



RC 19/20	LAB ASSIGNMENT	Guide.Part #:	5.0
From Application Layer to Link Layer		Issue Date:	2 Dec 2019
Analysis of DHCP, NAT, Ethernet and ARP		Due Date:	
Author: Prof. Rui Cruz		Revision:	1.0

1 Introduction

The objective of the experiments in this Lab assignment is to investigate the protocols at the Link Layer, namely the Ethernet protocol and the Address Resolution Protocol (ARP), as well as take a quick look at how the Dynamic Host Configuration Protocol (DHCP) is used to assign IP addresses to hosts, and also investigate the behavior of the Network Address Translation (NAT) protocol for hosts behind Firewalls with private IP addressing (non-routable).

RFC 826 (<https://tools.ietf.org/html/rfc826>) contains the details of the ARP protocol, which is used by an IP device to determine the IP address of a remote interface whose Ethernet address is known.

Recall also that DHCP and NAT are used extensively in corporate, university and home-networks. DHCP is used in wired and wireless LANs to assign IP addresses to hosts (as well as to configure other network configuration information). NAT is the process where a network device, usually a firewall or a router, assigns a public address to a computer (or group of computers) inside a private network. The main use of NAT is to limit the number of public IP addresses, for both economy and security purposes.

For NAT analysis we would need to capture packets at both the input and output sides of the NAT device. However, as we do not have easy access to a NAT device we will use **trace files** that were previously captured.

Recommendation: review sections 6.4.1 (Link-layer addressing and ARP) and 6.4.2 (Ethernet), as well as sections 4.3.3 and 4.3.4 of the Book.

Preliminary Notes

The instructions in this document are applicable to Computers at the IST Labs.

Nevertheless, one nice feature of the software stack we are going to use is that it is portable to many platforms including **YOUR OWN** personal computers, running the following Operating Systems:

- Microsoft Windows from version 10 up
- Apple macOS from versions 10.13 'High Sierra' up
- Debian-based Linux, such as Ubuntu (recommended) from versions 12.04 'Precise' up.

It is not recommended to apply this setup to a virtual machine (nested virtualization), although possible, as the configuration requires access to a hypervisor environment (recommended Virtualbox) in the host system.

Before proceeding you should verify if you have a “clean” environment, i.e., no Virtual Machine “instances” running (using precious resources in your system), or inconsistent

RC 19/20	LAB ASSIGNMENT	Guide.Part #:	5.0
From Application Layer to Link Layer		Issue Date:	2 Dec 2019
Analysis of DHCP, NAT, Ethernet and ARP		Due Date:	
Author: Prof. Rui Cruz		Revision:	1.0

instances in Vagrant and Virtualbox. For that purpose run the `vagrant global-status` command and observe the results (as in the following example):

```

:~$ vagrant global-status
id            name        provider    state      directory
-----
28fb48a      mininet     virtualbox  poweroff   /Users/x/Projects/mininet
f0ccec2      web1        virtualbox  running    /Users/x/Projects/multinode
f09c279      web2        virtualbox  running    /Users/x/Projects/multinode

```

In the above example, you can observe that there are three Virtual Machine instances, being the first “mininet”, which is powered off, but two “web” servers still running. It is **advisable to halt VMs** if they are running, and then **clean and destroy VMs from previous Lab experiments** that are not related with this Lab, or that are not anymore needed.

Note: Avoid copying text strings from the command line examples or configurations in this document, as pasting them into your system or files may introduce/modify some characters, leading to errors or inadequate results.

2 Setting up the Experimental Environment

For this Lab experiment you should use or create a project directory, named, for example, **nethack**.

Download the file `RC_19_20_LAB_05_support_files.zip` from the course website and uncompress the content to the **nethack** folder.

The **nethack** project folder should have a structure similar to the following:

```

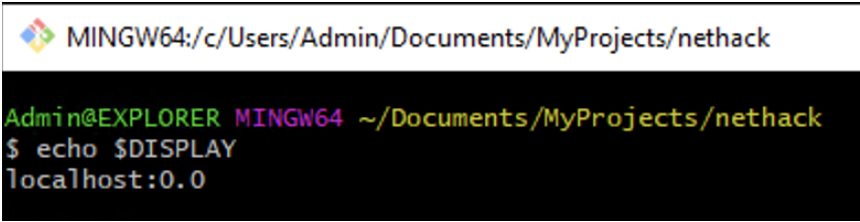
.
|-- Vagrantfile
|-- bootstrap-nethack.sh
|-- data
|   |-- NAT-ISP-side.pcap
|   |-- NAT-home-side.pcap
|   |-- dhcp-trace.pcap
|   |-- ethernet-ethereal-trace.pcap
|   |-- ssl-trace.pcap
|   |-- wifi-802-11.pcap

```

For Microsoft Windows hosts, you need to start “**VcXsrv**” before spin off the lab environment. The “**VcXsrv**” application will start a **X-Windows** server that will forward application GUIs running inside the VM to the host system.

RC 19/20	LAB ASSIGNMENT	Guide.Part #:	5.0
From Application Layer to Link Layer		Issue Date:	2 Dec 2019
Analysis of DHCP, NAT, Ethernet and ARP		Due Date:	
Author: Prof. Rui Cruz		Revision:	1.0

Verify also that you have an environment Variable with name **DISPLAY** and with **Variable value** of `localhost:0.0`, as illustrated in Figure 1.



```

MINGW64:/c/Users/Admin/Documents/MyProjects/nethack
Admin@EXPLORER MINGW64 ~/Documents/MyProjects/nethack
$ echo $DISPLAY
localhost:0.0

```

Figure 1: Verify DISPLAY Variable

For the experiments in this lab you will use **Wireshark** (A network Sniffer and Protocol dissector tool, provisioned and configured in the VM) to capture the packets in the network interface in order for you to analyse them.

For that purpose, you will need two Terminal (Bash) windows opened. On the first window start Wireshark with the following command:

```
$ vagrant ssh -c wireshark -- -X
```

In the second Terminal window start the ssh connection with the VM:

```
$ vagrant ssh
```

2.1 Using Shared Folders in Vagrant

One simple way to share information between one virtual machine, designated as **guest**, and the machine that hosts it, known as the **host**, is by mapping one folder or directory of the **host**'s file system to one folder on the **guest**'s file system.

For the VM in this Lab you have a shared folder, as you can observe in the Vagrantfile in the lines that define them, where the first path is related to the **host** and the second path refers to the **guest**.

```
xxxxx_config.vm.synced_folder "data", "/home/vagrant/data"
```

Having this type of share, you ensure that whatever you have/put on the **"data"** folder in your **host** will appear and be available inside the VM in the **"data"** **home** folder. Similarly, whatever is produced as result of commands or programs will be available on the **"data"** folder in your **host**.

RC 19/20	LAB ASSIGNMENT	Guide.Part #:	5.0
From Application Layer to Link Layer		Issue Date:	2 Dec 2019
Analysis of DHCP, NAT, Ethernet and ARP		Due Date:	
Author: Prof. Rui Cruz		Revision:	1.0

3 Experiment E1: Ethernet

For this experiment load into Wireshark the trace file **ethernet-ethereal-trace.pcap** using the **File** pull down menu, choosing **Open**, and then selecting that trace file from folder **data** (because Wireshark is running in the VM).

Take a look at Figure 2 of the resulting Wireshark window with a set of Ethernet frames to study, captured while visiting the webpage <http://gaia.cs.umass.edu/wireshark-labs/HTTP-ethereal-lab-file3.html> (which displays the rather lengthy US Bill of Rights). First, find the packet numbers (the leftmost column in the upper Wireshark window) of the HTTP GET message that was sent to host **gaia.cs.umass.edu**, as well as the beginning of the HTTP response message received from **gaia.cs.umass.edu**. You can see in the figure that **packet 10** contains the **HTTP GET** message.

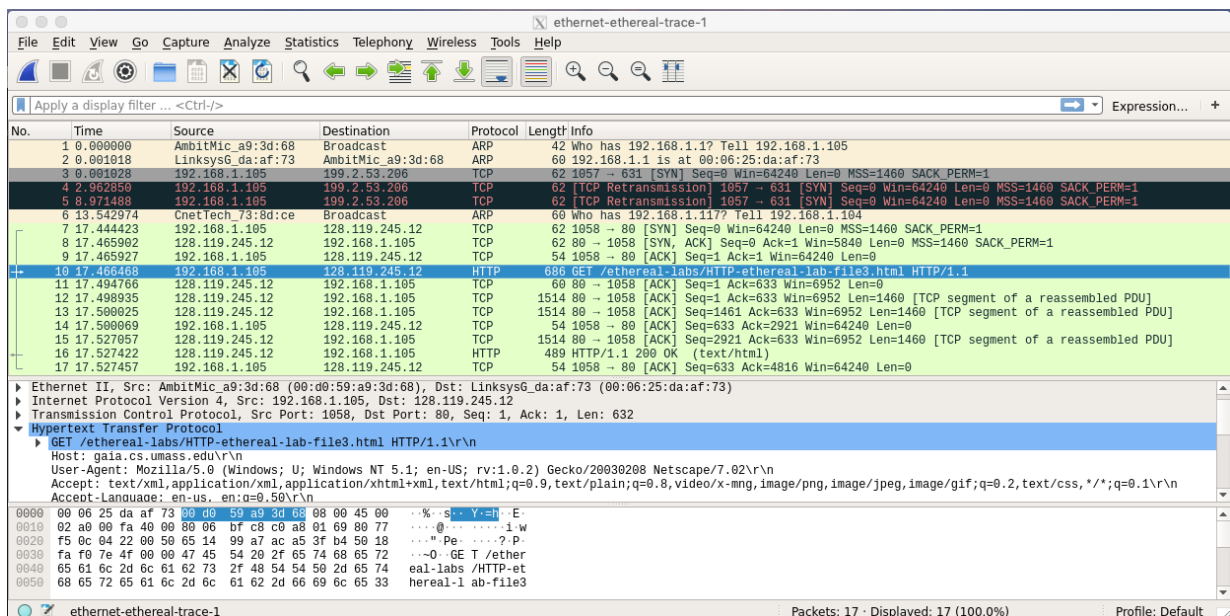


Figure 2: Wireshark window with packet capture

Since this lab is about Ethernet and ARP, we are not interested in IP or higher-layer protocols. So let's change Wireshark's listing of captured packets window so that it shows information only about protocols **below IP**. To have Wireshark do this, select **Analyze** → **Enabled Protocols**. Then uncheck the IPv4 box and select OK. You should now see a Wireshark window that looks like Figure 3:

In order to answer the following questions, you will need to look into the packet details and packet contents windows (the middle and lower display windows in Wireshark). Select the **Ethernet frame** containing the **HTTP GET** message.

Recall that the **HTTP GET** message is carried inside of a **TCP** segment, which is

RC 19/20	LAB ASSIGNMENT	Guide.Part #:	5.0
From Application Layer to Link Layer		Issue Date:	2 Dec 2019
Analysis of DHCP, NAT, Ethernet and ARP		Due Date:	
Author: Prof. Rui Cruz		Revision:	1.0

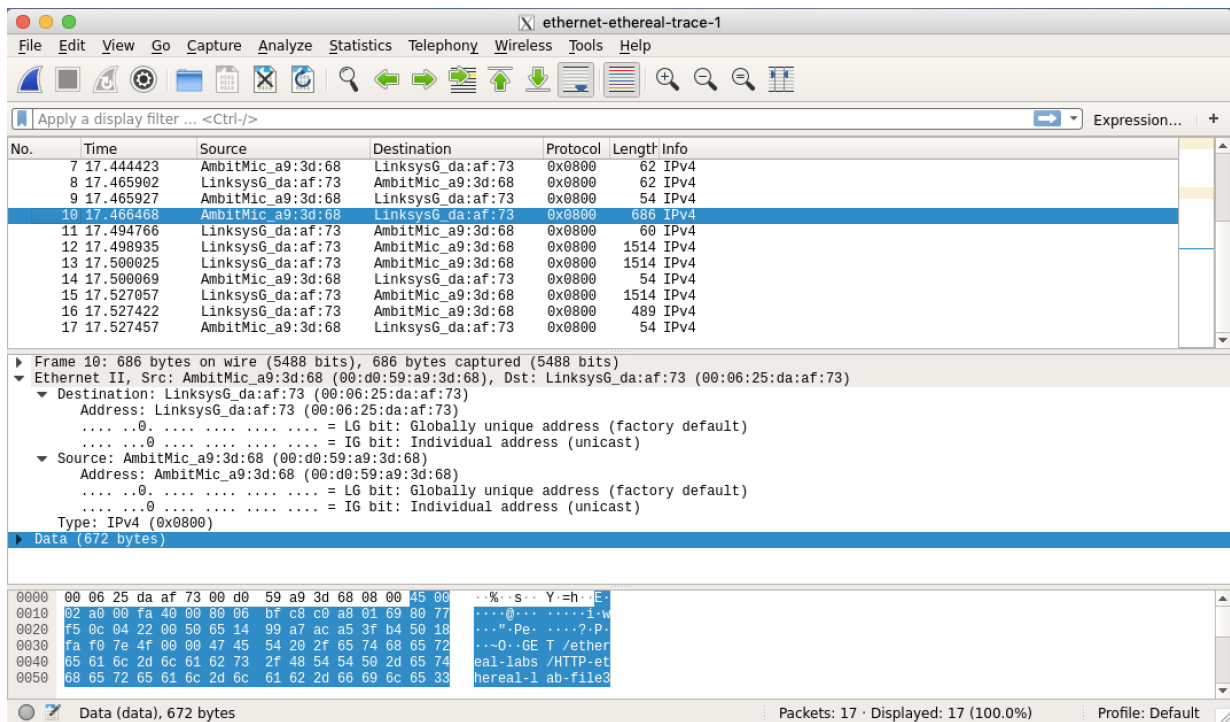


Figure 3: Wireshark window protocols below IP

carried inside of an **IP** datagram, which is carried inside of an **Ethernet frame**. Expand the **Ethernet II** information in the packet details window. Note that the contents of the **Ethernet frame** (header as well as payload) are displayed in the packet contents window.

Answer the following questions, **based on the contents of the Ethernet frame containing the HTTP GET message**.

When answering a question below, you should hand in a dissection of the packet(s) within the trace that you used to answer the question asked. To export a packet summary/data, use **File** → **Export Packet Dissections** → **As Plain text**, choose **Selected packet only**, choose **Packet summary line**, and select the minimum amount of packet detail that you need to answer the question.

1. What is the 48-bit Ethernet address of the source computer?
2. What is the 48-bit destination address in the Ethernet frame? Is this the Ethernet address of the server **gaia.cs.umass.edu**?
3. What device has that destination address as its Ethernet address? [Note: this is an important question, and one that students sometimes get wrong. Re-read

RC 19/20	LAB ASSIGNMENT	Guide.Part #:	5.0
From Application Layer to Link Layer		Issue Date:	2 Dec 2019
Analysis of DHCP, NAT, Ethernet and ARP		Due Date:	
Author: Prof. Rui Cruz		Revision:	1.0

pages 501-502 in the Book and make sure you understand the answer to give here.]

4. Give the hexadecimal value for the two-byte Frame type field. What upper layer protocol does this correspond to?
5. How many bytes can you count from the very start of the Ethernet frame until the ASCII “**G**” in **GET** appears? Give an interpretation of the meaning or purpose of those bytes.

Next, **based on the contents of the Ethernet frame containing the first byte of the HTTP response message**, answer the following questions.

6. What is the value of the Ethernet source address?
7. Is that source address the one of the destination computer, or of **gaia.cs.umass.edu** (Hint: the answer is no). What device has this as its Ethernet address?
8. What is the destination address in the Ethernet frame? Is this the Ethernet address of destination computer?
9. Give the hexadecimal value for the two-byte Frame type field. What upper layer protocol does this correspond to?
10. How many bytes can you count from the very start of the Ethernet frame until the ASCII “**O**” in the word **OK** appears? Give an interpretation of the meaning or purpose of those bytes.

4 Experiment E2: Address Resolution Protocol (ARP)

In this experiment we will observe the ARP protocol in action.

4.1 ARP Caching

Recall that the ARP protocol typically maintains a cache of IP-to-Ethernet address translation pairs on a computer. The **arp** command (in both Windows and Linux/Unix/macOS) is used to view and manipulate the contents of this cache. Since the **arp** command and the ARP protocol have the same name, it is understandably easy to confuse them. But keep in mind that they are different – the **arp** command is used to view and manipulate the ARP cache contents, while the ARP protocol defines the format and meaning of the messages sent and received, and defines the actions taken on message transmission and receipt.

RC 19/20	LAB ASSIGNMENT	Guide.Part #:	5.0
From Application Layer to Link Layer		Issue Date:	2 Dec 2019
Analysis of DHCP, NAT, Ethernet and ARP		Due Date:	
Author: Prof. Rui Cruz		Revision:	1.0

Let's take a look at the contents of the ARP cache on your own computer. For that purpose, in a (Bash) Terminal window run the **arp -a** command as explained above, and answer the following question:

11. Write down the contents of your computer's ARP cache. What is the meaning of each column value?

Now, back to Wireshark, look again at the first two Ethernet frames, as well as the 6th frame. Those frames contain ARP messages. Answer the following questions:

12. What are the hexadecimal values for the source and destination addresses in the Ethernet frame containing the ARP request message?
13. Give the hexadecimal value for the two-byte Ethernet Frame type field. What upper layer protocol does this correspond to?
14. In order to answer correctly to the following questions, download the ARP specification from <https://tools.ietf.org/rfc/std/std37.txt>. A readable, detailed discussion of ARP is also at <http://www.erg.abdn.ac.uk/users/gorry/course/inet-pages/arp.html>.
 - (a) How many bytes can you count from the very start of the Ethernet frame until the the ARP request **opcode** field begins?
 - (b) What is the value of the *opcode* field within the ARP-payload part of the Ethernet frame in which an ARP request is made?
 - (c) Does the ARP message contain the IP address of the sender?
 - (d) Where in the ARP request does the "question" appear, i.e., the Ethernet address of the machine whose corresponding IP address is being queried?
15. Now find the **ARP reply** that was sent in response to the **ARP request**.
 - (a) How many bytes can you count from the very start of the Ethernet frame until the the ARP **opcode** field begins?
 - (b) What is the value of the **opcode** field within the ARP-payload part of the Ethernet frame in which an ARP response is made?
 - (c) Where in the ARP message does the "answer" to the earlier ARP request appear, i.e., the IP address of the machine having the Ethernet address whose corresponding IP address is being queried?
16. What are the hexadecimal values for the source and destination addresses in the Ethernet frame containing the **ARP reply** message?

RC 19/20	LAB ASSIGNMENT	Guide.Part #:	5.0
From Application Layer to Link Layer		Issue Date:	2 Dec 2019
Analysis of DHCP, NAT, Ethernet and ARP		Due Date:	
Author: Prof. Rui Cruz		Revision:	1.0

17. In the trace, the first and second ARP packets correspond to an **ARP request** sent by the computer running Wireshark, and the **ARP reply** sent to the computer running Wireshark by the computer with the ARP-requested Ethernet address. But there is yet another computer on that network, as indicated by packet 6 – another **ARP request**. Why is there no **ARP reply** (sent in response to the **ARP request** in packet 6) in the packet trace?

5 Experiment E3: DHCP

For this experiment load into Wireshark the trace file **dhcp-trace.pcap** using the **File** pull down menu, choosing **Open**, and then selecting the trace file from folder **data** (because Wireshark is running in the VM).

In the Wireshark menu, select **Analyze** → **Enabled Protocols**. Then check the IPv4 box and select OK. Now 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. That is why you need to enter **bootp** and not **dhcp** in the filter in order to see DHCP packets in the current version of Wireshark.

You can see from Figure 4 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.

When answering a question below, you should hand in a dissection of the packet(s) within the trace that you used to answer the questions asked. To export a packet summary/data, use **File** → **Export Packet Dissections** → **As Plain text**, choose **Selected packet only**, choose **Packet summary line**, and select the minimum amount of packet detail that you need to answer the question.

18. Are DHCP messages sent over UDP or TCP?
19. Using <http://draw.io> draw a UML timing diagram 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. Export the diagram in PNG format. Are the port numbers the same as those indicated earlier in this lab assignment?
20. What values in the DHCP Discover message differentiate this message from the DHCP Request message?
21. 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) of DHCP messages? What is the purpose of the Transaction-ID field?

RC 19/20	LAB ASSIGNMENT	Guide.Part #:	5.0
From Application Layer to Link Layer		Issue Date:	2 Dec 2019
Analysis of DHCP, NAT, Ethernet and ARP		Due Date:	
Author: Prof. Rui Cruz		Revision:	1.0

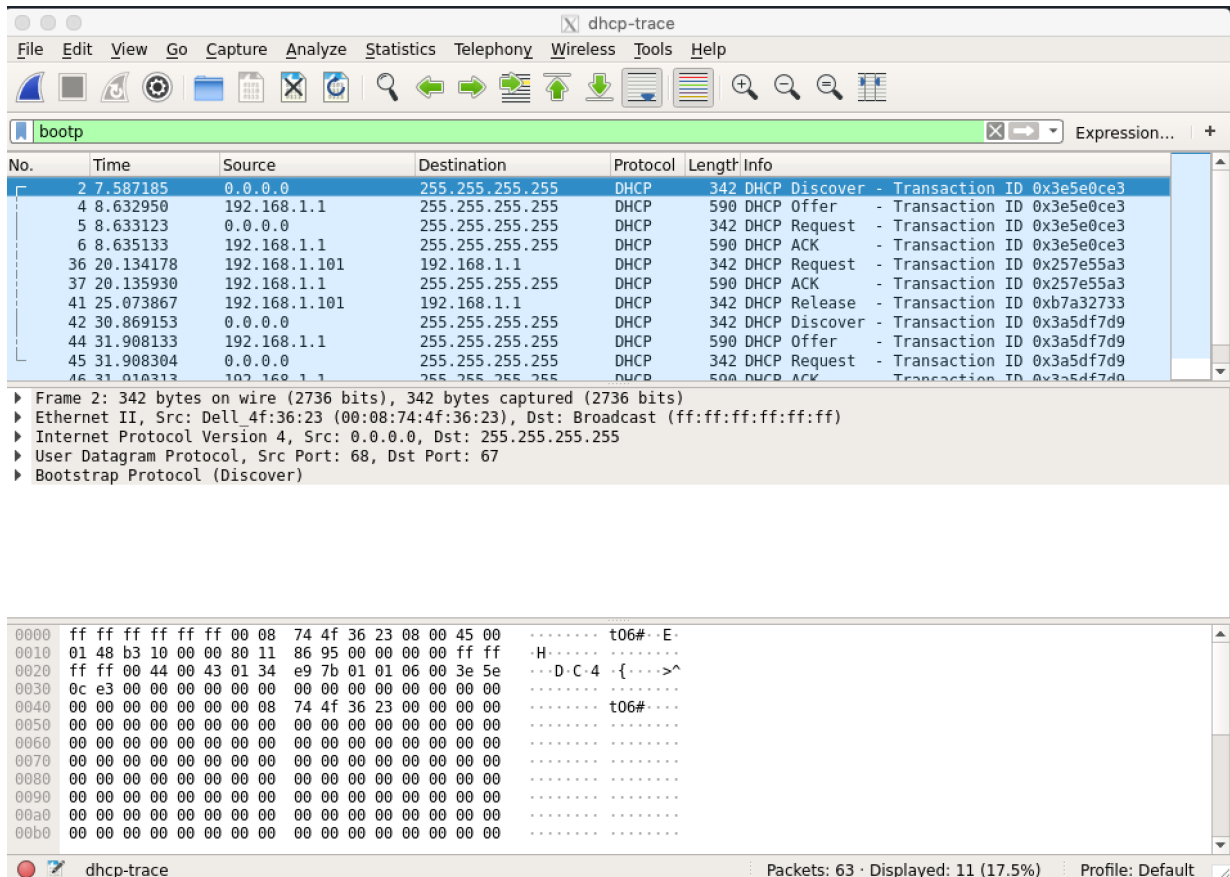


Figure 4: Wireshark window with first DHCP packet—the DHCP Discover packet—expanded

22. 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.
23. What is the IP address of the DHCP server?
24. What IP address is the DHCP server offering to the host in the **DHCP Offer** message? Indicate which DHCP message contains the offered DHCP address.
25. In the DHCP trace file, the DHCP server offers a specific IP address to the client. 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?

RC 19/20	LAB ASSIGNMENT	Guide.Part #:	5.0
From Application Layer to Link Layer		Issue Date:	2 Dec 2019
Analysis of DHCP, NAT, Ethernet and ARP		Due Date:	
Author: Prof. Rui Cruz		Revision:	1.0

26. Explain the purpose of the **lease time**. How long is the lease time in this experiment?
27. 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?

6 Experiment E4: NAT

For this experiment, a capture of packets was performed, of 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.

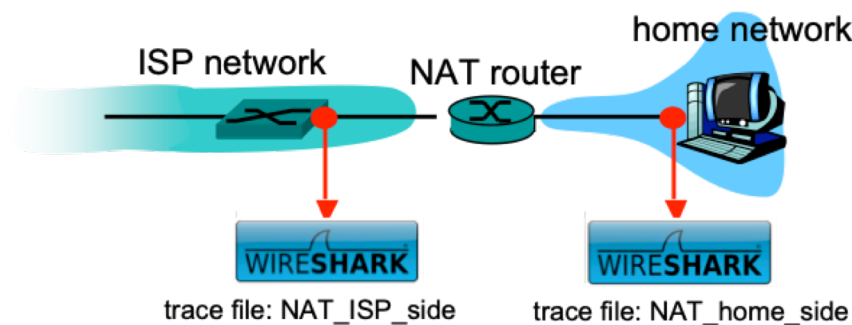


Figure 5: NAT trace scenario

Figure 5 shows the Wireshark trace-collection scenario. As previously said, a Wireshark trace was collected on the client PC in a home network. This file is called **NAT-home-side.pcap**. Because we are also interested in the packets being sent by the NAT router into the ISP, a second trace file was collected at a PC tapping into the link from the home router into the ISP network, as shown in Figure 5. 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.pcap**.

Start by opening in Wireshark the **NAT-home-side.pcap** file and answer the following questions. You might find it useful to [use a Wireshark filter so that only frames containing HTTP messages are displayed](#) from the trace file.

28. What is the IP address of the client PC in the home network?
29. The client actually communicates with several different Google servers in order to implement “safe browsing”. The main Google server that will serve up the main Google web page has IP address **64.233.169.104**. In order to display only those frames containing HTTP messages that are sent to/from this Google, server, enter the expression `http && ip.addr == 64.233.169.104` into the Filter field in Wireshark.

RC 19/20	LAB ASSIGNMENT	Guide.Part #:	5.0
From Application Layer to Link Layer		Issue Date:	2 Dec 2019
Analysis of DHCP, NAT, Ethernet and ARP		Due Date:	
Author: Prof. Rui Cruz		Revision:	1.0

30. Consider now the HTTP GET sent from the client to the Google server (whose IP address is **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?
31. At what time is the corresponding **200 OK** HTTP message received from the Google server? What are the source and destination IP addresses and TCP source and destination ports on the IP datagram carrying this **HTTP 200 OK** message?
32. Recall that before a GET command can be sent to an HTTP server, TCP must first set up a connection using the three-way SYN/ACK handshake. At what time is the client-to-server **TCP SYN** segment sent that sets up the connection used by the GET sent at time **7.109267**? What are the source and destination IP addresses and source and destination ports for the **TCP SYN** segment? What are the source and destination IP addresses and source and destination ports of the **ACK** sent in response to the **SYN**. At what time is this **ACK** received at the client?
(Note: to find these segments you will need to clear the Filter expression you entered above. If you enter the filter “tcp”, only TCP segments will be displayed by Wireshark).

In the following we will focus on the two HTTP messages (GET and 200 OK) and the TCP SYN and ACK segments identified above. Our goal below will be to locate these two HTTP messages and two TCP segments in the trace file (**NAT-ISP-side.pcap**) captured on the link between the router and the ISP. Because these captured frames will have already been forwarded through the NAT router, some of the IP address and port numbers will have been changed as a result of NAT translation.

Open the **NAT-ISP-side.pcap** in Wireshark. Note that the timestamps in this file and in **NAT-home-side.pcap** are not synchronized since the packet captures at the two locations shown in Figure 5 were not started simultaneously. You should discover that the timestamps of a packet captured at the ISP link is actually less than the timestamp of the packet captured at the client PC.

33. In the **NAT-ISP-side.pcap** 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.pcap** trace file). At what time does this message appear in the **NAT-ISP-side.pcap** 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.pcap** trace file)? Which of these fields are the same, and which are different, than in your answer to question 30 above?
34. Are any fields in the HTTP GET message changed? Which of the following fields in the IP datagram carrying the HTTP GET are changed: Version, Header Length,

RC 19/20	LAB ASSIGNMENT	Guide.Part #:	5.0
From Application Layer to Link Layer		Issue Date:	2 Dec 2019
Analysis of DHCP, NAT, Ethernet and ARP		Due Date:	
Author: Prof. Rui Cruz		Revision:	1.0

Flags, Checksum. If any of these fields have changed, give a reason (in one sentence) stating why those fields needed to change.

35. In the **NAT-ISP-side.pcap** trace file, at what time is the first **200 OK** HTTP message received from the Google server? What are the source and destination IP addresses and TCP source and destination ports on the IP datagram carrying this **HTTP 200 OK** message? Which of these fields are the same, and which are different than your answer to question 31 above?
36. In the **NAT-ISP-side.pcap** trace file, at what time were the client-to-server **TCP SYN** segment and the server-to-client **TCP ACK** segment corresponding to the segments in question 32 above captured? What are the source and destination IP addresses and source and destination ports for these two segments? Which of these fields are the same, and which are different than your answer to question 32 above?

7 Finishing your Experiments

In order to stop the Virtual Machine and to verify the global state of all active Vagrant environments on the system, we can issue the following commands:

```
:~$ vagrant halt
==> nethack: Attempting graceful shutdown of VM...
:~$ vagrant global-status
```

Confirm that the status of the VM is 'powered off'. In order to prevent the machine to keep using resources.

8 Submitting the Results of the Experiments

The experiments that you execute in this LAB will either produce results that you need to report or from which you will be asked questions about the execution. In order to report the results you achieved, proceed as follows:

8.1 General Procedure

The procedure for submission is quite simple:

1. In your Google Classroom for this course, you will find an Assignment for reporting this specific Lab experiment (with a Due Date);
2. The Assignment provides a Link to the TSUGI CLOUD Web Form with Exercise Questions;

RC 19/20	LAB ASSIGNMENT	Guide.Part #:	5.0
From Application Layer to Link Layer		Issue Date:	2 Dec 2019
Analysis of DHCP, NAT, Ethernet and ARP		Due Date:	
Author: Prof. Rui Cruz		Revision:	1.0

3. When you are prepared with the requested materials (screen-shots, command line outputs, developed code, etc.) you will submit the items into the respective Exercise Form questions of the Assignment;
4. In the same Exercise Form of the Assignment you may be asked to comment your submissions;
5. Please note that in some types of Exercises you may also be asked to evaluate (anonymously) and provide feedback to the answers from some of your classmates (this peer-grading feedback counts for your grading).
6. When finished answering the Exercise Form, click the button **Done** in the top left of the Form; You will be returned to the Google Classroom Assignment;
7. In the Assignment, do not forget to confirm (click the button) **MARK AS DONE** or **TURN IN** when the assignment is completed;

8.2 Specific Procedure

For this LAB Assignment you will provide answers to the questions related to the analysis of Ethernet and ARP protocols, as well as a UML timing diagram for the DHCP exchange between the client and server. Additionally, you will also provide answers to the questions related to the analysis of DHCP and NAT and some screenshots:

8.3 Experiment E1: Ethernet

1. Report (content in plain text) your analysis of the Ethernet frame containing the HTTP GET message, with the answers to Questions 1 to 5, to submit in the TSUGI Form where asked;
2. Report (content in plain text) your analysis of the Ethernet frame containing the HTTP response message, with the answers to Questions 6 to 10, to submit in the TSUGI Form where asked;

8.4 Experiment E2: ARP

1. Report (content in plain text) the ARP cache of your computer, with the answer to Question 11, to submit in the TSUGI Form where asked;
2. Report (content in plain text) your analysis of the ARP, with the answers to Questions 12 to 17, to submit in the TSUGI Form where asked;

RC 19/20	LAB ASSIGNMENT	Guide.Part #:	5.0
From Application Layer to Link Layer		Issue Date:	2 Dec 2019
Analysis of DHCP, NAT, Ethernet and ARP		Due Date:	
Author: Prof. Rui Cruz		Revision:	1.0

8.5 Experiment E3: DHCP

1. Submit a screenshot of the Wireshark window after opening the **dhcp-trace.pcap** file and setting the filter, to submit in the TSUGI Form where asked;
2. Submit the UML timing diagram for the DHCP in the TSUGI Form where asked;
3. Report (content in plain text) your analysis of the DHCP, with the answers to Questions 18 to 27, to submit in the TSUGI Form where asked;

8.6 Experiment E4: NAT

1. Submit a screenshot of the Wireshark window after opening the **NAT-home-side.pcap** file and setting the filter, to submit in the TSUGI Form where asked;
2. Report (content in plain text) your analysis of the NAT, with the answers to Questions 28 to 32, to submit in the TSUGI Form where asked;
3. Submit a screenshot of the Wireshark window after opening the **NAT-ISP-side.pcap** file and setting the filter, to submit in the TSUGI Form where asked;
4. Report (content in plain text) your analysis of the NAT, with the answers to Questions 33 to 36, to submit in the TSUGI Form where asked;

WARNING. Submissions MUST BE MADE in the TSUGI CLOUD Web Form through Classroom. No other type of submission will be considered for evaluation.