Wireshark Lab: DHCP

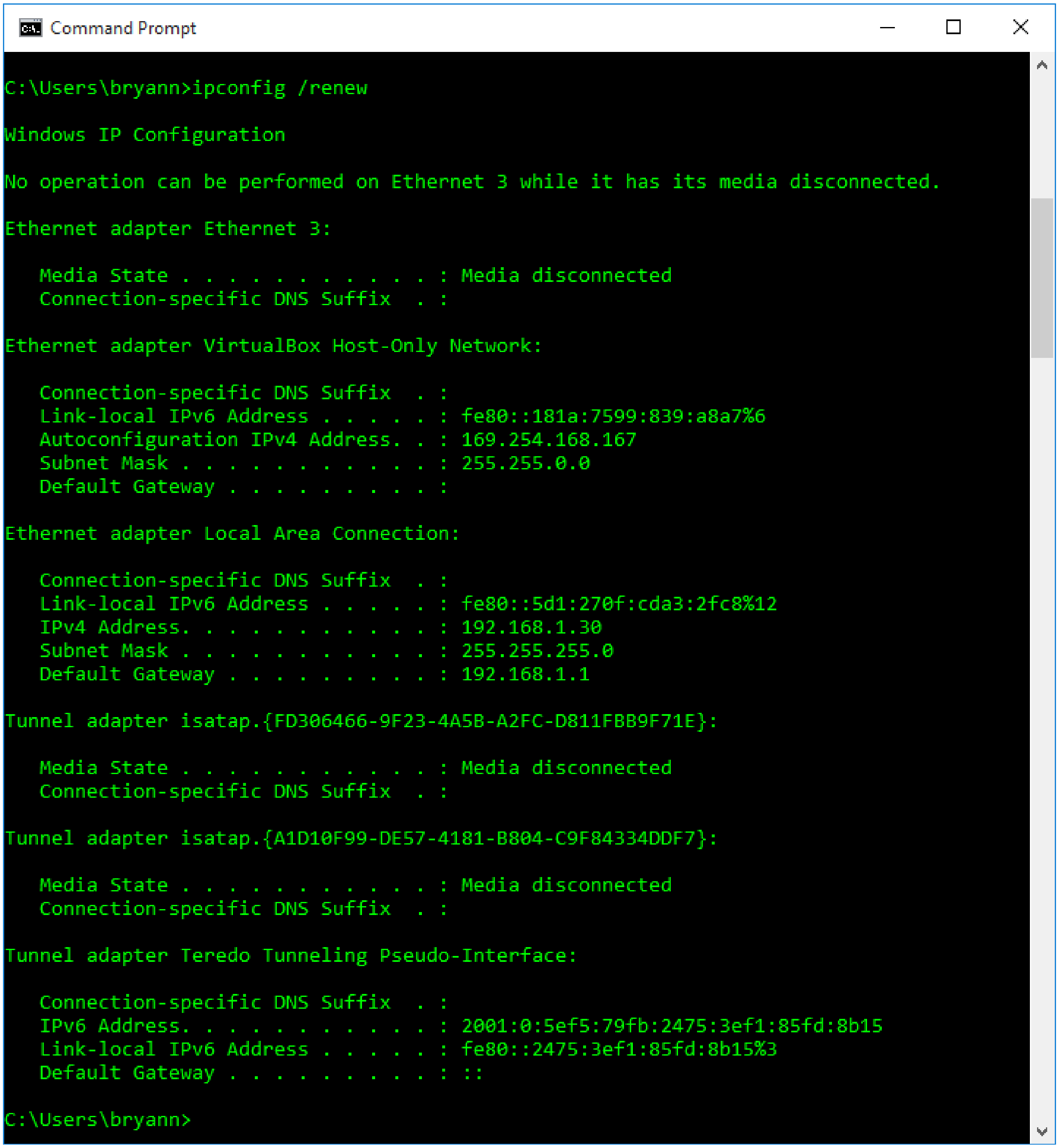
In this lab, we will look at DHCP. Recall from our lecture that DHCP is used extensively in corporate, university, and home-network and wireless LANs to dynamically assign IP addresses to hosts, as well as to configure other network configuration information.

This lab is brief and is designed to be completed at home, since we will only look at the DHCP packets captured by a host. Since changing the network settings of a host usually require administrator privileges, this lab is designed to be run on a Windows machine (since most of you are using Windows at home). If you are not using Windows and you don't know the corresponding commands in your OS, you can simply unplug/plug your LAN cable or disconnect/connect from your WiFi network. This makes your PC release and renew its IP address.

DHCP Experiment

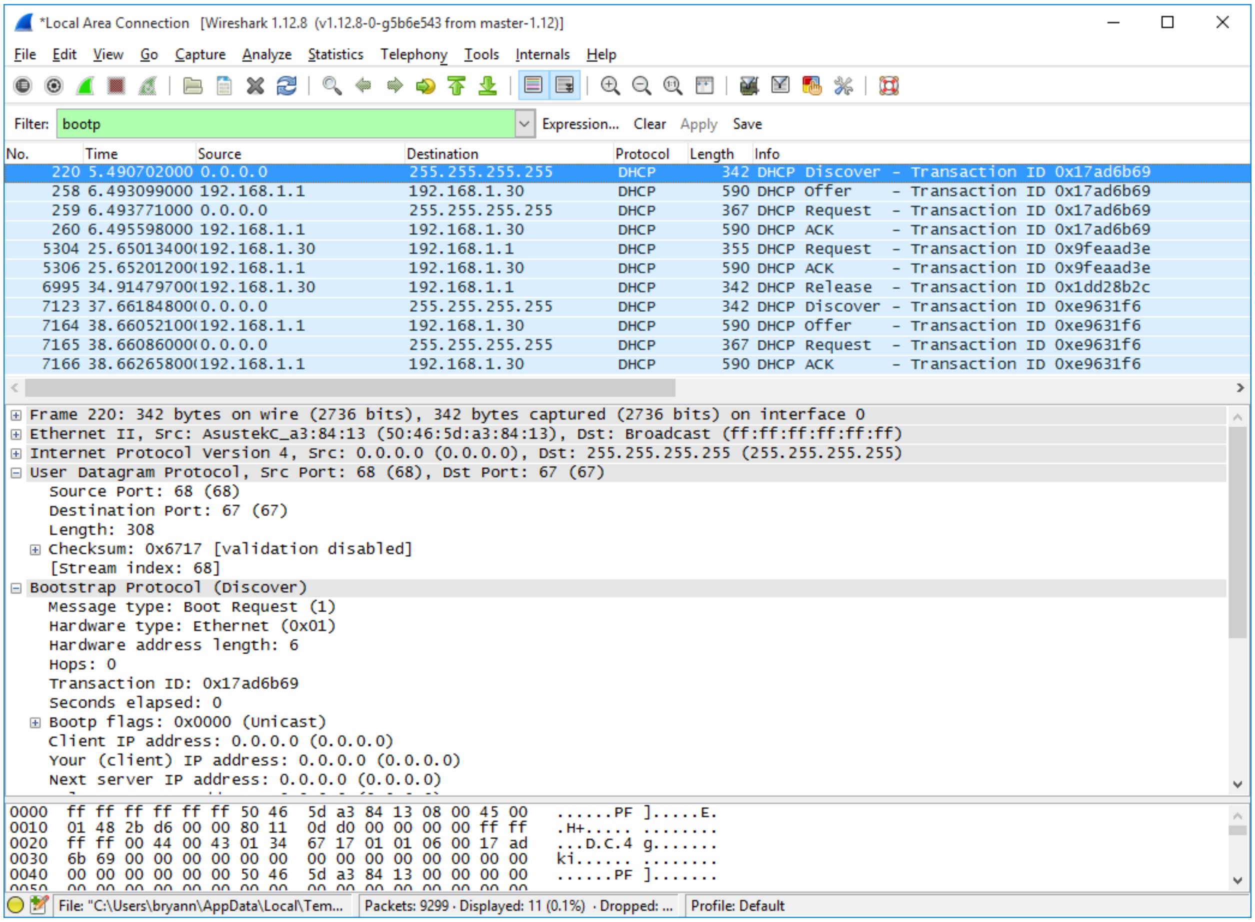
In order to observe DHCP in action, we'll perform several DHCP-related commands and capture the DHCP messages exchanged as a result of executing these commands. Do the following:

1. Open Command Prompt and enter the command "**`ipconfig /release`**" to release your current IP address. At this time, your host's IP address should be 0.0.0.0.
2. Start up the Wireshark packet sniffer.
3. At the command prompt, enter the command "**`ipconfig /renew`**". This will let your host obtain a network configuration, including a new IP address. In the figure below, it shows the host obtains IP address 192.168.1.30.
4. Then enter the same command "**`ipconfig /renew`**" again.
5. Then enter the command "**`ipconfig /release`**" to release the previously allocated IP address to your host.
6. Finally, enter "**`ipconfig /renew`**" to again get an IP address allocation for your host.
7. Stop the Wireshark packet capture.



```
C:\Users\bryann>ipconfig /renew

Windows IP Configuration

No operation can be performed on Ethernet 3 while it has its media disconnected.

Ethernet adapter Ethernet 3:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Ethernet adapter VirtualBox Host-Only Network:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::181a:7599:839:a8a7%6
   Autoconfiguration IPv4 Address. . : 169.254.168.167
   Subnet Mask . . . . . . . . . . . : 255.255.0.0
   Default Gateway . . . . . . . . . :

Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::5d1:270f:cda3:2fc8%12
   IPv4 Address. . . . . . . . . . . : 192.168.1.30
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.1.1

Tunnel adapter isatap.{FD306466-9F23-4A5B-A2FC-D811FBB9F71E}:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Tunnel adapter isatap.{A1D10F99-DE57-4181-B804-C9F84334DDF7}:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Tunnel adapter Teredo Tunneling Pseudo-Interface:

   Connection-specific DNS Suffix  . :
   IPv6 Address. . . . . . . . . . . : 2001:0:5ef5:79fb:2475:3ef1:85fd:8b15
   Link-local IPv6 Address . . . . . : fe80::2475:3ef1:85fd:8b15%3
   Default Gateway . . . . . . . . . : ::

C:\Users\bryann>
```

Now let’s take a look at the resulting Wireshark window. To see only the DHCP packets, use “bootp” in the filter field. (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 Wireshark, you need to enter “bootp” and not “dhcp” in the filter.) From the figure below, we see 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.


*Local Area Connection [Wireshark 1.12.8 (v1.12.8-0-g5b6e543 from master-1.12)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Expression... Clear Apply Save

Filter: bootp

```
No.     Time         Source          Destination       Protocol  Length  Info
    220 5.490702000 0.0.0.0          255.255.255.255   DHCP         342 DHCP Discover - Transaction ID 0x17ad6b69
    258 6.493099000 192.168.1.1      192.168.1.30      DHCP         590 DHCP Offer    - Transaction ID 0x17ad6b69
    259 6.493771000 0.0.0.0          255.255.255.255   DHCP         367 DHCP Request  - Transaction ID 0x17ad6b69
    260 6.495598000 192.168.1.1      192.168.1.30      DHCP         590 DHCP ACK      - Transaction ID 0x17ad6b69
   5304 25.65013400(192.168.1.30     192.168.1.1       DHCP         355 DHCP Request  - Transaction ID 0x9feaad3e
   5306 25.65201200(192.168.1.1      192.168.1.30      DHCP         590 DHCP ACK      - Transaction ID 0x9feaad3e
   6995 34.91479700(192.168.1.30     192.168.1.1       DHCP         342 DHCP Release  - Transaction ID 0x1dd28b2c
   7123 37.66184800(0.0.0.0          255.255.255.255   DHCP         342 DHCP Discover - Transaction ID 0xe9631f6
   7164 38.66052100(192.168.1.1      192.168.1.30      DHCP         590 DHCP Offer    - Transaction ID 0xe9631f6
   7165 38.66086000(0.0.0.0          255.255.255.255   DHCP         367 DHCP Request  - Transaction ID 0xe9631f6
   7166 38.66265800(192.168.1.1      192.168.1.30      DHCP         590 DHCP ACK      - Transaction ID 0xe9631f6
```

```
⊞ Frame 220: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits) on interface 0
⊞ Ethernet II, Src: AsustekC_a3:84:13 (50:46:5d:a3:84:13), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
⊞ Internet Protocol Version 4, Src: 0.0.0.0 (0.0.0.0), Dst: 255.255.255.255 (255.255.255.255)
⊟ User Datagram Protocol, Src Port: 68 (68), Dst Port: 67 (67)
    Source Port: 68 (68)
    Destination Port: 67 (67)
    Length: 308
  ⊞ Checksum: 0x6717 [validation disabled]
    [Stream index: 68]
⊟ Bootstrap Protocol (Discover)
    Message type: Boot Request (1)
    Hardware type: Ethernet (0x01)
    Hardware address length: 6
    Hops: 0
    Transaction ID: 0x17ad6b69
    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)
```

```
0000  ff ff ff ff ff ff 50 46  5d a3 84 13 08 00 45 00   ......PF ].....E.
0010  01 48 2b d6 00 00 80 11  0d d0 00 00 00 00 ff ff   .H+..... ........
0020  ff ff 00 44 00 43 01 34  67 17 01 01 06 00 17 ad   ...D.C.4 g.......
0030  6b 69 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ki...... ........
0040  00 00 00 00 00 00 50 46  5d a3 84 13 00 00 00 00   ......PF ].......
0050  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
```

File: "C:\Users\bryann\AppData\Local\Tem... | Packets: 9299 · Displayed: 11 (0.1%) · Dropped: ... | Profile: Default

What to Hand In:

You should hand in a screenshot of the command prompt window showing the IP address that was assigned to your host by the DHCP server. For each question, include a Wireshark screenshot with the corresponding parts that support your answer highlighted.

Answer the following questions:

1. Are DHCP messages sent over UDP or TCP?
2. Draw a timing diagram illustrating the sequence of the first four-packet Discover/Offer/Request/Ack DHCP exchange between client and server. For each packet, indicate the source and destination port numbers.
3. What is the data link layer (e.g. Ethernet) address of your host?
4. What values in the DHCP Discover message differentiate this message from the DHCP Request message?
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 of DHCP messages? What is the purpose of the Transaction-ID field?
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), indicate the source and destination IP addresses that are carried in the encapsulating IP datagram.

7. What is the IP address of your DHCP server?
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.
9. Is there a relay agent between the host and the DHCP server? If yes, what is the IP address of the relay agent? If none, how did you know there is none?
10. Explain the purpose of the router and subnet mask lines in DHCP offer message.
11. Explain the purpose of the lease time. How long is the lease time in your experiment?
12. What is the purpose of the DHCP release message? Does the DHCP server issue an acknowledgement of receipt of the client's DHCP request? What would happen if the client's DHCP release message is lost?
13. 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.