Bialystok University of Technology

Faculty of Electrical Engineering

Course name:
Computer Networks

Course code: IS-FEE-10082S

Laboratory classes manual guide

Laboratory exercise number: **1**

Subject of the laboratory exercise:

Network tools in Windows and Linux

Manual prepared by:
Andrzej Zankiewicz, PhD

Białystok 2025

1. General characteristics of the exercise

Virtually every operating system used today has the ability to work in a network environment and is equipped with a number of tools that enable configuration, diagnosis and supervision of a given device in terms of its cooperation with the network. In addition to the tools included in the operating system, there are usually many additional applications available that extend the range of functions provided by system tools.

The most popular operating systems for PCs and servers today are Microsoft Windows and Linux. These operating systems come with a variety of network troubleshooting utilities. In most cases, these are text-mode (command-line) utilities that are equivalent to those introduced earlier in UNIX.

The purpose of this exercise is to consolidate the knowledge you have in configuring network elements in Windows and Linux systems and to learn about the network utility programs included in these systems, as well as "protocol analyzer" applications, which are one of the basic tools for observing and analyzing network traffic. The exercise uses current client versions of Windows and Linux systems, which are fully compatible with the server versions of these systems in terms of the network tools used.

The knowledge and skills obtained during this exercise will constitute the necessary basis for subsequent exercises in the subject "Computer Networks".

2. Preparation for classes

Before starting the exercise, you should read the following materials:

- The entire contents of this manual
- Information about the network tools used in the exercise from any textbook on TCP/IP networks (e.g. in [1] the relevant parts of chapters 2, 3, 4, 5)
- Wireshark documentation [2]

The above-mentioned information is the **minimum** theoretical knowledge necessary to start and properly complete the exercise.

3. Basic information about the tools used in the exercise

1. `Ipconfig (Windows) and ifconfig (Linux) commands`
They allow you to display information about the configuration of the TCP/IP protocols and the station's network interfaces (cards), as well as to refresh the parameters dynamically assigned to the network station.

2. `Ping command`
It is used to test the connection between stations at the IP protocol level (layer 3 of the OSI model) by using ICMP echo request and echo replay messages.

3. `Tracert (Windows) and traceroute (Linux) commands`
It enables the execution of the traceroute procedure used to determine the route (in the sense of subsequent IP network nodes) between the station on which this command was executed and the station whose domain name or IP address was given as a parameter of the command.

4. `Netstat command`
Displays the current TCP/IP connections of a station and TCP/IP protocol traffic statistics.

5. `Arp command`
It is used to display the contents of the ARP table, which includes the pairs of logical addresses (IP numbers) of stations connected to a given local network and their physical addresses (MAC). It also allows to delete entries from this table and manually make the static entries.

6. `Nslookup command`
It is used to test the Domain Name System (DNS). This is quite an extensive program, which is the subject of one of the next exercises.

7. Software Protocol Analyzer (*Wireshark)*
This is one of many applications that allow you to perform the function of a software protocol analyzer. The basis of their operation is the ability to switch the network card into a mode in which it receives all frames sent on the transmission medium connected to the card (in normal mode, the card only accepts frames with its physical MAC address and frames with the broadcast address). This mode is called *promiscuous mode*.
One of the most important functions of this program is the registration of frames sent in the medium connected to the card and the decoding and presentation in a readable form of information sent in these frames. Another important feature is the ability to define the conditions (filters) that frames must meet in order to be registered. Thanks to this, it is possible to extract only those transmitted information that are of interest to us for specific reasons. Traffic statistics in the connected medium are also created based on the received frames.

4. Laboratory exercise plan

Supporting information

In Windows system the commands such as ipconfig or ping can be conveniently executed in a separately opened command line window. Such a window can be opened by right-clicking the Start icon, then the Run option and typing cmd.

In Windows, the contents of the command window can be copied to the system clipboard in text form. To do this, use the mouse to select the text to be copied while holding down the left mouse button and after releasing the left mouse button, press the Enter key. Then the selected text will be copied to the system clipboard and can be pasted into any document (e.g. in Notepad)

Performing the exercise

1. Start the Windows command prompt.
2. Review the options available in the Windows network configuration window (network connection properties). Read the physical (MAC) and logical (IP) addresses of the given station.

The physical address (MAC) of a particular network interface can be read in the following ways:

- by executing the `ipconfig` command with the `/all` option
- by selecting the properties tab of a given interface and pointing the mouse cursor at the interface name (“Connect Using” field)

The logical address (IP) assigned to a given network interface can be read using the following methods:

- if a given interface is active, its IP address is displayed after executing the `ipconfig` command
- by selecting the properties tab for the interface and then displaying the properties for the Internet Protocol (TCP/IP) component

Note: If the IP address is assigned dynamically (via DHCP), it can only be displayed by the first method listed above.

3. Open a terminal in Linux.
4. By executing the `ifconfig – help` command, familiarize yourself with its options. Then read the physical (MAC) and logical (IP) addresses of the given station.

5. Check the list of available options in the ping command (`ping /?` in Windows, `ping --help` in Linux). Perform a ping command to the host indicated by the instructor and record the results. Check and describe the operation of the following ping command options in Windows:

- -t - continuous polling of a specific host
- -l - specifying the size of sent packets
- -n - specifying the number of repetitions sent
- -a - translate IP number to host name (option relevant only when IP number is provided as `ping` command argument)

Locate and test the Linux ping options that achieve the actions listed above for Windows.

6. Check the list of available options in the traceroute command (`tracert /?` in Windows, `traceroute --help` in Linux). Execute the traceroute command to the host indicated by instructo and record the results. Check and describe the operation of the following tracer command options in Windows:

- -d - disabling the resolution of host names on the designated path
- -h - specifying the maximum number of hops on the designated path

7. Check the list of available options in the netstat command (`netstat /?` on Windows, `netstat --help` on Linux). Record and comment the information returned by netstat with the following options on Windows:

- -a – displaying, in addition to established connections, also TCP and UDP ports that are in the listening state
- -n – disabling hostname and port resolution
- -e – displaying Ethernet interface statistics

8. Check the list of available options in the arp command (`arp /?` in Windows, `arp --help` in Linux). Display and save the ARP table of the network station being used (`arp -a` in Windows). Ping one of the computers on the local network and display the ARP table again. By repeating the display of the ARP table periodically, specify the time after which dynamic entries are removed from it.

9. Start the Wireshark program. Familiarize yourself with the structure of the program window and the type of information displayed. Using the Wireshark program, perform the following operations:

- try out the frame capturing function
- save the contents of captured frames to a file
- familiarize yourself with the available frame filtering options. Configure frame filtering parameters according to the assumptions provided by the instructor.

Frame filtering is a very useful option that allows you to define the conditions that frames must meet in order to be placed in the received frame buffer. To activate frame filtering, enter the filter definition in the Filter field above the window with recorded frames. It is possible to define a filter based on, among others, the protocol and layer two (MAC), third (IP) and fourth (UDP and TCP ports) layer addresses. You can also combine different filters using logical operations (e.g. AND, OR).

Exercise report

The report should include a description of the steps performed and the results recorded at each point of the exercise, along with any necessary comments explaining the essence of the individual operations.

5. Health and safety requirements

According to the rules specified in the first class and confirmed by students held. Appropriate health and safety regulations are also posted in the laboratory room.

6. References

1. Joseph D. Sloan: *Network Troubleshooting Tools*. O'Reilly Media, Inc., 2001
2. Wireshark documentation (www.wireshark.org)
3. Lecture notes.