University of Cyprus
Department of Electrical and Computer Engineering

ECE 316 - Operating Systems and Networking Laboratory

Assignment 2: Basic Networking Features: Wireshark – Packet Analyzer

General Instructions

For each Assignment, a report (.pdf) and the source-code (.c or .cpp) of the solution should be submitted through Microsoft Teams "ECE316 – Operating Systems and Networks Laboratory" not later than the due date of the Assignment. The report should start with a cover page that clearly contains the assignment number and the Team number and the names of the members. In your report, include only the pseudocode, not the actual code, with any comments and description you may want to add, as well as a typical scenario that you used to test your programs. Please note that the report should be as concise as possible. Caution: You are not allowed to upload executables (.exe)!

If input test files are given, you are not allowed to make any changes to the provided input files.

Report File Naming Format: "Team#_Assignment#.pdf"

Description:

The purpose of the first set of exercises is to familiarize yourself with the basic networking capabilities of the Linux and Microsoft Windows family of operating systems (similar tools exist in both operating systems). In addition, you will have a first contact with Wireshark, which is a graphical protocol analysis tool. You can use either operating system commands or information through the graphical interface to find the items that are requested below.

Useful shell commands are ***hostname, ifconfig*** (Linux) or ***ipconfig*** (Windows), ***net, netstat, nbtstat*** and ***route***.

Deliverables:

- Each Member of the Team should upload a different report that illustrates the outcomes of the exercises as resulting from executing the procedures on a personal computer.

Exercise 1: Basic Networking Card Features

Each networking card has a physical address, the MAC address. Its length is 48 bits and its structure is defined in IEEE 802. The first bit specifies whether it is a Group or Individual address, the second bit whether it is Local or Unique address, the next 22 bits determine the card manufacturer and the latter 24 bit is the serial number of the card. Address with only "11 ... 1" indicates broadcast. For your computer, find the following:

1. The name of your networking card (Network Adapter)
2. The connection speed
3. The MAC address in Hexadecimal format
4. The manufacture of the networking card
5. The protocols that the card is using
6. The interrupt method it uses (interrupt – IRQ)

Exercise 2: Communication Protocol TCP/IP

Each web host interface has its own IP address, which is logical (not physical). The routers have multiple interfaces and each has its own IP address. The current version of IP is 4 and the corresponding addresses are called IPv4. IPv4 addresses may be represented in any notation expressing a 32-bit integer value. In the original design of IPv4, an IP address was divided into two parts:

1. the network identifier
2. the host identifier

The boundary between these layers is defined by the subnet mask. IP addresses are distinguished from the original address bits in classes:

- 0: class A (first byte <128)
- 10: class B (first byte in area <128-191)
- 110: class C (first byte in region <192-223)
- 1110: class D (first byte in area <224-239)
- 11110: class E (first byte in area <240-247)

After studying the help section of the hostname, ifconfig (Linux), ipconfig (Windows), route, netstat, nbtstat and net commands, focusing on the view and config options, answer the following questions and write the answer with exact syntax of the command used:

1. Your computer's hostname
2. The Workstation/Logon Domain of your computer
3. The IP address of your computer
4. The class that your computer's IP belongs to
5. The MAC address
6. The Subnet Mask
7. The IP address of your default gateway
8. The DNS domain name
9. The IP address of your DNS server
10. The IP address of your DHCP server and the length of the lease period
11. The number of the following that were sent / received from your computer:
    - IP packets
    - ICMP messages
    - TCP segments
    - UDP datasets

Exercise 3: Protocol Analyzer Wireshark

This exercise is an introduction to the use of the Wireshark protocol analyzer, whose basic functions are: a) capture and b) analysis of computer network traffic. For each operation, the user can set appropriate logging / analysis filters that restrict the traffic recorded / analyzed according to their criteria. Thus, according to the Wireshark terminology, we can distinguish the captured and display filters respectively, which will be analyzed in the following series of exercises.

As an introductory example you will notice the traffic generated by visiting a website. After you start Wireshark, the various logging options are adjusted following the options menu of the Capture | Options ...). In the window that appears, make sure that the Interface field indicates the name of your computer's network card (exercise 1.1), and that Enable network name resolution is enabled. Pressing Start will start the recording and a corresponding popup will appear.

Use a web browser (e.g., Chrome) to visit a website, (e.g. http://www.ucy.ac.cy/ece/en/). Once the page is fully loaded, press Stop to stop recording. In the Wireshark main window, where the recorded web traffic is displayed, you may notice traffic not related to the site visit. The requested traffic can be isolated by applying an observation filter as follows: go Analyze | DisplayFilters ... and press the Expression key. From the Fieldname field find the IP option, press +, select ip.addr, from the Relation field select ==, in the Value field (IPv4 address) type the IP address you are interested in (eg 194.42.1.70) and press OK. The filter is activated by pressing Apply. By closing the dialog box (OK) you will find that the movement is probably limited compared to the filter less observation. (Caution: The website you will visit must NOT use the HTTPS protocol but just the HTTP)

1. What is the IP of http://www.ucy.ac.cy/ece/en/
2. Which protocols are used for visiting this site
3. For each protocol find the its level according to the OSI model
4. Where there are so many connections for this site? (For example, a single link could transfer all data to that site?)
5. How can we identify which TCP packets a particular HTTP packet is associated with?
6. Place the cursor in an HTTP packet, press the right mouse button and select "Follow TCP Stream". The popup window shows the data transmitted via TCP, in this case, the HTTP protocol messages.
    a) From the text that appears, find:
        i. The type of web server that hosts the page you visited
        ii. The title and the corresponding HTML tag of the page you visited
        iii. Where in the browser window, this title appears
    b) What is the syntax of the filter that is now displayed in the analysis filter window?
    c) Close the new window created by "Follow TCP Stream".
        i. How many packets with TCP protocol and how many with HTTP protocol are now displayed in the main window?
        ii. What is the purpose of TCP and what is HTTP?
7. How long did it take to load the page based on Wireshark? (Time from first to last package downloaded.)

Exercise 4: Replay of “Voice over IP” (VoIP) call using Wireshark

Once you are familiar with Wireshark software we will see how we can represent VoIP using packages from Wireshark. For example we will use a ready file from the chat log.

1. Download the chat file from the Wireshark homepage using the link: Wireshark VoIP capture sample. (You can download more examples from the site if you want to get more involved)
2. Launch Wireshark
3. Upload the downloaded file. The main window will display the UDP (User Datagram Protocol), RTCP (Real Time Transport Control) protocols Protocol) and RTP (Real Time Transport Protocol). As you know UDP protocol is faster than TCP but cannot guarantee its reliability connection. 'So often used in conjunction with RTCP and RTP protocols to increase the reliability of the connection without sacrificing speed greatly. The RTCP assumes its credibility connection as the RTP takes over the message transmission via the UDP. (Caution: TCP protocol is required to ensure reliability)
4. After loading the file, select the "Telephony" button from the main menu and then select "VoIP Calls" from the options that appear.
5. A new window will open where calls that are included in the packages you loaded will be displayed
    a) Select the first conversation that appears, and then select button "Prepare Filter". What is the syntax of the filter that is displayed now in the filter window?
6. Press the "Play Stream" button from the new window to represent the conversation and take a screenshot of the new “RTP Player” dialog box that appears.