Wireshark Lab: DHCP and NAT

Submit online as a pdf in Canvas

General Instructions: What to hand in: Please answer the questions posed in this lab, please make it clear what questions you are answering, and please use screenshots to support your answers. Marks will be awarded for correctness, completeness, and professionalism. You'll also be using this document to study for your tests and exams.

Whenever possible, when answering a question below, create a screenshot 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.

Learning Outcome: At the end of this lab you should:

- Be familiar with the different DHCP message types.
- Understand the role of the DHCP server in any network.
- Be able to explain the operation of DHCP.
- Understand NAT translation tables.

Exercise 1

Objective for Exercise 1: Observe DHCP in action

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:

1. 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 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 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.
4. Wait until the "`ipconfig /renew`" has terminated. Then enter the command "`ipconfig/release`" to release the allocated IP address to your computer
5. Finally, enter "`ipconfig /renew`" to again be allocated an IP address for your computer.
6. Stop Wireshark packet capture (Note: the two renews can take a LONG time i.e. minutes).

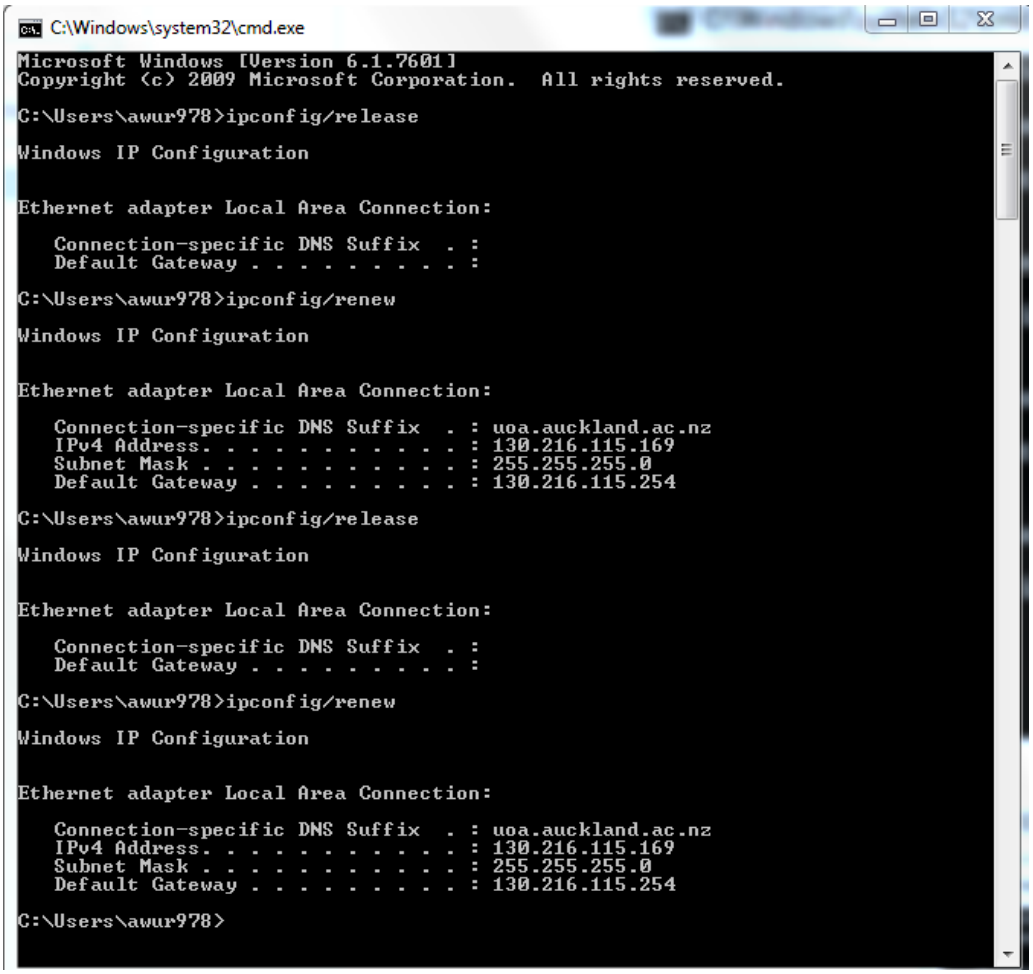

Figure 1 Command Prompt window showing sequence of `ipconfig` commands that you should enter.

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. 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.

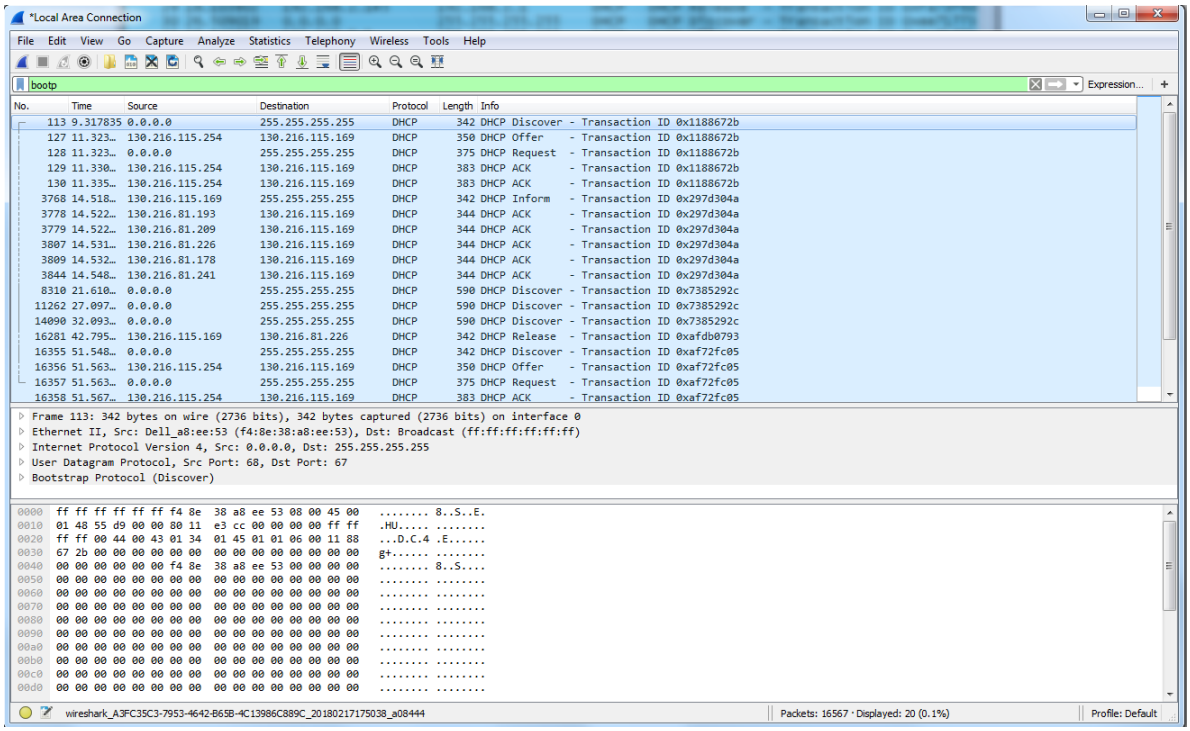

Figure 2 Wireshark window with the DHCP Release and Renew Process

Actions

You should create a screenshot of the Command Prompt window similar to Figure 1 above. Whenever possible, when answering a question below, create a screenshot 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.

Questions:

1.1 Using Statistics->Protocol Hierarchy, identify four other protocols in use during the packet capture,

1.2 Using Statistics->Protocol Hierarchy, identify what was the percentage of Bytes used by the bootstrap (DHCP) protocol.

1.3 Are DHCP messages sent over UDP or TCP?

1.4 Plot a flow graph illustrating the sequence of the first four-packet Discover/Offer/Request/ACK DHCP exchange between the client and server. For each packet, indicate the source and destination port numbers.

1.5 Apart from the Discover/Offer/Request/ACK DHCP message types, which other DHCP message types did you observe in your capture?

1.6 What three options in the DHCP discover message differentiate this message from the DHCP request message?

1.7 The DHCP packets can carry quite a lot of information to a client. Using the first Offer DHCP packet in your capture; answer the following

- 1.7.1 What is the transaction ID (transaction ID is a random number used to pair requests with responses)
- 1.7.2 What is the IP address of your DHCP server?
- 1.7.3 What IP address is the DHCP server offering to your host

1.7.4 What is the IP of the network's default gateway (a.k.a relay agent)
1.7.5 What does is the function of a relay agent?
1.7.6 What is the client's (host) MAC address

1.8 Explain the purpose of the router and subnet mask lines in the DHCP offer message.

1.9 Explain the purpose of the lease time?

1.10 How long is the lease time in your experiment?

1.11 Using the first Discover packet answer the following

1.11.1 What is the source IP address for this discover packet and why
1.11.2 What is the destination address of the discover packet and why
1.11.3 What is the source and destination port number

Exercise 2

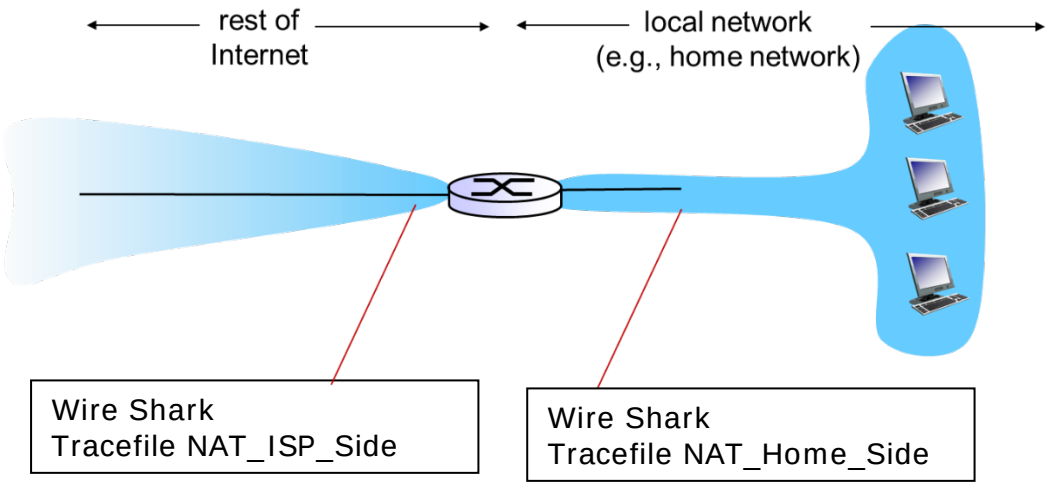

Figure 3 NAT trace collection Scenario

In this exercise, we investigate trace files of captured packets from a simple web request from a client PC in a home network to a www.google.com server. Within the home network, the home network router provides a NAT service, as discussed in Chapter 4. Figure 3 shows our Wireshark trace-collection scenario. There is a Wireshark trace on the client PC in a home network. This file is called `NAT_home_side`. Because we are also interested in the packets being sent by the NAT router into the ISP, there is a second trace file at a PC (not shown) tapping into the link from the home router into the ISP network, as shown in Figure 3. (The hub device shown on the ISP side of the router is used to tap into the link between the NAT router and the first hop router in the ISP). Client-to-server packets captured by Wireshark at this point will have undergone NAT translation. The Wireshark trace file captured on the ISP side of the home router is called `NAT_ISP_side`.

You are going to compare the files `NAT_home_side.pcap` and `NAT_ISP_side.pcap`. In the comparison set the Wireshark filter so it only shows HTTP messages sent to and from the main Google server (IP address 64.233.169.104).

Questions:

2.1 In the `NAT_home_side` trace file what packet number is the first HTTP get?

2.2 Consider now in the `NAT_home_side` trace file the HTTP GET sent from the client to the Google server (whose IP address is IP address 64.233.169.104) at time

7.109267. What are the source and destination IP addresses and TCP source and destination ports on the IP datagram carrying this HTTP GET?

2.3 In the NAT_ISP_side trace file, find the HTTP GET message was sent from the client to the Google server at time 7.109267 (where t=7.109267 is time at which this was sent as recorded in the NAT_home_side trace file). At what time does this message appear in the NAT_ISP_side trace file? What are the source and destination IP addresses and TCP source and destination ports on the IP datagram carrying this HTTP GET (as recording in the NAT_ISP_side trace file)?

2.4 Which of these fields in Q2.3 are the same, and which are different, than in your answer to Q2.2?

2.5 Create a NAT translation table from the information you have obtained in Q2.2 and Q2.3 (refer to lecture notes if you are unsure what a NAT translation table is).

2.6 Compare the two trace files and identify which of the following fields in the IP datagram carrying the HTTP GET are changed: Version, Header Length, Flags, Checksum. If any of these fields have changed, give a reason (in one sentence) stating why this field needed to change.