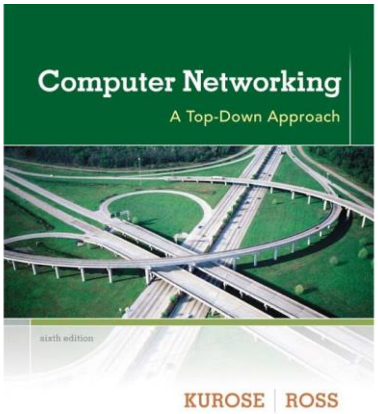
Wireshark Lab: DHCP v6.0



Supplement to *Computer Networking: A Top-Down Approach, 6th 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

Introduction

In this lab, we'll take a quick look at DHCP. 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).

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:

- Begin by opening the Windows Command Prompt application. 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.
- Start up the Wireshark packet sniffer.
- 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.
- Wait until the "*ipconfig /renew*" has terminated. Then enter the same command "*ipconfig /renew*" again.
- When the second *"ipconfig /renew"* terminates, enter the command "ipconfig/release" to release the previously-allocated IP address to your computer.
- Finally, enter "*ipconfig /renew*" to again be allocated an IP address for your computer.
- Stop Wireshark packet capture.

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.)

What to hand in

Modified by: Ifrah Saeed

You should hand in a screen shot of the Command Prompt window showing the execution of commands. 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.

Answer the following questions:

1. **Are DHCP messages sent over UDP or TCP?**
2. **Draw a timing datagram (in wireshark) 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 the book?**
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. **What is 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 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?**
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?**

Modified by: Ifrah Saeed