LESSON E20_EN. TROUBLESHOOTING THE INTERNET. MONITORING NETWORKS.

Parent Entity: IPA SA, Bucharest, Romania, 167 bis, Calea Floreasca; Fax: + 40 21 316 16 20
Authors: Professor Gheorghe Mincu Sandulescu, PhD, IPA SA, Bucharest, Romania, 167 bis, Calea Floreasca,
Mariana Bistran, Principal Researcher, IPA SA, Bucharest, Romania, 167 bis, Calea Floreasca, e-mail: san@ipa.ro. Consultations: Every working day between 9.00 a.m. and 12.00 p.m.

After studying this lesson, you will acquire the following knowledge:
- the principal types of tools for troubleshooting the Internet,
- the troubleshooting tools present on your machine,
- the technology of troubleshooting,
- important practical tools for troubleshooting, such as Data capture tools/sniffers, Data analysers tools,
- guiding in the wide world of troubleshooting tools,
- monitoring tools.

CONTENT OF THE LESSON

LEARNING OBJECTIVES:

After learning this lesson you will accomplish the ability to:
- select the tools for troubleshooting,
- know and exploit the troubleshooting tools present on your machine,
- to use important and largely used tools such as **tcpdump**
- to find knowledge for the specific and enlarged application of the troubleshooting tools,
- to navigate in the world of the troubleshooting and monitoring tools.

1. THE PRINCIPAL TOOLS FOR TROUBLESHOOTING.

The list of the diagnosis and troubleshooting tools is consistent. The diagnosis tools interfere in part with the monitoring tools.

The principal categories of tools for troubleshooting are [4.]:

- **Tools for connectivity testing (illustrated in the previous lesson).**
- **Tools for testing the Path Characteristics (approached in the previous lesson).**
- **Tools for the Packets Capture (Sniffers).**
- **Tools for devices discovery and mapping.**
- **Tools for monitoring with the SNMP – Simple Network Management Tools.**
- **Tools for the performances measurement, including RMON-Remote Monitoring.**
- **Tools for the testing of the connectivity protocols, inclusive Packet Injection Tools, Networks Emulators and Networks Simulators,**
- **Tools for testing the TCP/IP layers applications.**
- **Other tools.**

1.1. THE IDENTIFICATION OF THE NETWORK OPERATING SYSTEM PROBLEMS.

Knowing about the troubleshooting possibilities of the OS – Operating System is a first task.

The Event Viewer
Microsoft © Windows Server 2003 offers three types of log files:

- System Log, which indicates driver failures and failed services. Details are indicated by double clicking on the event selected from the list of events.
- Application Log,
- Security Log.

1.2. DIAGNOSIS HARDWARE PROBLEMS.

The OS-Operating System of machine permits the supervising of hardware parts.
Beside that, the action is helped by special, numerous and various network monitoring software applications.

In Windows, for instance in MS © Windows Server 2003, the **Performance Monitor** and **Network Monitor** help in the detection of the hardware problems.
The **Network Monitor** offers statistics such as:

- Percentage of network utilization.
- Number of frames travelling by the respective computer.

2. TROUBLESHOOTING TOOLS PRESENT IN THE OPERATING SYSTEM OF YOUR MACHINE: MICROSOFT, MS © XP.

For the following lessons it is recommended that the learner should use their own machine and to follow the explanations on their own machine or on a machine running separately, fig. 2.1.

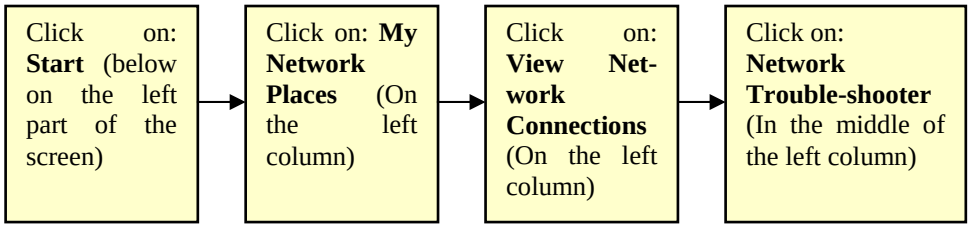
Fig.1.The learner is recommended to open the explained MS © XP tools and to follow, step by step, the practical actions, on the own machine or on other, machine.

1.) The MS © XP WINDOWS. HOW TO SOLVE NETWORKING PROBLEMS.

The first help in the troubleshooting process is offered by the operating system of your machine.
The Microsoft MS © XP operating system offers an important range of troubleshooting tools and procedures.

To arrive inside the **MS © XP** PAGE**: Networking Problems** it is necessary, first, to be open the MS © XP operating system on the Networking Problems page.

For this the following path will be followed:



Now clicking on: **Network Troubleshooter** (on the left column inside the page **View Network Connections**) the following important message is displayed:

Networking Problems.

The window **Networking Problems** offers a consistent number of facilities for troubleshooting, including:

1.1.)- Understanding and learning of troubleshooting aspects.

The regime allows the use of the menus of the MS © XP window **Networking Problems** and their ramifications for understanding and learning the troubleshooting aspects.
The MS © XP window

Networking Problems

helps, firstly, by means of numerous explanations and important clarifications.

The explanations presented inside the page **Networking problems** represent an important and consistent help.
The clarifications offered through the use of the **Index** regime avoid much confusion and enlarge the field of skills

The **Index** regime will be opened by clicking on the top horizontal menu of the window **Networking Problems**.

For this purpose:

Click on: **Index** (On the horizontal menu)

One Index with a large number of words and expressions of interest will be opened on screen:

- by clicking on one word or expression of interest, or
- by introducing the word or expression of interest in the box named "**Type in the keyword to find"**, the corresponding extended explanations will be presented in the right part of the display.

For each selected word, from the list of the searching possibilities, the MS © system offers thoroughly studied responses and, also, hyper-links.

Search in the web world.
The explanations are delivered, also, based on the use of the **Search** regime (in the top left side of the page).
For each selected word, from the list of searching possibilities, the MS © system offers the results of the world web search.

1.2.)- The MS XP page **Networking Problems** also includes the menu:

MS © XP page Networking Problems:
First Category: "Fix a problem" with the sub-categories [3.] :
"

- **Internet Connection Sharing Troubleshooter,**
- **Modem Troubleshooter,**
- **Home and Small Office Networking Troubleshooter,**
- **File and Printer Troubleshooter,**
- **Terminal Services Troubleshooter,**
- **Drives and Network Adapter Troubleshooter,**
- **Diagnose network configuration and run automated networking tests"**

MS © XP page **Networking Problems[3.]**:
Second Category: "Pick a task" with the sub-categories:

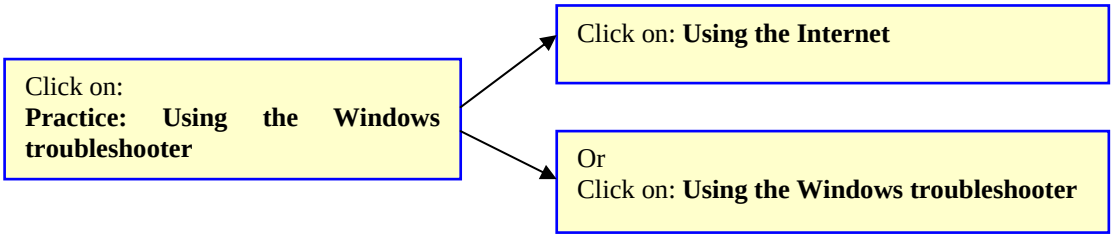
- **Test a TCP /IP configuration using the ping command,**
- **Test TCP / IP connections using the ping and net view commands"**

Each of the sub-categories of troubleshooting aspects presented above are detailed through the use of Wizards and hyper-links, and explained so that the diagnostics could be accomplished quickly.

1.3) – Window: **Networking problems. Practice: Using the Windows troubleshooter**
In the window: **Networking Problems** you may use the exceptional facilities offered by this tool through the pages:

Using the Windows troubleshooter → Using the Internet and
Using the Windows troubleshooter → Using the Windows troubleshooter.

Based on these facilities you may solve different Internet connections and troubleshooting aspects.
In order to use these facilities you will:



For each of the above two clicks, the MS© XP will permit the viewing of important learning materials related to the diagnosis and troubles procedures.

1.4.) Other multiple possibilities of clarification and learning.
These possibilities start, in this case, from the MS © XP page: **Networking Problems.**

3. THE USE OF THE MS © XP NETWORK DIAGNOSTICS.

There are many ways to reach the regime **Network Diagnostics.** One or several of these ways [1.) or 2.), as below] will lead you directly to working with the **Network Diagnostics**.

1.) Reaching the **Network Diagnostics** regime from the MS © XP window **Networking Problems**.

The MS © XP **Network Diagnostics** represents a powerful automatic set of tests which may be launched, at your command, by the MS© XP Operating System. This set of tests is launched with simple commands.

The MS © XP **Network Diagnostics** contribute to solving aspects of diagnosis of troubles in connectivity, as well as of other troubles.
The number of tests, which are all launched by a single click, is high and the Report provided is consistent.

The MS © XP Professional **Network Diagnostics** may be open, on your machine (PC, laptop etc), in the following way (and succession of clicks):

In the window **Networking Problem**, in the chapter **Fix a Problem**, click on **Diagnose Network Configuration, and Run Automated Networking Tests.**

At this point it is possible (under MS © XP Professional) to select which elements of your system (PC inside the network) will be scanned. For this purpose you will click on:

Set Scanning Options

and you will click on all the parameters which you intend to have tested.

After this operation you will click on:

Scan your System

The system will achieve the scanning and the diagnosis of the net environment of the machine inside the network environment in which it is involved.

Because scanning is achieved through the use of the **Ping** tests (towards many addresses of interest of the system) and other tests, the scanning process takes up a few minutes.

The test: MS© XP (Professional)
Diagnose Network Configuration and Run Automated Networking Tests is available to all owners of PCs or laptops, who use the MS© XP Operating System.

Based on the automatic diagnosis, the test: **MS© XP Network Diagnostics** offers results of major importance.

The results include:

- whether the NIC – Network Interface Card of the machine has passed the diagnosis test or not,
- results about the Internet Explorer web Proxy:
  - IEProxyPort (number)
  - IEProxy (IP Address), indicating the fact that the device which has this address is working,
  - The port on which the Server is running.
- other multiple Data and information.

As it is known, by clicking on the images of the specific results (of the **MS© XP Network Diagnostics)**, indicated by one rectangle with the sign **+**, the rectangles of the offered Report may be extended (by clicking on the +) to supplementary information or for the accomplishment of an extended description of the mode in which the Ping tests have evolved.

The MS © XP Network Diagnosis commands offer important Data about the situation of your machine inside the network.

The resulted file is saved (in HTML), for future reference, using the button: **Save To File Button**.

2.) Toward the regime **Network Diagnosis** in the way: Microsoft **Help And Support Center**.

In this case, inside Window © XP (Professional as well as Home Edition), the following chain of commands is achieved: **Start menu → Help and Support Center → Pick A Task→ Use Tools To View Your Computer Information and Diagnose Problems → Network Diagnosis.**

From this point the following two ways of action are possible:

Click: **Scan your System** and Click: **Set Scanning Options**

The MS © XP Network Diagnosis, through Scan your System, scans the entire system and provides important information about: hardware, software and network connections.

The results of scanning includes many pages of important Data, indicating the status of the machine, status of the net environment, addresses, Proxy IP Address, ports, POP port, SNMP port, devices, tests results etc.

The MS © XP Network Diagnosis, through Scan your System, represents an exceptional mirror about the mode of functioning of the machine within the net.

4. THE MS ® WINDOWS TOOLS: NetDiag.exe NET CONNECTIVITY TESTER AND NetCap.exe NETWORK MONITOR CAPTURE UTILITY.

The Windows XP © allows the installation, from the CD, of supplementary tools, part of which may be used with Windows XP ©, and part of which with MS © 2000 Server.

The installation from your licensed CD is achieved in the following steps:

- inserting the CD and selecting the command **Perform Additional Tasks**,
- Open with the **Browser** of the directory of the CD,
- Launch the **Setup.exe** by double-clicking, and open the **Windows Support Tool Wizard**,
- The use of the **Wizard,** and of the **Complete** command**.**
- Finishing the installation based on running the following sub-steps:
  - **Start**,
  - **All Programs**,
  - **Windows Support Tools**.

From the Windows Support Tools important programmes will be selected;

- **NetDiag.exe**
  or
- **NetCap.exe.**

The NetDiag.exe and the NetCap.exe are 2 Microsoft ® software packages which help solving:

- **Connectivity aspects;**

- **Networking aspects.**

1.) The Network Connectivity Tester **NetDiag.exe** also solves the following problems:
- Connection inside the LAN,
- Testing the default Gateway,
- Testing the DNSs,
- tests of the modem,
- Test of the NIC,
- Other.

2.) The **NetCap.exe** is a Packet Sniffing (Sniffer) Program.
The **NetCap.exe** captures Data Packets of the net (legislation, including that related to the protection of Data privacy, has to be taken into consideration. The capture of Data Packets requires compliance with the rules and legislation related to privacy and confidentiality).
The captured Data Packets are saved in a log file where they may be analysed.

The command is launched by typing (in MS-DOS):

C:\>Netcap [Press Enter]

The options of the NetCap are visible with the command:

C:\>Netcap /? [Press Enter]

The capture of Data Packets, because it includes information about
- the IP Addresses of the Source and Destination,
- the Data being sent,
- error-checking Data,
- other,

are useful in the complex troubleshooting aspects, for instance in determining the source which sends unwanted Data or which performs broadcastings that generate the decrease in network speed.

5. THE PING PLOTTER. INTERNET BASED TOOL.

The Ping Plotter [SUPP.3], http://www.pingplotter.com/ , is a useful diagnosis tool which allows the accomplishment of important and interesting results.
The principal features of the Ping Plotter are:
- performing the Tracert function,
- The presentation of results under a graphical form.
- performing other supplementary functions.
- It may be purchased, or simplified versions may be obtained as freeware.

6. THE VISUALROUTE (VisualRoute)

The VisualRoute [SUPP.4] www.visualroute.com is a useful diagnosis tool which allows the accomplishment of important and interesting results.
The principal features of the VisualRoute are:
- performing the Tracert function,
- The presentation of results under a graphical form.
- performing other supplementary functions.
- The achievement of a geographical map of the trajectory of the Data packet in the world.

7. NetPerSec.

The NetPerSec [SUPP.5] www.pcmag.com/article2/0,4149,4878,00.asp , www.extremetech.com/article2/0,3973,5085,00.asp, is a useful diagnosis tool which allows the accomplishment of important and interesting results.
The principal features of the NetPerSec plotter are:
- The accomplishment of the values of the speed and of the level of traffic sent and received by your machine.
- The results are presented in numeric and graphical formats.
- The presentation of results under a graphical form.
- performing other supplementary functions.
- The achievement of the geographical map of the trajectory of the Data packet in the world.

8. PRACTICAL DIAGNOSIS OF THE MACHINE.

8.1. The machine is not connectable to the net.
The mode to action is illustrated in the following table:

Symptom	**The cause**	**The next action**
The machine is not connectable to the net		The control of the Nick and of the cable
The machine is not connectable to the net	The functioning of NIC	Test the NIG with C:\> **Ping 127.0.0.1 [Press Enter]**
The symptom results from: • **The NIC installed: Icon on Network Connections (Start→ Control panel→ Network Connections),** • **The X signalling of the cable insertion in NIC, disappears.**	cable not connected	Plug the cable into the NIC
The machine is not connectable to the net (but the NIC is working and the cable is signalled as plugged in)	The TCP /IP configuration is not correct.	Test the configuration of the TCP/IP: The IP address and the subnet mask. In the **Control Panel→ Network Connections→ Right Clicking on the Icon representing the LAN connection → Repair** Run the Network Setup Wizard.
The machine is not connectable to the net (but the NIC is working, the cable is signalled as plugged in, the TCP / IP is correctly configured)	Other problems with the network	Test, if it is possible, the ping towards addresses of your own LAN.
The machine is not connectable to the net (but the NIC is working, the cable is signalled as plugged , the TCP / IP is correctly configured, Pinging towards the addresses of the LAN is working correctly)	The TCP /IP configuration of the Default Gateway is not correct.	Evaluate, control and test the Default Gateway, The configuration of the Default Gateway The IP Addresses of the Default Gateway, The IP Addresses of the DNS servers. Maintain the IPConfig inventory of all your machines.
The machine is not connectable to the net (but the NIC is working, the cable is signalled as plugged in, the TCP / IP is correctly configured, Pinging towards the addresses of the LAN is working correctly, the Gateway is working correctly, the DNS is working correctly). You may Ping one computer but you may not take resources from this computer.	Your rights of access are restricted because you do not have the permission to access other networks. For instance, in the case of the Guest category of accounts.	Requires changing the account.

8.2. Other machines do not access your machine.
You may access other computers but other machines do not have the possibility to access you: possible Firewall settings.

8.3. Your machine only works inside the LAN.
The computer of your net does not have the possibility to access the machines from other nets: possible Default Gateway problems.

9. tcpdump PACKET CAPTURE [4.]. www.tcpdump.org; ftp://ftp.ee.lbl.gov/tcpdump.tar.Z

The Packets Captures are very powerful diagnosis tools.

When using the Packets Capture applicable laws must be taken into consideration (including laws on the protection of privacy), as well as ethical aspects.

The Packets Capture consists of the real-time capture of the Data Packets transferred through the net.
The tools are also known by names such as: packets sniffers, packets or protocol analysers, traffic monitors.

1.) tcpdump [4.] (it works with UNIX and also, in variants, with the MS ®Windows software programs).

tcpdump represents a Packet Capture software tool with the following features:

- freely available,
- it runs on many Unix platforms,
- it is usable, in portable form, under Microsoft Windows.
- It is based on the **libpcap** capture software used by other capture programs,
- It may run remotely using a Telnet connection,
- the level of analysis offered by the **tcdump** is low,
- it works with the Unix commands **tee** and **script**, which allow viewing the results of the capture,
- it has many options. Options that may be achieved include:
  - the control of the operations of the program,
  - the control of how Data is displayed,
  - the control of what Data is displayed,
  - filtering commands
- tcpdump works with a wide variety of support tools, such as:
  - **sanitize**, which puts the captures in order (also eliminates confidential information),
  - **tcpdpriv,** which removes sensitive information,
  - **tcpflow,** which permits the capture of individual TCP flows or sessions,
  - **tcpshow,** which offers a good on-screen presentation of the capture results,
  - **tcptrace,** which offers different possibilities of analysing and plotting the results,
  - **trafshow,** which offers the continuous display of the traffic, showing:
    - Source address,
    - Destination address,
    - Protocol,
    - Number of bytes,

    and is also used for suspicious traffic.
  - **xplot** (X Windows MS © program).

The **tcpdump** has the following syntax:

tcpdump [-**adeflnNOpqRStuvxX**] [-**c** *count*]
[-**C** *file_size*] [-**F** *file*]
[-**i** *interface*] [-**m** *module*] [-**r** *file*]
[-**s** *snaplen*] [-**T** *type*] [-**w** *file*]
[-**E** *algo:secret*] [*expression*]…. ;
as in accordance with [8.] and [SUP 18.], and where all the elements between brackets are options.

Example: To print all packets arriving at or departing from *mar*:

$ **tcpdump host mary**

Example of the **tcpdump** command, working with the **–l** option (display in line) and **tee** display possibilities [4.]:

$ tcpdump –l | tee outfile

where additional arguments may also be used.

The **-w** option may also be used for writing the accomplished Data in the specified file [4.]:

$ tcpdump –w file1

The number of packets to be captured may be indicated with **c**, for instance 50 Data Packets:

$ tcdump –c50

The **tcpdump** has an option which offers the facility to take into consideration only the Data packets to or from a specified host:

$ tcpdump –c1 host 193.22.45.7

Examples of the results of captures with the **tcpdump:**

12:01:02.334258 192.165.2.1. > 192.166.1.10 : icmp: echo request

The above example illustrates the capture of a Data Packet which represents one Ping response (echo), (ICMP –Protocol). It is possible to see: the time, the Source IP Address, the Destination IP Address; the name of protocol; icmp; the function of the Data Packet.

tcpdump offers many other options, facilities and possibilities.

tcpdump also works with MS ®Windows.

10. Ethereal PACKETS ANALYSER WORKING WITH MS®WINDOWS AND WITH UNIX/LINUX [SUPP.7].

Ethereal is an open source licence software program. **Etherea**l works with:
- UNIX and
- with Microsoft MS ®Windows.

Ethereal works as a tool for capturing and analysing Data Packets.

The results of the **Ethereal** are presented on display under the following form and example:

No	**Time**	**Source**	**Destination**	**Protocol**	**info**
124	24.442260	193.33.24.5	193.22.42.5	HTTP	Details
244	……	……..	……..	……..	…….
Other information					
The binary image of the Data Packet					

The row selected with the cursor is developed and illustrated in the rectangles below the table.

11. DISCOVERING DEVICES ON THE NET.

Discovering devices on the net.
The tools of this category have an important task for the network administrator. They indicate who is connected to the network.
The aspect is necessary for managing:
- the DNS servers and DNS addresses,
- managing IP addresses and licensing,
- managing the level of security.
- other.

The managing of the IP Address is related to many trouble possibilities.
The avoidance of double IP Addresses, inside the net, is achieved through the **arp** test.
But **arp** test is non-concluding if, at the time of the test, a part of the machines are not switched on (powered on).

11.1. The Network Mapper: nmap [4.].

The **nmap** [4.] software program, www.insecure.org/nmap, achieves:
- IP scanning,
- port scanning,
- stack fingerprinting (which identifies which Operating System is working on the remote machine).

Among the regimes / options with which **nmap** works, there are [SUPP. 13]:
-sL: List Scan - list targets to scan, without verifying, through Ping, the presence of the respective host,
-sP: Ping Scan - “go no further than determining if host is online”.

For launching the **nmap the following information** is necessary:
- the IP Address or
- the Hostname

Example:

$ nmap sand

which represents the command for launching the **nmap** for testing the hostname ‘sand’.

nmap displays (for instance):

IP Address

Port	State	Protocol	Service
22	open	tcp	smtp
….	……	…..	……

Also **nmap** may scan a range of addresses:

$ nmap 162.12.4.50-78

Which will scan the addresses from 162.12.4.50 to 162.12.4.78.

$ nmap 162.12.4.*

will scan all the addresses of the subnet.

$ nmap target

Will scan hundreds of ports of the address **target**.

nmap has the possibility to discover and indicate, through "Ping-like probes", which addresses are currently in use.
For this facility the -sP option will be used:

$ nmap sP target

nscan classifies ports into the following states: **open, closed, filtered, unfiltered, open|filtered, or closed|filtered.**

11.2. arpwatch ftp://ftp.ee.lbl.gov/arpawatch.tar.Z

arpwatch is a tool quite similar to the previous **nmap**.

11.3. tkined.

Tkined represents an open-source mapping program [4.], usable for the mapping and management of nets.
It is available also for MS Windows ® platforms.

12. MONITORING TOOLS. SNMP. RMON.

1.) SNMP.
SNMP- Simple Network Management Protocol is a complex system destined for:

- acquiring information from remote systems of the net,
- monitoring the system,
- alerting about the situations from the system.

NET SNMP represents a system for learning the SNMP.

The SNMP works with medium and large networks. The SNMP uses **agents**. The agents are software programs which run on remote systems, collect information and send the information to the management station, that is to the SNMP server.

In MS ®Windows SNMP is also implemented as Win32 service [4.].

2.) RMON.
RMON- Remote Monitoring, represents a monitoring system, similar to the SNMP, but which collects and processes Data at the point of collection.

13. UNIX. MONITORING OF THE FEDORA SYSTEMS.

The following presentation is focused on the facilities offered, in terms of monitoring, by the Fedora Operating Systems for Servers (for instance for the ISP, mini-ISP or micro-ISP servers).

The accomplishment of the very clear image of the status and traces of the functioning of the Fedora system may be solved by using the Fedora system Analysis**: SRG: Squid Log Analysis**.

By opening the **SRG file** used in Fedora **Squid Log Analysis** an image is offered, as exemplified in the following figure, [SUPP.2]; [7.] (fictitious processed example, without using the original graphics):

SRG-Squid Log Analysis / Generated by SRG 1.1.
Select a time period to view reports for
2005Mar27 -2005Mar27
2005 Mar20-2005Mar25
……

Click on the period of interest

The table displayed above indicates time intervals which may be viewed regarding the use of the network.

We should emphasize that using Fedora tools (or other similar tools) to look inside the communications performed by the respective server may infringe ethical and legislative aspects.
Following the above remark, collecting and looking inside the Data may only be achieved in accordance with the national laws and, also, with ethical principles.

By clicking on one of the above lines, **SRG-Squid Log Analysis**, working with Fedora, offers a Table such as the following (this is only a fictitious example, without using the original graphics) [SUPP.2.], [7.]:

SRG-Squid Log Analysis / Generated by SRG 1.1.
Period: 2005Mar27 -2005Mar27
Grouped By: User
……

Click on one of the lines

SRG-Squid Log Analysis / Generated by SRG 1.1.								
Group	Requests	Bytes	BYTES%	IN-CACHE-OUT		TIME %	TIME (ms)	RATE (kb/s)
Ionesco Georges	295	804,329	92.71%	28.81%	71.19%	99.89%	190,178	
John John	36	57,742	6.66%	0.00%	100.00%	0.03%	57	1013%
……...		……	…….	…….	……	……	……...	…….
Totals								

By clicking on one of the rows of the above table, the respective row is opened and displays all the addresses of the web-sites which have been visited by the respective person, plus statistics about the visits as in the following table (only fictitious processed example, without using the original graphics) [SUPP.2.], [7.]:

SRG-Squid Log Analysis / Generated by SRG 1.1.
Period: 2005Mar27 -2005Mar27
Group Ionesco Georges
……

Also, the facilities offered include surfing statistics about the mode of navigation employed. This surfing statistics indicates the time, date, the PC addresses, the mode of processing the viewed data (viewing, downloading etc), the loaded files (http://), the type of loaded documentation (text, image etc).

SRG-Squid Log Analysis / Generated by SRG 1.1.								
Group	Requests	Bytes	BYTES%	IN-CACHE-OUT		TIME%	TIME(ms)	RATE (kb/s)
A22.com	14	204,885	25.47%	0.00%	100.00%	32.46%	61,739	3
John John	15	193,905	24.11%	0.00%	100.00%	5.89%	11,209	17
……...	……...	……	…….	…….	……	……	……...	…….

14. OTHER IMPORTANT NETWORK MONITORING SYSTEMS AND TOOLS.

14.1. OPEN-SOURCE NETWORK MONITORING TOOLS.

1.) The listing of essential monitoring tools.

Among the popular network monitoring tools offered by the open-source community there are [9.]:

- **Big Brother,**
- **Big Sister,**
- **NMIS- Network Management Information System,**
- **OpenNMS,**
- **Nagios/Netsaint,**

- **Spong.**

2.) Big Brother, [9.] www.bb4.org.

Big Brother is free for non-commercial use, and is destined for the Linux and Windows machines.
It offers monitoring services, including those for the in-system working protocols:
HTTP, DNS, FTP, SMTP, POP3, and the use of the CPU – Central Processing Unit.
It is quite simple to install [9.] and works with up to 1000 machines.
It offers web based GUI – Graphical User Interface – results and interactivity.

The installation of Big Brother requires:
- a C compiler,
- a web server, for instance Apache.

Before running, the Big Brother has to be first configured, www.bb4.org; www.bb4.org/features.html, demo.bb4.com/bb/ and started www.bb4.org/features.html.

14.2. THE TOOL FOR THE REMOTE CONTROL OF THE SERVER.

Putty (http://en.wikipedia.org/wiki/PuTTY) is the tool for the remote control of the server.
It works with Windows and with Unix platforms.
Putty is open source software and licenced under MIT licence (http://en.wikipedia.org/wiki/MIT_License) .

Among the Putty features there are:
Full terminal emulation (http://en.wikipedia.org/wiki/Terminal_emulator), (for specifications: XTerm, VT102, and ECMA-4
Control over the SSH (http://en.wikipedia.org/wiki/Secure_shell) encryption key and protocol version.
Other.

15. THE NET ADMINISTRATOR JOB [10].

1.) Elements of the Net administrator job.
- it is based on the accumulation of knowledge,
- the first steps in the accumulation of knowledge about your network consist of research about the Server with which you will work,
- it is important to know and do research on Servers in the following order: Data Base servers (including Back-Up Servers); File and Print Servers, Time and Clock Servers, DHCP Servers, E-mail Servers, DNS Servers, Web Servers, FTP Servers.
- it is important to understand the server room and server room devices: CSU/DSU (multiplexer/demultiplexer of signals); Routers; firewalls, Hubs and Switches, Patch Panel (the wiring block); UPS – Uninterruptible Power Supply;
- it is important to know how to use the Operating System,
  - back-up aspects require special strategies including:
  - full back-up: all files, including the last modified,
  - differential back-up: only newly modified files,
  - incremental back-up: all the files changed from the previous back-up,
  - “grandfather backup”, consisting of the monthly back-up, stored off-site,
  - other back-up solutions.
- Antivirus and security devices.
- Anti-attack devices.
- At least a minimum level of software knowledge.
- Troubleshooting tips.

2.) Minimum package of Tools for the Network Administrator:
  - Command Line Utilities: on the Microsoft server, in MS-DOS: **NET; NET USE; NET VIEW; NET SHARE.** Each of the commands is explained **with the facility: C:\>name of the command ?/ [Enter]**
  - Ping, (presented previously);
  - Tracert (trace-Route in Unix); (presented previously);
  - Protocol Analyzers (sniffers), such as: Commview; and also www.tamos.com/products/commview;
  - Telnet, utility to remotely connect to a router or computer, (presented previously);
  - nslookup such as explained at: www.trulan.com/nslookup.htm, http://www.die.net/doc/linux/man/man1/nslookup.1.html ; nslookup is a program to query Internet domain name servers;
  - whois, www.whois.net; which find information about IP Addresses and hostnames,
  - Netstat; (presented previously);

- Vulnerability assessment tools, such as solved with programs from: www.nessus.org/download.html;
- www.microsoft.com/technet/;
- Intrusion detection Systems: www.lucidsecurity.com
- Software licences.

- Administrator's main possible mistakes [10.]:
  - not to take into consideration that software companies are in business to make money and not for charity or helping actions,
  - Repairing people's home computers,
  - Respecting all the recommendations to install a service pack on all the machines,
  - Other.

- Supplementary Activities:
  - Activities for upgrading the network.

Key Point Summary Conclusions and Recommendations

The troubleshooting efforts and results have assured the Internet and LANs functioning.

The number of tools for the Internet or LANs / net diagnosis and monitoring is very high.
Many of these tools are very efficient and, moreover, they are open-source licensed (possibly having some facilities that have to be paid). Among these tools are: tools for connectivity testing, tools for testing the Path Characteristics, tools for Packets Capture, tools for the discovery and mapping of devices, tools for monitoring with the SNMP – Simple Network Management Tools, tools for performance measurement, including RMON – Remote Monitoring, tools for testing the connectivity protocols, including Packet Injection Tools, Networks Emulators and Networks Simulators, tools for testing the TCP/IP layers applications, other tools.

Study Guide

ESSENTIAL QUESTIONS TO EVALUATE THE ACQUIRED KNOWLEDGE

1. Which are facilities offered by the **MS © XP WINDOWS: NETWORKING PROBLEMS?**
2. Which are the principal categories of the troubleshooting tools?
3. How can the MS © XP NETWORK DIAGNOSTICS be used? Which are the ways to reach the diagnostics programs?
4. Which tests are achieved by the MS © XP NETWORK DIAGNOSTICS?
5. Are the software programmes of the MS © XP NETWORK DIAGNOSTICS already in your machine?
6. Which elements are tested with the Network Connectivity Tester MS ® WINDOWS TOOLS **NetDiag.exe?**
7. What is a Packet Capture Tool? Please give an example.
8. Which is the basic information offered by a Packet Capture Tool?
9. How do you think the Data Packet Capturing Tools may be used for detecting the transfer of incorrect sendings, for instance with viruses?
10. What is **ethereal**, and where can you find complete documentation about the ethereal?
11. For which networking systems are SNMP and RAMON recommended, in principle?

BIBLIOGRAPHY. REFERENCES.

[1.] The describing of the elements of the Net MSDOS commends (are presented inside the http: www.computerhope.com/nethlp.htm).
[2.] ***: *Basic Network Trouble shooting*, Reference Number CH000445, Computerhope.com, www.computerhope.com/issues/ch000445.htm
[3.] Microsoft ™ ®©: Troubleshooting materials and tools inside Microsoft XP Operating System.
[4.] Joseph D. Sloan: *Network Troubleshooting Tools.* O'REILLY, O'reillly Media Inc.,2001, 0-596-00186-X.. www.sauronz.com/imprimir/OReilly%20-20Network%20Troubleshooting%20Tools.pdf
[5.] Curt Simmons, James Causey: *Microsoft Windows XP ® Networking. Inside OUT.* Microsoft Press. Redmond. Washington, 2003, 07356-1652-3.
[6.] Harry M. Brelsford: *Window ®2000 Server Secrets*, IDG Books Worldwide, Inc. 2000, 0-7645-4620-1.
[7.] *** Fedora system in function.
[8.] tcpdump - dump traffic on a network; http://www.tcpdump.org/tcpdump_man.html
[9.] Anand Deveryia: *Network Administrators Survival Guide*, Cisco Press, Cisco Systems Inc. 2006, IN 46240 USA, 1-58705-211-3.
[10.] Douglas Chick: *What All networks Administrators Know*, The Network Administrator.Com, 2003, 0-9744630-0-0
[11.] Joe Habraken: *Absolute Beginner's Guide to Networking*, Que Publishing, 2004, 1-800-382-3419

IMPORTANT SUPPLEMENTARY BIBLIOGRAPHY. REFERENCES. (www)

[SUPP.1.] www.mentortech.com/learn/tools/tools.shtml Mentor Technologies, Inc. (including the ports scanner)
[SUPP.2.] http://www.crc.net.nz/software/srg.php Network Research Group, The University of Waikato.
[SUPP.3] www.pingplotter.com Ping Plotter.
[SUPP.4] www.visualroute.com Visual Route.
[SUPP.5] http://www.firetower.com/forum/tcpdump.html
[SUPP.6] http://www.tcpdump.org tcpdump source and binaries
[SUPP.7] http://www.ethereal.com/ Ethereal (tcpdump GUI)
[SUPP.8] http://www.rt.com/man/tcpdump.1.html Online tcpdump man pages
[SUPP.9] http://www.tamos.com/products/commview/sniffer.htm?r1=overture&r2=cv_words Tamo Soft: A professional packet sniffer can help you get the full picture of your network traffic
[SUPP.10] ftp://ftp.ee.lbl.gov/tcpdump.tar.Z
[SUPP.11] www.sauronz.com/imprimir/OReilly%20-20Network%20Troubleshooting%20Tools.pdf
[SUPP.12] http://www.tcpdump.org/tcpdump_man.html tcpdump - dump traffic on a network.

[SUPP.13] http://www.insecure.org/nmap/man/man-briefoptions.html nmap
[SUPP.14] http://www.bb4.org/ Big Brother monitoring system.
[SUPP.15] www.en.wikipedia.org

SUPPLEMENTARY INDICATIONS ABOUT THE CONTENTS OF THE LESSON

It is also recommendable to consult the documentation available at: www.cisco.com; www.pingplotter.com; www.visualroute.com, http://www.tcpdump.org, http://www.ethereal.com/; ftp://ftp.ee.lbl.gov/tcpdump.tar.Z

ANSWERS TO QUESTIONS

1. The facilities offered by the **MS © XP WINDOWS: NETWORKING PROBLEMS** includes: the learning about the Networking Problems and also Fix a Problem, with many facilities, Pick a Task with many facilities, Using the Troubleshooter and other.
2. The principal categories of troubleshooting tools are: tools for connectivity testing, tools for testing the Path Characteristics, tools for Packets Capture, tools for devices discovery and mapping, tools for monitoring with the SNMP – Simple Network Management Tools, tools for performance measurement, including RMON-Remote Monitoring, tools for testing the connectivity protocols, including Packet Injection Tools, Networks Emulators and Networks Simulators, tools for testing the TCP/IP layers applications, other tools.
3. START→ Control Panel → Network and IUnternet Connections → Troubleshooters → Networking Problems → Set Scanning Options → Scan your System.
Or
Start menu → Help and Support Center → Pick A Task→ Use Tools To View Your Computer Information and Diagnose Problems → Network Diagnosis → Set Scanning Options → Scan your System.
4. Between the results are included:
   the fact that the NIC – Network Interface Card of the machine, has passed or not the diagnosis test,
   the results about the Internet Explorer web Proxy:
   - IEProxyPort (number)
   - IEProxy (IP Address), indicating the fact, that the device which has this address is working,
   - The port at which is running Server.

   other multiple Data and information.
5. Yes.
6. The Network Connectivity Tester **NetDiag.exe** solves inclusive the following problems of testing: Connection inside LAN, Testing of the default Gateway, Testing of the DNSs, The tests of the modem, Test of the NIC, Other.
7. The Data Packet Capture Tool is a software package which permits the capture of the net's Data Packets and their presentation. One popular example is **tcpdump** which works, alternatively, with Linux and with MS ® WINDOWS.
8. The basic information offered by the **tcpdump** Data Packet Capture Tool (as instance) is:
the date and time, the IP Address of the Source, the IP Address of the Destination, the type of protocol, other details.
9. The registration with the **tcpdump** may be used for supervising the incorrect sendings through the offered information about the Source Address and Destination Address and the time. The capture of the Data Packets has to be achieved in accordance with applicable laws, regulations and ethical principles.
10. The **ethereal** is a software package which achieves the captures of Data Packets and analyses the captured Data Packets.
11. For the medium and large systems.

WORDS TO THE LEARNER: ***"Do not wait for opportunities. Create them."*** (After Bernard Shaw)