

**《计算机网络》实验报告**

(2022~2023 **学年第一学期**)

## 实验名称：Wireshark 软件使用与ARP协议分析

## 学 院：软件学院

## 姓 名：郁万祥

## 学 号：2013852 指导老师：张圣林

### 2022 年 11 月 13

实验名称 (实验 1:Wireshark 软件使用与 ARP

协议分析)

# 实验目的

学习 Wireshark 的基本操作，抓取和分析有线局域网的数据包；掌握以太网 MAC 帧的基本结构，掌握 ARP 协议的特点 工作过程。

# 实验条件

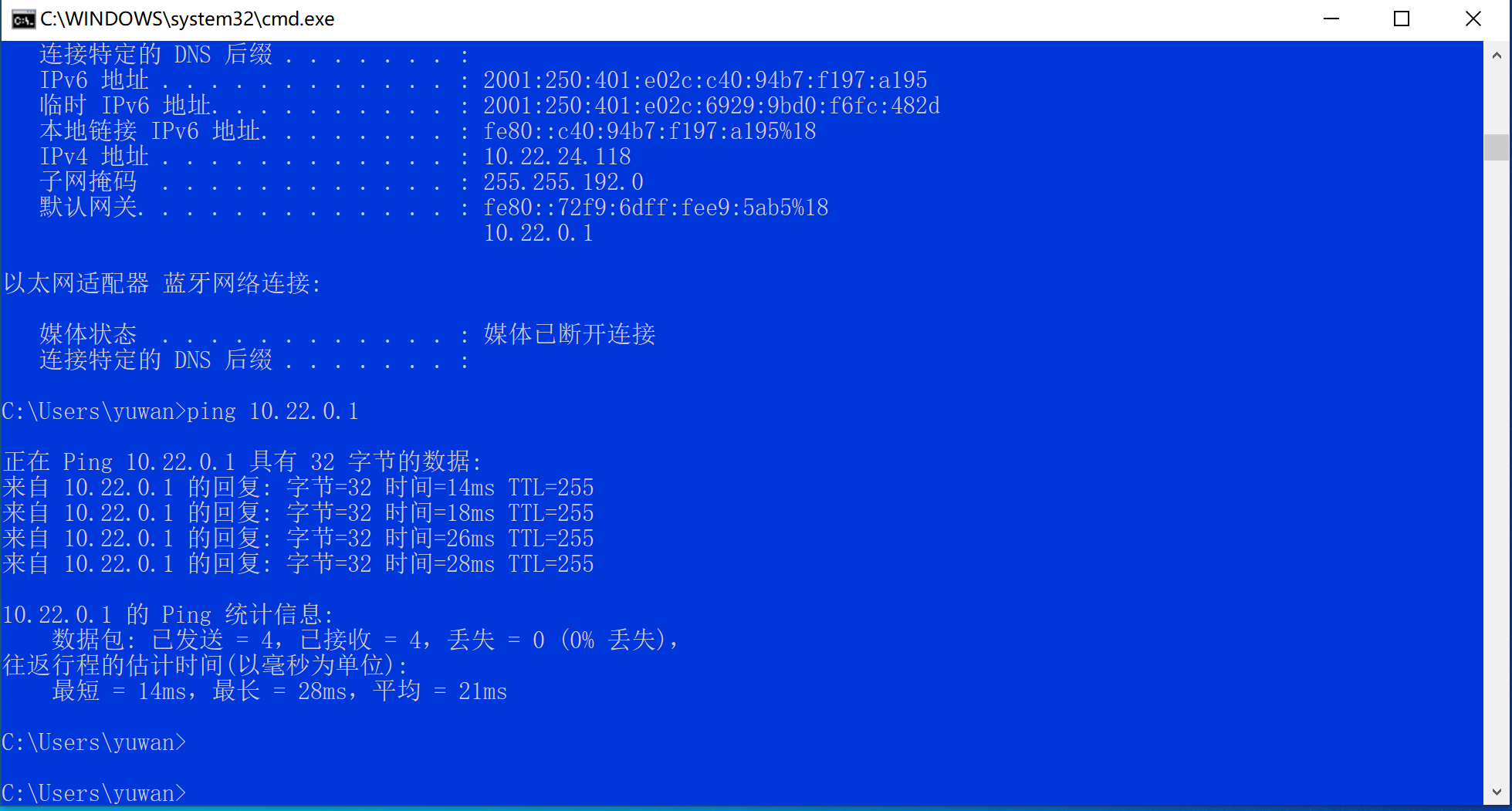
设备：PC 机一台，连入局域网

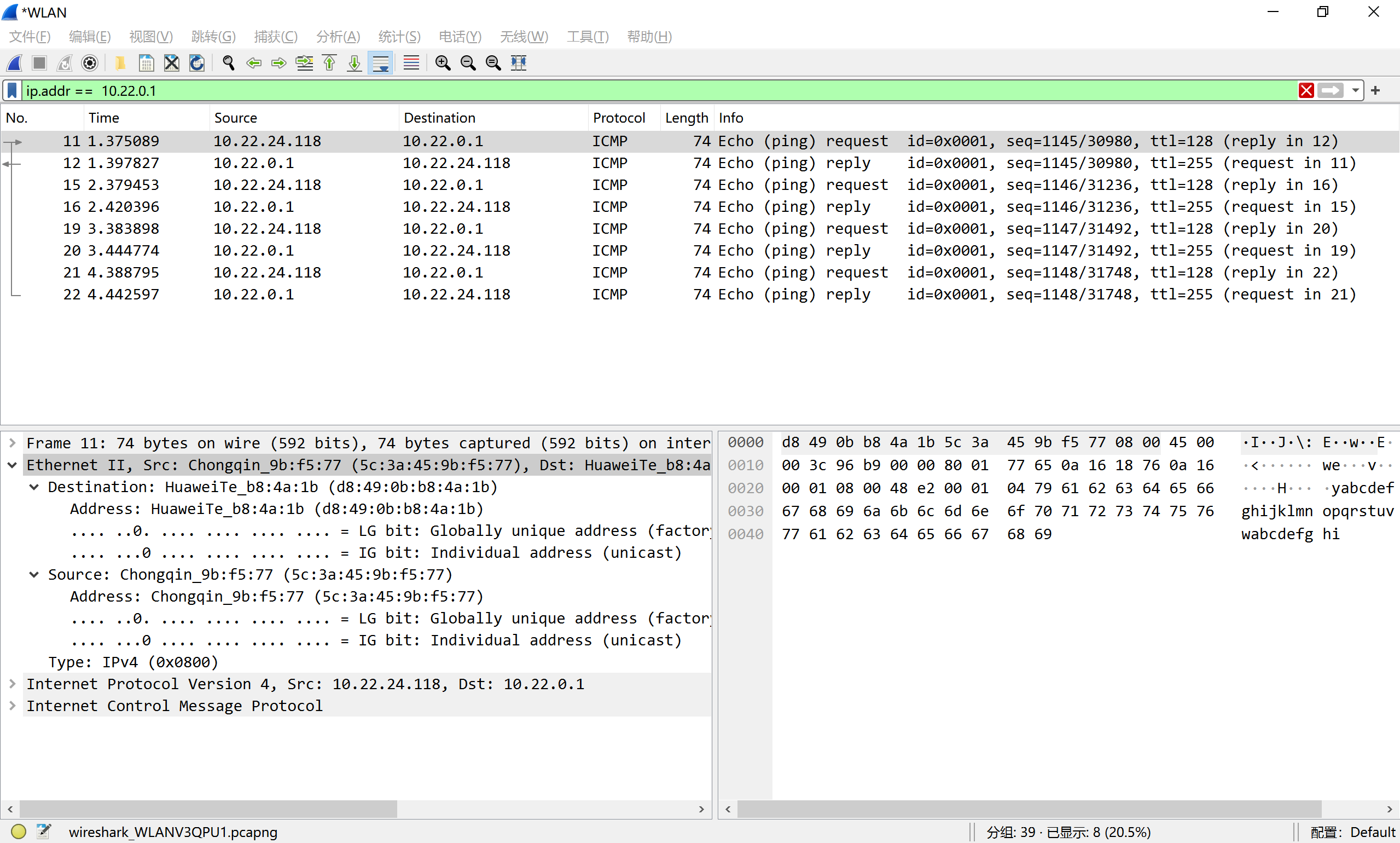
所用工具：VirtualBox、Wireshark、eNSP、WinPcap

# 实验报告内容及原理

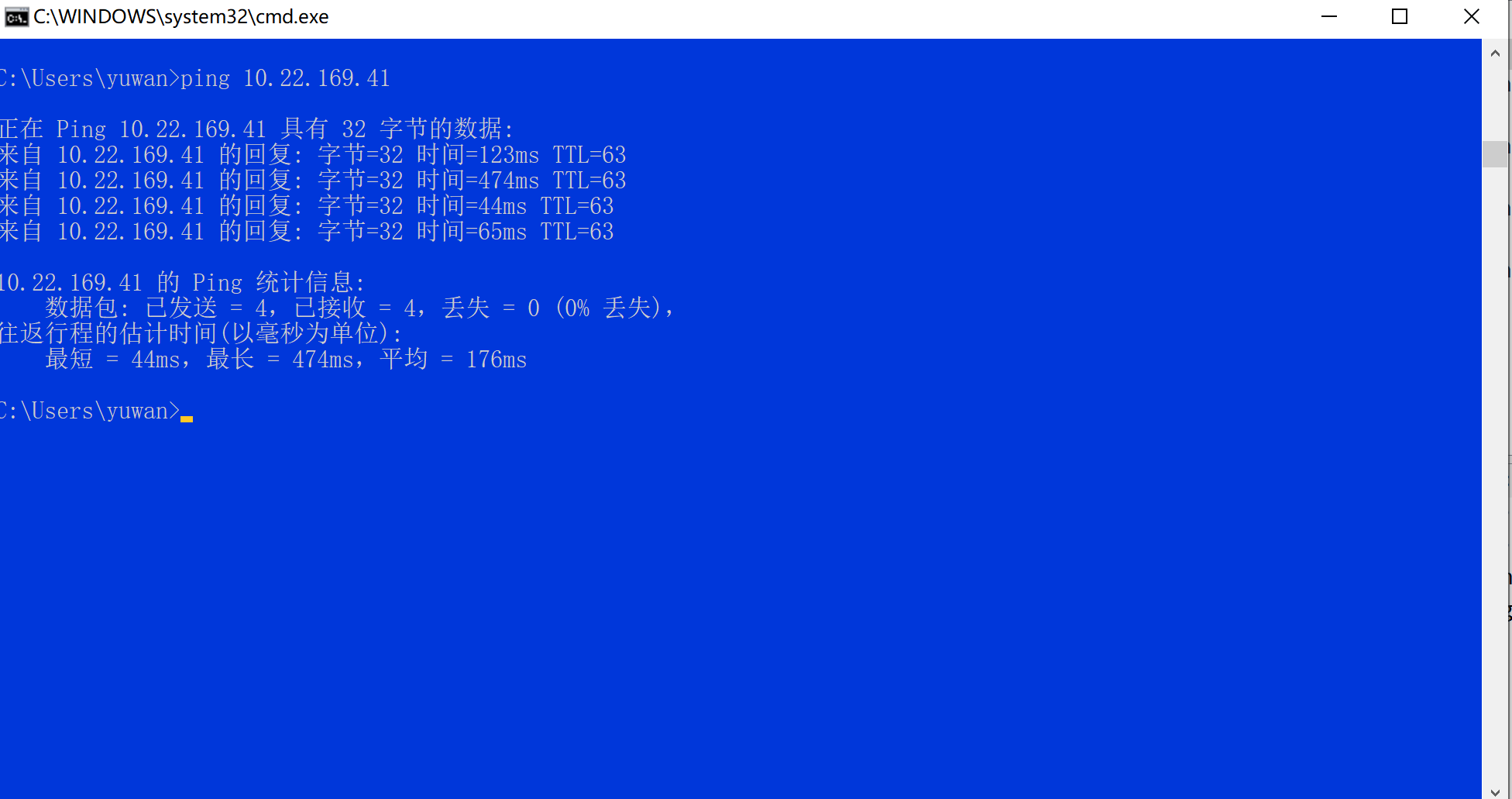
1. **学习 Wireshark 基本操作：重点掌握捕获过滤器和显示过滤器。**
2. **观察 MAC 地址，启动 Wireshark 捕捉数据包，在命令行窗口分别 ping 网关和 ping 同网段的一台主机，分析本机发出的数据包。重点观察以太网帧的 Destination 和 Source 的 MAC 地址，辨识 MAC 地址类型，解读 OUI 信息、I/G 和 G/L 位。**

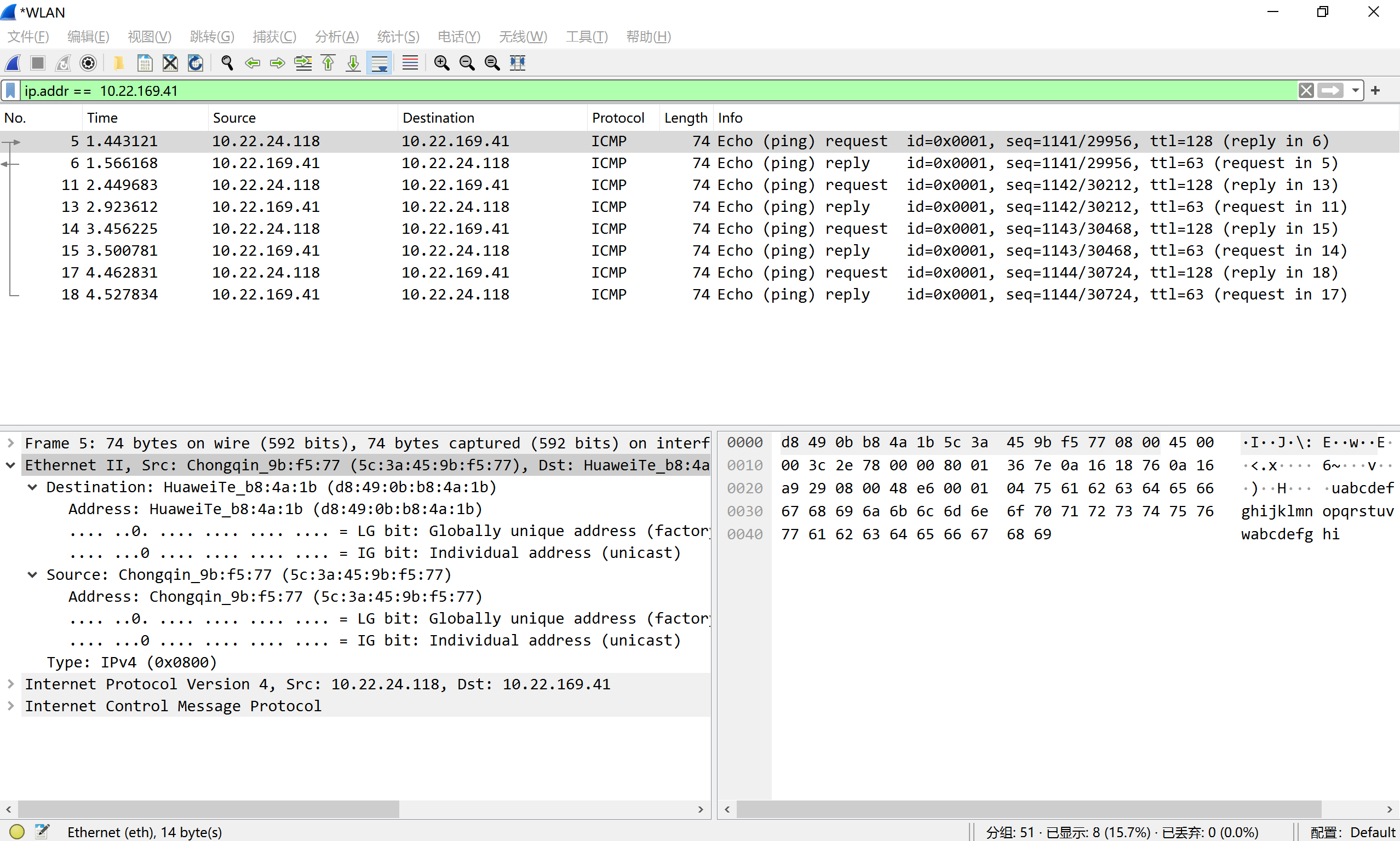
**2.1、ping 网关**：（如果观察自己发出的数据包的，命令为：ip.src==10.22.24.118 and ip.dst==10.22.0.1）Ping 同网段的一台主机（：如果观察自己发出的数据包的，命令为：ip.src==10.22.24.118 and ip.dst ==10.22.169.41）





**2.2、Ping同网段的一台主机**：（如果观察自己发出的数据包的，命令为：ip.src==10.22.24.118 and ip.dst ==10.22.169.41）





**2.3辨识MAC地址类型：**

本机MAC地址为：5c：3a：45：9b：f5：77，

根据第一个字节5c，转换为二进制为1011100，所以最低位为0，MAC地址为单播MAC地址，

网关MAC地址为：d8：49：0b：b8：4a：1b，

根据第一个字节d8，转换为二进制为11011000，所以最低位为0，MAC地址为单播MAC地址。

**2.4解读OUI信息：**

一个制造商在生产制造网卡之前，必须先向IEEE注册，以获取到一个长度为24bit的厂商代码， 也就是OUI，对于单播MAC地址而言，前三个字节就是OUI信息，也就是厂商代码。

本机MAC地址前三个字节为：5c：3a：45，对应到截图中的Chongqin\_9b:f5:77。

网关的MAC地址前三个字节为：d8：49：0b，对应到截图中的HuaweiTe\_b8：4a：1b。

**2.5解读I/G和G/L位：**

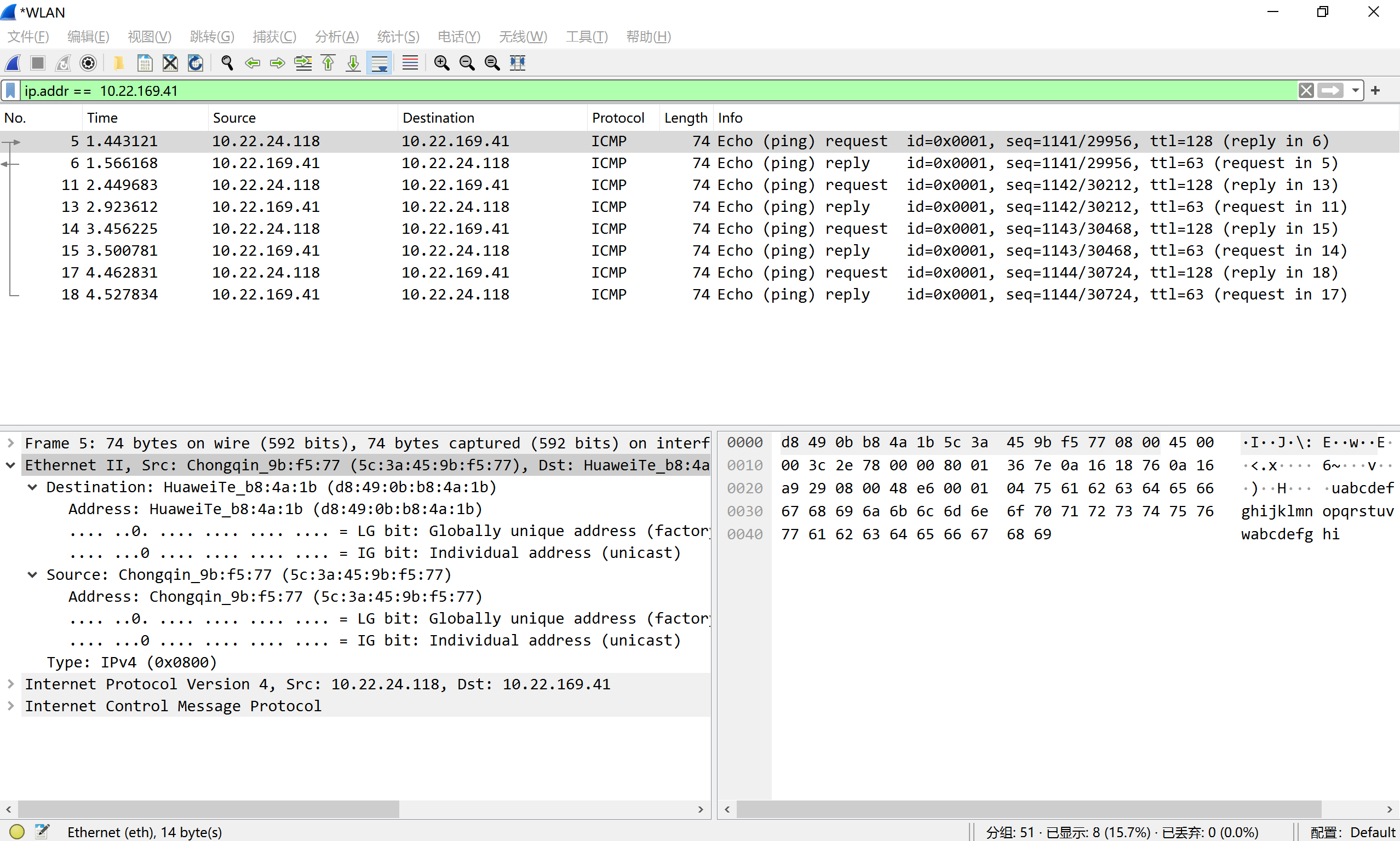
I/G位，如果为0，则是某台设备的MAC地址，即单播地址，如果为1，则是多播地址。

G/L位：如果为0，则是全局管理地址，由IEEE分配，如果为1，时忘了管理员为了加强自己对 网络管理而指定的地址。

I/G位和G/L位在MAC地址的第一个字节的最低为和次低位。

因此我们可以看到，无论是5c（1011100）：3a：45：9b：f5：77，还是d8（11011000）：49： 0b：b8：4a：1b，I/G位与G/L位都是0。

1. **分析以太网的帧结构，MAC 地址类型、头部信息、长度及封装**



类型为IPv4

源MAC地址

目的MAC地址

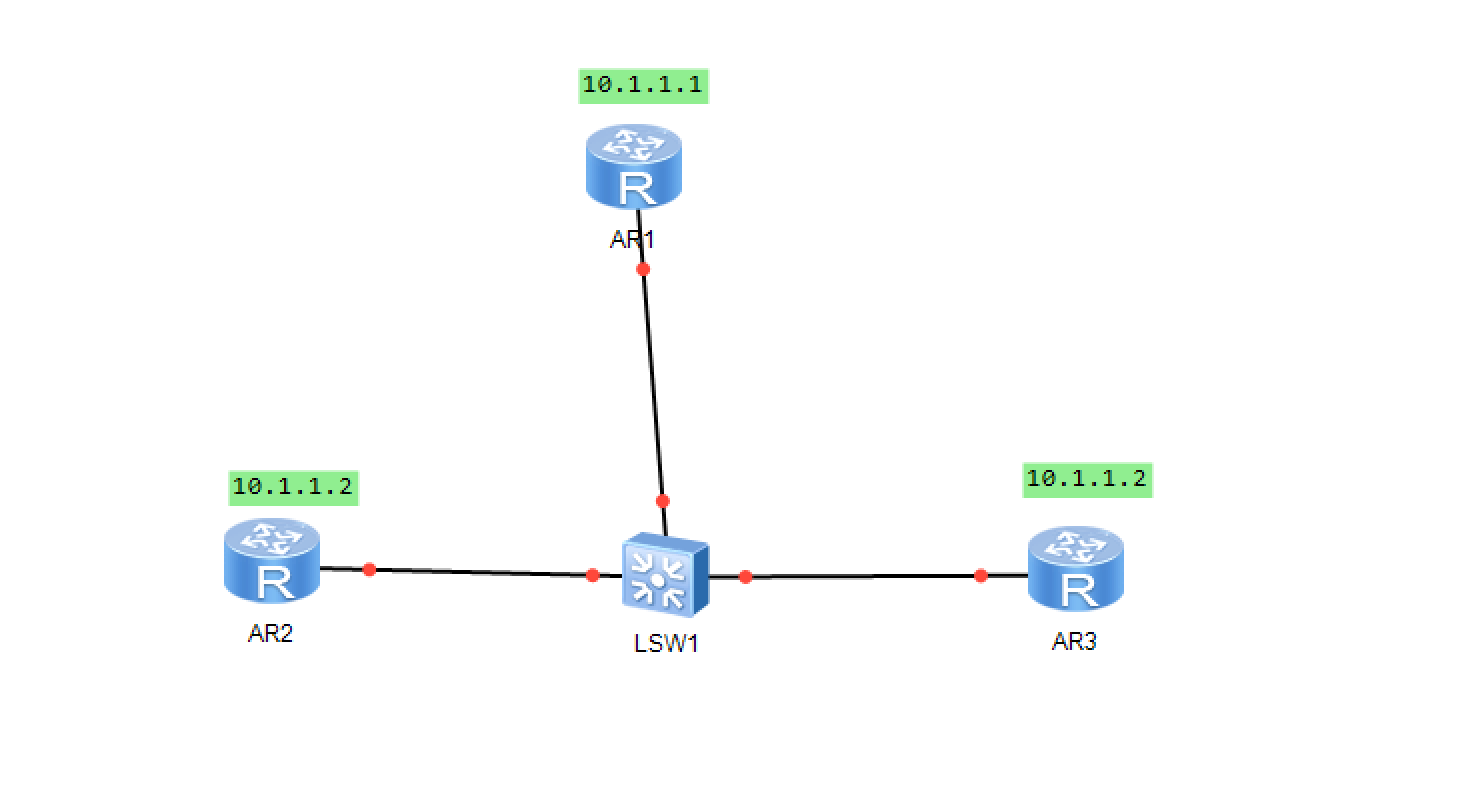
以太帧头部信息

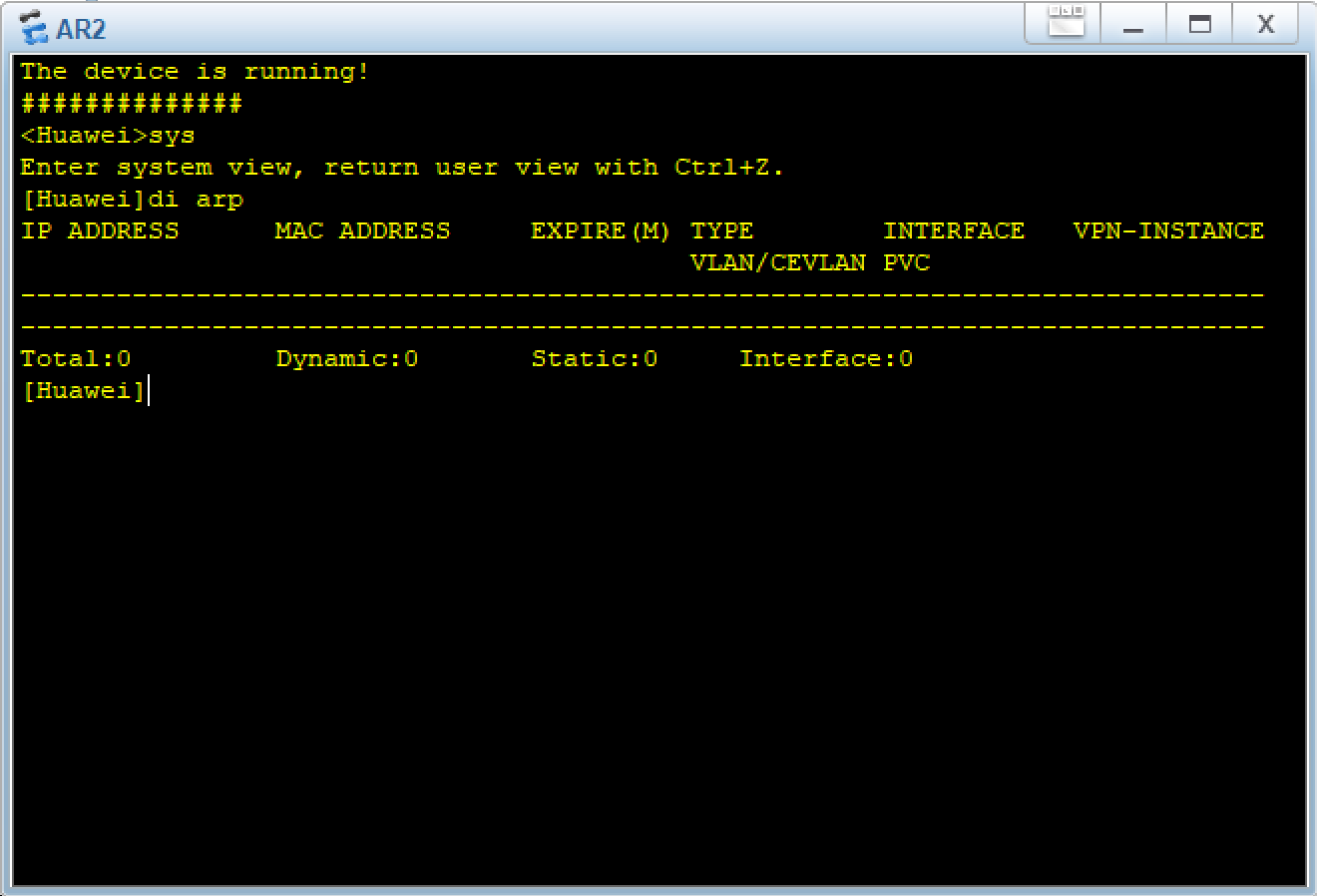
以太帧总信息，长度为74474747474bytes

**4、结合捕捉的网络数据，分析 ARP 数据包，描述 ARP 协议工作过程；**

**4.1 使用ensp创建拓扑，启动，并观察arp缓存表**

使用命令：di arp ：查看arp缓存表



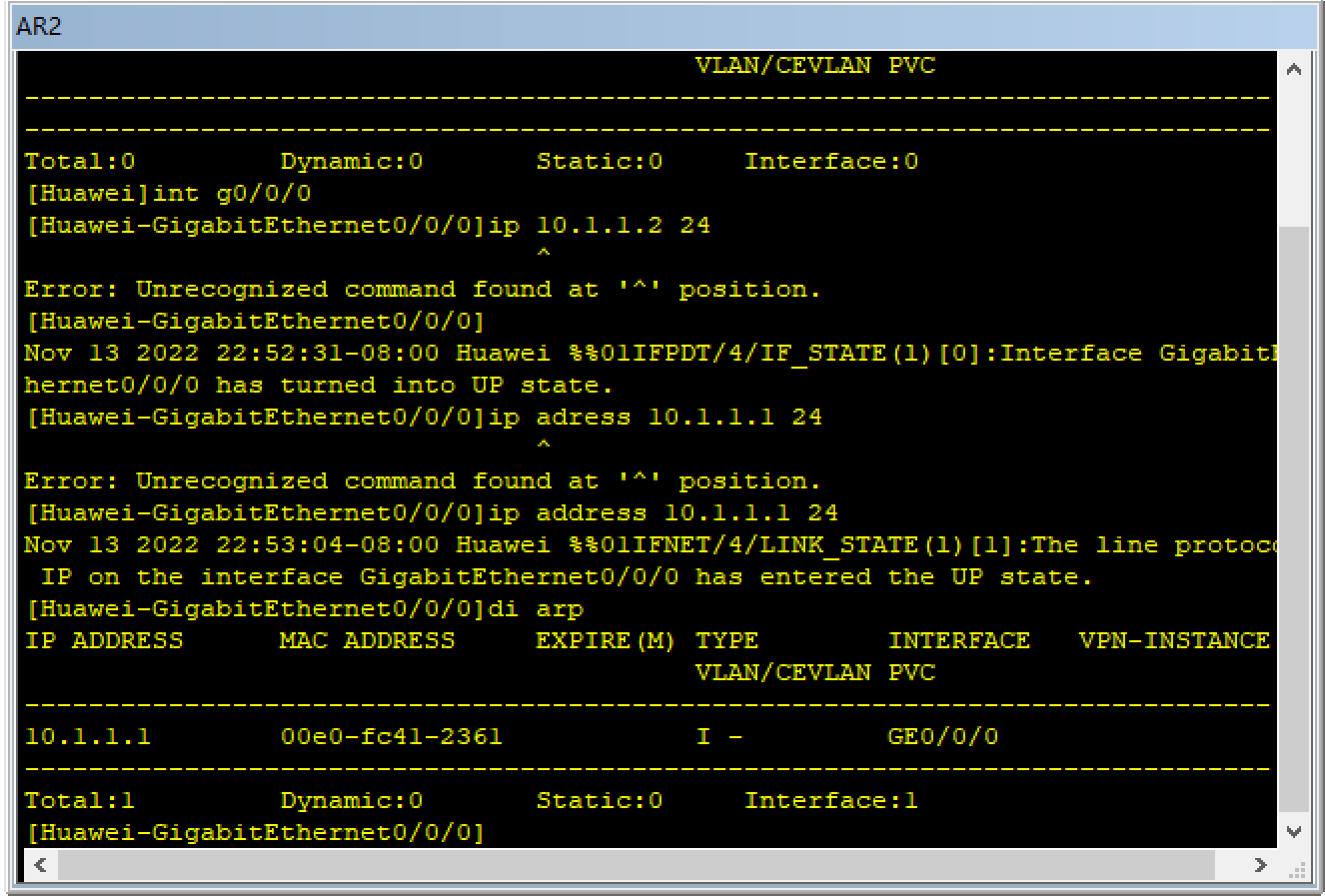


**此时arp缓存表中没有数据**

**4.2 对于路由器的端口进行IP地址和掩码的设置、在观察arp缓存表**

使用命令

1. int g0/0/0 ：进入端口
2. ip 10.1.1.1 24 ：设置ip地址和掩码



**此时arp缓存表中只存在本机的arp地址。**

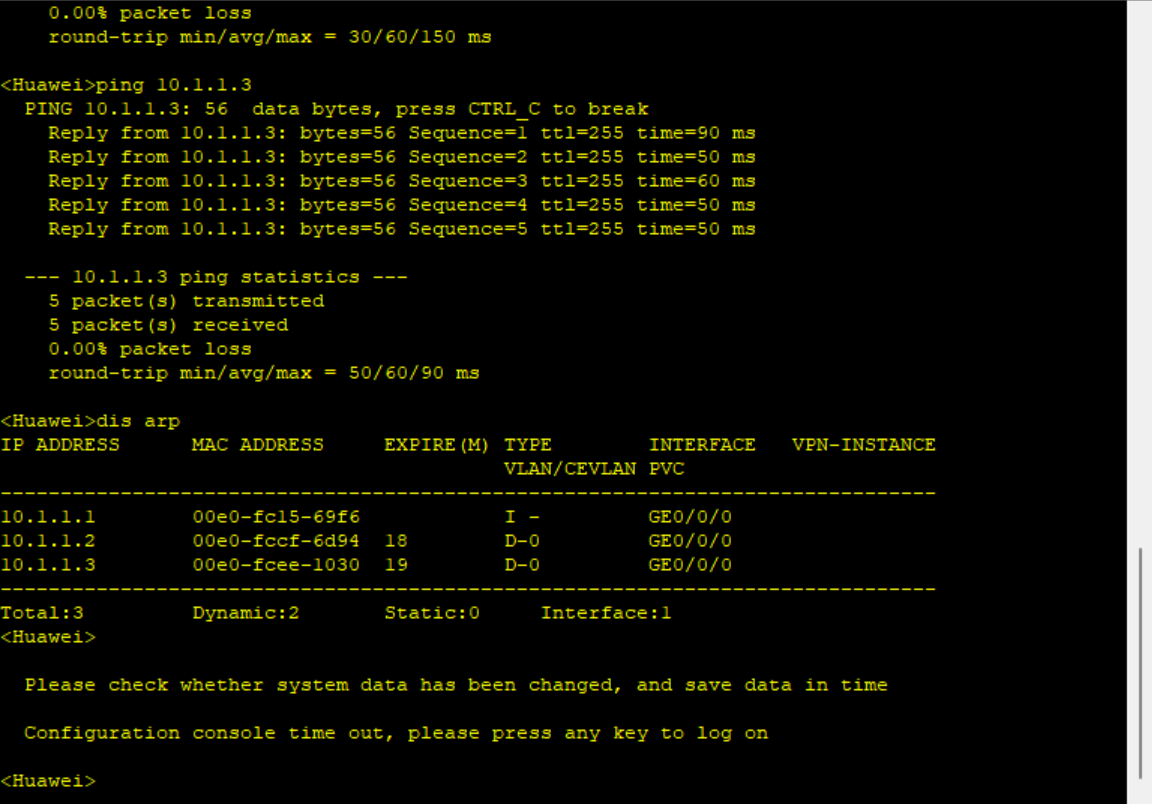
**4.3 对同一网段的ip地址进行ping命令**

使用上述设置的10.1.1.1 分别对10.1.1.2、10.1.1.3 继续ping，之后观察arp协议包，以及查看10.1.1.1的arp缓存表

在arp1中继续命令：

Ping 10.1.1.2

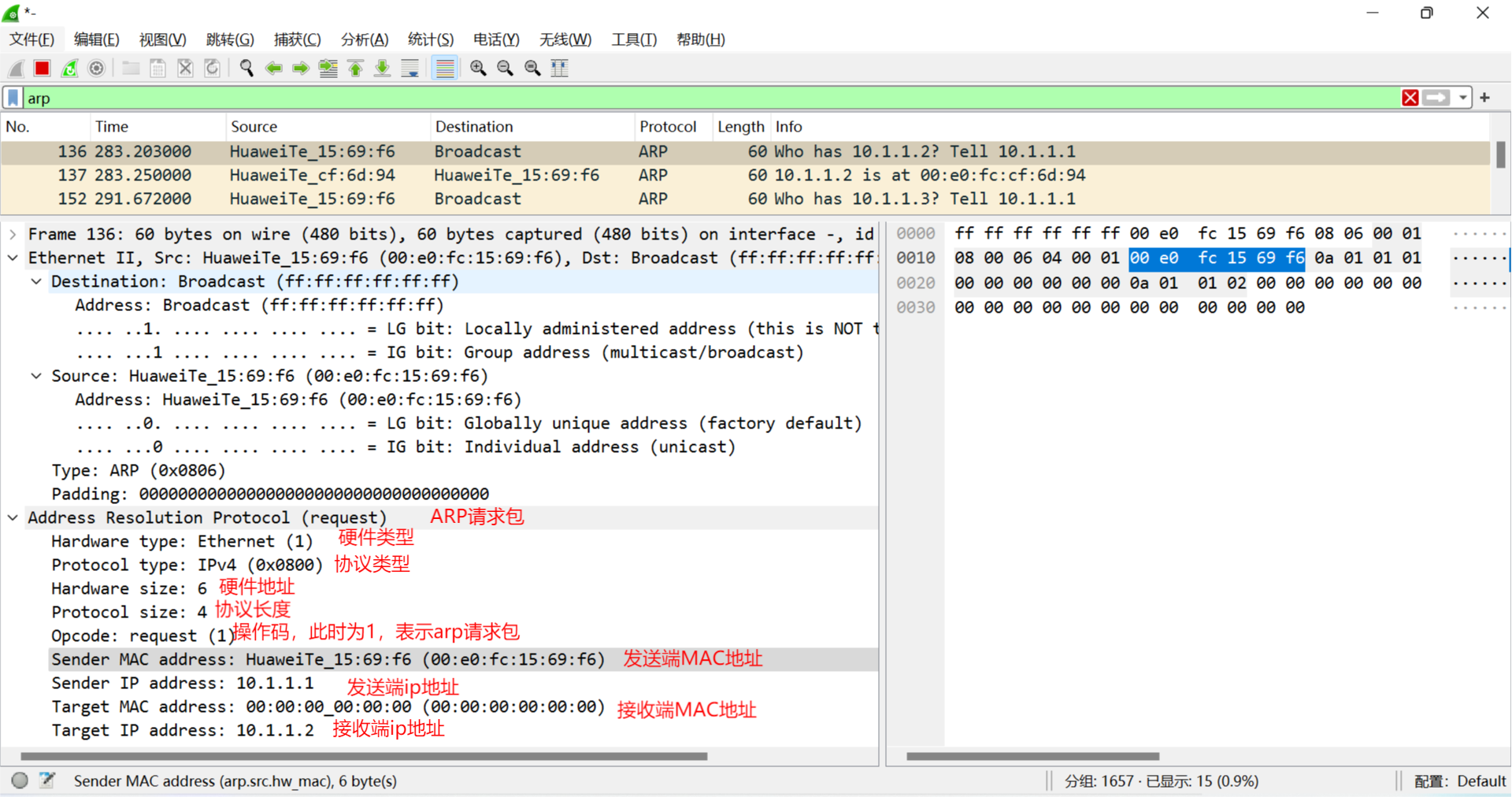
Ping 10.1.1.3



**此时可以看到在端口的arp缓存表中同时存在10.1.1.1、10.1.1.2、10.1.1.3**

**4.4 抓取arp包，对arp数据包进行分析。**

在过滤器中使用代码：arp 进行arp包的抓取。



源MAC地址

广播，目标MAC地址为：ff:ff:ff:ff:ff:ff

头部信息

第一帧报文详细信息，长度为136

**因此我们分析arp协议工作过程：**

1)、 如果主机A想发送数据给主机B，主机A首先会检查自己的ARP缓存表，查看是否有主机B的IP地址和MAC地址的对应关系，如果有，则会将主机B的MAC地址作为源MAC地址封装到数据帧中。如果没有，主机A则会发送一个ARP请求信息，请求的目标IP地址是主机B的IP地址，目标MAC地址是MAC地址的广播帧(即FF-FF-FF-FF-FF-FF)，源IP地址和MAC地址是主机A的IP地址和MAC地址。

2)、 当交换机接受到此数据帧之后，发现此数据帧是广播帧，因此，会将此数据帧从非接收的所有接口发送出去。

3) 、当主机B接受到此数据帧后，会校对IP地址是否是自己的，并将主机A的IP地址和MAC地址的对应关系记录到自己的ARP缓存表中，同时会发送一个ARP应答，其中包括自己的MAC地址。

4）、主机A在收到这个回应的数据帧之后，在自己的ARP缓存表中记录主机B的IP地址和MAC地址的对应关系。而此时交换机已经学习到了主机A和主机B的MAC地址了。

4.5 **ping不同网关的ip地址**，过程与上述一致（判断是否为同一网关的根据：ip地址与子码掩码每一位and，转换为十进制，就是网络表示，网络标识一致，就是同一网关）

**不同网关arp工作协议：**

1）、如果主机A要ig主机C,那么主机A发现主机C的IP和自己不是同一网段，他就去找网关转发，但是他也不知道网关的MAC地址情况下呢？他就会向之前那个步骤一样先发送一个ARP广播，学到网关的MAC地址，再发封装ICMP报文给网关路由器。

2）、当路由器收到主机A发过来的CMP报文，发现其目的地址是本身MAC地址，根据目的的P2.1.1.1,查路由表，发现2.1.1.1/24的路由表项，得到一个出端口，去掉原来的MAC头部，加上自己的MAC地址向主机C转发。（如果网关也没有主机C的MAC地址，还是要向前面一个步骤一样，ARP广播一下即可相互学到。路由器2端口能学到主机D的MAC地址，主机D也能学到路由器2端口的MAC地址。

3）、最后，在主机C已学到路由器2端口MAC地址，路由器2端口转发给路由器1端口，路由1端口学到主机A的MAC地址的情况下，他们就不需要再做ARP解析，就将CMP的回显请求回复过来。

# 实验结论及心得体会

本次实验，通过ensp模拟，实现多台路由器之间的通信，从而获取arp数据包，并对arp数据包的结果进行了分析，同时对于同一网关内的arp协议工作方式和不同网关的arp协议工作方式进行了研究。进一步理解了arp协议的工作原理以及方式。

实验中，需要通过改变掩码，从而实现建立不同网关的ip地址，然而，在同一网关ip地址ping成功后，不同网关的ip地址有时候并不能够ping成功，对这个问题我会有这样的设想：哪里出现了问题，是否说明一定是链路没有连通的情况，经过网上搜索资料，其实发现这并不是严谨的：首先，Ping功能发送的是ICMP包，并不是完整的TCPP议包，如果没有三层交换机Q路由Ping功能得出结论就有待商榷。假如你Ping的是和本机同一网段的P地址，如果Ping不通，目的IP与本地链路不通，结论成立。如果Pig的目的P地址与本地lP地址不在同一网段，比如说本地1P地址为：192.168.2.106，目的P地址为：192.168.20.157，使用PIg功能，两个主机相互Ping,如果Ping不通，不能得出两者连路不通的说法。