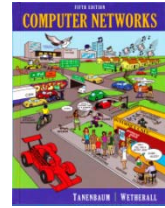# Lab Exercise – DHCP

Objective

To see how DHCP (Dynamic Host Configuration Protocol) works. DHCP is an essential glue protocol that is used to configure your computer with an IP address, as well as other information. It is covered in §5.6.4 of your text. Review those sections before doing this lab.

Requirements

Wireshark: This lab uses the Wireshark software tool to capture and examine a packet trace. A packet trace is a record of traffic at a location on the network, as if a snapshot was taken of all the bits that passed across a particular wire. The packet trace records a timestamp for each packet, along with the bits that make up the packet, from the lower-layer headers to the higher-layer contents. Wireshark runs on most operating systems, including Windows, Mac and Linux. It provides a graphical UI that shows the sequence of packets and the meaning of the bits when interpreted as protocol headers and data. It color-codes packets by their type, and has various ways to filter and analyze packets to let you investigate the behavior of network protocols. Wireshark is widely used to troubleshoot networks. You can download it from www.wireshark.org if it is not already installed on your computer. We highly recommend that you watch the short, 5 minute video "Introduction to Wireshark" that is on the site.

ipconfig (windows) / **ifconfig** (mac) / **dhclient** (linux): This lab uses a command-line utility to cause the computer renew its IP address lease using DHCP. The commands are installed on Windows/Mac/Linux computers, but there is a different command for each different operating system. The commands require administrative privileges to run when they change the state of the interface.

Network Setup

Recall that DHCP is normally used to assign a computer its IP address, as well as other parameters such as the address of the local router. Your computer, the client, uses the DHCP protocol to communicate with a DHCP server on the local network. Other computers on the local network also interact with the DHCP server. The setup is as shown in the example below. In deployments, there are several variations. For example, the local agent may be a DHCP relay that relays messages between local computers and a remote DHCP server. Or the DHCP server may be replicated for reliability, so that there are two or more local DHCP servers. For our purposes, it is sufficient to think about a single DHCP server.
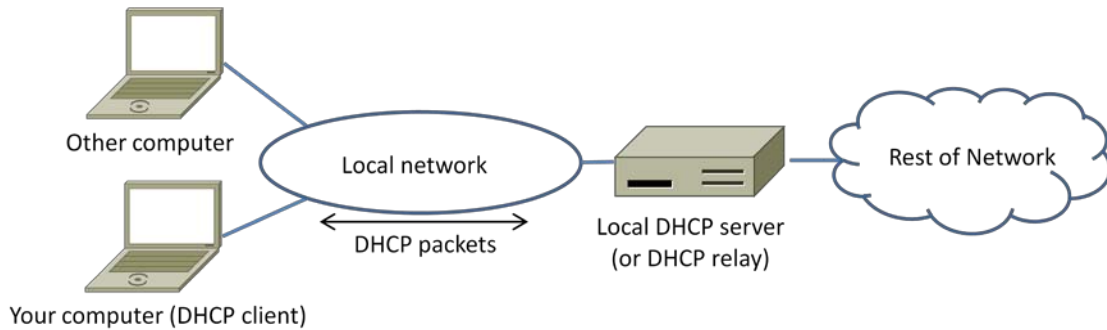
Figure 1: Network setup under which we will study DHCP

The complete DHCP exchange for your computer to lease an IP address from a DHCP server is shown below. It involves four types of packets: Discover, for your computer to locate the DHCP server; Offer, for the server to offer an IP address; Request, for your computer to ask for an offered address; and Ack, for the server to grant the address lease. However, when a computer is re-establishing its IP address on a network that it has previously used, it may perform a short exchange involving only two types of DHCP packets: Request, to ask for the same IP address as from the same server as was used before; and ACK for the server to grant the address lease.
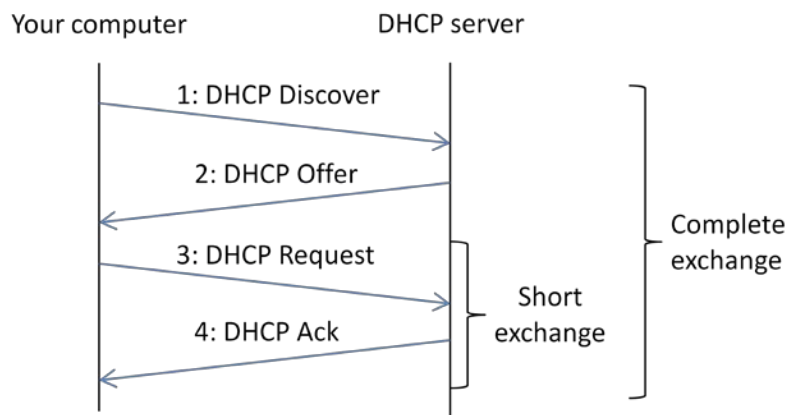

Figure 2: DHCP message sequences

Step 1: Capture a Trace

Proceed as follows to renew your IP address and gather a trace of DHCP traffic. Note, however, that the following procedure will not work in the unlikely case that your computer's IP address is statically assigned. Alternatively, you may use a supplied trace. Take care not to perform this lab remotely, since when you tell your computer to shut down and restart its network interface you will lose connectivity!

1. *Launch Wireshark and start a capture with a filter of* "`(udp port 67) or (udp port 68)`". There is no shorthand to indicate DHCP, so we filter traffic using the UDP ports reserved for DHCP. Your capture window should be similar to the one pictured below, other than our highlighting. Select the interface from which to capture as the main wired or wireless interface used by your computer to connect to the Internet. If unsure, guess and revisit this step later if your capture is not successful. Uncheck "capture packets in promiscuous mode". This mode is useful

to overhear packets sent to/from other computers on broadcast networks. We only want to record packets sent to/from your computer. Leave other options at their default values. The capture filter, if present, is used to prevent the capture of other traffic your computer may send or receive. On Wireshark 1.8, the capture filter box is present directly on the options screen, but on Wireshark 1.9, you set a capture filter by double-clicking on the interface.
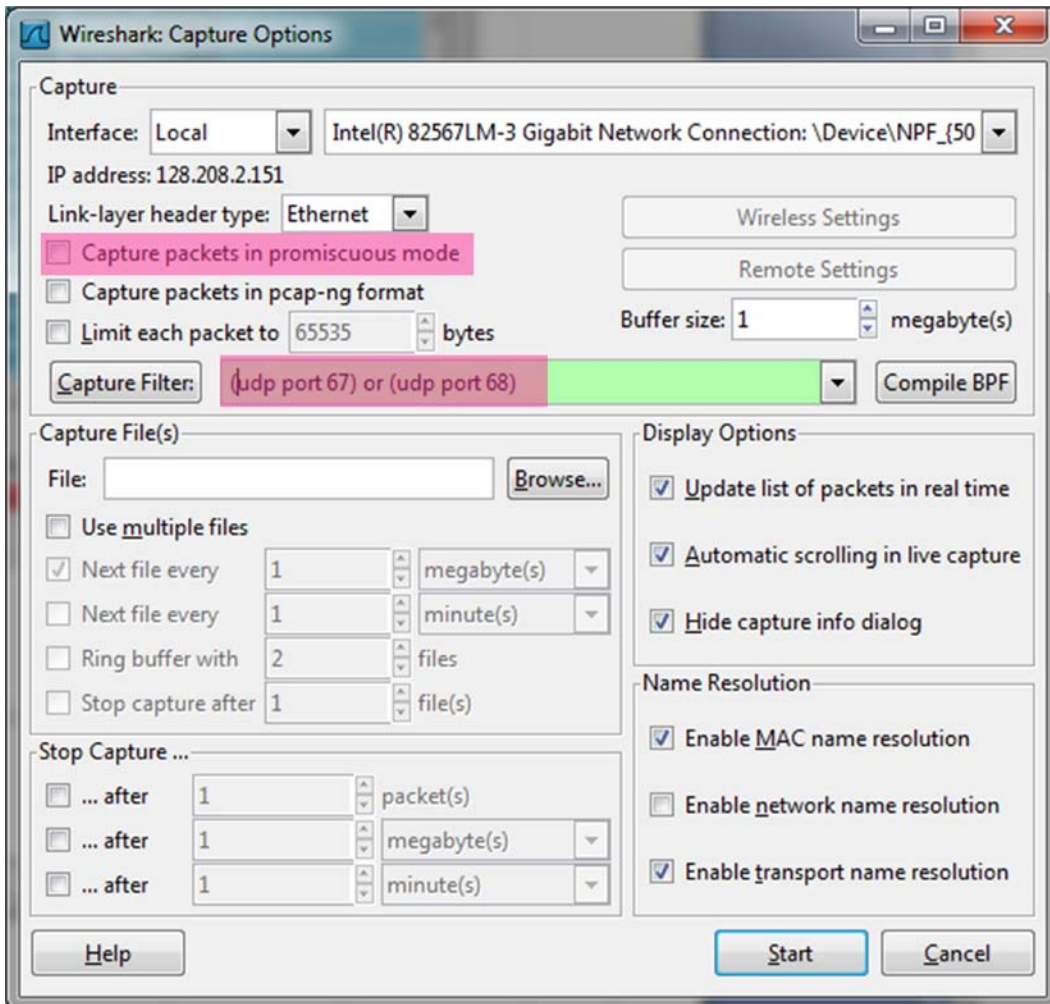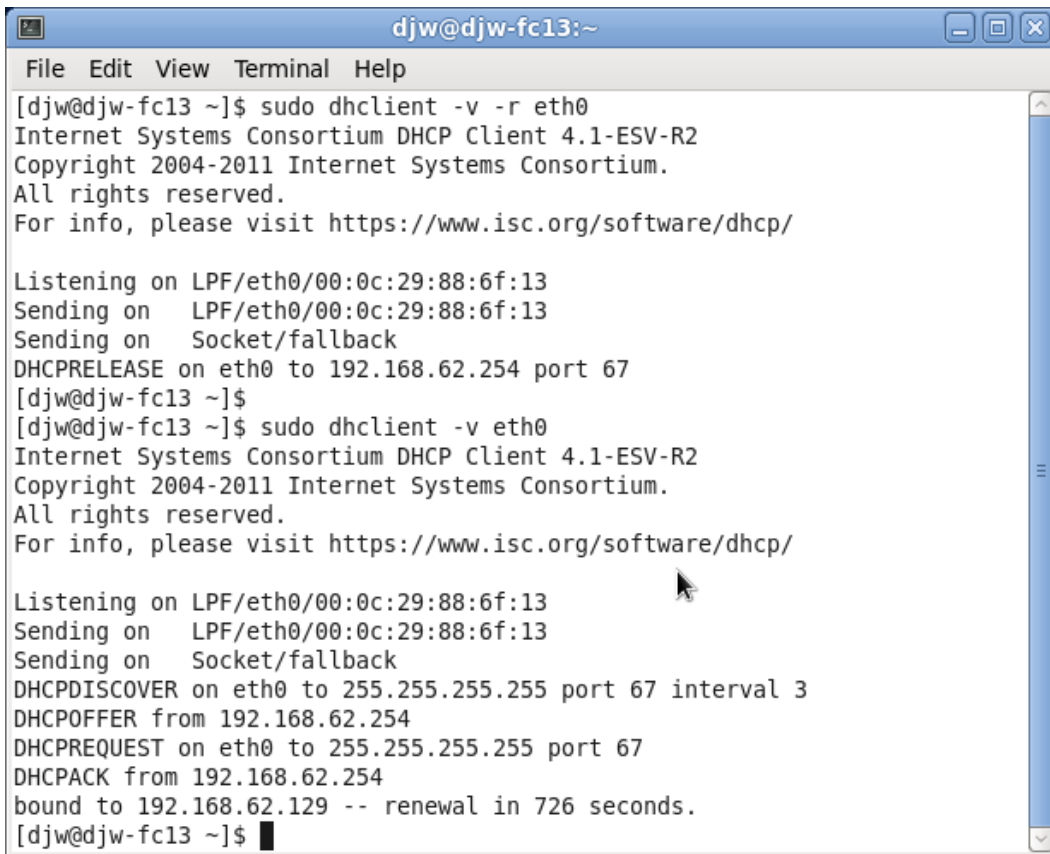

Figure 3: Setting up the capture options

2. *When the capture is started, release and renew your IP address with the command given below.* This procedure may cause your computer to lose network connectivity temporarily, and depending on the operating system it may disrupt network connections. To minimize the disruption, close any programs that are using remote servers and enter the commands into a local window.

Windows: Type the command "`ipconfig /release`" followed by "`ipconfig /renew`". (See figure below.)

Mac: Find the name of the main network interface by typing "`ifconfig`" and observing the output. The interface may be called "en0" or something else. Now use "`ifconfig`" to shut the main interface down and then bring it back up. This will force your computer to renew its IP ad-

dress lease. Note that the commands may require administrator privilege. Type, for example, "`sudo ifconfig en0 down`" followed by "`sudo ifconfig en0 up`". Alternatively, you may use the Network panel under System Preferences to turn the main network interface off and then back on without using the command line interface. Note: do not use the button "Renew DHCP lease" under Advanced options, as it will generate more restricted DHCP traffic.

Linux: Find the name of the main network interface by typing "`ifconfig`" and observing the output. The interface may be called "eth0" or something else. Now use the "`dhclient`" command to first release the leased IP address and then to renew the lease. Type, for example, "`sudo dhclient -r eth0`" to do the release followed by "`sudo dhclient eth0`" to renew the lease. (See figure below, with the "-v" option used to provide verbose output.)

```
djw@djw-fc13:~
File  Edit  View  Terminal  Help
[djw@djw-fc13 ~]$ sudo dhclient -v -r eth0
Internet Systems Consortium DHCP Client 4.1-ESV-R2
Copyright 2004-2011 Internet Systems Consortium.
All rights reserved.
For info, please visit https://www.isc.org/software/dhcp/

Listening on LPF/eth0/00:0c:29:88:6f:13
Sending on   LPF/eth0/00:0c:29:88:6f:13
Sending on   Socket/fallback
DHCPRELEASE on eth0 to 192.168.62.254 port 67
[djw@djw-fc13 ~]$
[djw@djw-fc13 ~]$ sudo dhclient -v eth0
Internet Systems Consortium DHCP Client 4.1-ESV-R2
Copyright 2004-2011 Internet Systems Consortium.
All rights reserved.
For info, please visit https://www.isc.org/software/dhcp/

Listening on LPF/eth0/00:0c:29:88:6f:13
Sending on   LPF/eth0/00:0c:29:88:6f:13
Sending on   Socket/fallback
DHCPDISCOVER on eth0 to 255.255.255.255 port 67 interval 3
DHCPOFFER from 192.168.62.254
DHCPREQUEST on eth0 to 255.255.255.255 port 67
DHCPACK from 192.168.62.254
bound to 192.168.62.129 -- renewal in 726 seconds.
[djw@djw-fc13 ~]$
```

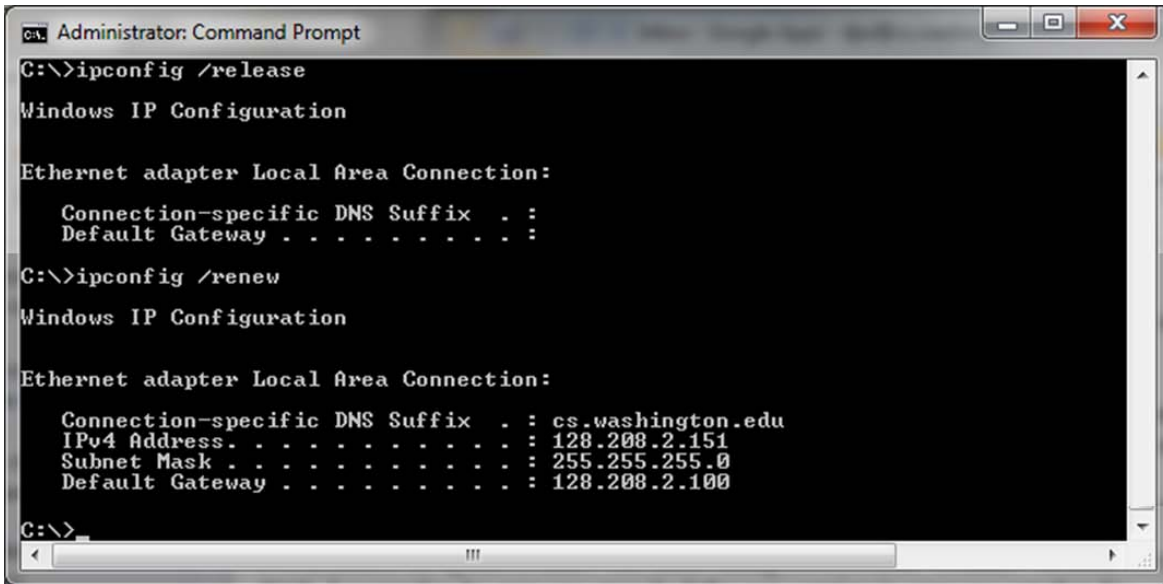Figure 4: Releasing and renewing the IP address on Linux

Figure 5: Releasing and renewing the IP address on Windows

3. *Once you have captured some DHCP traffic, stop the capture.*

Step 2: Inspect the Trace

In this step and the steps that follow, we will inspect only the short DHCP exchange described above. This is because the traffic you have captured can vary widely across settings. You may have as few as two DHCP packets on a quiet network or many DHCP packets on a busy network (especially if a class is running this lab!). The details of DHCP packets may vary depending on how the computers implement DHCP. There may be multiple packets of a single kind in an exchange due to replicated servers, and different types of DHCP packets too.

Look for the short DHCP exchange (of a DHCP Request packet followed by a DHCP Ack packet) in your trace. Select the DHCP Request packet, and observe the protocol stack to see how DHCP messages are carried. The link protocol is likely Ethernet, and the next higher protocol is IP. Then comes UDP, so each DHCP message is carried in a UDP packet. On top of UDP, Wireshark is likely to say BOOTP (Bootstrap Protocol) instead of DHCP. This is a bit confusing, but DHCP is implemented as an extension of an older protocol called BOOTP. You can think of the BOOTP section as the DHCP header and message. An example window is shown below.
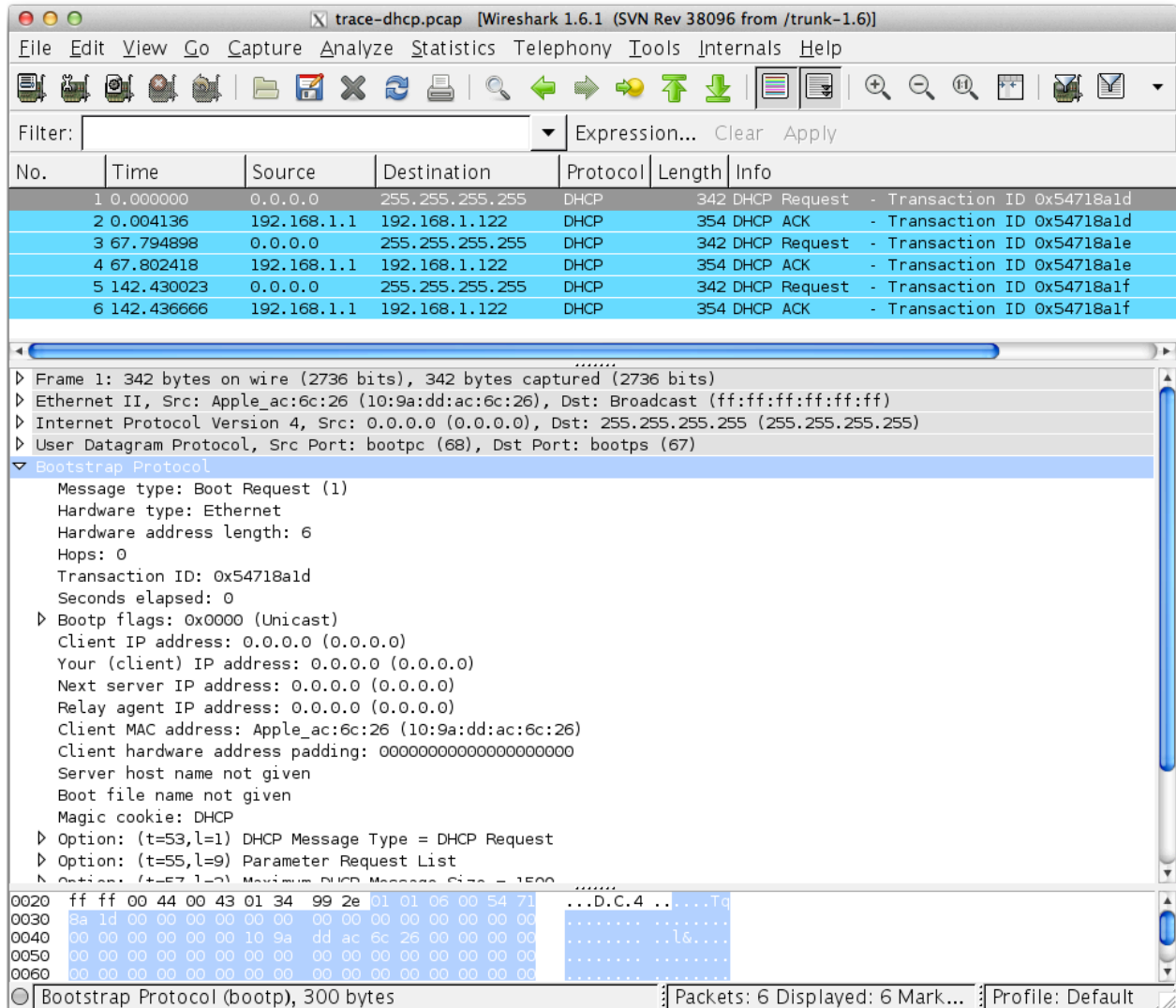
Figure 4: Capture of DHCP packets, showing details of a DHCP Request

Expand the BOOTP (DHCP) section (using the "+" expander or icon) to look at the details of a DHCP Request message. There are many fields, and we will only point out a few rather than cover them all. These fields are carried in all DHCP messages, though they have different values in different messages.

- The message begins with a Message Type. It is a Boot Request, which is used for all DHCP messages sent from your computer to a DHCP server.
- After a few fields there is a Transaction ID field. All DHCP packets in a specific exchange between a client and server carry the same transaction ID; that is how both ends know that the packets belong to the exchange rather than another concurrent DHCP operation.
- There are several IP address fields. These fields are used to carry IP addresses such as the one that the computer is being assigned.
- There is a Magic Cookie field. It carries a value that indicates the rest of the message contains a series of DHCP Options. That is, this really is a DHCP message, not a BOOTP message.

- Each DHCP option is self-contained, with a type code saying what it represents, along with a length and value. The first option is DHCP Message Type, which says what kind of DHCP message is being carried. The other options vary with the type of DHCP message. For example, a DHCP Request will have a Requested IP Address option to ask for a specific address, which a DHCP Ack will have a IP Address Lease Time option to say for how long the IP address is being assigned.

Now select a DHCP Ack packet and compare the BOOTP fields. We will ask questions about these fields in the next section, but for now want you to observe that the DHCP Ack has the same overall format, but different values for the fields and carries different DHCP options.

You can browse the options for DHCP Requests and Acks to learn about DHCP. You can see, for example, how long the IP address is assigned by the server, whether seconds, minutes, hours or days. You will also see the other configuration parameters that are assigned by the DHCP server, such as the IP address of the domain name server and router, the subnet mask, the domain name for the host, and more.

You can also try to make out the whole sequence of DHCP messages that is exchanged for your network setup. If may be as simple as the short exchange of Request and Ack, or it may be the complete exchange of Discover, Offer, Request and Ack. It may have additional messages such as Release, and it may have multiple of the messages (e.g., two or more Offers or Acks) due to multiple local DHCP servers. Complicating the exchange with your computer is that the trace may capture concurrent DHCP traffic from other local computers. You can use the Transaction IDs to separate the different exchanges, and look at the Ethernet source address to see which DHCP messages were sent by your computer. It is likely that other DHCP traffic is mixed in with your exchange.

Step 3: Details of DHCP Messages

To show your understanding of DHCP, draw a figure that shows a DHCP message. Show the position of the Ethernet, IP, UDP, and BOOTP protocol blocks, but divide the BOOTP protocol block into BOOTP fields (the initial part) and DHCP options (the last part). As usual, you can draw this message as a long thin rectangle, with the fields that are sent first over the network to the left.

Answer the following questions based on your examination of the BOOTP/DHCP fields for both the DHCP Request and DHCP Ack:

1. *What are the two values of the BOOTP Message Type field?*
2. *How long is the Transaction ID field? Say whether it is likely that concurrent DHCP operations done by different computers will happen to pick the same Transaction ID.*
3. *What is the name of the field that carries the IP address that is being assigned to the client?* You will find this field filled in on the DHCP Ack, as that message is completing the assignment.
4. *What is the value of the Magic Cookie that stands for DHCP?*
5. *The first DHCP option is DHCP Message Type. What option value stands for this type?*
6. *DHCP Requests will typically have a Client Identifier option. Look at the value of this option. How does it identify the client? Take a guess.*
7. *DHCP Acks will typically have a Server Identifier option. Look at the value of this option. How does it identify the server? Take a guess.*

8. *What option value stands for the Requested IP Address option? And for the IP Address Lease Time option?*
9. *How does the recipient of a DHCP message know that it has reached the last option?*

Turn-in: Hand in your drawing of a DHCP message and the answers to the questions.

Step 4: DHCP Message Addressing
Now we will look at how DHCP messages are addressed to computers at the UDP, IP and Ethernet layers. This is interesting because DHCP is used to assign IP addresses – a computer requesting a DHCP address may neither have its own IP address nor know the IP address of the DHCP server!

Start by selecting a DHCP Request packet and looking at its UDP details in the middle Wireshark panel. We will only look at the DHCP Request message to keep things simple, as the details of addressing differ for other DHCP messages.

1. *What port number does the DHCP client use, and what port number does the DHCP server use?* Ports matter because UDP messages are addressed using ports. Both of these port numbers are on the Request in the source and destination port fields (and you will also see them on the Ack).

Now look at the IP addresses in the IP protocol header of the packet for the next question. Do not look inside the BOOTP fields for the DHCP parameters, as we care about how DHCP messages are addressed at lower protocol layers. When the request is sent, your computer has no IP address and may not even know the IP address of the DHCP server, so the IP addressing differs from a routine IP packet.

2. *What source IP address is put on the Request message?* It is a special value meaning "this host on this network" used for initialization.
3. *What destination IP address is put on the Request message?* It is also a reserved value designed to reach the DHCP server wherever it is on the local network.

Finally, look at the Ethernet addresses for the next question.

4. *What source Ethernet address is put on the Request message, and what destination Ethernet address is put on the Request message?* One of these addresses is a reserved address.

Looking at the addressing should help you to understand why your computer may record the DHCP traffic of other local computers in your trace. Since the IP addressing is not yet established, many DHCP messages are sent to all computers on the local network. This makes sure every computer receives DHCP messages intended for them, but it poses a difficulty: one computer may receive DHCP messages intended for another computer.

5. *How does a computer work out whether a DHCP message it receives is intended as a reply to its DHCP Request message, and not a reply to another computer?* Hint: if you are not sure then go over the fields you inspected previously in Step 2 above.

Turn-in: Your answers to the above questions.

Explore on your own

We encourage you to explore DHCP on your own once you have completed this lab. Some ideas:

- Identify where your DHCP server is on your network, e.g., your AP, or a computer in your ISP?
- Look to see if you can work out the DHCP sequence used by your computer. It is likely to be more involved than the short exchange we studied.
- Find out how a DHCP Relay works to allow one DHCP server to serve multiple networks.
- Find out how replicated DHCP servers work to provide added reliability.
- Look for other kinds of DHCP messages, such as Release and Inform.
- Gather a trace of DHCP activity from different computer to see how DHCP implementations vary from platform to platform.

[END]