电子科技大学信息与软件工程学院

**实 验 报 告**

学 号 2017221302009

姓 名 陆圣珩

（实验） 课程名称 计算机网络

理论教师 刘梦娟

实验教师 刘梦娟

**电子科技大学教务处制表**

**电 子 科 技 大 学**

**实 验 报 告**

**学生姓名：陆圣珩 学号：2017221302009 指导教师：刘梦娟**

**实验地点：信软楼西305 实验时间：2019.4.26**

**一、实验名称：网络层协议验证实验**

**二、实验学时：2学时**

**三、实验目的：**

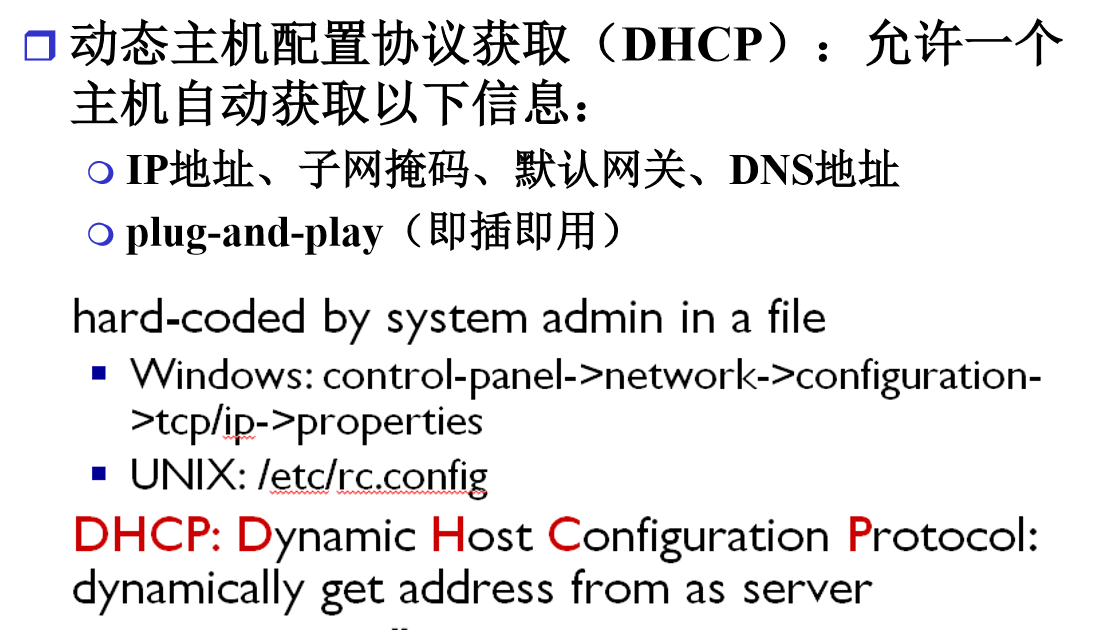
掌握网络层头部的基本格式

掌握DHCP协议的交互过程以及报文格式

掌握NAT的基本原理。

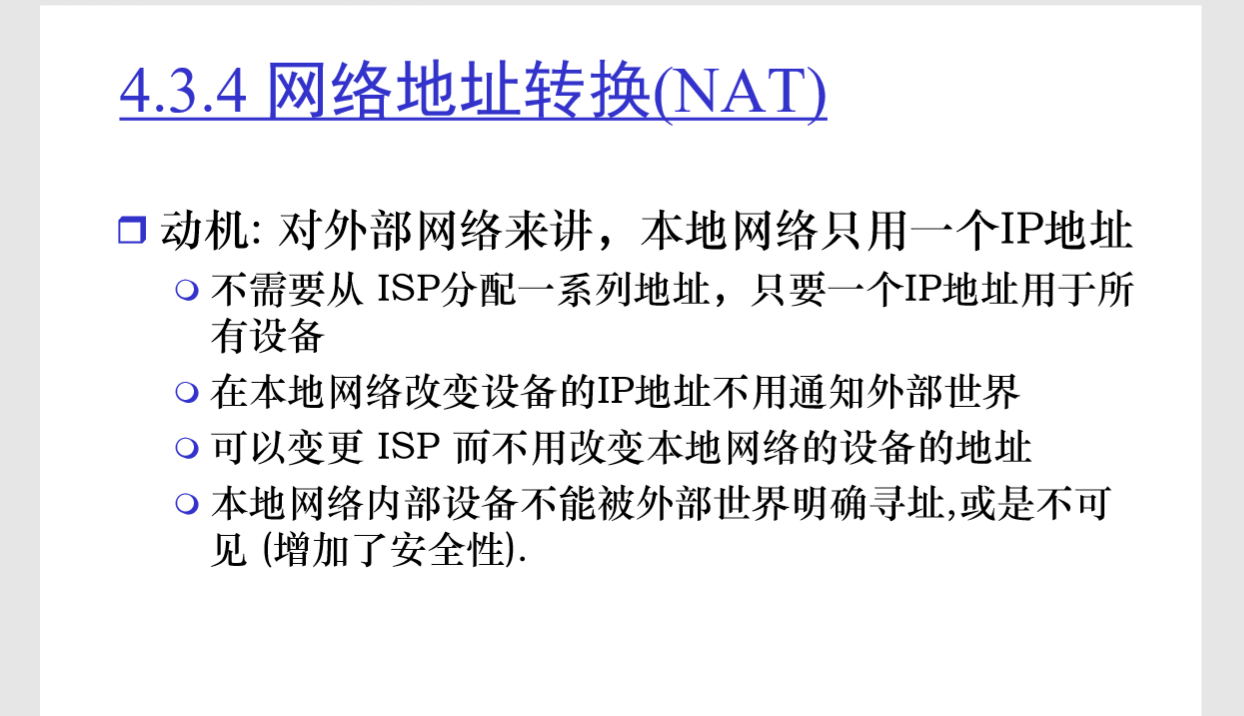
**四、实验原理：**

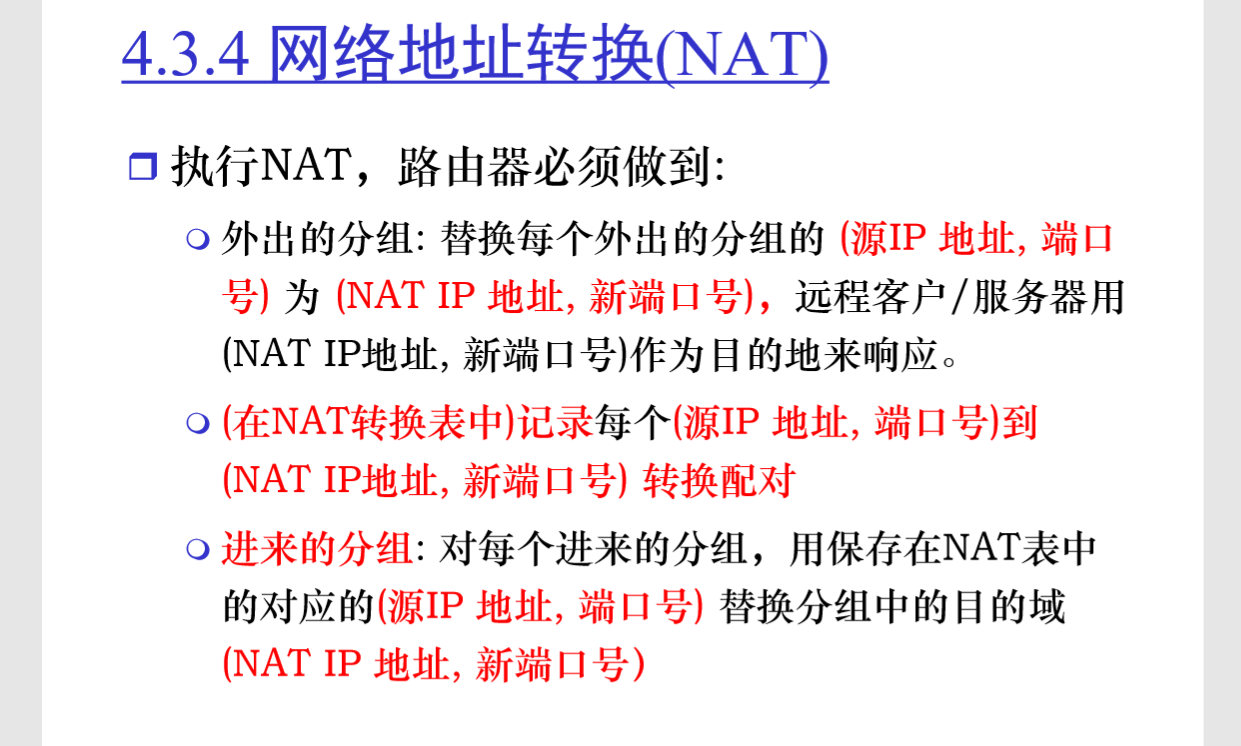
**DHCP协议的工作原理**

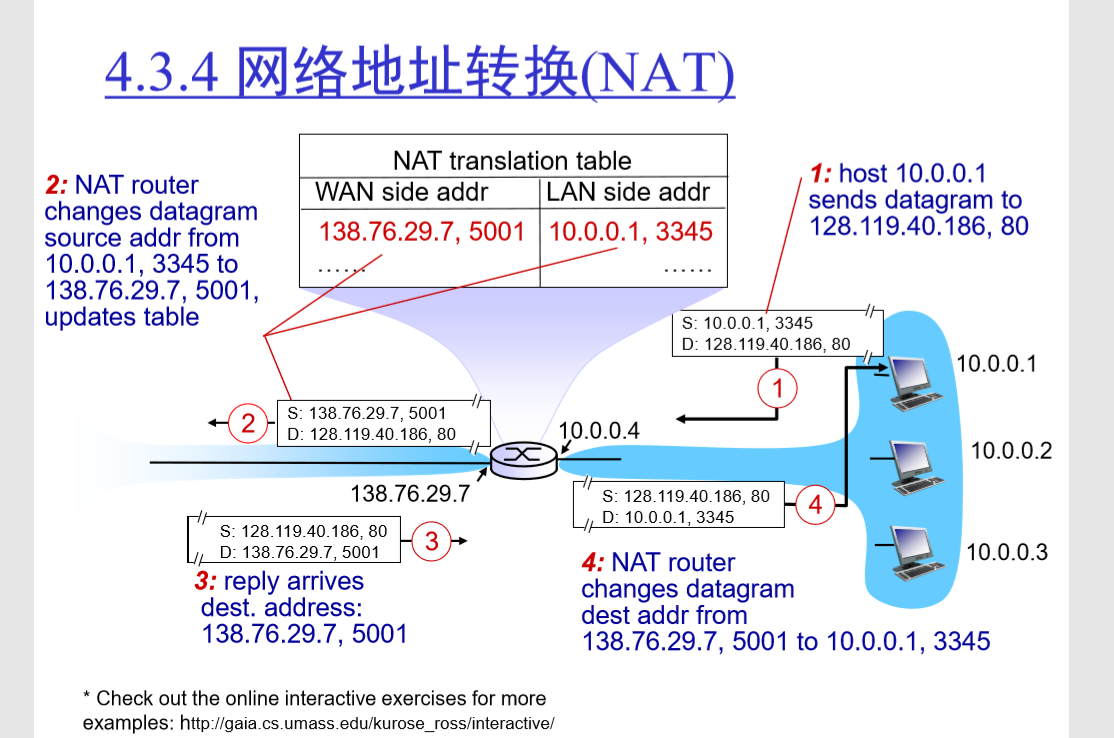




**NAT协议的工作原理**







**五、实验内容：**

实验内容主要包括两个部分：

第一个部分是关于DHCP协议的验证实验

第二个部分是NAT协议的验证实验

**六、实验器材（设备、元器件）：**

台式机，软件Wireshark

**七、实验步骤：**

**DHCP的实验步骤：**

步骤1：首先通过命令行界面，输入”ipconfig /release”，释放本机的IP地址；

步骤2：启动Wireshark，开始捕获数据包；

步骤3：通过命令行界面，输入”ipconfig /renew”，获得IP地址；

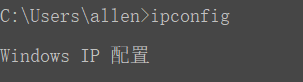
步骤4：再次输入”ipconfig /renew”，重新获得IP地址；

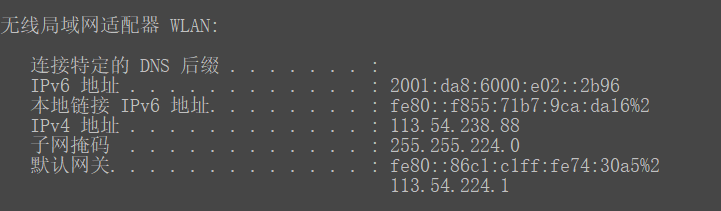
步骤5：通过命令行界面，输入”ipconfig /release”，释放本机的IP地址；

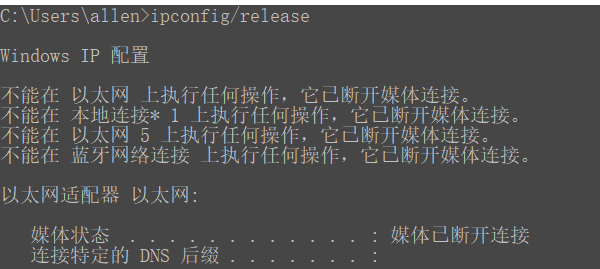
步骤6：再次输入”ipconfig /renew”，重新获得IP地址；

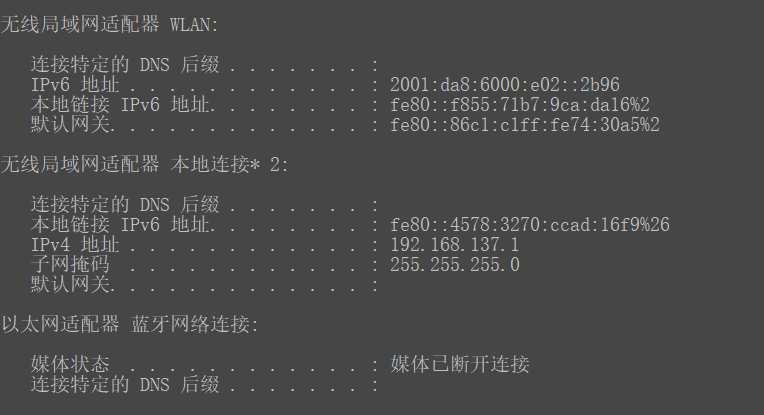
步骤7：停止Wireshark。

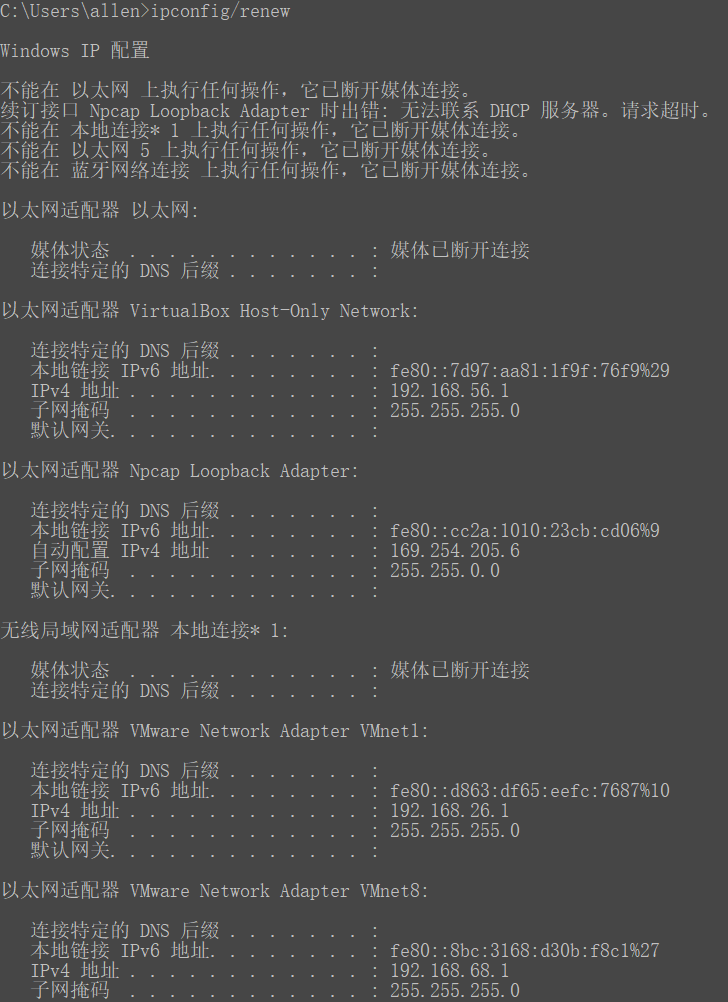
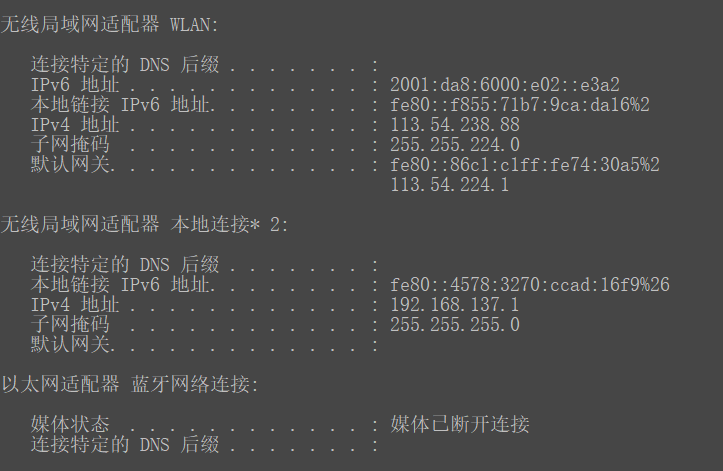
控制台命令行界面：





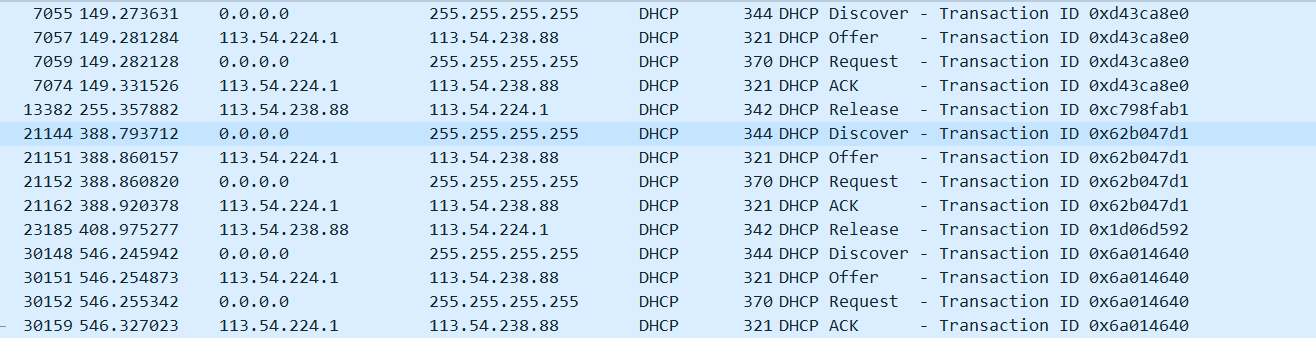




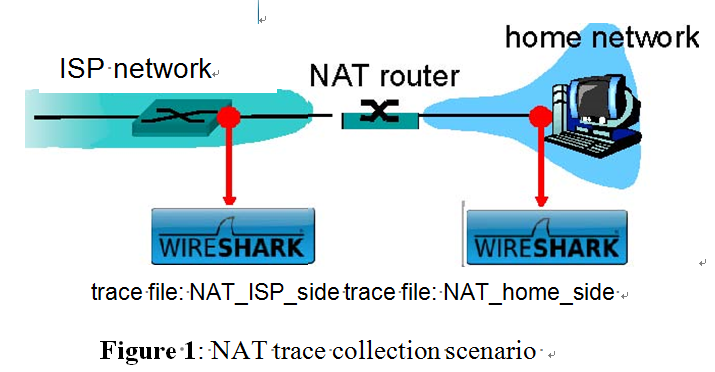
捕获包的截图：

You need to enter “bootp” and not “dhcp” in the filter.



NAT实验：

这个实验考察NAT协议的行为。这个实验将采用提供的一个trace文件来进行分析。因为我们需要捕捉NAT设备的输出和输入，而学生通常不太容易接入一个NAT设备来完成Wireshark抓包。因此在这个实验中，我们将使用提供的trace文件来进行分析。NAT的测量方案如下：



NAT\_home\_side：client pc上捕获的。

NAT\_ISP\_side：ISP路由上捕获的。

**八、实验结果与分析（含重要数据结果分析或核心代码流程分析）**

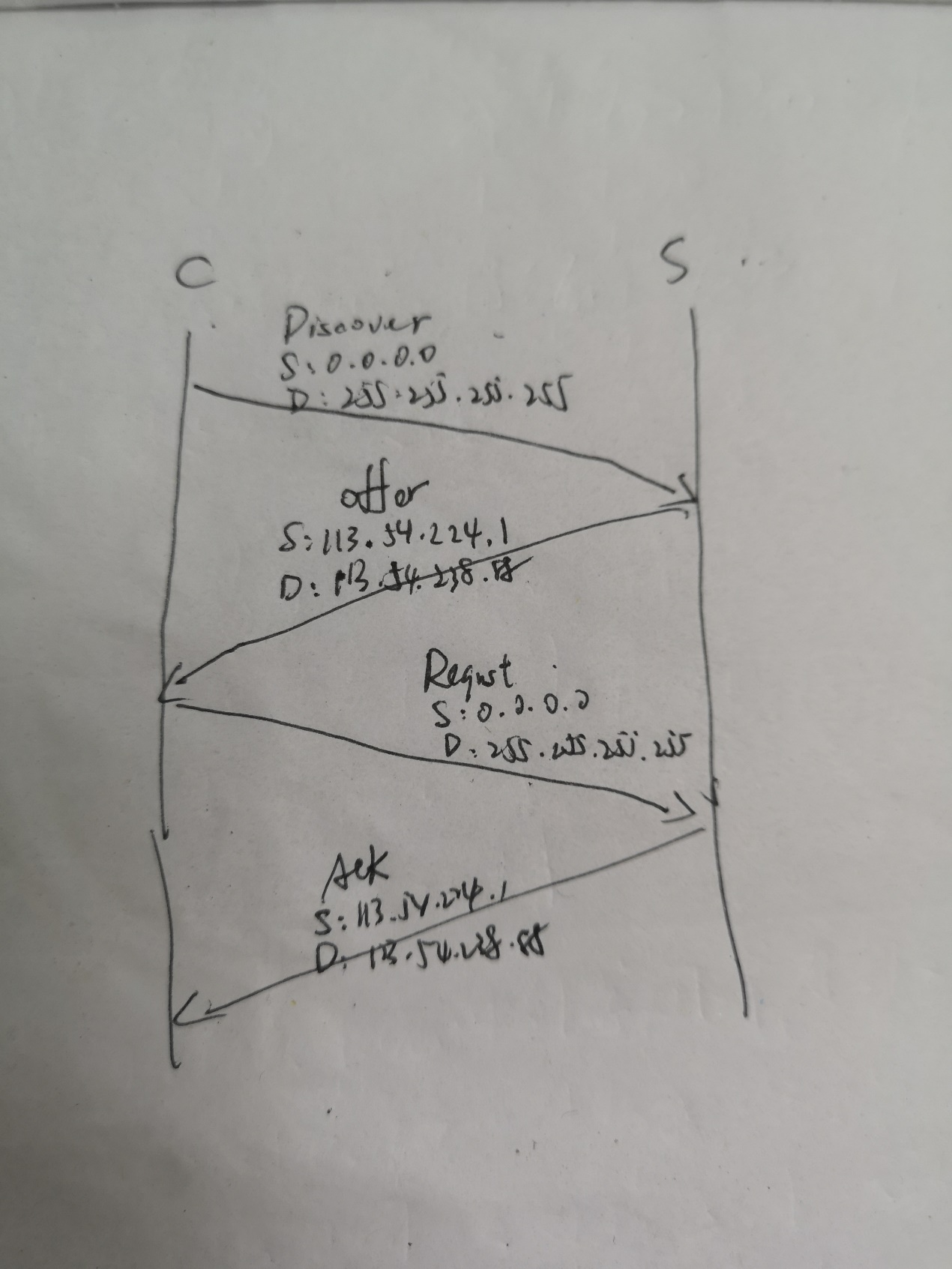
根据DHCP的实验结果回答以下问题：

* Are DHCP messages sent over UDP or TCP?

回答：UDP

* Draw a timing datagram illustrating the sequence of the first four-packet Discover/Offer/Request/ACK DHCP exchange between the client and server（画出时序图，4个分组在client和server之间的交互过程）. For each packet, indicated the source and destination port numbers（对于每个分组要标识出源、目的IP地址，源、目的端口号）. Are the port numbers the same as in the example given in this lab assignment? （在这个实验中的端口号与例子中的端口号是否相同）。

回答：时序图



* What is the link-layer (e.g., Ethernet) address of your host?（你的主机的链路层地址）

回答：我的主机的链路层地址是：

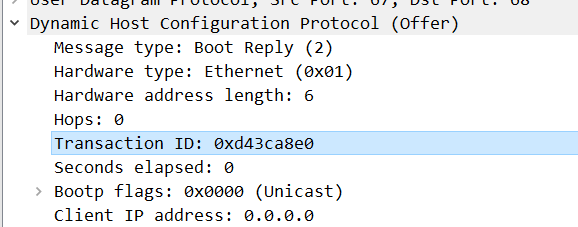
* What values in the DHCP discover message differentiate this message from the DHCP request message? DHCP discover消息中携带的哪个值用于区分这个消息和DHCP request消息？

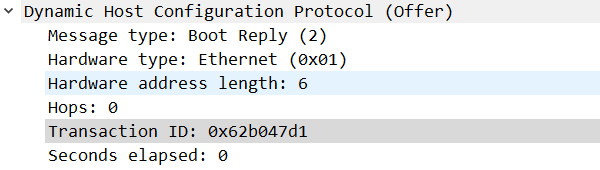
回答：DHCP的消息类型字段

DHCP Message Type

* What is the value of the Transaction-ID in each of the first four (Discover/Offer/Request/ACK) DHCP messages? （在第一组4个DHCP消息中的Transaction-ID的值是多少） What are the values of the Transaction-ID in the second set (Request/ACK) set of DHCP messages?(在第二组DHCP消息中的Transaction-ID是多少？) What is the purpose of the Transaction-ID field? （该字段的目的是什么？）

回答：





便于DHCP服务器区别客户端

* A host uses DHCP to obtain an IP address, among other things. But a host’s IP address is not confirmed until the end of the four-message exchange! If the IP address is not set until the end of the four-message exchange, then what values are used in the IP datagrams in the four-message exchange? For each of the four DHCP messages (Discover/Offer/Request/ACK DHCP), indicate the source and destination IP addresses that are carried in the encapsulating IP datagram.

回答：

Discover:源IP:0.0.0.0,目的IP：255.255.255.255

Offer:源IP:113.54.224.1,目的IP:113.54.238.88

Request:源IP:0.0.0.0,目的IP：255.255.255.255

ACK:源IP: 113.54.224.1,目的IP: 113.54.238.88

* What is the IP address of your DHCP server?

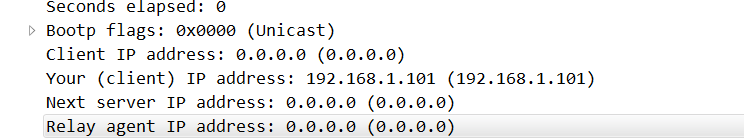
回答：113.54.224.1

* What IP address is the DHCP server offering to your host in the DHCP Offer message? Indicate which DHCP message contains the offered DHCP address. （指出哪个DHCP消息包含提供的DHCP地址）

回答： 113.54.238.88

* In the example screenshot in this assignment, there is no relay agent between the host and the DHCP server. What values in the trace indicate the absence of a relay agent? （哪个字段的值说明缺少一个中继代理） Is there a relay agent in your experiment? If so what is the IP address of the agent? （在你的使用中有中继代理吗？如果有哪个IP地址是代理的？）

回答：Hops字段的值为0



* Explain the purpose of the router and subnet mask lines in the DHCP offer message.

回答：子网掩码可以区分该网段，得知相同网段的电脑 IP 范围，默认网关（路由地址）

* In the DHCP trace file noted in footnote 2, the DHCP server offers a specific IP address to the client (see also question 8. above). In the client’s response to the first server OFFER message, does the client accept this IP address? Where in the client’s RESPONSE is the client’s requested address?

回答：客户端接受此IP地址

* Explain the purpose of the lease time. How long is the lease time in your experiment?

回答：解释租赁时间的含义：就是分配的IP地址可以使用的时间，2小时。

* What is the purpose of the DHCP release message? Does the DHCP server issue an acknowledgment of receipt of the client’s DHCP request? What would happen if the client’s DHCP release message is lost?

回答：

释放分配的IP地址

不会发出确认

会继续使用之前的IP并进行续订的判断

* Clear the bootp filter from your Wireshark window. Were any ARP packets sent or received during the DHCP packet-exchange period? If so, explain the purpose of those ARP packets.

回答：有，在 DHCP 获取 IP 后同样发送了 ARP 广播消息用来获取路由的 MAC 地址并且到本机的 ARP 缓存表，用以网络传输。

根据NAT实验提供的两个trace文件回答以下问题：

首先打开NAT\_home\_side文件，回答问题：

* What is the IP address of the client?

回答： 192.168.1.100

* The client actually communicates with several different Google servers in order to implement “safe browsing.” (See extra credit section at the end of this lab). The main Google server that will serve up the main Google web page has IP address 64.233.169.104. In order to display only those frames containing HTTP messages that are sent to/from this Google, server, enter the expression “http && ip.addr == 64.233.169.104” (without quotes) into the Filter: field in Wireshark .

回答：

* Consider now the HTTP GET sent from the client to the Google server (whose IP address is IP address 64.233.169.104) at time 7.109267. What are the source and destination IP addresses and TCP source and destination ports on the IP datagram carrying this HTTP GET?

回答：

* At what time4 is the corresponding 200 OK HTTP message received from the Google server? What are the source and destination IP addresses and TCP source and destination ports on the IP datagram carrying this HTTP 200 OK message?

回答：

Time：7.158797

源IP地址：64.233.169.104 目的IP地址：192.168.1.100

源端口：80 目的端口：4335

* Recall that before a GET command can be sent to an HTTP server, TCP must first set up a connection using the three-way SYN/ACK handshake. At what time is the client-to-server TCP SYN segment sent that sets up the connection used by the GET sent at time 7.109267? What are the source and destination IP addresses and source and destination ports for the TCP SYN segment? What are the source and destination IP addresses and source and destination ports of the ACK sent in response to the SYN. At what time is this ACK received at the client? (Note: to find these segments you will need to clear the Filter expression you entered above in step 2. If you enter the filter “tcp”, only TCP segments will be displayed by Wireshark).

回答：

SYN段：源IP:192.168.1.100,目的IP:64.233.169.104;

源端口号：4335，目的端口号：80；

SYN响应段：源IP:64.233.169.104,目的IP:192.168.1.100;

源端口号：80，目的端口号：4335；

客户端收到此ACK的时间：7.108986

打开NAT\_ISP\_side文件，回答问题：

* In the NAT\_ISP\_side trace file, find the HTTP GET message was sent from the client to the Google server at time 7.109267 (where t=7.109267 is time at which this was sent as recorded in the NAT\_home\_side trace file). At what time does this message appear in the NAT\_ISP\_side trace file? What are the source and destination IP addresses and TCP source and destination ports on the IP datagram carrying this HTTP GET (as recording in the NAT\_ISP\_side trace file)? Which of these fields are the same, and which are different, than in your answer to question 3 above?

回答：时间：6.069168，源:71.192.34.104,4335，目的：64.233.169.104,80,

这些字段相同的是目的IP，目的端口号，源端口号，不相同的是：源IP。

* Are any fields in the HTTP GET message changed? Which of the following fields in the IP datagram carrying the HTTP GET are changed: Version, Header Length, Flags, Checksum. If any of these fields have changed, give a reason (in one sentence) stating why this field needed to change.

回答：在HTTP GET消息中，并非所有字段都发生了变化。以下字段：Version, Header Length, Flags, Checksum，哪些发生了变化。说明发生变化字段变化的原因。

Checksum变化了，因为源IP地址变化，而校验和中包含源IP地址字段，所以它也变化了。

* In the NAT\_ISP\_side trace file, at what time is the first 200 OK HTTP message received from the Google server? What are the source and destination IP addresses and TCP source and destination ports on the IP datagram carrying this HTTP 200 OK message? Which of these fields are the same, and which are different than your answer to question 4 above?

回答：收到来自google服务器the first 200 OK HTTP message的时间。

* In the NAT\_ISP\_side trace file, at what time were the client-to-server TCP SYN segment and the server-to-client TCP ACK segment corresponding to the segments in question 5 above captured? What are the source and destination IP addresses and source and destination ports for these two segments? Which of these fields are the same, and which are different than your answer to question 5 above?

回答：

* Using your answers to 1-8 above, fill in the NAT translation table entries for HTTP connection considered in questions 1-8 above.

回答：基于上述情况，回答NAT转化表：

|  |  |
| --- | --- |
| WAN端 | LAN端 |
| 71.192.34.104:4335 | 192.168.1.100:4335 |
| 74.125.91.113:4330 | 192.168.1.100:4330 |
| 71.192.34.104：4331 | 192.168.1.100:4330 |
| 71.192.34.104：4336 | 192.168.1.100:4336 |
| 71.192.34.104：4337 | 192.168.1.100:4337 |

**九、总结及心得体会：**

本次实验主要是对DHCP以及NAT理解和操作，除了DHCP中ipconfig/renew这个过程会耗费大量的时间，其他操作实质上没有太多值得注意的部分，只要熟悉DHCP和NAT就可以较好的掌握本次实验。

**十、对本实验过程及方法、手段的改进建议：**

**无**

**报告评分：**

**指导教师签字：**