**计算机网络实验报告**

班 级： 1803

学 号： 19170333

姓 名： 樊世雄

实验日期： 2020-11-18

南京师范大学 计算机科学与技术学院制

# 实验五-7.4-利用Wireshark分析ICMP和DHCP

## 实验目的：

1. 分析ICMP
2. 分析DHCP

## 实验环境：

本次实验环境包括：与因特网连接的计算机，操作系统为Windows，安装有wireshark，IE等软件。

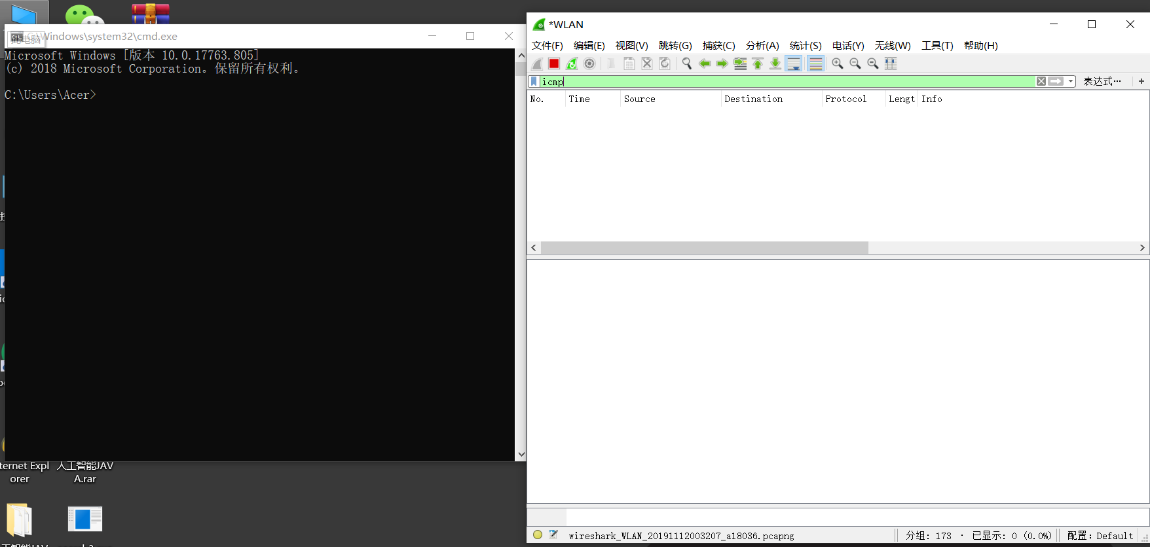
## 实验内容：

1. 通过实验掌握ICMP；
2. 通过实验掌握DHCP；

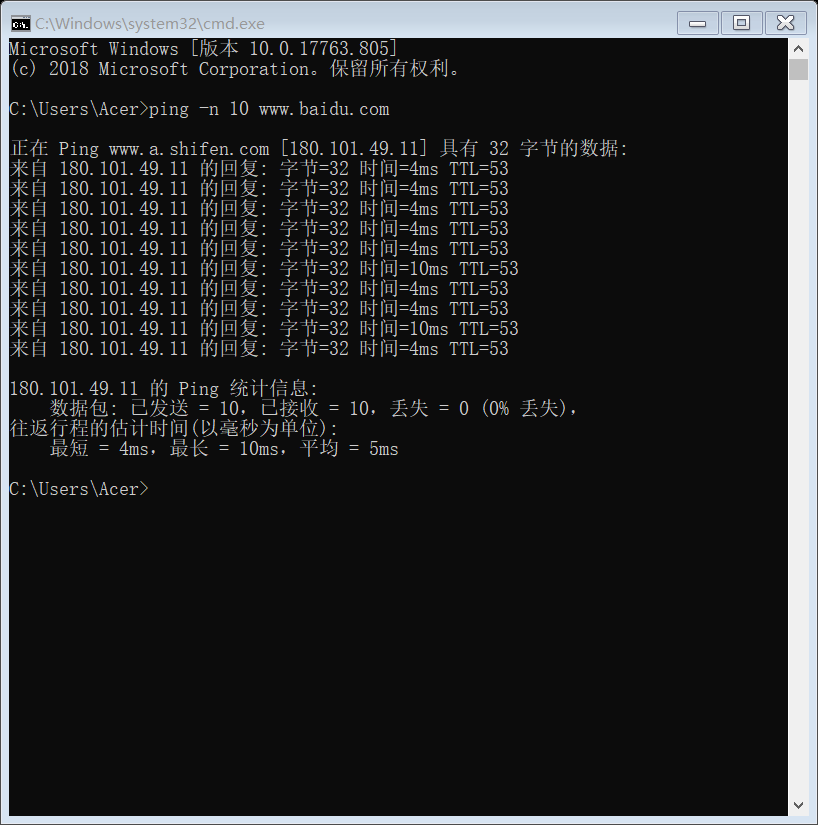
## 实验步骤：

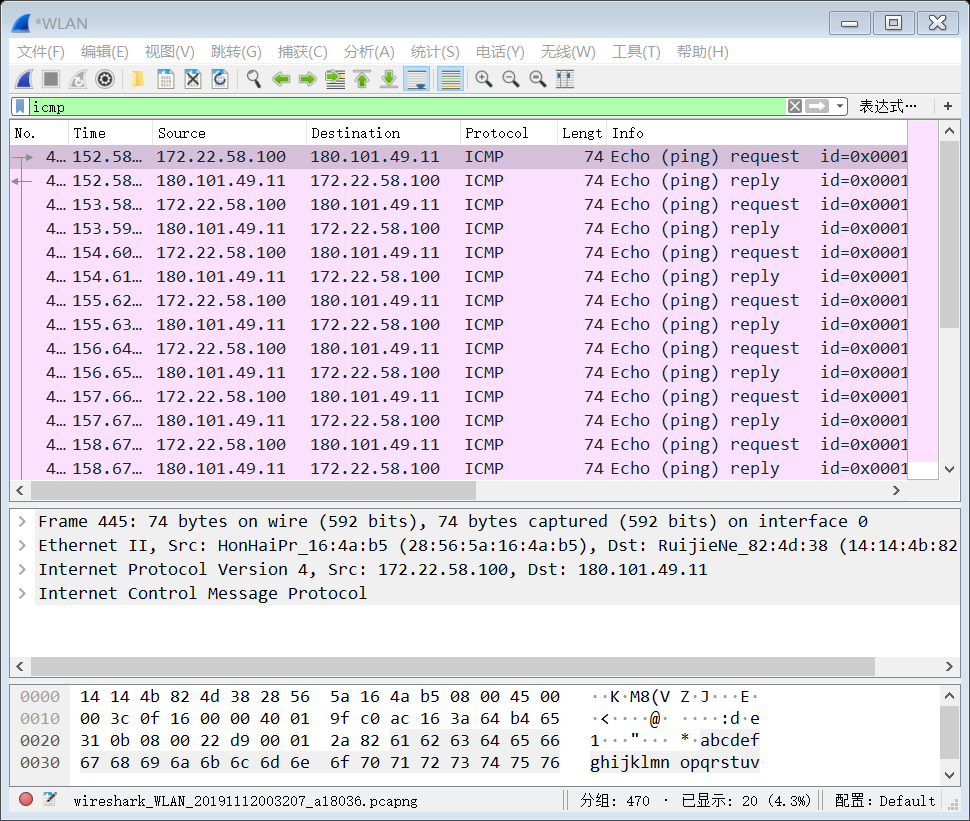
### 1．Ping和ICMP

1. 打开命令行窗口；
2. 启动wireshark，过滤窗口输入“icmp”，开始分组俘获



1. 输入“ping -n 10 hostname”
2. 当ping结束后，停止wireshark分组俘获

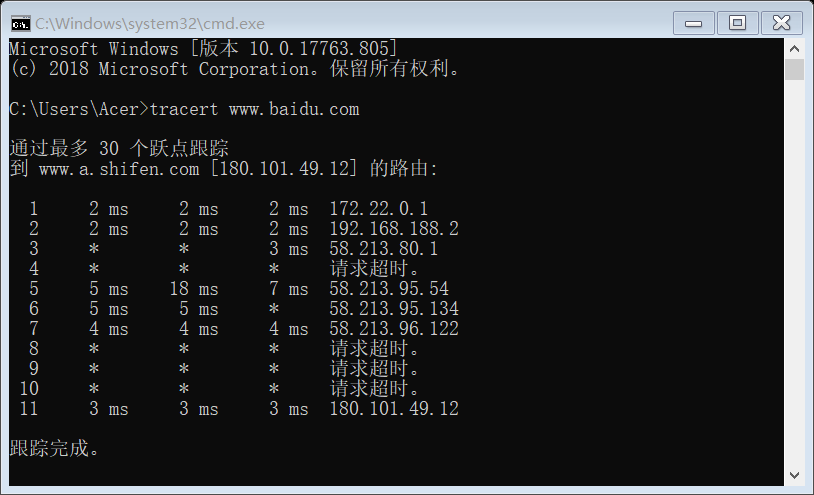


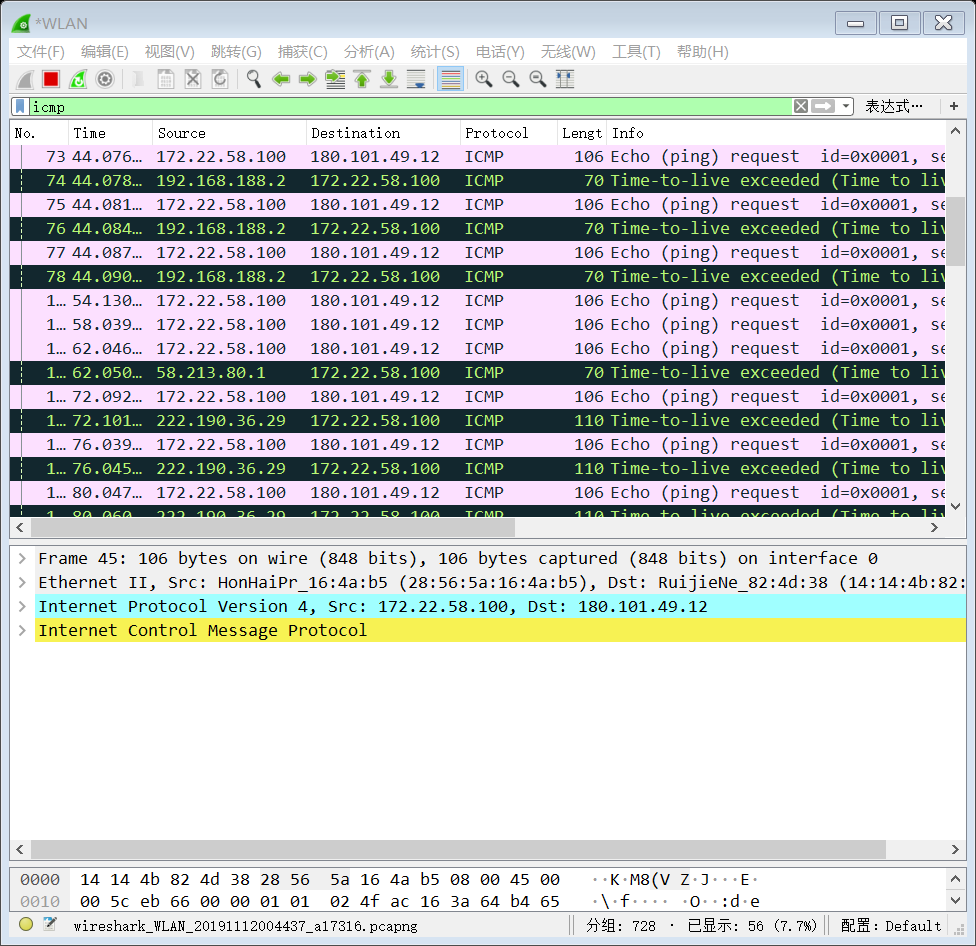


1. 问题答案
2. 所在主机IP地址：172.22.58.100，目的主机地址为180.101.49.11
3. ping请求分组，ICMP的Type和code是8，0
4. 响应信息，ICMP的type和code为0，0

### ２．ICMP和Traceroute

1. 启动Windows命令行提示符窗口
2. 启动Wireshark数据包嗅探器，开始分组俘获
3. 在MS DOS命令提示行下输入“tracert hostname”
4. 当tracertroute程序终止时，停止分组俘获

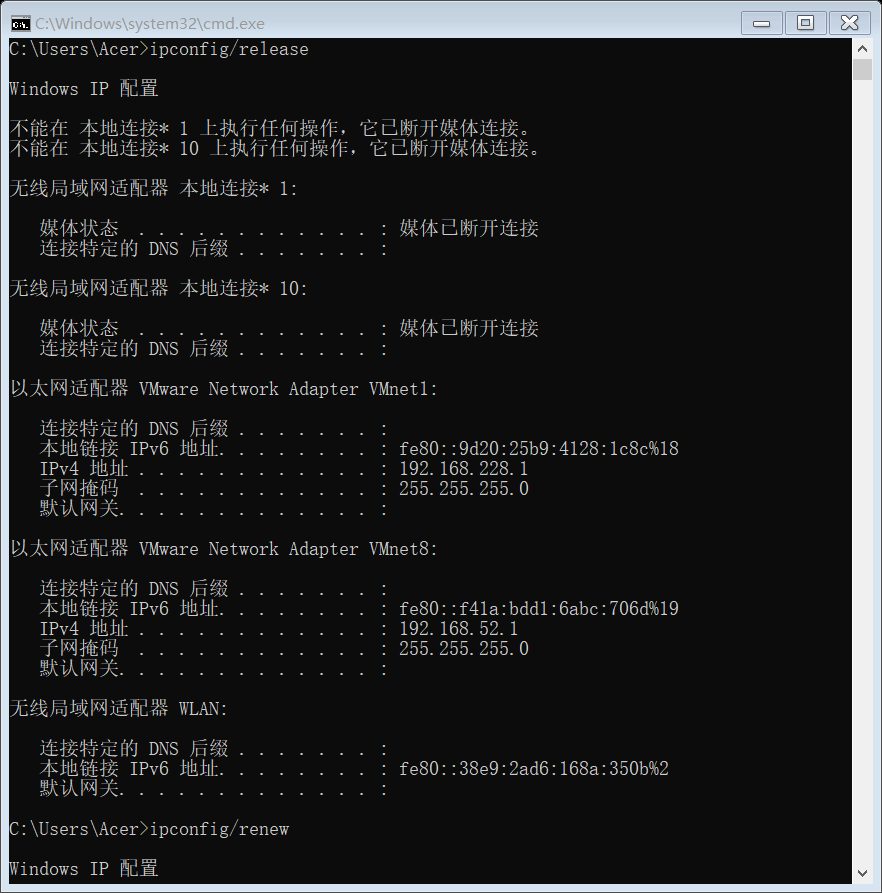




1. 回答问题
2. 不一样，之前数据部分是32bytes, 之后数据部分是64bytes
3. 多包含的信息有，时间信息，错误返回信息等

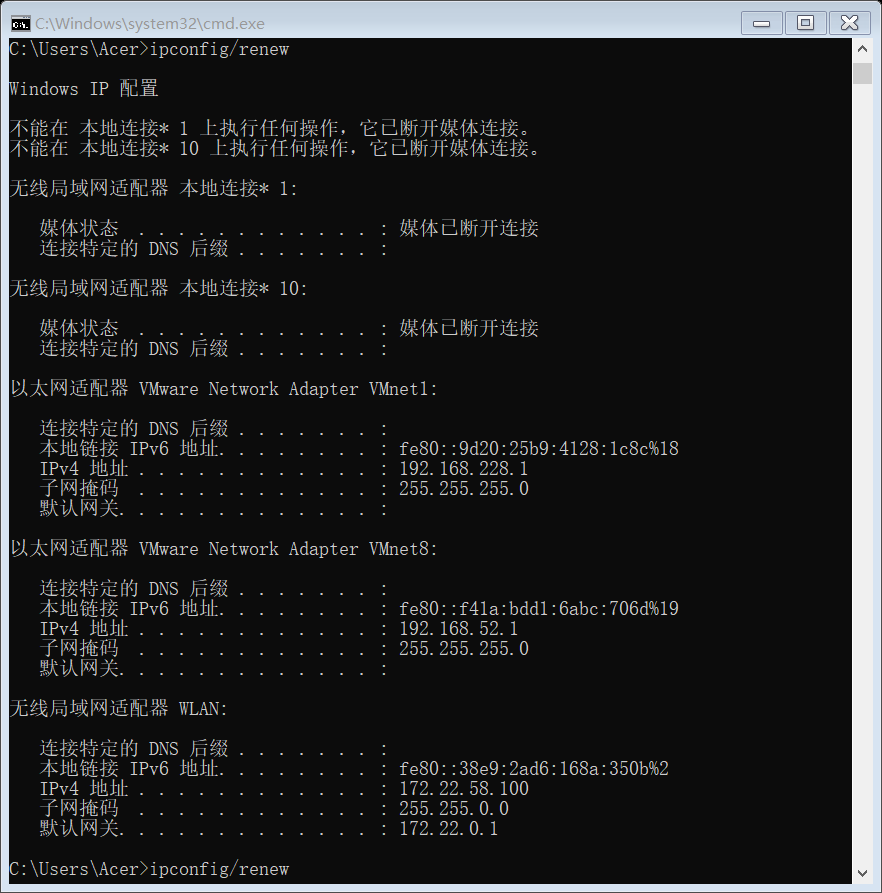
### 3．分析DHCP

（1）启动Windows命令行提示符窗口，输入“ipconfig/release”命令，释放主机当前的IP地址，此时主机IP地址变为0.0.0.0

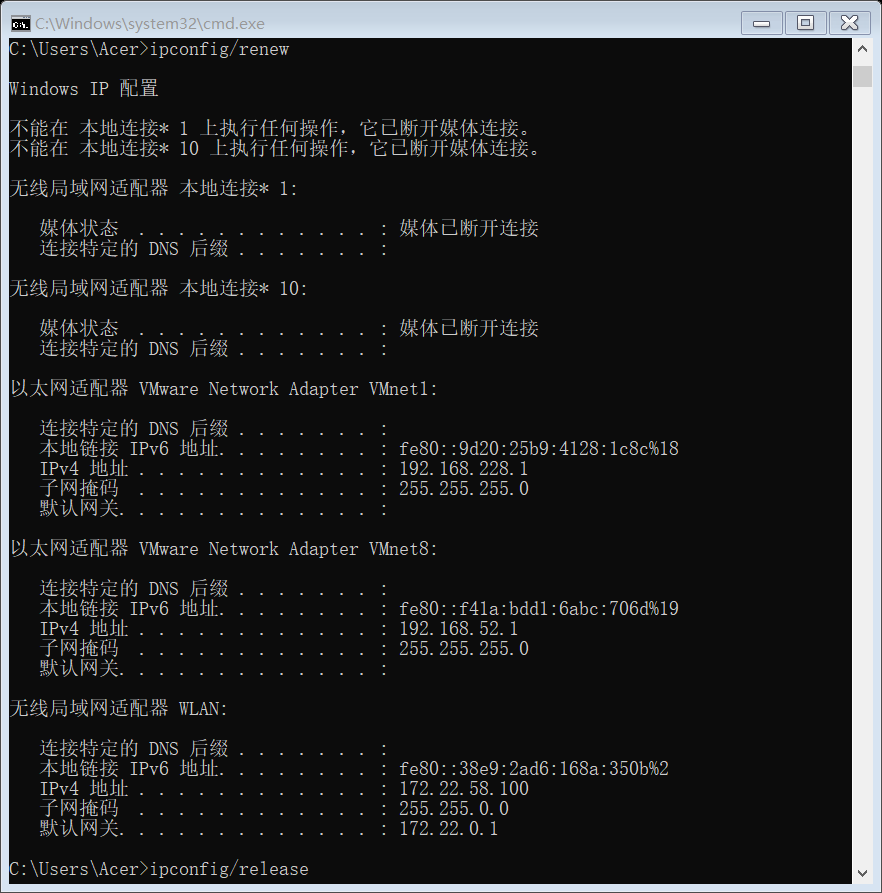


（2）启动Wireshark数据包嗅探器，开始分组俘获

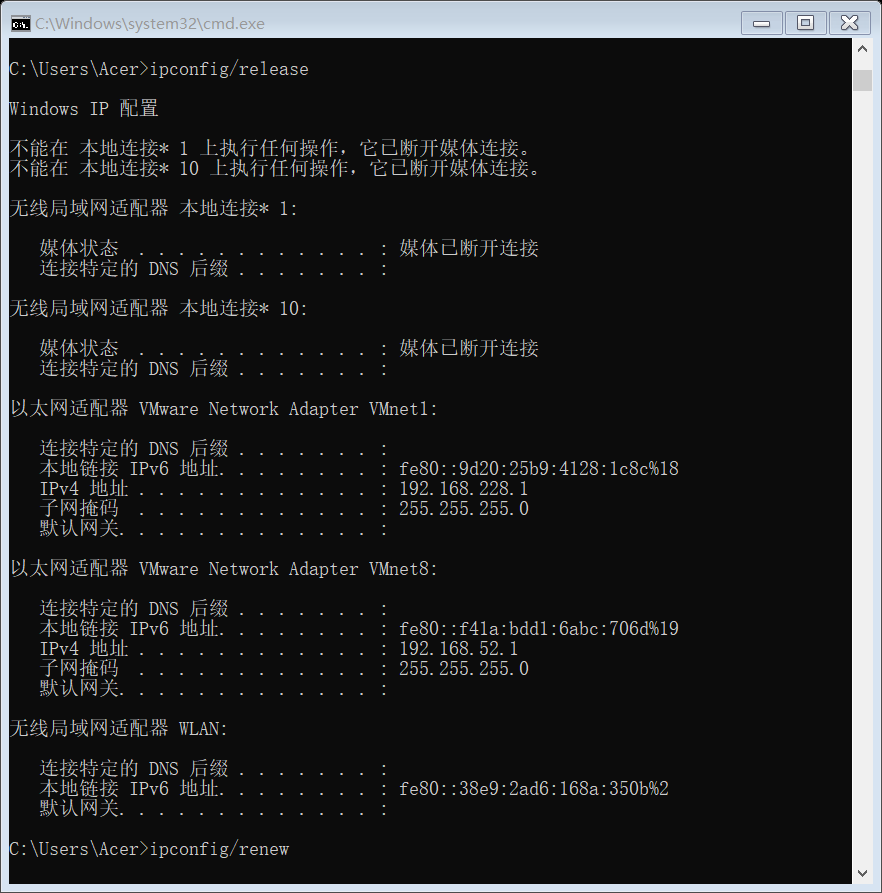
（3）返回命令提示符窗口，输入“ipconfig/renew”命令，获得一个网络配置



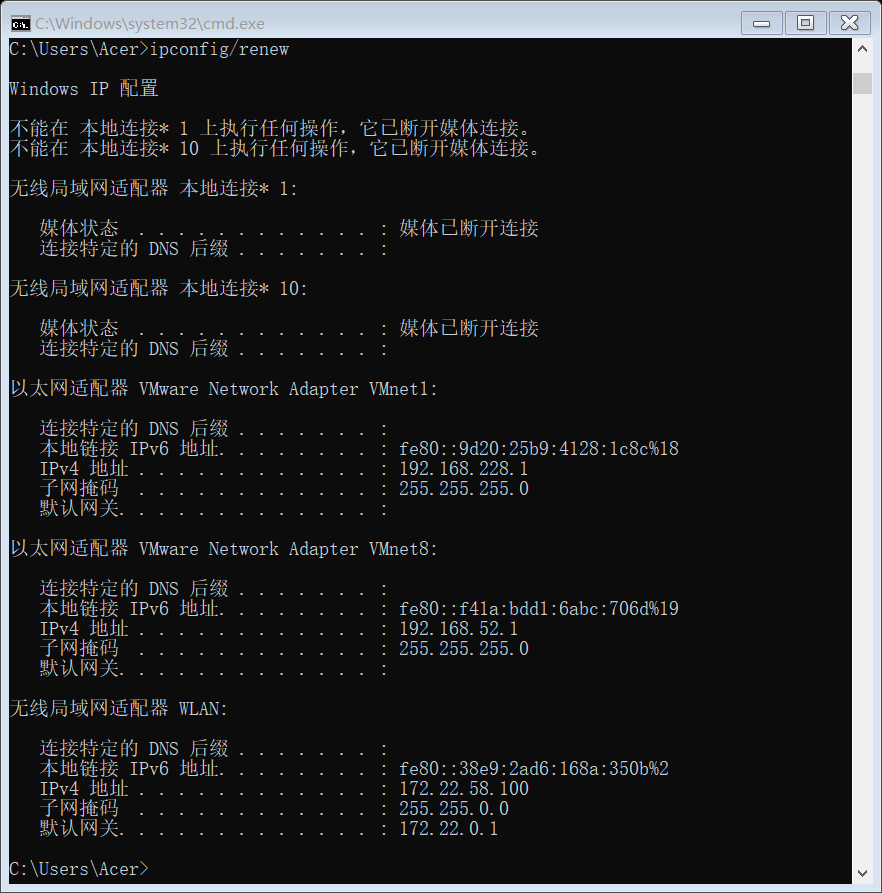
（4）等待一段时间后，再次输入“ipconfig/renew”命令；



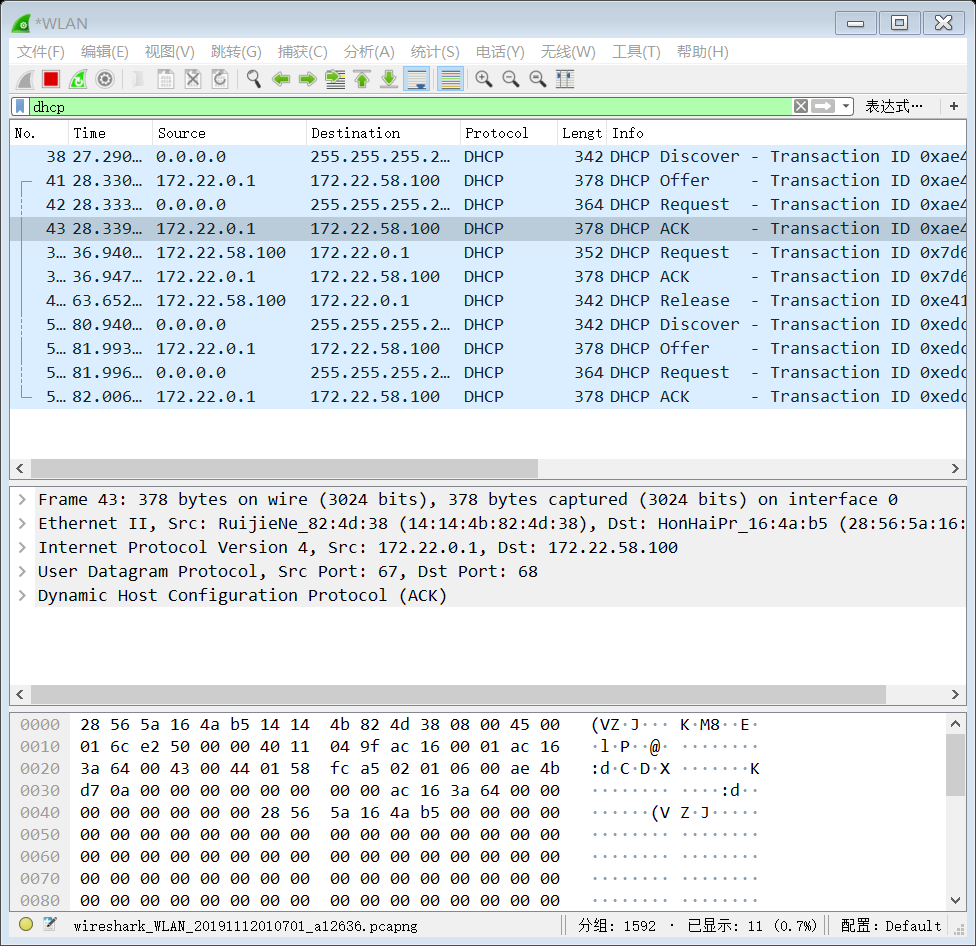
（5）当第二个“ipconfig/renew”命令终止时，输入命令“ipconfig/release”释放原来的已经分配的IP地址。



1. 最后，输入“ipconfig/renew”，再次给主机分配IP地址。



1. 停止分组俘获；



## 实验总结与体会：

１：实验遇到的问题：无

２：实验体会：本次实验较为简单，但是实验完成之后要注意分析和了解ICMP不同的分析方法以及DHCP的内容形式。

**ICMP类型**

| **TYPE** | **CODE** | **Description** | **Query** | **Error** |
| --- | --- | --- | --- | --- |
| 0 | 0 | Echo Reply——回显应答（Ping应答） | x |  |
| 3 | 0 | Network Unreachable——网络不可达 |  | x |
| 3 | 1 | Host Unreachable——主机不可达 |  | x |
| 3 | 2 | Protocol Unreachable——协议不可达 |  | x |
| 3 | 3 | Port Unreachable——端口不可达 |  | x |
| 3 | 4 | Fragmentation needed but no frag. bit set——需要进行分片但设置不分片比特 |  | x |
| 3 | 5 | Source routing failed——源站选路失败 |  | x |
| 3 | 6 | Destination network unknown——目的网络未知 |  | x |
| 3 | 7 | Destination host unknown——目的主机未知 |  | x |
| 3 | 8 | Source host isolated (obsolete)——源主机被隔离（作废不用） |  | x |
| 3 | 9 | Destination network administratively prohibited——目的网络被强制禁止 |  | x |
| 3 | 10 | Destination host administratively prohibited——目的主机被强制禁止 |  | x |
| 3 | 11 | Network unreachable for TOS——由于服务类型TOS，网络不可达 |  | x |
| 3 | 12 | Host unreachable for TOS——由于服务类型TOS，主机不可达 |  | x |
| 3 | 13 | Communication administratively prohibited by filtering——由于过滤，通信被强制禁止 |  | x |
| 3 | 14 | Host precedence violation——主机越权 |  | x |
| 3 | 15 | Precedence cutoff in effect——优先中止生效 |  | x |
| 4 | 0 | Source quench——源端被关闭（基本流控制） |  |  |
| 5 | 0 | Redirect for network——对网络重定向 |  |  |
| 5 | 1 | Redirect for host——对主机重定向 |  |  |
| 5 | 2 | Redirect for TOS and network——对服务类型和网络重定向 |  |  |
| 5 | 3 | Redirect for TOS and host——对服务类型和主机重定向 |  |  |
| 8 | 0 | Echo request——回显请求（Ping请求） | x |  |
| 9 | 0 | Router advertisement——路由器通告 |  |  |
| 10 | 0 | Route solicitation——路由器请求 |  |  |
| 11 | 0 | TTL equals 0 during transit——传输期间生存时间为0 |  | x |
| 11 | 1 | TTL equals 0 during reassembly——在数据报组装期间生存时间为0 |  | x |
| 12 | 0 | IP header bad (catchall error)——坏的IP首部（包括各种差错） |  | x |
| 12 | 1 | Required options missing——缺少必需的选项 |  | x |
| 13 | 0 | Timestamp request (obsolete)——时间戳请求（作废不用） | x |  |
| 14 |  | Timestamp reply (obsolete)——时间戳应答（作废不用） | x |  |
| 15 | 0 | Information request (obsolete)——信息请求（作废不用） | x |  |
| 16 | 0 | Information reply (obsolete)——信息应答（作废不用） | x |  |
| 17 | 0 | Address mask request——地址掩码请求 | x |  |
| 18 | 0 | Address mask reply——地址掩码应答 | x |  |