CSCI 466 Lab 3 – IP & DHCP

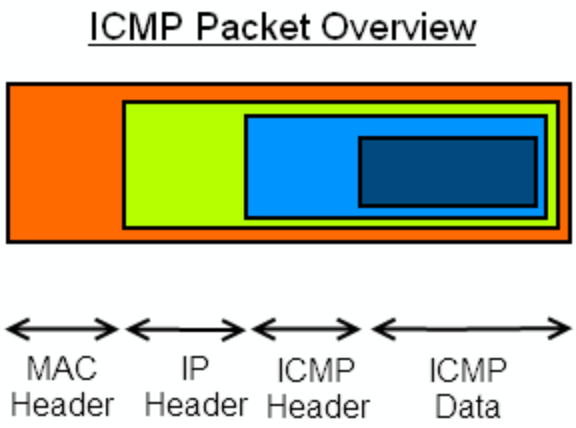
Due Monday October 21st at 11:59 PM

In this lab, you will look at two different Wireshark traces. The first consists of IP traffic, and second consists of DHCP traffic.

Part I: IP Traffic

Inside the same ZIP folder that you downloaded for Lab 2 and Lab 3 (http://gaia.cs.umass.edu/wireshark-labs/wireshark-traces.zip), there should be a file called ***ip-ethereal-trace-1***. Open this file in Wireshark.

This traffic was generated by running the traceroute command (`traceroute gaia.cs.umass.edu 2000`). The traceroute program is a diagnostic command for displaying possible routes and measuring transit delays of packets across an internet network. It does this by sending a series of ICMP packets, which are wrapped in an IP header to a destination host. In the trace, you should be able to see the series of ICMP Echo Requests. As a reminder, here is the structure of an ICMP packet (note that there is not a transport layer header for these packets).



Tasks

1. Select **the first ICMP Echo Request message** sent by the computer and expand the Internet Protocol part of the packet in the packet details window. Take a screenshot and include it in your lab report.
2. What is the IP address of the computer issuing the echo request?
3. What is the IP address of the gaia.cs.umass.edu server?
4. Within the IP packet header, what is the value in the upper layer protocol field? What protocol does this number represent?
5. How many bytes are in the IP header? How many bytes are in the payload of the IP datagram? Explain how you determined the number of payload bytes. **Hint:** You can look at the total length of the captured packet in wireshark. You are welcome to google the size of an IP header and Ethernet header.
6. What is the Time to Live (TTL) value of the packet? What does Time to Live mean?
7. In the IP header, there is a header checksum value. What is the header checksum value used for?
8. Within the ICMP header, there is also a checksum. Why do we have a checksum here when there is already a checksum in the Transport layer?

Next, sort the traced packets according to IP source address by clicking on the Source column header; a small downward pointing arrow should appear next to the word Source. If the arrow points up, click on the Source column header again. Filter for just ICMP traffic by typing "icmp" in the display filter bar. Select **the first ICMP Echo Request message** sent by your computer, and expand the Internet Protocol portion in the "details of selected packet header" window (you might need to scroll down a bit to find this packet). Once you find the packet, use the down arrow on your computer to move through the ICMP messages sent by your computer.

9. Which fields in the IP datagram always change from one datagram to the next within this series of ICMP messages sent by the computer?
10. Which fields stay constant?
11. Describe the pattern you see in the values in the Identification field of the IP datagram.

Part II: DHCP Traffic

Inside the same ZIP folder that you downloaded for Lab 2 and Lab 3 (http://gaia.cs.umass.edu/wireshark-labs/wireshark-traces.zip), there should be a file called ***dhcp-ethereal-trace-1***. Open this file in Wireshark.

This traffic was generated by running the command ***ipconfig/renew***, which instructs a host to obtain a new network configuration, including a new IP address from DHCP. This command was run several times to generate multiple DHCP requests.

Filter for just DHCP traffic by typing "dhcp" inside the display filter bar.

12. Take a screenshot of your Wireshark screen and include it in your lab report.
13. What is the purpose of the DHCP protocol?
14. Are DHCP messages sent over UDP or TCP?
15. What are the four types of DHCP messages?
16. What ports are being used for DHCP traffic?
17. What is the IP address of the DHCP server?
18. What is the link-layer (e.g, Ethernet) address of the host?
19. The packet containing the DHCP Discover message has a source IP of 0.0.0.0 and a destination IP of 255.255.255.255. Are these the *actual* IP addresses of the host/server? What is special about these IP addresses?
20. What IP address is the DHCP server offering to the host? Indicate which DHCP message contains the offered DHCP address.
21. Explain the purpose of the lease time. How long is the lease time for the accepted IP address?
22. Clear the "dhcp" filter from your Wireshark window. Were there any ARP packets sent or received during the DHCP packet-exchange period? If so, explain the purpose of *one* of these packets.