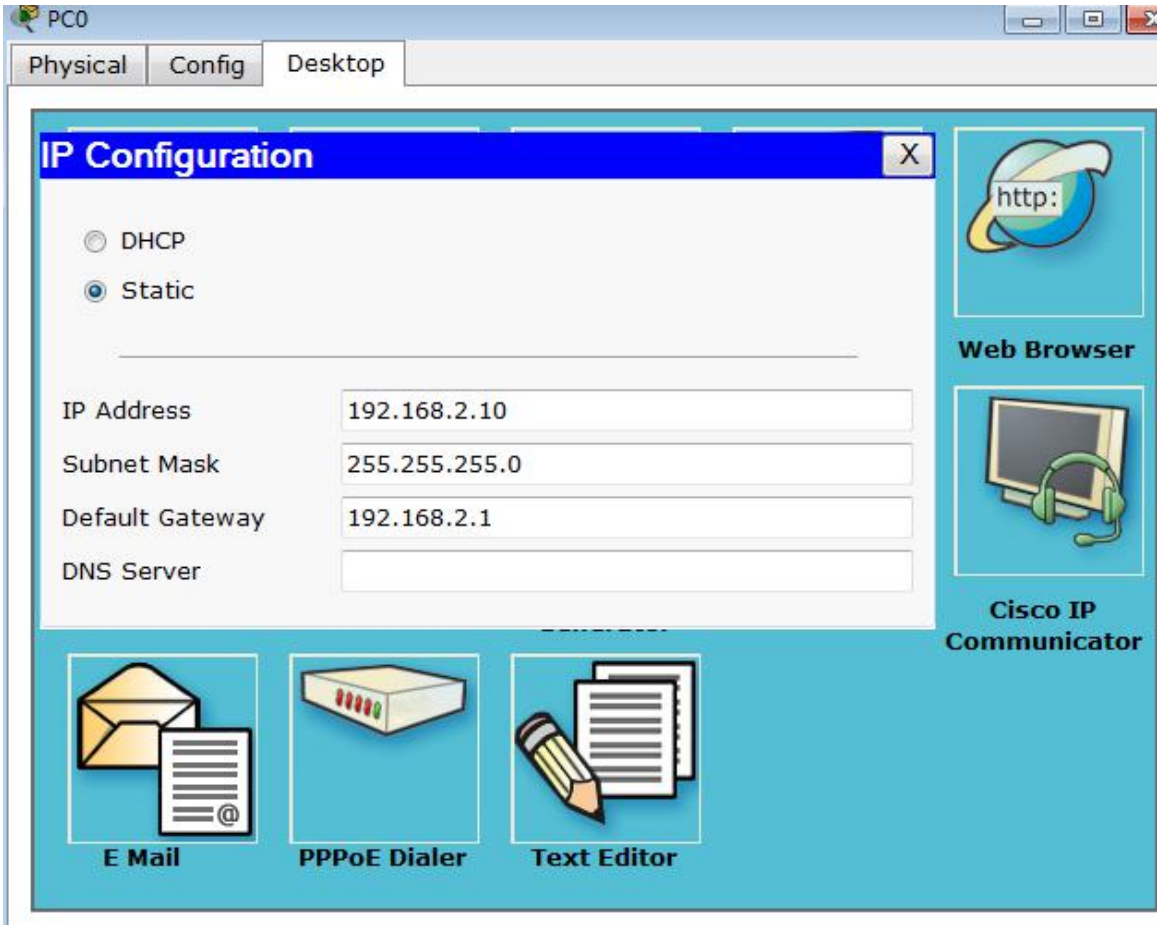
2：路由器端口设计：

1.


Router0
Physical
Config
CLI
GLOBAL
Settings
Algorithm Settings
ROUTING
Static
RIP
SWITCHING
VLAN Database
INTERFACE
FastEthernet0/0
FastEthernet0/1
FastEthernet0/0
Port Status
On
Bandwidth
Auto
10 Mbps
100 Mbps
Duplex
Auto
Full Duplex
Half Duplex
MAC Address
0002.1796.D101
IP Address
192.168.2.1
Subnet Mask
255.255.255.0
Tx Ring Limit
10
Equivalent IOS Commands
Router(config-if)#
Router(config-if)#exit
Router(config)#interface FastEthernet0/0
Router(config-if)#


Router0
Physical
Config
CLI
GLOBAL
Settings
Algorithm Settings
ROUTING
Static
RIP
SWITCHING
VLAN Database
INTERFACE
FastEthernet0/0
FastEthernet0/1
FastEthernet0/1
Port Status
On
Bandwidth
Auto
10 Mbps
100 Mbps
Duplex
Auto
Full Duplex
Half Duplex
MAC Address
0002.1796.D102
IP Address
192.168.3.1
Subnet Mask
255.255.255.0
Tx Ring Limit
10
Equivalent IOS Commands
Router(config-if)#
Router(config-if)#exit
Router(config)#interface FastEthernet0/1
Router(config-if)#

3. PC 端端口设计:



4. 实现不同 Vlan 下的 PC 通信正常

PC0 ping PC7 成功，PC0 是 VLan2 下的，PC7 是 VLan3 下的。

```
Control-C
^C
PC>ping 192.168.3.17

Pinging 192.168.3.17 with 32 bytes of data:

Request timed out.
Reply from 192.168.3.17: bytes=32 time=13ms TTL=127
Reply from 192.168.3.17: bytes=32 time=18ms TTL=127
Reply from 192.168.3.17: bytes=32 time=15ms TTL=127

Ping statistics for 192.168.3.17:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 13ms, Maximum = 18ms, Average = 15ms

PC>
```

五、 实验思考题

1. 路由器的配置可以通过哪几种方式?

   答：通过 console 端口输入命令配置，使用 telnet 远程控制配置。

2. 怎样进入特权模式(Privileged Exec Mode)?

答：在用户模式下输入 enable，然后输入密码，进入特权模式。

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

   答：在特权模式下输入 configure terminal 进入全局配置模式。

4. 使用什么命令来显示系统的硬件配置，软件版本等信息?

   答：在特权模式下使用 show version ,show running-config

5. 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：在特权模式下使用 ip address 命令配置

6. 根据你的理解，简述 RIP 与 OSPF 的比较。

   答：路由协议类型： RIP 是距离矢量协议，而 OSPF 是链路状态协议。距离矢量协议使用跳数来确定传输路径。链路状态协议分析不同的源，如速度，成本和路径拥塞，同时识别最短路径。

   路由表构造： RIP 使用周围的路由器请求路由表。然后合并该信息并构造自己的路由表。该表定期发送到相邻设备，同时更新路由器的合并表。在 OSPF 中，路由器通过仅从相邻设备获取所需信息来合并路由表。它永远不会获得设备的整个路由表，并且路由表构造非常简单。

   跳数限制： RIP 最多只允许 15 跳，而在 OSPF 中没有这样的限制。

   使用的算法：RIP 使用距离向量算法，而 OSPF 使用最短路径算法 Dijkstra 来确定传输路由。

   网络分类：在 RIP 中，网络分为区域和表格。在 OSPF 中，网络被分类为区域，子区域，自治系统和骨干区域。

   复杂性级别： RIP 相对简单，而 OSPF 则要复杂得多。

   RIP 与 OSPF 应用： RIP 适用于较小的网络，因为它具有跳数限制。OSPF 非常适合大型网络。