## Wireshark Lab: DHCP v6.0

Supplement to *Computer Networking: A Top-Down* Approach,  $6^{ih}$  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

© 2005-21012, J.F Kurose and K.W. Ross, All Rights Reserved

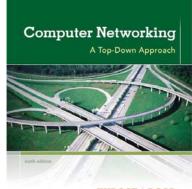
In this lab, we'll take a quick look at DHCP. DHCP is covered in Section 4.4.2 of the text. Recall that DHCP is used extensively in corporate, university and home-network wired and wireless LANs to dynamically assign IP addresses to hosts (as well as to configure other network configuration information).

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.

## **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  $\stackrel{2}{:}$ 

 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



KUROSE ROSS

References to figures and sections are for the 6<sup>th</sup> edition of our text, *Computer Networks, A Top-down Approach,* 6<sup>th</sup> ed., J.F. Kurose and K.W. Ross, Addison-Wesley/Pearson, 2012.

If you are unable to run Wireshark live on a computer, you can download the zip file <a href="http://gaia.cs.umass.edu/wireshark-labs/wireshark-traces.zip">http://gaia.cs.umass.edu/wireshark-labs/wireshark-traces.zip</a> 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.

command releases your current IP address, so that your host's IP address becomes 0.0.0.0.

- 2. Start up the Wireshark packet sniffer, as described in the introductory Wireshark lab and begin Wireshark packet capture.
- 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
- 4. Wait until the "*ipconfig /renew*" has terminated. Then enter the same command "*ipconfig /renew*" again.
- 5. When the second *"ipconfig /renew"* terminates, enter the command "ipconfig/release" to release the previously-allocated IP address to your computer.
- 6. Finally, enter "*ipconfig /renew*" to again be allocated an IP address for your computer.
- 7. Stop Wireshark packet capture.

🔤 Command Prompt	
C:\WINDOWS\SYSTEM32>ipconfig/release	<u> </u>
Windows IP Configuration	
IP Address for adapter Local Area Connection has already	y been released.
C:\WINDOWS\SYSTEM32>ipconfig/renew	
Windows IP Configuration	
Ethernet adapter Local Area Connection:	
Connection-specific DNS Suffix . : ne2.client2. IP Address 192.168.1.10 Subnet Mask 255.255.	ð1
C:\WINDOWS\SYSTEM32>ipconfig/renew	
Windows IP Configuration	
Ethernet adapter Local Area Connection:	
Connection-specific DNS Suffix .: ne2.client2. IP Address	<b>31</b>
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. IP Address	ð1
C:\WINDOWS\SYSTEM32>_	
5005	
•	<u>)</u>

Figure 1 Command Prompt window showing sequence of *ipconfig* commands that you should enter.

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.

<mark>((Untitled) - Wireshark</mark> <u>Fi</u> le <u>E</u> dit <u>V</u> iew <u>G</u> o <u>C</u> a	oture <u>A</u> nalyze <u>S</u> tatistics <u>t</u>	<u>H</u> elp										
	💓 🕞 🗔 🗙	°, 🖪	3	⇔ ⇔	<del>©</del> 7	<b>卫</b>		<b>P</b>	€,	Q	Q	<b>F</b>
ilter: bootp			•	<ul> <li><u>Expression</u></li> </ul>	<u>⊂</u> l∋ar	Apply						
lo, . Time	Source	Destination		Protoco	I Info							
1 0.000000	0.0.0.0	255.255.2		DHCP		Discove					0xe22	0d8c
3 0.996942	192.168.2.1	255.255.2				Offer		ransa	a state of the second second		0xe22	
4 0.997777 5 0.998501	0.0.0.0 192.168.2.1	255.255.2		DHCP	DHCP	Request ACK		ransa ransa				
25 10.366799	192.168.2.145	192.168.2		DHCP		Request		ransa			0xb40	
26 10.367574	192.168.2.1	255.255.2		DHCP	DHCP			ransa				
29 18.103802 30 26.509019	192.168.2.145 0.0.0.0	192.168.2 255.255.2		DHCP		Release Discove		ransa				
32 27.502890	192.168.2.1	255.255.2		DHCP		offer		ransa				
33 27.503705	0.0.0.0	255.255.2				Request		ransa				
34 27.504404	192.168.2.1	255.255.2	55.255	DHCP	DHCP	ACK	- T	ransa	ction	ID	0xee7	1773
											1	12
Destatuse Durta										_		D
Bootstrap Protoc	(a) (A) is a single set of the											
	Boot Request (1)											
Hardware type:												
Hardware addre	ss length: 6											
Hops: 0												
Transaction ID												
Seconds elapse												
Bootp flags: 0     Solution     Sol	김 승규가 같은 것 같아요. 한 것 같은 것 같아요. 같은 것 같아요. 이야한다											
	ess: 0.0.0.0 (0.0.0	CONST NO NO NORA										
(C.M.) Sec	IP address: 0.0.0.0	201 TO 101 101 101										
	address: 0.0.0.0 (											
	address: 0.0.0.0 (	221 DZ DB DS		IC								
	ress: Netgear_61:8e	e:oa (00:09	:50:61	.:8e:6d)								
Server host na	이 가지 않는 것 같은 것 같은 것 같은 것 같은 것 같아요.											
Boot file name	전 1 1 1 1 1 2 2											
Magic cookie:												
	l=1) DHCP Message T			iver								
	,l=1) DHCP Auto-Cor											
	l=7) ⊂lient identif			0.295								
	1=4) Requested IP A			3.2.145								
	1=10) Host Name = '			65								
	1=8) Vendor class i		= "MSF	т 5.0"								
	l=11) Parameter Rec	quest List										
- 양양 - 가슴 가슴, 가슴 가슴 밤												
End Option												
- 가슴 그 것 같아요. 이 것 같은 것 … 신생한 … 같아? 것 ?												
End Option Padding	0 43 01 34 79 dF	01 01 06 00	) e2 20	0D	c.4 v 1							
End Option Padding 020 ff ff 00 44 ( 030 d8 c3 00 00 (	00 00 00 00 00 00	01 01 06 00 00 00 00 00	0 00 00	0	c.4 y.							_
End Option Padding 020 ff ff 00 44 ( 030 d8 c3 00 00 040 00 00 00 00	00 00 00 00 00 00 00 00 00 00 09 56 61	00 00 00 00 8e 6d 00 00	$   \begin{array}{ccccccccccccccccccccccccccccccccccc$	0	<b>c.4 y.</b>	 .m						
End Option Padding 200 ff ff 00 44 ( 300 d8 c3 00 00 ( 40 00 00 00 00 ( 550 00 00 00 00 00 (	00 00 00 00 00 00 00 00 00 00 09 55 61 00 00 00 00 00 00 00	00 00 00 00 8e 6d 00 00 00 00 00 00	0 00 00 0 00 00 0 00 00	0 0 0	<b>c.4 y.</b> [a							
End option Padding 20 ff ff 00 44 0 30 d8 c3 00 00 0 40 00 00 00 00 0 50 00 00 00 00 0 50 00 00 00 00 0	00 00 00 00 00 00 00 00 00 00 09 56 61 00 00 00 00 00 00 00 00 00 00 00 00 00	00 00 00 00 8e 6d 00 00 00 00 00 00 00 00 00 00	0 00 00 0 00 00 0 00 00	0 0 0	<b>c.4 y.</b> _a	. m						
End Option Padding 20 ff ff 00 44 ( 300 d8 c3 00 00 ( 40 00 00 00 00 ( 50 00 00 00 00 00 00 00 00 ( 50 00 00 00 00 00 00 00 00 ( 50 00 00 00 00 00 00 00 00 00 ( 50 00 00 00 00 00 00 00 00 ( 50 00 00 00 00 00 00 00 00 00 ( 50 00 00 00 00 00 00 00 00 00 ( 50 00 00 00 00 00 00 00 00 00 00 ( 50 00 00 00 00 00 00 00 00 00 00 00 00 ( 50 00 00 00 00 00 00 00 00 00 00 00 00 0	00         00<	00 00 00 00 8e 6d 00 00 00 00 00 00 00 00 00 00 00 00 00	0 00 00 0 00 00 0 00 00 0 00 00 0 00 00 0 00 0		<b>C.4 y.</b> [a	. m						
End Option Padding 20 ff ff 00 44 ( 30 d8 c3 00 00 ( 40 00 00 00 00 ( 50 00 00 00 00 00 00 ( 50 00 00 00 00 00 ( 50 00 00 00 00 00 ( 50 00 00 00 00 00 00 00 ( 50 00 00 00 00 00 00 00 00 00 ( 50 00 00 00 00 00 00 00 ( 50 00 00 00 00 00 00 00 00 00 00 ( 50 00 00 00 00 00 00 00 00 00 00 00 00 0	$\begin{array}{cccccccccccccccccccccccccccccccccccc$	00 00 00 00 8e 6d 00 00 00 00 00 00 00 00 00 00 00 00 00	0 00 00 0 00 00 0 00 00 0 00 00 0 00 00 0 00 0	0 0 0 0 0 0 0	<b>c.4 y.</b>							

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

## What to Hand In:

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 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.

## Answer the following questions:

- 1. Are DHCP messages sent over UDP or TCP?
- 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?
- 3. What is the 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 (Request/ACK) 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 DHCP), 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. 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?
- 10. Explain the purpose of the router and subnet mask lines in the DHCP offer message.
- 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

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.

first server OFFER message, does the client accept this IP address? Where in the client's RESPONSE is the client's requested address?

- 12. Explain the purpose of the lease time. How long is the lease time in your experiment?
  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?
  14. Client's DHCP release message is lost?
- 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.