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.
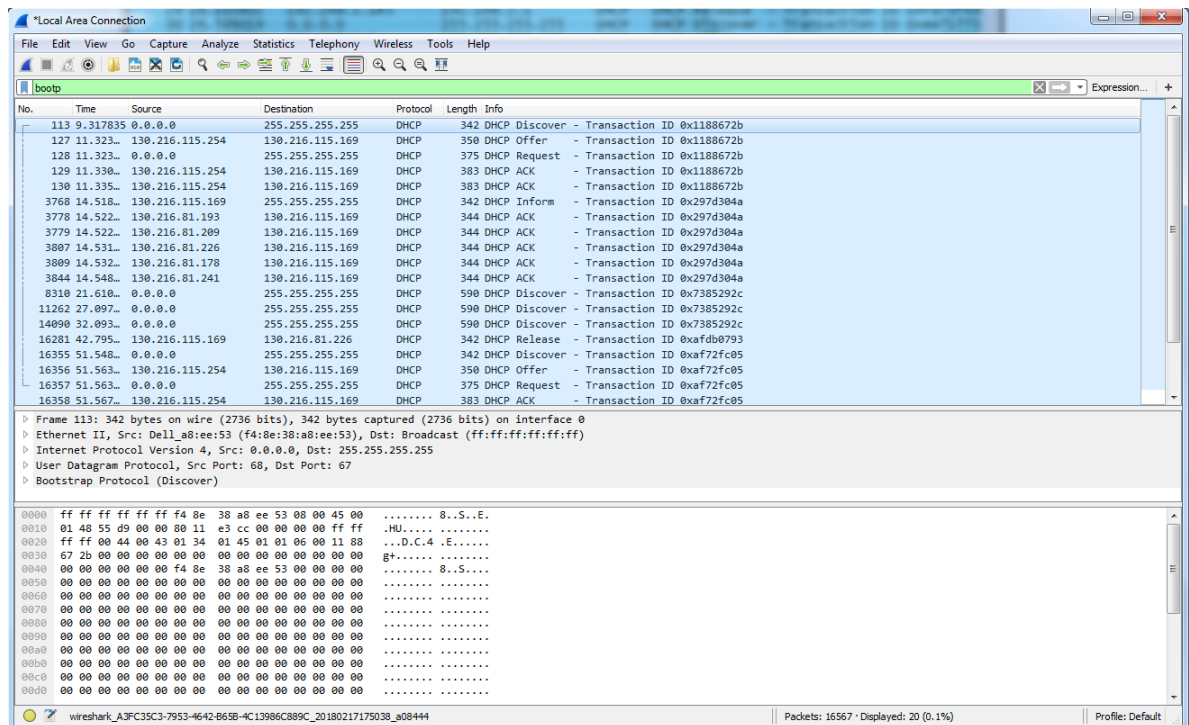
Figure 2 Wireshark window with the DHCP Release and Renew Process

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,

Frame, Ethernet, Internet Protocol, User Datagram Protocol

1.2 Using Statistics->Protocol Hierarchy, identify what was the percentage of Bytes used by the bootstrap (DHCP) protocol.
87.7% of the bytes were used by DHCP protocol

1.3 Are DHCP messages sent over UDP or TCP?
UDP as shown in the photo

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.

Time	0.0.0.0	255.255.255.255	192.168.1.1	192.168.1.11	Comment
12.533903	68 DHCP Discover - Transaction ID 0x6d... 67				DHCP: DHCP Discover - Transaction ID 0x6d72f209
12.539181			67 DHCP Offer - Transaction ID 0x6d7... 68		DHCP: DHCP Offer - Transaction ID 0x6d72f209
12.539679	68 DHCP Request - Transaction ID 0x6d... 67				DHCP: DHCP Request - Transaction ID 0x6d72f209
12.546229			67 DHCP ACK - Transaction ID 0x6d... 68		DHCP: DHCP ACK - Transaction ID 0x6d72f209

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

```
   130 12.539679    0.0.0.0          255.255.255.255   DHCP    370 DHCP Request  - Transaction ID 0x6d72f209
   131 12.546229    192.168.1.1      192.168.1.11      DHCP    326 DHCP ACK       - Transaction ID 0x6d72f209
  1517 29.467149    192.168.1.11     192.168.1.1       DHCP    342 DHCP Release   - Transaction ID 0xba98c38b
  1675 35.170165    0.0.0.0          255.255.255.255   DHCP    344 DHCP Discover  - Transaction ID 0x9a36d49a
```

DHCP Release message type

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

```
Magic cookie: DHCP
> Option: (53) DHCP Message Type (Discover)
> Option: (61) Client identifier
> Option: (50) Requested IP Address (192.168.1.11)
> Option: (12) Host Name
> Option: (60) Vendor class identifier
> Option: (55) Parameter Request List
∨ Option: (255) End
    Option End: 255
```

```
> Option: (53) DHCP Message Type (Request)
> Option: (61) Client identifier
> Option: (50) Requested IP Address (192.168.1.11)
> Option: (54) DHCP Server Identifier (192.168.1.1)
> Option: (12) Host Name
> Option: (81) Client Fully Qualified Domain Name
> Option: (60) Vendor class identifier
> Option: (55) Parameter Request List
> Option: (255) End
```

The DHCP message type for discover

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)

```
Hops: 0
Transaction ID: 0x6d72f209
Seconds elapsed: 0
```

0x6d72f209

1.7.2 What is the IP address of your DHCP server?

```
∨ Option: (54) DHCP Server Identifier (192.168.1.1)
    Length: 4
    DHCP Server Identifier: 192.168.1.1
```

192.168.1.1

1.7.3 What IP address is the DHCP server offering to your host?

```
Seconds elapsed: 0
> Bootp flags: 0x0000 (Unicast)
  Client IP address: 0.0.0.0
  Your (client) IP address: 192.168.1.11
  Next server IP address: 0.0.0.0
```

192.168.1.11

1.7.4 What is the IP of the network's default gateway (a.k.a relay agent)

```
Relay agent IP address: 0.0.0.0
```

0.0.0.0

1.7.5   What does is the function of a relay agent?
A relay agent relays DHCP messages between clients and servers on
different networks.

1.7.6   What is the client's (host) MAC address

```
Relay agent IP address: 0.0.0.0
Client MAC address: IntelCor_7f:06:84 (c0:b8:83:7f:06:84)
Client hardware address padding: 00000000000000000000
```

The client's MAC address is c0:b8:83:7f:06:84

1.8   Explain the purpose of the router and subnet mask lines in the DHCP offer
message.
The router option informs the host of the IP address for the router, so the
host can make requests later on.
The subnet mask tells the user how much of the ip address is dedicated to
the network, and how much is for host addresses.

1.9   Explain the purpose of the lease time?
The lease time is how long the host has access to that particular IP
address. No other host will be able to use that IP address for the lease
time, and this lease can be renewed upon negotiation.

1.10   How long is the lease time in your experiment?

```
∨ Option: (51) IP Address Lease Time
     Length: 4
     IP Address Lease Time: (86400s) 1 day
```

86400s or 1 day

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

```
∨ Internet Protocol Version 4, Src: 0.0.0.0, Dst: 255.255.255.255
```

The src ip is 0.0.0.0, which is a special IPv4 address indicating the
host computer, and is used during bootstrap.

1.11.2 What is the destination address of the discover packet and why

The destination ip is 255.255.255.255. This is a special IPv4 address
which indicates a limited broadcast to the entire local network.

1.11.3 What is the source and destination port number

```
∨ User Datagram Protocol, Src Port: 68, Dst Port: 67
```

The source port number is 68. The destination port number is 67.

Exercise 2

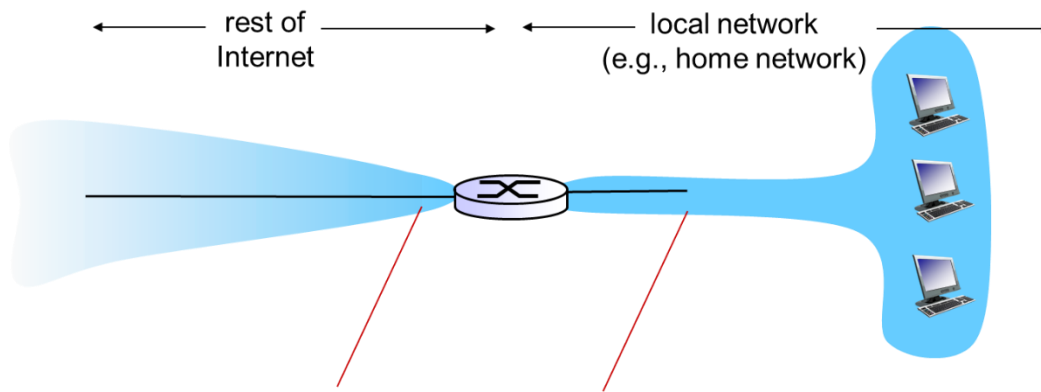| Wire Shark	Wire Shark
Tracefile NAT_ISP_Side	Tracefile NAT_Home_Side

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?

55 7.109053	192.168.1.100	64.233.169.104	TCP	54 4335 → 80 [ACK] Seq=1 Ack=1 Win=260176 Len=0	
56 7.109267	192.168.1.100	64.233.169.104	HTTP	689 GET / HTTP/1.1	
57 7.140728	64.233.169.104	192.168.1.100	TCP	60 80 → 4335 [ACK] Seq=1 Ack=636 Win=7040 Len=0	

Packet number 56 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?

> Internet Protocol Version 4, Src: 192.168.1.100, Dst: 64.233.169.104
> Transmission Control Protocol, Src Port: 4335, Dst Port: 80, Seq: 1, Ack: 1, Len: 635

Src ip addr: 192.168.1.100
Dst ip addr: 64.233.169.104
Src port: 4335

Dst port: 80

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)?

84 6.068754	71.192.34.104	64.233.169.104	TCP	60 4335 → 80 [ACK] Seq=1 Ack=1 Win=260176 Len=0
85 6.069168	71.192.34.104	64.233.169.104	HTTP	689 GET / HTTP/1.1
87 6.099637	64.233.169.104	71.192.34.104	TCP	60 80 → 4335 [ACK] Seq=1 Ack=636 Win=7040 Len=0

The time that the message appears in the NAT_ISP side trace file is 6.09168s.
Src ip addr: 71.192.34.104

> Internet Protocol Version 4, Src: 71.192.34.104, Dst: 64.233.169.104
> Transmission Control Protocol, Src Port: 4335, Dst Port: 80, Seq: 1, Ack: 1, Len: 635

Dst ip addr: 64.233.169.104
Src port: 4335
Dst port: 80

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

The destination ip address, source port, and destination port are the same. The
source ip address is different.

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).

WAN-Side Address	LAN-Side Address
71.192.34.104, 4335	192.168.1.100, 4335

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.

```
∨ Internet Protocol Version 4, Src: 192.168.1.100, Dst: 64.233.169.104        ∨ Internet Protocol Version 4, Src: 71.192.34.104, Dst: 64.233.169.104
    0100 .... = Version: 4                                                          0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)                                         .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)                  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 675                                                               Total Length: 675
    Identification: 0xa2ac (41644)                                                  Identification: 0xa2ac (41644)
  > Flags: 0x4000, Don't fragment                                                  > Flags: 0x4000, Don't fragment
    Fragment offset: 0                                                              Fragment offset: 0
    Time to live: 128                                                              Time to live: 127
    Protocol: TCP (6)                                                               Protocol: TCP (6)
    Header checksum: 0xa94a [validation disabled]                                   Header checksum: 0x022f [validation disabled]
    [Header checksum status: Unverified]                                           [Header checksum status: Unverified]
    Source: 192.168.1.100                                                          Source: 71.192.34.104
    Destination: 64.233.169.104                                                    Destination: 64.233.169.104
  > Transmission Control Protocol, Src Port: 4335, Dst Port: 80, Seq: 1, Ack: 1, Len: 635    > Transmission Control Protocol, Src Port: 4335, Dst Port: 80, Seq: 1, Ack: 1, Len: 635
```

Version, header length, and flags are the same. The checksum has changed, as the
checksum is calculated using the source ip address, which has changed.