LESSON E8_EN. TCP/IP PRACTICE. PRACTICAL TRANSPOSITION OF THE TCP/IP. TREATMENT OF THE TCP / IP TROUBLES.

Parent Entity: IPA SA, Bucharest, Romania, 167 bis, Calea Floreasca; Fax: + 40 21 316 16 20
Authors: Gheorghe Mincu Sandulescu, University Professor Dr., 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:

- How the TCP/IP Layers are transposed into practical network components: repeaters, bridges, routers, gateways,
- The practical manner of achievement of networks including routers, hubs, switches and work machines,
- How the configuration of the TCP/IP settings/parameters is accomplished practically,
- The treatment of the essential symptoms of the problems with the TCP/IP implementation,
- The DHCP functioning and the DHCP configuration on the work machines,
- The functioning, features and applications of the ARP and RARP protocols and others.

CONTENT OF THE LESSON

LEARNING OBJECTIVES:

After learning this lesson you will achieve the ability to:

- To understand the TCP/IP configuration of network components: repeaters, bridges, routers, gateways,
- To know and apply the practical construction of networks,
- To set TCP/IP on your work machine,
- To treat the essential symptoms of the troubles of TCP/IP implementation and to repair the network,
- To understand and to put into practice the Dynamic Hosting Configuration Protocol,
- To understand the detailed functioning of ARP and RARP protocols and others.

1. THE TCP/IP STRUCTURES OF THE NETWORK COMPONENTS.

The different practical components of the networks may cover 4, or 3, or 2 or 1 layers. It is important to know how many TCP/IP Layers each common component of the networks has.

The number of Layers involved in the device indicates the complexity of the component and the level of involvement of the respective device in the networking processes.

1.) Repeaters.

The Repeater reconstructs /regenerates the physical signal.

The Repeater lacks intelligence and it is a simple hardware device. It includes only one single layer: the layer 1/ Physical Link.

In fact TCP/IP layer 1 hidden inside the 2 sub-layers:

- The sub-layer Data link and
- The sub-layer Physical link.

The repeater refers only to the Physical Link.

The placement of the repeater inside the network as inferior part of Layer 1 is illustrated in fig. 1.1.

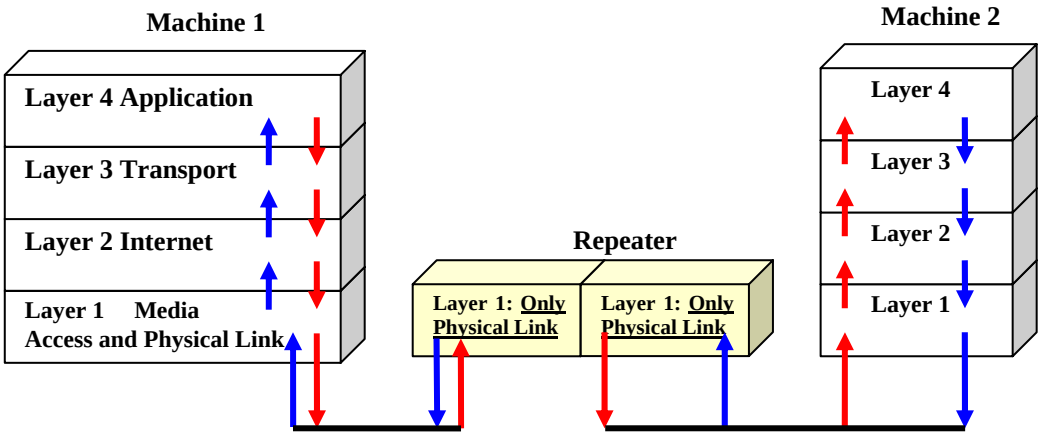

Fig. 1.1. The inclusion of Repeater inside TCP /IP (in this case used for Ethernet LAN).

2.) Bridges

The bridges link similar and non-similar networks.
They have the level of intelligence offered by the complete use of the TCP Layer 1:

- The sub-layer Data link and
- The sub-layer Physical link.

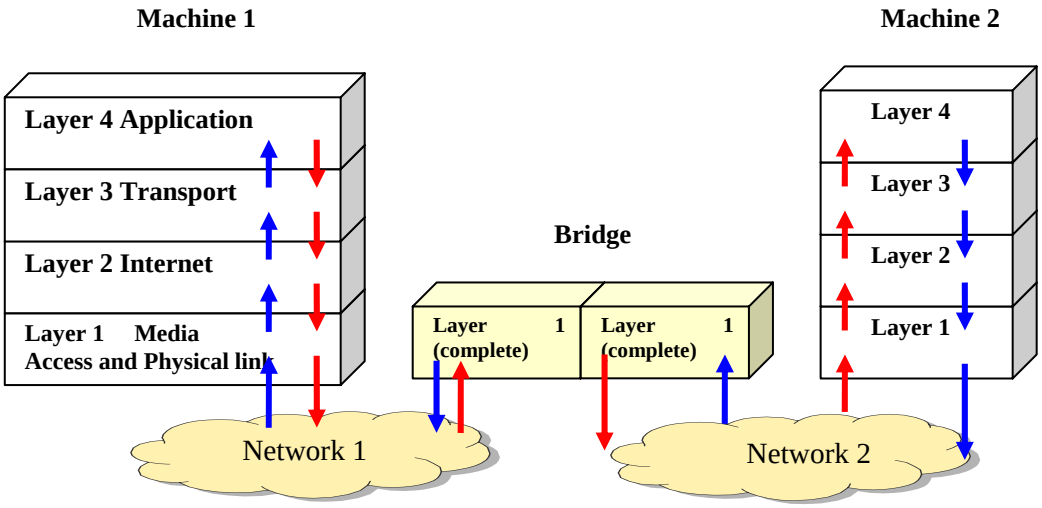

Fig. 1.2. The inclusion of bridge inside TCP/IP

3.) Routers.

The routers evaluate the IP Destination Addresses of Data packets and decide if the correspondent Data Packet must remain inside the initial network or it must be sent toward other network, respectively if it must be sent by an other, specified NIC (Network Interface Card) of the router.

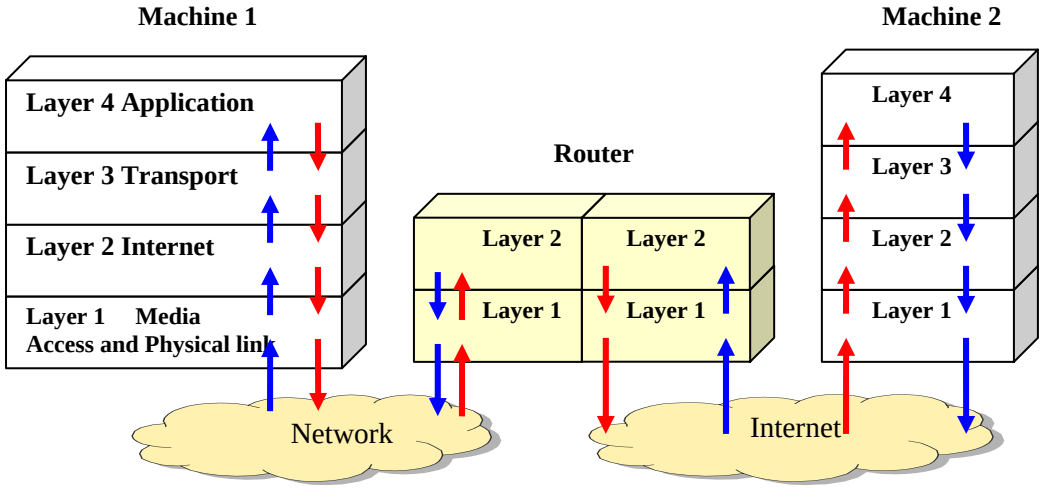

Fig. 1.3. The inclusion of a Router inside TCP/IP

4.) Gateways.

Gateways are frequently confused with Routers because gateways also include the functions of the Routers.

In some configurations the gateway may be replaced by a Router.

The Gateway is a device which interconnects a network to another network, but also administers more complex functions.

Therefore the involvement of all TCP/IP Layers is required and consequently the software processing of Data is achieved on t all the TCP /IP Layers 1 to 4.

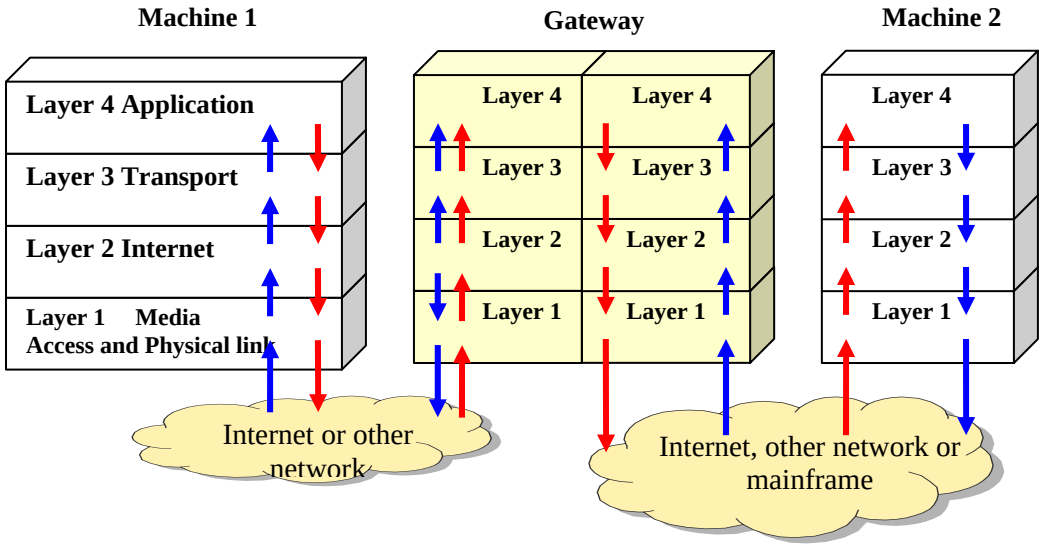

Fig. 1.4. The inclusion of Gateway inside TCP/IP

The devices for the LANs' access to the Internet may be, according to the requirements, Gateways or Routers.

2. EXAMPLES OF PRACTICAL, REAL NETWORKS.

The following fig. 2.1 illustrates real practical and interconnected networks.

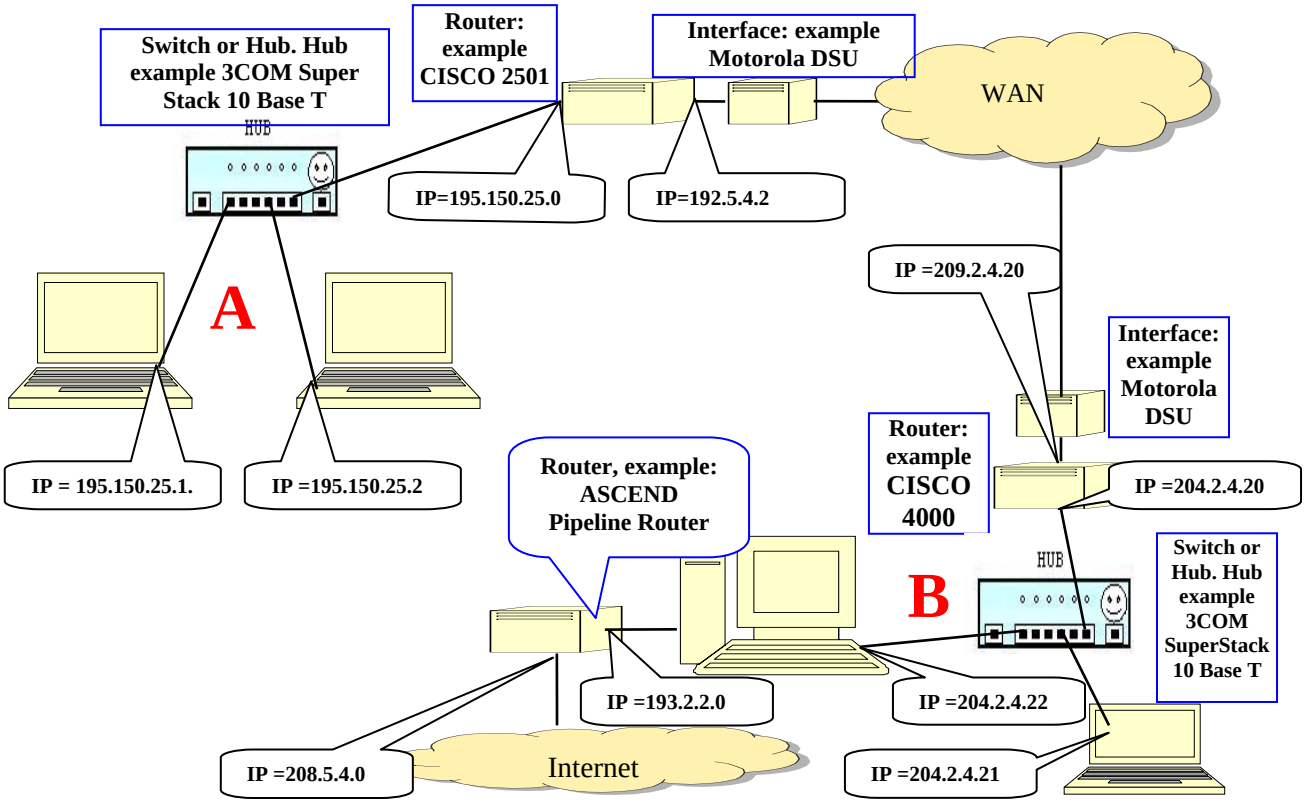

Fig. 2.1. Network A connected through the frame Relay to Network B, which is connected to the Internet.

In the fig. 2.1. above [10.] network **A** is connected through one WAN to network **B.**

3. THE CONFIGURATION OF THE TCP/ IP PARAMETERS.

3.1. THE INSTALLATION AND CONFIGURATION OF THE NIC - NETWORK INTERFACE CARD AND OF THE RELATED SOFTWARE DRIVERS.

The NIC - Network Interface card includes one transceiver. The transceiver is one device consisting in one transmitter and one receiver.
The NIC converts the Data from parallel to serial to send them to the physical media and vice-versa, the arriving Data from serial to parallel.

The NIC may be under the form of a separate, typical card, compatible with the motherboard.
For laptops, and some types of PCs, the NIC is included in the basic board (mother board).

For the selection of the NIC it is necessary to know:

- Which type of PC motherboards will be used: PCI NIC for PCI slots or ISA NIC for ISA slots.
  Some motherboards accept ISA NIC and also PCI NIC.
  The IBM PC or compatible ones may allow different choices: ISA slot or PCI slot or EISA slot.

  The ISA (Industry Standard Architecture) bus, for the PC's motherboard, is an IBM specification. In 1984 the specification passed from 8 bits to 16 bits.

  The PCI (Peripheral Component Interconnect) bus, for the PC's motherboard, is an Intel specification from 1993 of 32 bits. The PCI, Version 2.1., allows 64 bits.

- The necessary throughput of the network: for working with Ethernet of 10 Mbps or with fast Ethernet of 100 Mbps, or the possibilities to accommodate both types of bandwidth (10 Mbps or 100 Mbps).

- Other NIC's features such as:
  - The buffering / memory chips capacity,
  - DMA – Direct Memory Access; the possibility to transfer the data directly to the RAM of the machine.

- Bus mastering; the possibility to transfer the data directly to the RAM of the machine without using the machine's processor.

The NICs in present systems are PnP devices: Plug and Play devices.
Normally the machines recognise their own NIC automatically.

The NICs have the MAC-Media Access Control / Physical Address burned from the manufacturing (before delivery).
If the NIC is changed, the Physical Address of the machine is changed: the MAC is not owned by the machine, the MAC is owned by the NIC (of the machine).

The Installation.

Precautions:

- Against the static electricity 9which may destroy NIC's or motherboard's components it is necessary to use an antistatic wristband electrically connected to the PC case, work on the antistatic mat and not go on carpets.
- The screwdriver is necessary to be appropriate and must not have magnetized elements.
- The machine is not powered on.

The installation consists in: opening the case → mounting the NIC → close the case → start the power / the machine → verify that the PnP NIC is in operation. For instance the Windows XP professional will identify and signal the new hardware (of the NIC) presence.
If the NIC is not PaP then it is necessary to assign and arrange the IRQ: Interrupt Request. Each device has its own IRQ. The existent IRQs may be visualised on the PC's regime Device Manager.
An available value for the NIC's IRQ will be assigned.

3.2. THE INSTALLATION AND CONFIGURATION OF THE NIC's SOFTWARE DRIVERS.

The software drivers may be delivered with the operating system of the machine or may be delivered when purchasing the respective NIC (Network Interface Card).
At the PnP systems (Plug and Play Systems), for instance Windows XP, the software drivers are already included in the system.

3.3. THE MANUAL IMPLEMENTATION AND CONFIGURATION OF THE PERSONAL MACHINE INSIDE THE LAN / LOCAL AREA NETWORK OF A CLIENT [in MS (Microsoft) XP Operating System].

If the allocation of the Internet parameters will not be achieved automatically, then the manual setting of the Machine's Settings will be applied.
Frequently the settings are indicated by the Network Administrator for LANs and by the ISP- Internet Service Provider for clients connected to Internet.

In the independent LAN, depending on the mode of LAN construction (with or without: NAT, PROXY, DHCP), the settings are set by the LAN manager (human factor) or by the owner of the machine in cooperation with the LAN manager.

For one network, initially not-connected to Internet, the main elements that must be configured are:
- **1. The IP Address of the respective machine,**
- **2. The subnet mask of the respective machine.**

If it is expected that the network will be connected to Internet and also NAT and /or PROXY procedures will not be used, the IP address must be unique for the entire (world) space of the Internet IP Addresses.

The subnet mask, which indicates (illuminates) the NETID portion of the IP address, is the same for all the machines from one subnet (for the same network segment).

The IP Addresses.
The IP Address of the machine establishes the Destination Address, when different Data Packets are sent toward the respective machine.
The same IP Address becomes the Source Address, when the respective machine sends Data Packets.

- if the NETID of the IP Address of the destination subnet **is the same** with the NETID of the source (the machine which sends the Data Packet), then the Data Packet will be transmitted to a partner **from the same network,**
- if the NETID of the IP Address of the destination subnet **is different** from the NETID of the source (the machine which sends the Data Packet), then the Data Packet will be transmitted to a machine which is placed in another network.

The subnet mask.
The subnet mask, through the "lighting"of the bits of the NETID of the IP Address, indicates:

- the class and the mode of segmentation of the IP Addresses, the segmentation of the network respectively.

Supplementary settings to insure the connection of the machine to the Internet.

- the IP Address of the Default Gateway, which assures the IP Address of the channel toward Internet,
- the IP Address of the DNS servers, which assure the IP Addresses of the Servers which contain the Tables of equivalence between the IP Addresses and DNS Addresses.
  The IP Addresses of the DNS Servers allow the work with the addresses expressed in DNS form.

The Default Gateway must be set when the respective local net will be connected to another network or to the Internet.
Normally the Gateway address is the IP Address of the local Router, in the point of view of the machine, of the LAN-Local Area Network respectively (fig.3.1.).

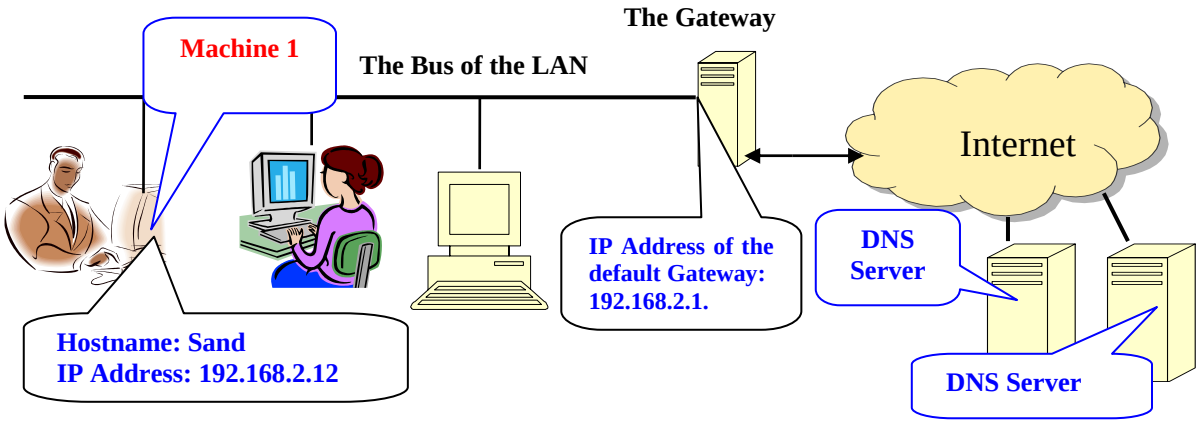

Fig. 3.1 Elements at TCP/IP configuration of machine 1

More Gateways may be connected to one single network. In these cases, the favourite Gateway will be set as Default Gateway for the connection toward the exterior.

As the Default Gateway IP Address is an address in the point of view of the local network, the address of the Default Gateway is an address from the same segment of the network, respectively an IP Address having the same NETID as all the machines from the respective local subnet.

The Default Gateway has the same NETID as all the machines connected inside the respective network, respectively the IP Address of the Default Gateway is an address belonging to the local subnet.

It is recommended that the implementation and configuration of the TCP/IP settings for an Internet client is achieved through the opening and the use of the Windows indications of the MS XP Operating System.

The steps inside the MS XP Operating Systems are the following:

1. The opening of the MS XP screen image

2. The activation of the key / icon: **Start** (left, bottom corner)

3. Click on the icon: **Control Panel** (in the image activated by the previous action)

4. Click on the icon: **Network and Internet Connections**

5. Click on the **Local Area Connection** (on an icon activated by the previous action)

6. Click on the **Internet Protocol TCP /IP** (in the image activated by the previous action)

With action number 6 we open the classic MS – Microsoft® page of settings for Internet parameters for the client:

This screen / image, has, as it is illustrated in fig. 3.2., the following fields of elements:

Field 1.- "Obtain an IP automatically < ? >" .
For the manual setting of the TCP/IP parameters, the rectangle indicating "Obtain an IP automatically <?>" will remain blank.
Field 2.- "Use the following IP address", which requests the following elements:
1.) - "IP address" represents the IP address allocated to the respective device. The allocation is performed by the ISP - Internet Service Provider of superior rank.
In this example and image, you may introduce for instance the IP address: **192.108.1.104**

If you do a right-hand key click with the mouse inside the rectangle of the IP Address, the IP Address may be modified, cancelled and introduced.
In view of the introduction of a new IP address, the previous IP address must be cancelled. This operation is performed by moving the cursor inside the respective rectangle, for the characters which will be cancelled, on the right of these characters, and use the PC / Lap-Top key backwards toward the left side of the rectangle, so as to cancel the desired characters. Also the previous characters may be deleted with the PC key DEL.
New values may not be written if the previous numbers are not deleted.
After these operations the IP value (established by the network manager received from the ISP) is written, for instance: **192.168.2.104.**

Note: for the use of the regime**: "Use the following IP address"** inside the above screen the radio button will be activated: **Use the following Address** and consequently the radio button: **Obtain an IP address automatically** will be automatically invalidated.

2.) **– "Subnet mask".**

The dotted-decimal value of the subnet mask is introduced in the same way as at in point 1.).

If the network is of the type C, and in the mask of the sub nets there are no bits to indicate ("to highlight") bits of the network IP addresses segmentation, then the value to be written is: **255.255.255**.

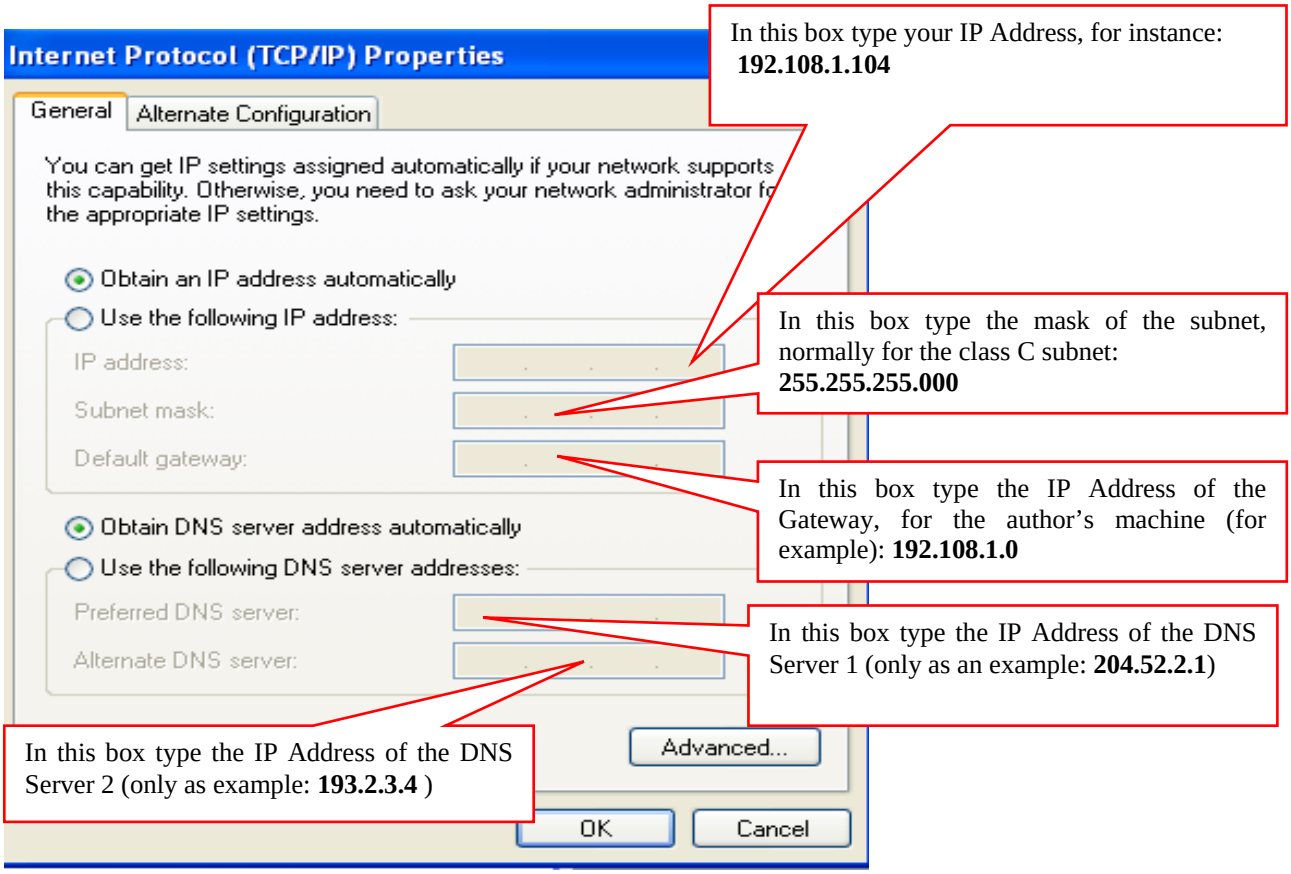

Fig. 3.2 Working with your Windows (MS-Microsoft®) dialog boxes for the TCP/IP configuration of your machine.

3.) –**"Default Gateway ".**
The setting of the "Default Gateway" values representing the **IP Address of the Gateway** by which the LAN communicates with the Internet is performed as in the previous actions 1.) and 2.).
The value of the "Default Gateway "is indicated also by the ISP or by the manager of network.
In this case, as an example, the IP Address of the Gateway is: **192.108.1.0**
Please remember that the IP Address of the Gateway must have the same NETID (in this instance **192.108.1** with the entire LAN, respectively with the IP Addresses on the side of your machine).

Field 3. – In field 3, the addresses of one or 2 DNS (Domain Name Systems) will be completed also based on the Data received from the ISP or from the LAN manager,:

- **" Server Addresses"**
- **"Alternate DNS Server".**

In the image the IP Address: "Server Addresses": **204.52.2.1** and **193.2.3.4** was selected**.**

After the correct writing of the IP address, all the above information is validated and set by striking the key **OK** from the rectangle named: Internet Protocol TCP / IP Properties.

3.4. THE PRACTICE OF TCP/IP CONFIGURATION OF ONE CLIENT. IF YOU ARE THE ISP OR LAN MANAGER.

If you are the ISP, and you have to apply to your clients the manual settings of the TCP / IP configuration values, instead of the automatic procedure DHCP-Dynamic Host Configuration Protocol, then you must deliver the value / parameters to be set.

The following Data must be delivered to partners (clients) of the network:
- The IP Address of the machine,
- The subnet mask,
- The IP Address of the Default Gateway,
- The IP Addresses of the DNS Servers (1 and 2)

- A. The IP Address of the client's machine:

- Will be delivered from the list of the IP addresses available for the respective sub-net (Local Network).
- This list is constructed by the ISP or by the LAN manager based on:
  - the range of IP Addresses achieved from the ISP of the superior rank,
  - the configuration / topology of the administrated net,
  - the policy of accomplishment of network speed (for instance through the sub-segmenting of the network and the use of the correspondent switches),
  - other policy considerations, such as mode of division into subnets, following the security considerations,
  - the physical connections to the switches and hubs, so as to assure a rational repartition of IP Addresses in correspondence with the physical network topology.

- B. The IP subnet mask. Normally for the C networks and, without the sub-segmenting, the sub-net mask is:

255.255.255.000

- C. The IP Address of the Gateway. The IP Address of the Gateway is the IP Address of the point (NIC) by which the Local Network communicates with the Internet. This point is viewed on the machine side of the position of the respective client, respectively from the side of the Local Network. This point is illustrated in fig. 3.1 above.

- D. The IP Addresses of the DNS servers. These DNS servers are servers which maintain the important correspondences between the DNS addresses of some hosts and the IP Addresses of the respective hosts.

The respective Tables of correspondence are used in the procedures of the DNS addresses resolution. That is when the client's machine must achieve the IP Address of a host.

It is highly important that for the many hosts that the DNS addresses correspondence with their IP Addresses is achieved from many other world DNS Servers and not by the DNS servers indicated in the correspondence above. When the correspondence between one DNS address and one IP Address may not be found inside the DNS Servers with the known and indicated IP Addresses, then these servers launch a search in the entire world. .

2 types of name servers are used:

1.) – DNS, Domain Name Systems, which offers the DNS names based on the reception of the correspondent IP Address, and

2.) – WINS, Windows Internet Name Systems, which offers the IP Addresses, when the NetBIOS names, used in the Microsoft networks, are received.

Fig. 3.1 illustrates the elements of the communication environment which require the Data setting. (for the client's machine, respectively a work station):

- 1.)-the IP Address,
- 2.)-the Subnet Mask,
- 3.)-the Default Gateway,
- 4.)-the IP addresses of the DNS Servers.

4. HOW TO FIX THE COMMUNICATION PROBLEMS OF THE LOCAL NET WITH THE EXTERIOR?

4.1. PRACTICAL TROUBLESHOOTING IN THE SETTING AND USE OF THE DEFAULT GATEWAY.

The Default Gateway representing the path by which the local subnet communicates with the external networks, with Internet.

When the local subnet communicates locally (inside the LAN) correctly, but does not communicate towards the external parts, for instance with the internet, the faulty zone must be searched in relation to the Default Gateway.

Among the main troubles and faults the following are indicated:

- A. The Router (or the Default Gateway itself) which represents the Default Gateway is not connected:
  - to the local LAN,
  - to the external networks, respectively to the Internet,
- B. The Router which supports the Default Gateway is not in operation or is in faulty state,
- C. The cables or the interfaces which connect the Default Gateway to the local segment do not function correctly,

- D. The address of the Default Gateway is set wrongly / improperly or is not set.

- Other possible troubles, inside LAN- local area network, are generated with the Physical Address of the Default Gateway. But these troubles are, normally, automatically rejected inside the network through the hidden network self-control.

These self-controls are in function, for instance, in the PnP-Plug and Play networks, such as XP.

It should be reminded that:

- in all the networks, the transfer of Data inside the local network is possible only through the use of the Physical Addresses. The injection of the Data Packet inside a machine placed in the local network is possible only through the use of the **Physical Address**.
  In other words, the transfer of the Data Package between machines placed inside the same network is achieved based on the Physical Addresses of the partner machines.

  If the Physical Address of the Default Gateway on the LAN side does not correspond to the known Physical Address of the Default Gateway, then the communication toward the exterior seems to be impossible.
  In reality this communication becomes possible through automatic and hidden process, through the work of the **ARP** and **RARP** protocols.
  The ARP protocol, automatically and periodically launched, manages to find the correct MAC / Physical Addresses. This aspect is described in the following chapters of this lesson.

- The path of the Data Packets from Source up to the network of Destination is directed based on the use of the **IP Address**.

Troubles related to MAC / Physical Address may however be generated by:

- the replacements of NICs (Network Interface Cards), if the new Physical Address is not detected automatically by the ARP protocol, or
- in relation with the functioning of the ARP protocol.

These troubles may normally be solved automatically by re-starting the client's machine, a fact which leads to the re-reading, by the ARP protocol, of the correct correspondence between the IP Address and the Physical address of each machine, including the addresses of the Gateway machine on the LAN side.

If the ARP protocol does not operate, for instance because the correspondence between the IP Addresses and the Physical addresses is achieved statically, without the dynamic intervention of the ARP protocol, then at the re-starting of the client's machine, the trouble will not be solved.

4.2. HOW TO FIX COMMUNICATION PROBLEMS WITH THE EXTERIOR OF THE LOCAL NET. PRACTICAL TROUBLESHOOTING AT THE SETTING AND USE OF DNS SERVERS.

The first symptom referring to the troubles in the work with the DNS Servers consists in the fact that:

- You may communicate with the Internet by using the IP Addresses from Internet (external to LAN), but
- You may not communicate (navigate, etc) with the DNS addresses.

Supplementary information is offered by the fact that you may not apply the diagnosis tools:
Ping, Tracert toward the DNS addresses.

The explanation of these non-functionalities consists in the fact that the DNS Servers do not offer the IP Addresses (correspondent to the desired DNS addresses) to your machine.
Because your machine does not receive from the DNS Servers the IP Address correspondent to the DNS Address, the software programs which support TCP / IP suite of protocols, more precisely the protocol IP from Layer 2 does not have the possibility to create Data Packets the IP Destination Address in the Header.

In the situation above, if you launch the diagnosis tools toward the IP Address (if you know the IP Address), respectively you do not use the DNS Address in the tests, the diagnosis tools Ping and Tracert will function correctly.

The suspected explanation for these troubles includes:

- The DNS Servers are not connected. The connections to the DNS Servers are in a faulty state.

- The DNS Server or Servers which support the DNS addresses are not in operation or are in a faulty state,

- The IP Addresses of the DNS Servers are not correct.

- Other possible troubles are generated in relation to the external network functioning:
  - a Router between the local subnet and the DNS Server is not in operation,
  - a connection between the subnet and the DNS Server is produced while the connection between the subnet and the external network operates correctly,
  - **the respective DNS name does not exist (or it is not registered).**

5. DHCP-DYNAMIC HOST CONFIGURATION PROTOCOL.

DHCP (RFC 1531, RFC 1534, RFC 2131 and RFC 2132) is a TCP/IP protocol developed and applied for the automatic assignment of the IP Addresses.

The DHCP Server is a server that, based on the DHCP protocol, dynamically assigns:
- IP Addresses,
- Subnet Masks,
- Other settings,

to the network partners (machines), which are set to work with the DHCP configuration assignment.

The DHCP comes into operation at the powering of your machine. After the powering, the software package which supports the DHCP protocol requests an IP Address.

The DHCP IP Address is accomplished after the automatic negotiation between the 2 machines: the server and your machine.

The steps for the accomplishment of a DHCP IP Address are the following [4.]:

Step 1: The start of the software program TCP/IP (at the powering of your machine).
Step 2: The DHCP software programme requests an IP Address.
Step 3: The DHCP servers respond at the broadcasted request of your machine and offer:
- The proposal of IP Address,
- The proposal of the subnet mask,
- The time interval for which the above 2 values are allocated (leased).

Step 4: The DHCP Client (your machine) sends the information, through broadcasting, about the selection of a DHCP server and of related value of IP and subnet mask (including the fact that the respective values are not to be leased by another world machine).
Step 5: The selected DHCP Server acknowledges your machine through the DHCPACK message and indicates to your machine the conditions and the final time interval for the use of the respective IP Address and subnet mask.
Step 6: Your machine has one IP Address and subnet mask and you may work on the Internet.

DHCP Servers. In order to function as DHCP the Server must be set for this function.

DHCP Client. The aspect is solved through invoking the possibility of having IP Addresses offered automatically.
For this action, please return to the screen illustrated in fig.3.2 above.

To launch the DHCP configuration you simply click the mouse on the radio button:
Obtain an IP Address automatically.

The rest of the actions are performed automatically and in a hidden mode by the TCP/IP software of your machine and by the Internet System.

6. THE ARP AND RARP PROTOCOLS.

1.) ARP –Address Resolution Protocol. (RFCs: 826, 903, 1981, 814, 1029, 1166, 1166].

The IP Addresses, virtual addresses, assure in the travel of the Data Packets from Source to Destination the finding of the path. The path is accomplished by the direction (NIC used for output) in each Hop, in which the Data Packet arrives.
The IP Addresses have the character of addresses seen on a worldwide scale.

The Physical Addresses / MAC –Media Address Control work at a lower level, a physical level, inside the final network in which the addressed device is placed.
The NIC takes into consideration only the Physical Address.
Through the NIC of the device connected at the network may enter the machine only the Data Packages with the Physical address from the header of the Data Packet corresponding to known Physical address.

When one Data Packet (TCP / IP Data Packet) arrives in a network, normally it has only the IP Destination Address in the header, respectively the address of one of the machines of the local net.

It does not include the Physical Destination Address, nor the Physical Addresses of the device in which the Data Packet is temporarily hosted.

Following this situation, in which the Data Packet arrives in the network without having the Physical Address of the Destination machine, somebody must give to the Data Packet the Physical Address through which the Data Packet is taken by the NIC of the Destination machine.

The activities for the accomplishment of the refreshment, respective of the new correspondences, between the IP Addresses and the Physical Addresses, are achieved only in the local nets.

Therefore, the correspondence between the IP Addresses and the Physical Addresses is searched and accomplished only **in the respective local physical network,** and in the following situations:

- either the Destination represents the End point of the End to End communication (the final machine),
- either the temporary Destination represents one Hop (Router etc) on the path of the Data Packets.

When the IP Address of the respective Destination is known, there are 2 procedures for the accomplishment of a Physical Addresses of the respective Destination machine:

1.) - First solution: the establishment and storage, at the level of the local subnet device, in a device in which the information can be read by other hosts, i.e. in a device which can be questioned regarding this information (for instance in a Gateway), of the Tables containing the correspondence between the IP Addresses and the Physical Addresses of the respective local subnet.

2.) - Second solution: The use, for each new Data Packet arrived in the network (arrived normally at the Server of the Network, respectively at the Gateway), of the broadcasting procedure (toward the Physical Addresses of the respective net) therefore toward all the devices of the respective local net.
The Device with the correspondent IP Address will return, through a Data Packet, its Physical Address.

The second solution is used also for the periodical refreshment of the Table of MAC Addresses in correspondence

The disadvantage of the first solution mentioned above consists in the fact that the Table of correspondence must be brought up-to-date after each modification inside the respective net.

To avoid this disadvantage, the ARP Protocol questions cyclically, based on the broadcast toward the Physical Addresses, all the devices from the respective local net.
The ARP protocol starts the broadcasting by sending one questioning packet toward all the devices connected inside the respective local net.

To respond to the frequent modifications, the Tables of correspondence are maintained in the "cache" memory of the LAN's Server.

The information of the Tables of correspondence between the MAC addresses and the IP Addresses of the LAN's machines is maintained in the cache memory. The time of refreshment may be, for instance, of 15 minutes.

The fact that the ARP protocol operates only inside the local subnet simplifies the ARP functioning
The broadcasting for the accomplishment of the Physical Address must be achieved only inside the respective local net, toward all the physical Addresses of the respective local net.

The Tables of correspondence between the IP Address and Physical Addresses include:

PHYSICAL PORT OF THE INTERFACE TO THE NET	PHYSICAL ADDRESS	IP ADDRESS	TYPE OF ENTRY

The ARP protocol:

- search firstly in the Table of correspondences placed in the personal **cache** memory,
- renew periodically the content of the table from the cache memory,
- renew the content of the Table when no confirmation is received.

The ARP works in TCP /IP Layer 2, Internet, of the stack of the TCP/IP protocols, and cooperates intensively with the TCP / IP Layer 1 Network Access.

The practical steps of the ARP protocol are the following:

1.) The Data Packet has arrived in a device placed on the path of the Data Packet toward the destination.
The Data Packet has the IP Destination Address but does not have the Physical Destination Address.

2.) The device mentioned above at point 1.) prepares the sending of the Data Packet towards other devices placed in the same net,
The first device knows from the Data Packet header the IP Address of this intermediary (or final) device but does not know the Physical Address of the respective intermediary (or final) device.

3.) The first device **sends a broadcasting Packet toward all the Physical Addresses of the devices in the respective local net.**

Through this broadcast the device tries to receive a reply from the device which has the respective IP Address. The respective device is expected to send feedback which should deliver the value of its own Physical Address. For this broadcast, in the packet which question is also introduced the Physical Address of the Device which Questions (the Physical Address of the Source), so that the Device which has the respective IP Address has the possibility to send a feedback response (Data Packet) toward the device which has broadcasted.

4.) The device from the respective net, device which has its own IP Address identical with that which is indicated inside the questioning Packet, **responds** to the Physical Address which has questioned with a Data Packet which includes the information about the requested Physical Address.

5.) The Device which has initiated the broadcasting places the received Physical Address in the correspondent position in the header of the Data Packet to be sent toward the Destination and sends the Data Packet inside the LAN.

6.) Based on the presence of the correct Physical Address in the Header of the Data Packet, the Data Packet is taken by the device from this local net having the respective Physical address.

The functioning of the ARP protocol is illustrated in fig. 6.1.

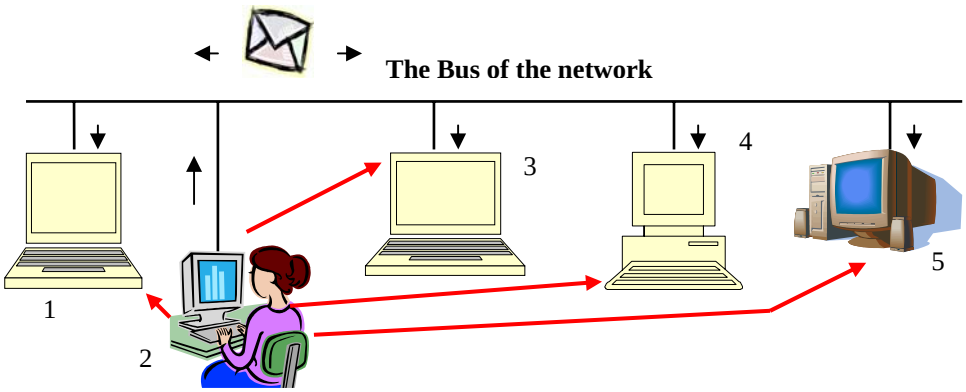

Fig.6.1. Machine no. 2 broadcasts the Questioning Data Packets towards all the LAN Partners.
Normally, the machine having the correspondent IP responds with a Data Packet.
This data Packet announces its own MAC.

One illustrative example of the ARP protocol operation is presented in the following Table.
The device which intends to send the Data Packet knows the IP address (from the IP header of the Data Packet) of the targeted device of the LAN, but does not know the Physical Address of this machine.

No of the	The Physical Address of	The Physical address	Type of	The IP Address	Explanations

Operation, respectively No of the Packet	**the Source**	**of the Destination**	**Protocol**	**of the Source**	
1	00A244000012	FFFFFFFFFFFF (broadcasting on the Physical Addresses).	ARP	195.102.44.0	The Source which has the Physical Address 00A244000012 has sent broadcasting message toward all the devices of the respective local net. For the broadcasting it is used the Physical Address FFFFFFFFFFFF which covers all the possible Physical Addresses from the respective local network. The IP Address is introduced in the Packet, address for which the Physical Address is questioned: 195.102.44.5
2	00A244000300	00A244000012	ARP	195.102.44.5	The device which has the IP address 195.102.44.5 has responded, indicating to the device which has questioned its Physical Address: 00A244000300
3	00A244000012	00A244000300	Ether net	195.102.44.0	The device which has questioned sends the Data Package toward the accomplished Physical Address. The Physical address is present inside the response of the machine which replies.

Practically, in real situations, the Device which questions the local net about the Physical Address of a device from this net initially sends one Packet having its own IP Address as IP search Address, in order to verify if, by a dangerous mistake, there is no other device which has the same IP address as the device which questions.

If it receives a Data Packet including the MAC Address, then it is clear that another Device has the same IP Address.

No of the Operation, respectively No of the Packet	**The Physical Address of the Source**	**The Physical address of the Destination**	**Type of the Protocol**	**The IP Address of the Source**	**Explanations**
1	00A244000012	FFFFFFFFFFFF	ARP	195.102.44.0	The Source which has the Physical Address 00A244000012 has sent a broadcasting message toward all the devices of the respective local net. The Physical Address FFFFFFFFFFFF is used For the broadcasting. The Packet includes the IP Address for which the Physical Address is questioned: 195.102.44.0
2		00A244000012	ARP		Within the established, a response is not received. This confirms that the IP address of the device which questions is unique.

Based on the procedure above, the ARP may and is used for the detection of the doubling of the IP addresses of the machine which initiates an ARP test. The procedure is used for the detection of the important network mistakes:

Supplementary explanations: Broadcasting toward the Physical Address.

In the ARP protocol broadcasting was used toward all the Physical Addresses of the LAN.

Inside a subnet, for instance inside the Ethernet LAN (Local Area Network), when one Data Packet is sent to the network, the Data Packet is received at the input of the NICs (Network Interface Cards) of all the machines of the respective network.

Each NIC compares the Physical Address of the Destination from the Header of the Data Packet with its own Physical Address.
If the Physical Address of the destination of the Packet placed in the Data Packet header is the same with the Physical Address stored in the NIC, then the Data Packet is taken over by the respective NIC.

In the broadcasting toward the Broadcast Physical Address FF FF FF FF FF FF respectively
11111111111111111111111111111111111111111111111111111111,
all the possible Physical Addresses are included in this combination.

The RARP – Reverse Address Resolution Protocol.

In the situations in which the devices know only one Physical Address and need the IP Address the RARP protocol is applied

The RARP protocol functions (STD 38, RFC 903) similarly as the ARP protocol.
Also, based on the knowledge of the Physical address of the machine with an un-known IP, it is possible to target directly the respective machine.

Moreover, the protocol operations are based on the existence of the RAR Servers which have the table of correspondence between the Physical Addresses and the IP Addresses.

If the RARP Server does not respond (for instance it has failed), then the RARP requests may be sent repeatedly. This action contributes to the net congestion and to the lowering of the network speed.

Key Point Summary Conclusions and Recommendations

The TCP/IP protocols are transposed, practically, in each main component of the net: repeaters, bridges, routers, gateways.
The practical manner of achievement and interconnection of networks and inter-networks includes the correct use of the IP addressing.
The setting of the TCP /IP parameters may be achieved manually or automatically (DHCP). After having the parameters (IP Address, subnet mask etc), the verification of the functioning of Default Gateway and of the DNS Servers is necessary.
The treatment of the main symptoms of the troubles in the TCP/IP implementation is based on the Addressing mode, systematized topology and the diagnosis tools.
The ARP and RARP protocols are powerful remote tools for the fixing of network problems and for the hidden assurance of the right operation.

Study Guide

ESSENTIAL QUESTIONS TO EVALUATE THE ACQUIRED KNOWLEDGE

1. Please indicate which TCP / IP Layers are included in the repeater.
2. Which TCP/IP Layers are included in the bridges?
3. Which TCP/IP Layers are included in the Routers?
4. Which TCP/IP Layers are included in the gateways?
5. After the configuration of the TCP /IP on a machine, the machine communicates inside the LAN but does not have the possibilities to communicate with the Internet. Where may we locate the first and main causes of the trouble?
6. After the configuration of the TCP /IP on one machine, the machine works with Ping and Tracert toward IP Addresses but does not allow the Ping or Tracert toward the DNS addresses.. Where may we locate the first causes of the trouble?
7. How can we detect the overlapping / doubling of the2 IP Addresses?
8. What happens if in the network there are simultaneously 2 (or more) identical IP Addresses?
9. Which parameters are necessary for the configuration /setting of the TCP/IP and why?
10. Which are the preliminary, partial tests in the correct configuration of the TCP/IP?

BIBLIOGRAPHY. REFERENCES.

[1.] Ron Gilster: *Cisco Networking for Dummies*, 2nd Edition, Wiley Publishing, Inc, 2002, 0-7645-1668-X.
[2.] Joe Casad: *TCP / IP*, Campus Press, Paris, 2002, 2-7440-1501-6.
[3.] Tim Parker, Mark Sportack: *TCP / IP* , Teora, Bucharest, 2002, 973-20-0243-3.
[4.] Candace Leiden , Marshall Wilensky: *TCP /IP for DUMMIES*, 5-th Edition, Wiley Publishing, Inc, 2003, 0-7645-1760-0.
[5.] Karanjit S. Siyan: *TCP/IP* CampusPress, Paris, 2002, 2-7440-1562-8 ,
[6.] Lukas T. Gorys: *TCP/IP Arbeitsbuch*, Huthig Buch Verlag Heidelberg, 1989, ISBN 3-7785-18884-4.
[7.] Andrew S. Tanenbaum: *Computer Networks*, 4th ed., Pearson Education, Inc, Prentice Hall PTR , Upper Saddle River, New Jersey 07458,2002, translated in Romanian and edited by BYBLOS s.r.l., Bucharest,2003, under the ISBN 973-0-03000-6.
[8.] Gilbert Held: *Ethernet Networks*, John Wiley and Sons Ltd, England, 2003, ISBN 0-470-844476-0
[9.] Lukas T.Gorys: *TCP /IP Arbgeitsbuch. Komminkatiosprotocolle zur Datenübertagung*, Hüthig Buch Verlag Gmbh, Heidelberg, 1989, 3-775-1884-4.
[10.] Harry M. Brelsford: *Windows ® 2000 Server Secrets* ®, IDG Books Worldwide Inc., Foster City, California, 2000, 0-7645-4620-1.

IMPORTANT SUPPLEMENTARY BIBLIOGRAPHY. REFERENCES. (www)

[Supplem. 1.] http://www.prenhall.com/tanenbaum, Prentice Hall, Andrew S. Tanenbaum
[Supplem. 2.] www.cisco.com/univercd/cc/td/doc/cisintwk/idg4
[Supplem. 2.] www.cramsession.com

SUPPLEMENTARY INDICATIONS ABOUT THE CONTENT OF THE LESSON

It is recommendable to be consulted also the documentations from: www.cisco.com; www.cramsession.com;

ANSWERS TO QUESTIONS

1. The repeater involves only one part of the TCP /IP layer 1, respectively the part without intelligence, without software. This part of the Layer 1 is the Link / Access to the Physical media.
2. The bridges include the TCP/IP Layers 1, complete, including both sub-layers of Layer 1.
3. The routers include the TCP/IP Layers 1 and 2.
4. The gateways include all 4 TCP /IP Layers.
5. The main causes are in the area of the Default Gateway and its Addressing.
6. The main causes are in the area of the DNS Servers and their IP Addressing.
7. The launching of the ARP protocol diagnosis tool toward the indicated IP Address. If one network partner responds, that means that other devices already have this IP Address.
8. An addressing conflict is generated, involving network malfunctioning; the error is indicated on the server.
9. IP Address, subnet mask, the IP of the Default Gateway, IP Addresses of the DNS servers. IP Address defines the Internet Destination address.
The subnet mask defines (“illuminates”) the NETID of the network.
IP Address of the Default Gateway indicates the gate / channel by which the LAN is connected to the Internet.
The IP Addresses of the DNS Servers indicate the IP Addresses of the Servers where the tables of equivalence between the IP addresses and DNS addresses are stored.
10. Ping 127.0.0.1 (Ping toward the loop-back address); IPConfig; ARP; Ping toward the DNS addresses, sending e-mails, navigation toward DNS addresses and other.

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