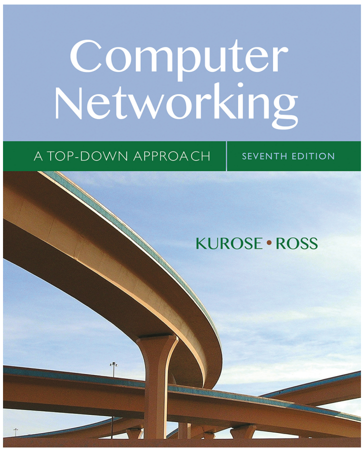
Wireshark Lab: DHCP v7.0

Supplement to *Computer Networking: A Top-Down Approach, 7th ed.,* J.F. Kurose and K.W. Ross



"Tell me and I forget. Show me and I remember. Involve me and I understand." Chinese proverb

In this lab, we'll take a quick look at DHCP. DHCP is covered in Section 4.4.3 of the text[1]. Recall that DHCP is used extensively in corporate, university and home-network wired and wireless LANs to dynamically assign IP addresses to hosts (as well as to configure other network configuration information).
在本实验中，我们将快速了解 DHCP 动态主机设置协议。 DHCP 在课本的第 4.4.3 节中介绍。 回想一下，DHCP 广泛用于企业，大学和家庭网络有线和无线 LAN，以动态地为主机分配 IP 地址（以及配置其他网络配置信息）。
This lab is brief, as we'll only examine the DHCP packets captured by a host. If you also have administrative access to your DHCP server, you may want to repeat this lab after making some configuration changes (such as the lease time). If you have a router at home, you most likely can configure your DHCP server. Because many linux/Unix machines (especially those that serve many users) have a static IP address and because manipulating DHCP on such machines typically requires super-user privileges, we'll only present a Windows version of this lab below.
这是一个小实验，我们只要通过分析我们本机的捕获 DHCP 数据包。不过如果您有对 DHCP 服务器管理访问权限，则您可以试试进行一些更改 DHCP 配置（例如租用时间）后重复此实验。同样的如果您家里有路由器，您或许也会配置 DHCP 服务器。因为许多 Linux / Unix 机器（特别是为许多用户提供服务的机器，译注：这里指的是 DHCP 服务器）需要具有静态 IP 地址，并且因为在这些机器上操作 DHCP 通常需要超级用户权限，所以（为了实验简单）我们将仅在下面提供此实验的 Windows 版本。

DHCP Experiment　DHCP 实验

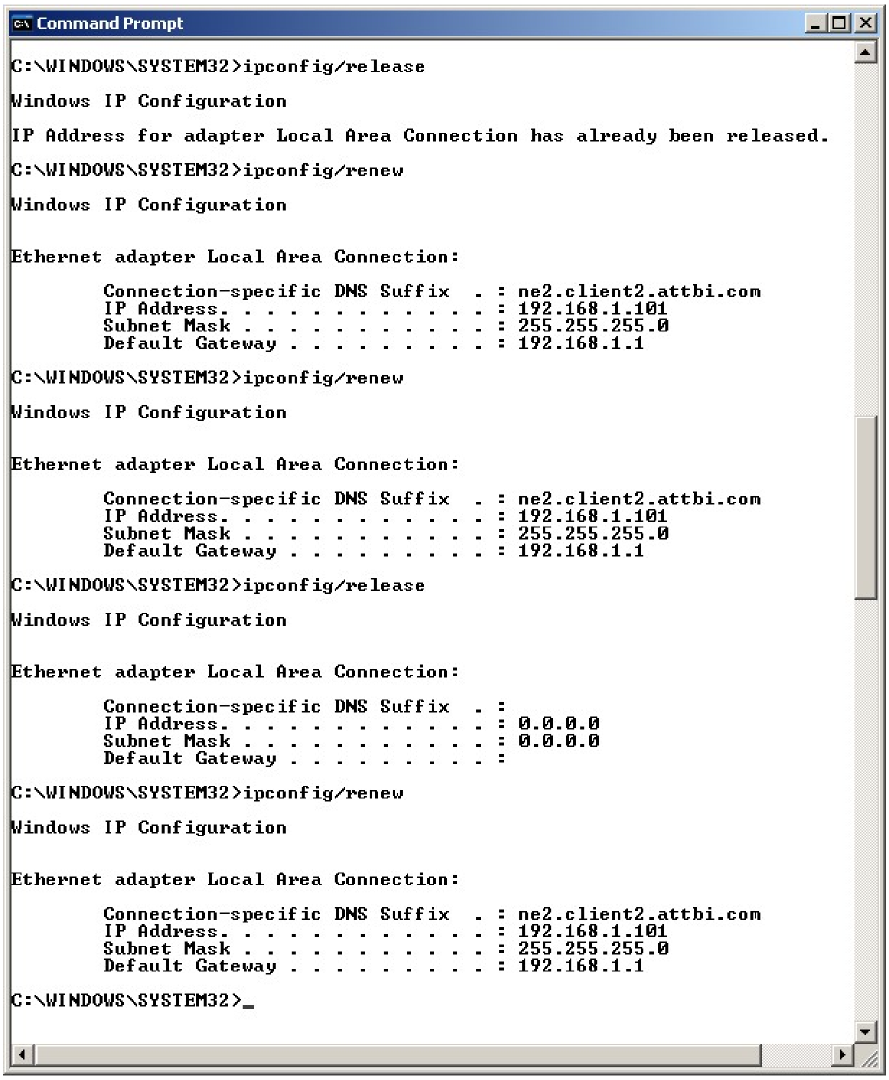
[1] References to figures and sections are for the 7th edition of our text, *Computer Networks, A Top-down Approach, 7th ed., J.F. Kurose and K.W. Ross, Addison-Wesley/Pearson, 2016.*
课本：计算机网络 自顶向下方法第 7 版 中文版由机械工业出版社翻译发行

In order to observe DHCP in action, we'll perform several DHCP-related commands and capture the DHCP messages exchanged as a result of executing these commands. Do the following[2]:
为了了解 DHCP 如何的工作，我们将执行几个与 DHCP 相关的命令，并捕获由于执行这些命令而传输的 DHCP 消息。请执行下列操作：

1. Begin by opening the Windows Command Prompt application (which can be found in your Accessories folder). As shown in Figure 1, enter "*ipconfig /release*". The executable for *ipconfig* is in C:\windows\system32. This command releases your current IP address, so that your host's IP address becomes 0.0.0.0.
   首先打开 Windows 命令提示符应用程序（可在"附件"文件夹中找到）。如图 1 所示，输入" ipconfig /release "（注意是引号内容，且不包括引号）。ipconfig 的可执行程序位于 C:\windows\system32 中。此命令会释放您当前的 IP 地址，以便主机的 IP 地址变为 0.0.0.0
2. Start up the Wireshark packet sniffer, as described in the introductory Wireshark lab and begin Wireshark packet capture.
   打开 Wireshark 并且进行抓包。
3. Now go back to the Windows Command Prompt and enter "*ipconfig /renew*". This instructs your host to obtain a network configuration, including a new IP address. In Figure 1, the host obtains the IP address 192.168.1.108
   现在继续在 Windows 命令提示符并输入 " ipconfig /renew " （注意是引号内容，且不包括引号）。这会指示您的主机获取网络配置，包括新的 IP 地址。在图 1 中，主机获得 IP 地址 192.168.1.108
4. Wait until the "*ipconfig /renew*" has terminated. Then enter the same command "*ipconfig /renew*" again.
   等到" ipconfig /renew " 命令执行完毕。然后再次输入相同的命令"ipconfig / renew"。
5. When the second *"ipconfig /renew"* terminates, enter the command "ipconfig/release" to release the previously-allocated IP address to your computer.
   等到第二遍" ipconfig /renew " 命令执行完毕。再次在命令提示符输入 " ipconfig /release "命令释放您刚获取的 IP。
6. Finally, enter "*ipconfig /renew*" to again be allocated an IP address for your computer.
   最后，输入 "ipconfig /renew"命令再次为您的计算机分配一个 IP 地址。

[2] If you are unable to run Wireshark live on a computer, you can download the zip file http://gaia.cs.umass.edu/wireshark-labs/wireshark-traces.zip and extract the file *dhcp-ethereal-trace-1*. The traces in this zip file were collected by Wireshark running on one of the author's computers, while performing the steps indicated in the Wireshark lab. Once you have downloaded the trace, you can load it into Wireshark and view the trace using the *File* pull down menu, choosing *Open*, and then selecting the dhcp-ethereal-trace-1 trace file. You can then use this trace file to answer the questions below.
同样如果您无法抓包，建议您下载作者的抓包结果 http://gaia.cs.umass.edu/wireshark-labs/wireshark-traces.zip 解压并且使用 Wireshark 打开 dhcp-ethereal-trace-1 进行分析。

7. Stop Wireshark packet capture. 停止抓包。



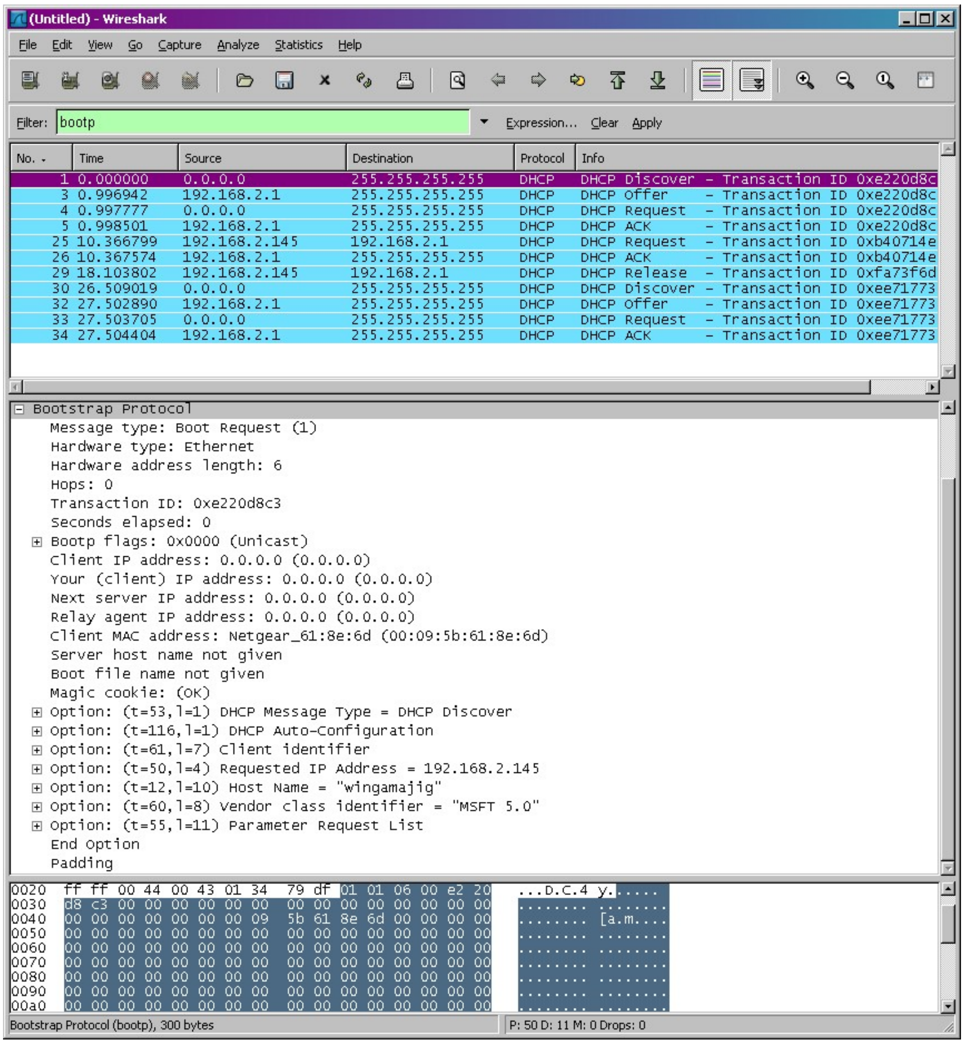
```
C:\WINDOWS\SYSTEM32>ipconfig/release

Windows IP Configuration

IP Address for adapter Local Area Connection has already been released.

C:\WINDOWS\SYSTEM32>ipconfig/renew

Windows IP Configuration


Ethernet adapter Local Area Connection:

        Connection-specific DNS Suffix  . : ne2.client2.attbi.com
        IP Address. . . . . . . . . . . . : 192.168.1.101
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . : 192.168.1.1

C:\WINDOWS\SYSTEM32>ipconfig/renew

Windows IP Configuration


Ethernet adapter Local Area Connection:

        Connection-specific DNS Suffix  . : ne2.client2.attbi.com
        IP Address. . . . . . . . . . . . : 192.168.1.101
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . : 192.168.1.1

C:\WINDOWS\SYSTEM32>ipconfig/release

Windows IP Configuration


Ethernet adapter Local Area Connection:

        Connection-specific DNS Suffix  . :
        IP Address. . . . . . . . . . . . : 0.0.0.0
        Subnet Mask . . . . . . . . . . . : 0.0.0.0
        Default Gateway . . . . . . . . . :

C:\WINDOWS\SYSTEM32>ipconfig/renew

Windows IP Configuration


Ethernet adapter Local Area Connection:

        Connection-specific DNS Suffix  . : ne2.client2.attbi.com
        IP Address. . . . . . . . . . . . : 192.168.1.101
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . : 192.168.1.1

C:\WINDOWS\SYSTEM32>_
```

Figure 1 Command Prompt window showing sequence of *ipconfig* commands that you should enter.
图 1 您应该在命令提示符所输入一系列 ipconfig 命令

Now let’s take a look at the resulting Wireshark window. To see only the DHCP packets, enter into the filter field “bootp”. (DHCP derives from an older protocol called BOOTP. Both BOOTP and DHCP use the same port numbers, 67 and 68. To see DHCP packets in the current version of Wireshark, you need to enter “bootp” and not “dhcp” in the filter.) We see from Figure 2 that the first *ipconfig* renew command caused four DHCP packets to be generated: a DHCP Discover packet, a DHCP Offer packet, a DHCP Request packet, and a DHCP ACK packet.

现在让我们来看看抓包结果。 要仅查看 DHCP 数据包，请进入过滤器字段“bootp”。 （DHCP 来自一个名为 BOOTP 的旧协议.BOOTP 和 DHCP 都使用相同的端口号 67 和 68.要查看当前版本的 Wireshark 中的 DHCP 数据包，您需要在过滤器中输入“bootp”而不是“dhcp”。）

我们从图 2 中看到，第一个“ipconfig/ renew”命令导致生成四个 DHCP 数据包：DHCP Discover 数据包，DHCP Offer 数据包，DHCP Request 数据包和 DHCP ACK 数据包。



Filter: bootp

```
No. -  Time        Source          Destination      Protocol  Info
    1 0.000000    0.0.0.0         255.255.255.255  DHCP      DHCP Discover - Transaction ID 0xe220d8c
    3 0.996942    192.168.2.1     255.255.255.255  DHCP      DHCP Offer    - Transaction ID 0xe220d8c
    4 0.997777    0.0.0.0         255.255.255.255  DHCP      DHCP Request  - Transaction ID 0xe220d8c
    5 0.998501    192.168.2.1     255.255.255.255  DHCP      DHCP ACK      - Transaction ID 0xe220d8c
   25 10.366799   192.168.2.145   192.168.2.1      DHCP      DHCP Request  - Transaction ID 0xb40714e
   26 10.367574   192.168.2.1     255.255.255.255  DHCP      DHCP ACK      - Transaction ID 0xb40714e
   29 18.103802   192.168.2.145   192.168.2.1      DHCP      DHCP Release  - Transaction ID 0xfa73f6d
   30 26.509019   0.0.0.0         255.255.255.255  DHCP      DHCP Discover - Transaction ID 0xee71773
   32 27.502890   192.168.2.1     255.255.255.255  DHCP      DHCP Offer    - Transaction ID 0xee71773
   33 27.503705   0.0.0.0         255.255.255.255  DHCP      DHCP Request  - Transaction ID 0xee71773
   34 27.504404   192.168.2.1     255.255.255.255  DHCP      DHCP ACK      - Transaction ID 0xee71773
```

```
⊟ Bootstrap Protocol
    Message type: Boot Request (1)
    Hardware type: Ethernet
    Hardware address length: 6
    Hops: 0
    Transaction ID: 0xe220d8c3
    Seconds elapsed: 0
  ⊞ Bootp flags: 0x0000 (Unicast)
    Client IP address: 0.0.0.0 (0.0.0.0)
    Your (client) IP address: 0.0.0.0 (0.0.0.0)
    Next server IP address: 0.0.0.0 (0.0.0.0)
    Relay agent IP address: 0.0.0.0 (0.0.0.0)
    Client MAC address: Netgear_61:8e:6d (00:09:5b:61:8e:6d)
    Server host name not given
    Boot file name not given
    Magic cookie: (OK)
  ⊞ Option: (t=53,l=1) DHCP Message Type = DHCP Discover
  ⊞ Option: (t=116,l=1) DHCP Auto-Configuration
  ⊞ Option: (t=61,l=7) Client identifier
  ⊞ Option: (t=50,l=4) Requested IP Address = 192.168.2.145
  ⊞ Option: (t=12,l=10) Host Name = "wingamajig"
  ⊞ Option: (t=60,l=8) Vendor class identifier = "MSFT 5.0"
  ⊞ Option: (t=55,l=11) Parameter Request List
    End Option
    Padding
```

```
0020  ff ff 00 44 00 43 01 34  79 df 01 01 06 00 e2 20   ...D.C.4 y.......
0030  d8 c3 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0040  00 00 00 00 00 00 00 09  5b 61 8e 6d 00 00 00 00   ........ [a.m....
0050  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0060  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0070  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0080  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0090  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00a0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
```

Bootstrap Protocol (bootp), 300 bytes   P: 50 D: 11 M: 0 Drops: 0

Figure 2 Wireshark window with first DHCP packet – the DHCP Discover packet – expanded.

图 2 Wireshark 窗口展开详细显示第一个 DHCP 数据包 - DHCP Discover 数据包

What to Hand In:　回答问题

You should hand in a screen shot of the Command Prompt window similar to Figure 1 above. Whenever possible, when answering a question below, you should hand in a printout of the packet(s) within the trace that you used to answer the question asked. Annotate the printout[3] to explain your answer. To print a packet, use *File->Print*, choose *Selected packet only*, choose *Packet summary line,* and select the minimum amount of packet detail that you need to answer the question.
请尽量清晰的展示您的答案，必要时您可以在图中用标记辅以说明。您的答案应该简单可读。

Answer the following questions: 请您回答以下问题

1. Are DHCP messages sent over UDP or TCP?
   DHCP 消息是通过 UDP 还是 TCP 发送的？
2. Draw a timing datagram illustrating the sequence of the first four-packet Discover/Offer/Request/ACK DHCP exchange between the client and server. For each packet, indicated the source and destination port numbers. Are the port numbers the same as in the example given in this lab assignment?
   绘制时间流图形。说明客户端和服务器之间第一次四个 DHCP 发现，DHCP 提供，DHCP 请求以及 DHCP 响应的顺序，说明您的结果中对于每个数据包，指示源和目标端口号是否与本实验分配中给出的示例相同？
3. What is the link-layer (e.g., Ethernet) address of your host?
   主机的链路层（例如以太网）地址是什么？
4. What values in the DHCP discover message differentiate this message from the DHCP request message?
   DHCP 发现消息中的哪些值将此消息与 DHCP 请求消息区不同？
5. What is the value of the Transaction-ID in each of the first four (Discover/Offer/Request/ACK) DHCP messages? What are the values of the Transaction-ID in the second set (Request/ACK) set of DHCP messages? What is the purpose of the Transaction-ID field?
   第一次四个 DHCP 发现，DHCP 提供，DHCP 请求以及 DHCP 响应的 Transaction-ID 值是多少？ Transaction-ID 字段目的是什么。
6. 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.

[3] What do we mean by "annotate"? If you hand in a paper copy, please highlight where in the printout you've found the answer and add some text (preferably with a colored pen) noting what you found in what you 've highlight. If you hand in an electronic copy, it would be great if you could also highlight and annotate.
请善用标记来展示您的答案

主机使用 DHCP 获取 IP 地址。主机在 DHCP 的 4 次问询和回答之后获取了地址。请问如果在这 4 次 DHCP 问询和回答中，如果主机没有 IP 地址，那么 IP 数据报的值是什么？请分别指出这 4 个 DHCP 的消息 IP 数据报源头和目标 IP。

7. What is the IP address of your DHCP server?
   您的 DHCP 服务器的 IP 地址是多少？
8. 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.
   发送 DHCP Offer 消息的 DHCP 服务器 IP 是什么，指示哪条 DHCP 消息包含提供的 DHCP 地址。
9. 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? Is there a relay agent in your experiment? If so what is the IP address of the agent?
   在作者的例子中，主机和 DHCP 服务器之间没有中继代理。 跟踪中的哪些值表明没有中继代理？ 您的实验中是否有中继代理？ 如果是这样，代理的 IP 地址是什么？
10. Explain the purpose of the router and subnet mask lines in the DHCP offer message.
    解释 DHCP offer 消息中路由器和子网掩码字段的用途。
11. 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?
    在脚注 2 作者提供的抓包结果中，DHCP 服务器会向作者提供特定的 IP 地址（请见上面问题 8）。请问客户端接受使用是否对第一个提供 DHCP offer 消息的 DHCP 地址？客户端的响应（DHCP 请求中）哪里是它所要求的地址。
12. Explain the purpose of the lease time. How long is the lease time in your experiment?
    解释租约时间的目的。 您的实验中的租约时间有多长？
13. 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?
    DHCP 释放消息的目的是什么？DHCP 服务器是否发出收到客户端 DHCP 释放请求的确认。如果客户端的 DHCP 释放消息丢了会发生什么。
14. 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.
    从 Wireshark 窗口中清除 bootp 过滤器。 在 DHCP 数据包交换期间是否发送或接收了任何 ARP 数据包？ 如果接收到了，请说明这些 ARP 数据包的用途。