

The experimental study of this lab session consists of \*eight parts. In each of them all the steps that the student must perform are described, **if you have any questions consult with the professor in charge of the practical session.** In the case of not completing all the parts of the experimental study, before leaving the laboratory you must perform point \*35.

**(DO NOT TURN ON YOUR PC UNTIL INSTRUCTED BY THE PROFESSOR)**

### Part One: Previous Steps

1. Turn on the PC. When booting, a screen with a white background will be displayed with a series of options that will allow you to restore or log in to various operating systems, which will remain fixed until we select one of the options. **If you do not see that white background screen, you must notify the professor.** The professor will tell you whether you need to restore the Windows 7 operating system, depending on whether it has previously been restored this operating system.
2. Log in to Windows 7 and disable The Windows Firewall in the same way that was explained to you in the first part of the previous lab session.

### Part Two: Using ipconfig to view the TCP/IP settings of the Internet access network (ETSII network)

In the previous lab session, we saw that, in the classroom PCs, the TCP/IP configuration is obtained automatically from a DHCP server. We also saw that the **ipconfig** command executed as is, without additional parameters, serves to examine only part of the TCP/IP configuration of the PC, the most basic. The **minimum TCP/IP configuration of a final system** is composed of these **three basic parameters**:


- A network-level address (IP address) that uniquely identifies you on the Internet.
- The network-level address of a **border router** that gives you Internet access, known in Windows as the default gateway.
- A **subnet mask**.

(Note: the meaning and use of these parameters will be seen later in the subject).

Now we will see how to use **ipconfig** to show us not only the basic information but many other parameters that are part of the TCP/IP configuration.

3. Open a Command Prompt window and run the **ipconfig /all** command in it to view all the TCP/IP settings on your PC. Unlike (or done in) previous lab session, we are now using the **/all** parameter when executing the **ipconfig** command. It is very common that the same command can be executed without using parameters or adding one or more parameters that modify the behavior of the command. Remember that the only interesting information displayed by this command is the one related to the **Ethernet Adapter Local Area Connection**, so you should not pay attention to the information on the other two adapters labeled **Tunnel Adapter**.
4. What is the IPv4 address assigned to your PC?
5. What is the subnetmask?
6. What is the IP address of your default gateway (your border router)?
7. What is the IP address of the DHCP server?
8. The TCP/IP configuration obtained automatically from a DHCP server does not normally have an "infinite" validity, but the server grants us a "license" of use that expires after a while (although we can renew this "license" of use). How many hours and minutes of "license" does your PC? Write here when the "license" to use your IP address expires.
9. Run the **ipconfig /release** command in a Command Prompt window. Then, after at least 10 seconds, also run the **ipconfig /all** command and look at what happened when you "released" the TCP/IP configuration. Write here the current value of the three basic parameters of your TCP/IP configuration. The IPv4 address you have now should start with 169.254, the subnet mask should be 255.255.0.0, and it should not have a default gateway. This is because being used automatic configuration by DHCP and having run out of IP configuration, **the PC has automatically configured this type of special IP address that begins with 169.254** and that it is only valid to communicate with other computers on the same network. It is not possible to communicate with other networks because we do not have the default gateway configured. If in this or another lab session you

notice that your address begins with 169.254 you should be aware that there is problem related to the DHCP server and you should try to solve it, notifying the professor if you cannot.

10. Indim what happens when you run the **ipconfig /renew** command (look closely at the three basic parameters of your TCP/IP configuration). Then also run the **ipconfig /all** command and think about what you have achieved by doing the "renew" of the TCP/IP configuration.
11. In the notification area of the taskbar there is an icon  that reports on the status of the **Local Area Connection**, changing the appearance it presents. If you click on that icon and then click on **Open Network and Sharing Center** and then click on the text **Local Area Connection** you will see a window titled **Local Area Connection Status** in which you can see the status of the connection. What is the bandwidth (R) of the network connection? Remember that bandwidth is measured in bits per second (bits/s or bps), usually preceded by some multiple.

### Third part: Connectivity at level 3. Round-trip delay (ping)

In the previous lab session, we used the **ping** command to check if we had an Internet connection. Now, after the last theory classes, we know something more about computer networks, so we can better understand the technical details behind that connectivity test.

The **ping** command is used to test that two computers that have the network level implemented (end systems and routers). When you run this command from a source computer to a destination computer the source sends to the destination a N\_PDU with a special data (an **echo request**) that when it receives it is required to respond to the source with another N\_PDU with a special data (an **echo response**).

12. The **ping** command must be executed in a Command **Prompt** window and requires the IP address or name of the destination computer as a mandatory parameter. Ping from your PC using the IP of your border router as the destination computer (you wrote down your IP address in point6). By default, the Windows 7 **ping** command sends four N\_PDUs to the target computer. The **ping** command shows us on the screen a line of information for each of the four **echo requests** sent. If an **echo request** has received an **echo response**, the information line begins with "Response from" and then the IP of the computer that sent us that **echo response N\_PDU appears**. Be careful because there are circumstances in which responses of **another type** are obtained (they are not echo response) and that come from a computer that is not the target computer of the **echo request**. How many responses from the border router has the **ping** command you just executed received?
13. Is it mandatory that on the other endpoint (destination computer) there is a network-level peer entity for the **ping** command to receive a response from that target computer?
14. Does the **ping** command uses the services of some level, on your own computer, to be able to send the N\_PDU? if yes, indicate the name of the level and the reason to use this service.
15. Ping the 8.8.8.8 computer. Notice how the information provided by the **ping** command when it receives the response of each of the **echo requests** reports the time elapsed from when the sending of the N\_PDU began on the source computer until the **echo response N\_PDU** was received. Check if the four requests have received a response from 8.8.8.8 and if they have done so in exactly the same time.
16. The N\_PDU on its round trip crosses several intermediate nodes (routers), each of which contributes its nodal delay to the delay shown by the **ping** command. What are the four sources of delay that contribute to nodal delay?

### Part Four: Connection to the Laboratory Intranet (LAB\_DTE)

17. Following the procedure learned in the previous lab session, disconnect your PC from the current network (ETSII network) and connect it to the Laboratory Intranet (LAB\_DTE), specifically to the **HUB\_ASIA** (if you are in the G1.31 laboratory) or to the **HUB\_NORTEAMÉRICA** (if you are in the G1.33). **IMPORTANT: If there are no free ports on the HUB, ask the professor what to do.**
18. Your computer will have automatically obtained a new TCP/IP configuration and your IPv4 address will have changed. Write down your IPv4 address here and verify that it starts with 193. If not, try "release" and "renew" your TCP/IP configuration, running the **ipconfig /release** command first and then the **ipconfig /renew** command. After trying that, if your IP address doesn't start with 193, you need to let the professor know.
19. Find out the bandwidth (R) of your network connection and write it down here. Would you be able to explain why the current R is different from the one you noted earlier in paragraph 11? If you don't know, ask the professor.

## Part Five: Tracert Delay

The next command that we are going to study is **tracert**, which is a command that serves to see which routers pass the N\_PDU on the way from a source computer to a destination computer. The **tracert** command is executed on the source computer in a **Command Prompt** window, and like the **ping** command, the only required parameter is the IP address or name of the destination computer.

The output of the **tracert** command shows us a line of information for each of the routers that are part of the path from the origin to the destination. The first router is the closest to the source computer and appears on the first line. Each line associated with a router displays the **round-trip delays** (in ms) of **three** different N\_PDU that have reached that router and returned to the source computer. That's why **three** numbers appear on each line.

The last line is different, since it shows information about the delays to the **destination computer**, which is not normally a router, although it could be.

The **tracert** command uses more complex techniques to make these time measurements than those used by the **ping** command, which we will study later in the theory classes, during the course.

20. If the label on your computer is red-x run a tracert command directed to the target computer com-101.nam.lab and if it is com-x run the tracert command directed to the target computer red-10.as.lab

You should know that the **com-101.nam.lab** and **red-10.as.lab** computers are end systems connected to the laboratory Intranet. It is a good idea to run at least twice the **tracert** command that you are being asked to execute, because sometimes the times that **tracert** shows us in the first execution can be much longer than the norm. Taking a photo or screenshot of the output is also very interesting, to be able to use it as a reference in the future.

21. Look at the output of the **tracert** command and write how many routers are on the way from your PC to the target computer.
22. Write the IP address of the **router closest to the source computer** and the IP address of the **router closest to the destination computer.**
23. Write down here the three round-trip delays that have been measured between the source computer and the router furthest from it. **Write the minimum round-trip delay measured between those two devices.**
24. **Draw in the gap on the next page a graphic** representing the two end systems and the intermediate routers assuming they are connected to each other by wired communication links. Label the first router with **R1**, with **R2** the second, etc. The graph should indicate the **minimum round-trip delay** between the final source system and each of the routers on the way to the destination system, as well as the **minimum round-trip delay from** the final system to the destination. **Notify the professor to review the chart you just made.**
25. Explain why the delays back and forth to the routers that appear in the graph in the section increases as we move away from the source computer.
26. Using the graph, you have made in paragraph 24, calculate an **estimate of the round-trip delay** between the first router and the second router. Make the same estimation between the second and third and so on, until you get to estimate the round-trip delay between the last router and the final target system. **write this information down in the same chart you made in paragraph 24**

27. In the graph in paragraph 24 we are assuming that the equipment represented there is connected to each other by means of communication links. Suppose also that the most influential factor in the round-trip delay between two adjacent computers is the bandwidth of the link between the two. Order from lowest to highest the bandwidth of the links involved in the path shown

by the **tracert** command and take note that information in the graph in section 24 by tagging the links with E1, E2, E3, etc. **E1** would be the link with the lowest bandwidth and **in** the highest bandwidth, with n being the number of links. In case of a tie between two links, choose at random which is the fastest. **Notify the professor to review the chart.**

**Part Six: Familiarizing Yourself with the Wireshark Analyzer**

**Wireshark** is a program that, executed on a final system, can capture all network traffic received or sent by that system through its network interface. It captures all frames or L\_PDU's that enter or leave the network interface of the computer on which it is running. It is a very useful tool, because it not only captures the network traffic of the computer but is also able to analyze it by showing the user detailed information of the protocols used in each of the levels (from the data link level to the application level). That's why this program, **Wireshark**, gets the name protocol **analyzer**.

28. Double-click the desktop icon to start the **Wireshark protocol analyzer**. Figure 1 shows the initial screen that appears when starting **Wireshark** and Table 1 shows a summary of the **Wireshark** icons that will be used most in the lab sessions.

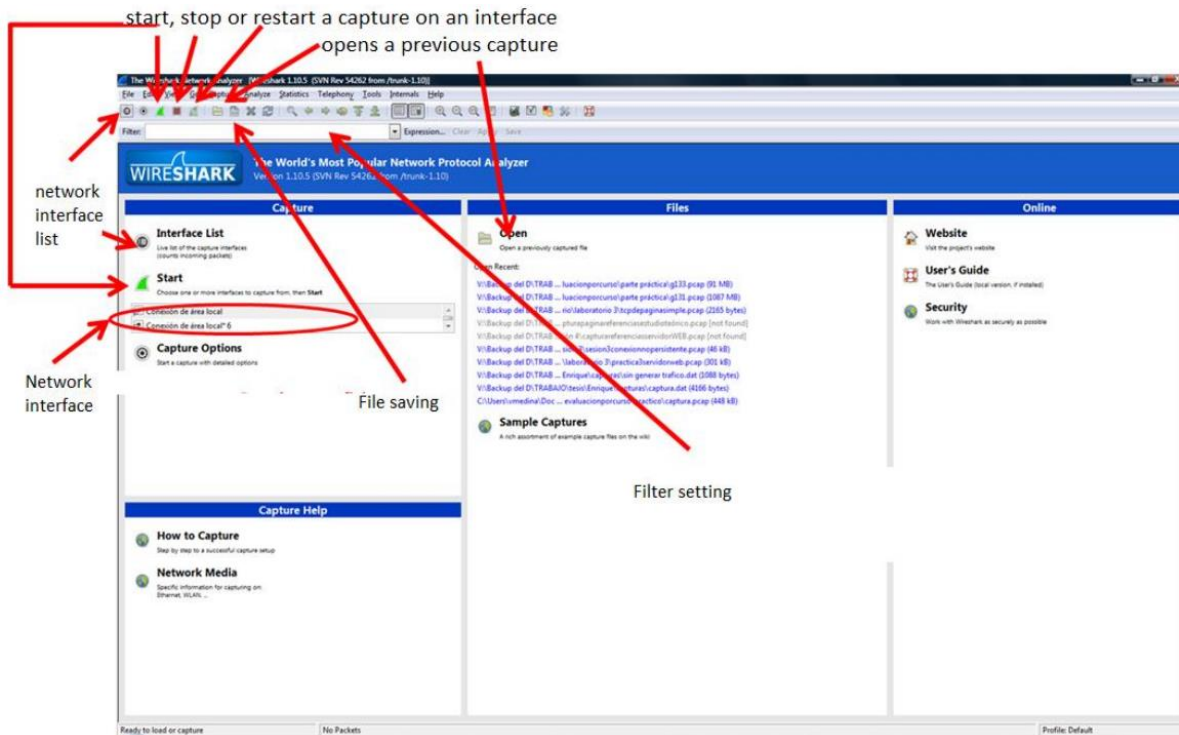


Figure 1

	Displays the interfaces available to capture		Restart a capture (stop the current one and start a new one).
	Stops a capture		Start a capture
	Open a file with a previous capture		Save a file with the current capture

Table 1

29. You can start a capture in a variety of ways. The first way is, while on the initial Wireshark screen, select on that screen (if it was not already selected), the **Local Area Connection** and then click **Start**. Another way is to click on the icon that appears in the menu. Other way is to click on the menu icon to open a window in which the list of all the network interfaces that can be used appears, select the one that you enter (the **Local Area Connection** described as **Realtek PCIe GBE Family Controller**) and then press the **Start** button. Knowing this, use **Wireshark** to capture traffic. If you have done everything right, you will see in a window the frames that are currently coming or leaving your PC, which are being captured by. **Notify the professor before proceeding to verify that you are capturing network traffic.**

30. Open the **Mozilla Firefox** browser and access to the page <http://www.redes.lab> by typing that URL in the address bar. That web page is located on a web server accessible from the intranet of the laboratory.

31. Wait a few seconds and stop the capture of **Wireshark** by clicking on the icon. Save the capture to a file to take it with you when the lab session is over. To do this click on the icon, enter the name of the file and then on save. To upload this previous capture, you would only have to open it by clicking on the icon and indicate the location of the file with the capture so that **Wireshark** shows it.

32. Move through the list of frames and, using the information that appears in the column "Protocol". Note that clicking on the column name "Protocol" will sort the list of frames by this field.) Note that at the link level all captured frames use the Ethernet protocol and also that **the "Protocol" column indicates the name of the highest-level protocol that Wireshark has found encapsulated inside that frame. It is a mistake to think that in a frame there are only encapsulated data from a single protocol. It is also wrong to think that all frames encapsulate protocols at all levels of the TCP/IP architecture.**
33. Click a frame dthe list of frames whose encapsulated highest-level protocol is **HTTP**. For that frame, taking advantage of the information shown in the "**Details s of the frame**" part, draw below, in the available gap, a very simple block diagram in which is shown, one on top of the other, the levels of the TCP/IP architecture that are used, starting with the highest level and **ending in the link**, and another block diagram indicating for each level the specific protocol that is being used.
34. Click a frame in the frame list whose encapsulated highest-level protocol is **DNS**. For that frame, taking advantage of the information shown in the "**Details of the frame**" part, draw below, in the available gap, a very simple block diagram in which is shown, one on top of the other, the levels of the TCP/IP architecture that are used, starting with the highest level and **ending in the link**, and another block diagram indicating for each level the specific protocol that is being used.
35. Close **Wireshark** and the **Mozilla Firefox** browser and any other windows you have opened on your PC.  
Connectyour PC from the Lab Intranet.  
Leave the hose you connected to the **HUB\_ASIA** or **HUB\_NORTEAMÉRICA** back in place.  
Connect your PC to the Internet access network (ETSII network).  
Copy to a pendrive the capture file that you have saved in section31.  
Turn off your PC.