Student Handout

Duration: 1 hour

Objectives:

At the end of this lab students will be able to:

a) Observe UDP packet data
b) Generate UDP traffic
c) Answer key questions based on the UDP packets.

Summary:

You will generate UDP traffic using two methods. You will observe the UDP packets. Then you will generate UDP traffic using Skype and answer the questions.

Procedure

1. Start capturing packets in Wireshark
2. To generate UDP traffic you must Open a command prompt
3. Type **ipconfig /renew** and press **Enter** to renew your DHCP assigned IP address. If you have a static address, this will not generate any UDP traffic.
4. Type **ipconfig /flushdns** and press **Enter** to clear your DNS name cache.
5. Type **nslookup 8.8.8.8** and press **Enter** to look up the hostname for IP address 8.8.8.8.
6. Close the command prompt.
7. Stop the Wireshark capture
8. After stopping packet capture, set your packet filter so that Wireshark only displays the UDP packets sent and received at your host. Pick one of these UDP packets and expand the UDP fields in the details window.
9. Choose a packet and expand various sections, observing information.
10. **To do the rest of the steps you will need to generate packets using Skype. Or you can load the Wireshark_802_11 file.**
11. Select one packet. From this packet, determine how many fields there are in the UDP header. (Do not look in the textbook! Answer these questions directly from what you observe in the packet trace.) Name these fields.
12. From the packet content field, determine the length (in bytes) of each of the UDP header fields.
13. The value in the Length field is the length of what? Verify your claim with your captured UDP packet.
14. What is the maximum number of bytes that can be included in a UDP payload.
15. Examine a pair of UDP packets in which the first packet is sent by your host and the second packet is a reply to the first packet. Describe the relationship between the port numbers in the two packets. (hints use Follow UDP stream)