# LESSON E11_EN. ETHERNET. ETHERNET PROTOCOL. DESIGNING AND PUTTING THE LANs INTO SERVICE. NAT. DHCP.

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 learning this lesson, you will acquire the following knowledge:***
- How the Ethernet Data Packet is achieved. Designing the Ethernet LANs.
- The phases and the manner of creation of the isolated Ethernet networks / workgroups.
- The advantages of using the TCP / IP protocols and IP Addresses, also, within the isolated Ethernet networks.
- The phases of connecting the Ethernet LAN to the Internet.
- The final steps of connecting the Ethernet LANs to the Internet. The involvement of the NAT and DHCP.
- The elements of troubleshooting.

**CONTENT OF THE LESSON**



**LEARNING OBJECTIVES:**

**After learning this lesson, you will have the ability to:**
- Construct, put into service and troubleshoot the workgroup connections of the Ethernet LANs,
- Use the TCP/IP inside the Ethernet LANs. How to design the Ethernet LANs.
- To understand the possible cooperation between the NAT and DHCP Servers for serving the LANs,
- To extend the Ethernet LANs toward connections to the Internet.
- To understand the essential elements of the Ethernet Protocol and different connections of the Ethernet LANs external to the LAN.

## 1. THE ETHERNET PROTOCOL.

The Ethernet protocol is supported by multiple different specifications.
These different specifications have generated different variants, types of Ethernet networks.

The Ethernet is supported by the standards: IEEE Standards 802.2 and 802.3.
The variations of the different Ethernet Protocols are indicated in the RFC -1340 (IETF RFC – 1340).

The Ethernet is a protocol working with Data Packets. It is developed separately from the TCP /IP, but finally, the TCP / IP is included.

**All the modern operating systems, supported in software packages of PCs and Laptops, such as the MS XP operating system of Microsoft®, implicitly include the Ethernet protocol**.

The properties of the Ethernet:
- The topology is of the type: **shared bus,** (the partners of the bus share the possibilities and the time of using the bus),
- It works with the **broadcast technology** (all the partners of the bus receive the Data Packet placed on the bus),
- It is considered as the “best-effort delivery” [22.] technology, because the hardware is not used to indicate where the sender is.
- The Ethernet protocol 802.3 is included in TCP/IP,
- It works with CSMA/CD- Carrier Sense Multiple Access with Collision Detect (explained in the previous lessons).
- It is a democratic network. All the partners are equal.
- If it is not used as connected to the Internet , a server (Gateway, Router) is not necessary
- Regarding the **broadcasting** notion, please take into consideration the double meaning of this word:

- The implicit Ethernet **broadcast** procedure, through the normal physical functioning of the Ethernet: each station of the LAN is sending the Data Packets toward all the NIC's connected to the respective LAN. Only one NIC has the Physical address corresponding to the Ethernet address from the header of the Ethernet Data Packet. The respective PC, with the respective NIC, takes the Data Packet.
- The networking procedure of broadcasting towards many different Ethernet addresses or IP Addresses. This broadcasting differs from the above mentioned "physical" broadcasting. Finally, the broadcasting is generated through the special forming of the destination address, so as to include all the addresses of interest.

The (networking) sending of the Ethernet Data Packet may be achieved towards a:
- Unicast address- towards the physical address of a network interface,
- Broadcast address, (all the 1, in the value of the address),
- multicast address, which represents the poll of addresses of interest.

Ethernet Addresses.
The Ethernet addresses are Physical addresses (also named: MAC- Media Access address or layer 2 addresses), respectively included in the NIC's hardware.

The Ethernet frame. The Ethernet frame is made of minimum 64 octets and maximum 1518 octets.
Mainly, the Ethernet frame is made of: header, Data and CRC (Cyclic Redundancy Code for the control of the data integrity).
The sender computes the CRC and attaches the CRC to the Data Packet, when sending the Data Packet. The receiver re-computes the CRC of the Data Packet and detects the situation of the Data packet integrity.

The Cyclical Redundant Check is a procedure for the detection of errors inside a message, respectively the detection of modifications of the content. The control is achieved by the mathematical calculation.
If the CRC value received at the Destination is the same with the CRC value mathematically calculated at the Destination, the probability of errors is low.
If the correspondence (equality) between the 2 values does not exist, that denotes an error and the requirement to re-send the respective message is normally generated.

The shortest Ethernet packet is of: 6+6+2+46 = 60 bytes, representing the C,D,E,F fields of the Ethernet Packet..
The longest Ethernet packet is of: 6+6+2+1500= 1514 bytes, also representing the C,D,E,F fields of the Ethernet Packet.

The Ethernet Data Packet (generally) looks as follows:

| **62 bits** | **2 bits** | **6 bytes** | **6 bytes** | **2 bytes** | **46 bytes to 1500 bytes** | **4 bytes** |
|---|---|---|---|---|---|---|
| **A** | **B** | **C** | **D** | **E** | **F** | **G** |
| **Preamble** | **Preamble** | **Destination Address** | **Source Address** | **Type of frame** | **Data** | **CRC** |

Where the above fields, indicated by the A,B,C,D,E,F,G characters, signify:
A.- The Preamble. The succession of bits and zeros which allows the receiver to accomplish the synchronization (IEEE 802.3 page 24, 42).
B.- The delimiter which indicates the Start of the Frame. SFD – Start Frame Delimiter is a sequence of "10101011", following the preamble. The SFD indicates the starting of the frame (in the Ethernet II, respectively in accordance with the IEEE 802.3).

C.- The Ethernet Address of the Destination: 6 bytes, respectively 48 bits.

D.- The Ethernet Address of the Source: 6 bytes, respectively 48 bits.

E. - The E field has 2 variants:
- at the original Ethernet: types of Data,
- in the IEEE 802.3.: The length of the field of Data.

F. - Data.

G. – The control of the Data integrity, through CRC (Cyclical Redundant Check based on the Cyclical Redundant Codes).

**It must be emphasized that the Ethernet Address of Destination and the Ethernet Address of Source are both Physical Addresses (MAC addresses).**
**The Ethernet works at the physical level and not at virtual levels.**

This use of the MAC (Physical addresses) and IP Addresses must be understood in the sense that the Ethernet works only on the Physical / hardware MAC addresses.

Also, the Ethernet works at the physical level (level 1), which uses the MAC (Physical Addresses).

The stack of the TCP/IP protocols of each machine, present in the Operating System, such as in MS XP, creates the possibility for the IP Addresses for the virtual identification of each machine to also be used in the LANs, but at the bus level of the addresses' identification, it works only with Physical addresses.
It is clear that the LAN may work isolated from the Internet, without IP Addresses, but in any case, it does not have the possibility to work without the Physical, Ethernet addresses.

The use in the Ethernet LANs (including in isolated LANs) of the TCP / IP protocol and of the IP addresses permits:
- the immediate connection, when this becomes necessary, of the separate, isolated LANs to the Internet,
- the simplification of the work of the machines inside the LAN,
- the use of the generalized TCP /IP procedures and technologies,
- the use of the advanced TCP / IP testing and troubleshooting procedures at the isolated and non-isolated Ethernet LANs,
- the use of the improved facilities of the operating systems installed in the PCs, Laptops, etc., when monitoring the LANs.
- the simple configuration of the Machines within the Ethernet LAN.

For instance, the MS XP operating system implicitly offers (the initial process of configuration is necessary) the important features of TCP / IP protocols. These features include the IP virtual addressing facilities in the monitoring troubleshooting, etc.
This IP addressing is, in all cases, superposed on the Physical addressing. The LAN may not work without the physical addressing.

It must be remembered that:
- The MAC / Physical address is used in the TCP / IP Layer 1, Network Access, and is placed in the Ethernet header of the Data Packets,

- The IP Address is used in the TCP / IP Layer 2, IP header. In the IP header of the TCP/IP data Packet, the IP Address of the Destination and the IP Address of the Source are placed.

**The IP virtual addresses inside the Ethernet LANs are superposed on the Ethernet (Physical) Addresses. This leads to:**
- **simplifications and improvements of the Ethernet LAN construction in the LAN monitoring,**
- **the simple connection of the LAN towards the exterior, respectively towards the Internet,**
- **the efficient exploitation of the TCP /IP protocol, already present inside the operation systems of the machines ( PCs , Laptops, etc ).**

# 2. THE CREATION OF AN ETHERNET (LAN) NETWORK? ***NOTHING SIMPLER!***

1.) The simple network: Ethernet, peer to peer, democratic, without Server.

The creation of the **peer to peer** Ethernet LAN (isolated net).

A **peer to peer** Ethernet LAN is recommended for the small networks, for instance those with less than 10 machines.

The peer to peer Ethernet LAN is a democratic network. It is a network without a Server.
All the partners are equal and, consequently, have the same rights.

Considering the fact that:
- the TCP / IP protocols are implicitly installed in the majority of Operating Systems, such as in Microsoft MS XP,
- the Ethernet protocol is implicitly installed in the TCP/IP, on Layer 1,
the creation of an Ethernet separate LAN is extremely facile and:
- quasi-automatic (if the establishment of the IP addresses is achieved manually inside the TCP/IP configuration) or
- automatic, if the IP addresses are offered by the DHCP-Dynamic Host Configuration Protocol programme. For the use of the DHCP, a server with the DHCP function must exist within the respective isolated net).

**Despite the fact that the Ethernet is working at the physical level of the network, with physical addresses (MAC), the use of the TCP / IP protocol, including of the IP virtual addresses, leads to important facilities within the isolated (and non-isolated) LANs, such as:**

- **the possibility for the machines to recognize each other (through hidden ARP protocol activities);**
- **troubleshooting facilities, respectively, the use of the TCP/IP troubleshooting tools at the LANs.**

2.) The design of the Ethernet LANs.

The design phase of the Ethernet LAN is simple and influenced by:

- the necessary speed (bandwidth, estimated throughput) of the Ethernet LAN,
- the necessary lengths, which decide the types of cables, the types of components/ interfaces (up to the NICs),
- the wire limitations (single-room, multi-room, permitted trajectories of the cables, cable economy etc.),
- the features of the location,
- the initial physical topology,
- the estimated maximum number of partners of the LAN network;
- constraints in the placement of the Hubs or Switches,
- physical constraints (heat, noise, access to power outlets) at the placement of the equipment,
- type of topology:
  - dispersed (machines at some distances),
  - multi-segment (machines in different segments connected through bridges or through other devices),
- the possibilities of future extensions,
- the initial repartition of the IP Addresses, based on the clear, pre-established, pallet of IP addresses:

If the existent LAN is expected to be connected to the Internet, then these IP Addresses must:

- either belong to the pallet of IP Addresses allocated by the ISP (Internet Service Provider) to the respective network and where all the IP Addresses have the same NETID and all the respective IP Addresses are respected (integrated) by the Internet. These IP Addresses must be registered, unique IP Addresses.

- either the pre-management of the IP Addresses allocated to the LAN's participants will be achieved if the network will be connected to the Internet through the intermediary components, such as Proxy and / or NAT Server. These separated IP Addresses, for the partners of LAN, are selected from the game of the IP Addresses reserved for the internal (LAN) networks. These IP Addresses are:
  - 10.0.0.0 through 10.255.255.255
  - 172.16.0.0 through 173.31.255.255
  - 192.168.0.0 through 192.168.255.255

  These IP Addresses are not visible, with the respective address value, from the Internet side.

- Either the IP Addresses from the above segments will be used if it is estimated that the network will not be connected to the Internet (extremely rare cases, but possible).

If the respective LAN will work with DHCP, an initial IP Address must be manually (see previous lessons) given, for initial tests, to each machine of the network.

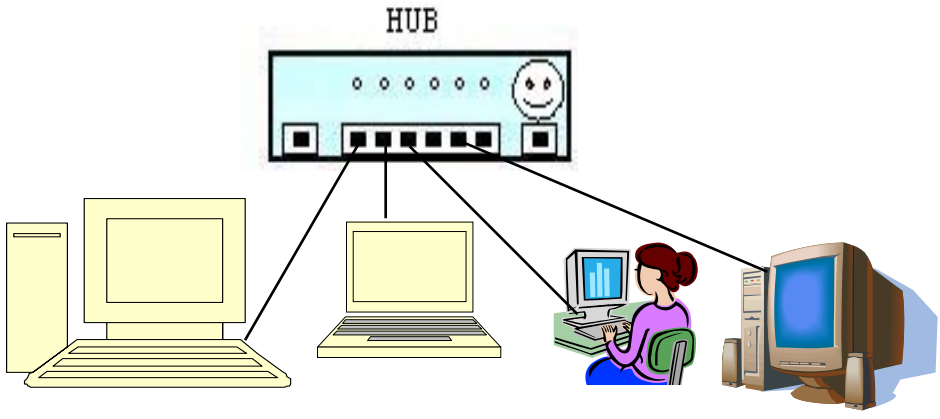


Fig. 2.1. An isolate Ethernet network, **workgroup** achieved in star configuration.

Putting into service.

The phases of putting into service consist in:

- receiving the drawings of the network configuration, placements of the devices, cables, outlets and the manner of placement and mounting of the cables,
- the mounting and installation of the network, including of the cables,
- the installation of each machine, **as client**, one after the other, within the Ethernet network,
- the verification, including automatic, of the operation.

The installation of a machine, **as client,** in the Ethernet separate (isolated) LAN consists in the following simple steps:

1.)- Plugging the connectors of the cables (such as the connector of the 100BASE-T) in the NIC connectors, respectively connecting the NIC- Network Interface Card of each machine to the LAN. Practically, the operation consists only in plugging the cable connectors inside the NIC connectors.The presence of the connection of the cable at the respective NIC is automatically detected by the Operating System of each machine.

2.)- The accomplishment of the TCP /IP configuration of each machine, including the allocation and installation of the IP Address. The process may be achieved through:

A. Manual configuration, as described in the previous lessons.

B. An automatic one, based on the DHCP.
The DHCP Server is not used and it is not present in the democratic, peer to peer LAN.
The DHCP may not be used in the isolated LAN.
The DHCP may only be used when the Ethernet LAN is connected to the Internet.

**After these very simple operations:**

- **plugging the connector into the NIC of the machine,**
- **the configuration of the IP Addresses,**

**the installation of the machine within the Ethernet LAN network is practically achieved (and usually successfully).**

3.) After the installation. The machines work hard to know the partners of the same (Ethernet) LAN's.

The Operating System of each machine connected to the LAN network tries to identify and to announce on its own display (for the selected regime of the screen dialogue, as shown below) **the presence of a new partner inside the network.**

With the aim of accomplishing this function, each installed machine (including the last one installed) will send, when the physical medium permits (through the non-presence of the Data transmission on the cable), a broadcasting towards all the network addresses. At this broadcasting, the machine receives responses offering information about each machine connected to the network.
This information includes:

- The Name of the machine,
- IP Address
- Physical Address.

Based on this information, the present partners inside the respective Ethernet LAN may see, on their own screen, information about each other's machines connected to the same LAN.

In the Microsoft ® MS XP Operating system, the Ethernet LAN's partners may see the presence of other partners on the screen of each machine. The partners (machines) appear and disappear on the display according to powering on or off the machines of the network partners.

The Microsoft ® MS© XP offers an important facility through this operation:
To see all the LAN machines connected (including powered), at the respective time, to the respective Ethernet LAN.

# 3. MS©XP FACILITIES AT THE PUTTING INTO SERVICE OF LOCAL NETS.

**Attention:**

**In view of understanding and exercising the aspects presented in chapter 3, it is necessary for the learner to achieve the indicated succession of commands, on his own PC / Laptop, in parallel with reading the lesson.**

**This chapter 3 unfolds in parallel with your actions on your running machine, by following each action indicated in the lesson step by step.**

## 3.1. MICROSOFT ® MS © XP: VIEWING THE PARTNERS OF THE MACHINE WITHIN THE SUBNET AND OTHER FACILITIES OFFERED BY MS© XP.

The MICROSOFT ® MS © XP Operating System offers great possibilities of testing the nets and subnets.
In order to see the machine partners of the Ethernet LAN, at the use of the MS © XP Operating System, the following steps must be achieved:

1. On the normal screen of the **MS © XP** Operating System, start by activating the **Start** Icon (left corner, below). In detail: click on the Start Icon → click on **Settings.**
2. Click on the **Control Panel** Icon. It opens the **Control Panel** screen**.**
3. In the **Control Panel** displayed screen click on **Network and Internet Connections.**

4. In the **Network and Internet Connections** screen**,** click on the **Network Connections** Icon (placed **down**, on the right side of the screen)**.**
5. Now the **Network Connections** page is opened**.** The page has 2 sections:
 - On the right side, the section of the screen named: **LAN or High Speed Internet** is positioned,
 - On the left side of the screen, the regime: **Network Tasks** is positioned
6. The first above-mentioned screen, **LAN or High-Speed Internet**, is a very important element for the supervision of the Internet Connections of the machine.

**The status / life of the machine in different networks (LANs , Wi-Fi LANs, etc.) may be identified by the communications on this screen.**
On this screen, Icons related to different existent connections of the machine are displayed.
For instance, the Icon formed from 2 PCs connected to a network, the Icon which indicates the present connection of the machine to the LAN, written explanatory elements.

7. On the left side of the **Network Connections** page, under the title:
**Network tasks,** a column with the following regimes can be found:
   **1. Create a new connection,**
   **2. Set up a home or small office network**

   See also
   **3. Network Troubleshooter**

   Other places:
   **4. Control Panel**
   **5. My Network Places**
   **6. My Documents**
   **7. My Computer**

   **8. Network connections**
   System folder

Clicking on the above-mentioned **Create a new connection** Icon opens the **New Connection Wizard**, an intelligent assistant, which leads to the following operating regimes and possibilities:

- **Connect to the Internet**
- **Connect to the network at my place**,
- **Set up a home or small office network**,
- **Set up an advanced connection**.

The above regimes of the **New Connection Wizard** may be launched individually and will help solve the respective task and desire.

* * *

Clicking on the above-mentioned **Set up a home or small office network** Icon opens the **Network Setup Wizard**, an intelligent assistant, which leads to the following operating regimes and possibilities:

- Connecting directly to the Internet,
- Connecting to the Internet through another computer.

Also, the same **Network Setup Wizard** regime allows the opening of the indications: **checklist for creating a network**.
The **checklist for creating a network** indications include important explanations about the networking and related aspects.

* * *

Clicking on the **Network Troubleshooter** regime opens the important page:
**Networking problems.**

## 3.2. VIEWING THE LAN PARTNERS ON THE DISPLAY THROUGH THE USE OF THE MS © XP.

In order to see the machine partners of the Ethernet LAN, at the use of the MS © XP operating system, first of all, as explained in the above rectangles, the following must appear on the screen page:
**Network Connections.**

This page appears on your screen by following the procedure illustrated in the above rectangles, at point 5.

The **Network Connections** page presents exceptional importance for:
- The operations of putting the network into service,
- The operations for integrating and configuring a machine inside the network
- Supervising and monitoring, at a moment in time, the network situation and the evolution / status of the network.

By clicking on one of the complex Icons on the right side of the page, the left side of the page automatically reacts through new positions (new menu categories and details) in the vertical menu from the left side of the screen, including with:

1.)- The regime indicated in the menu on the left side of the screen:
**View status of this connection**.

By clicking on the **View status of this connection,** one can read:
- about connection: duration, speed, status, signal strength,
- about activity: number of packets sent, number of packets received,
- properties and other.

The **View status of this connection** menu has 2 regimes:
- general and
- support

each with multiple types of information.

For instance, in the regime
- **general**, the following may be presented by clicking on **properties**:
  - **Connect using. Connect using** indicates the type of NIC (Network Interface Card), for instance "RTL8139 Family PCI Fast Ethernet NIC". This regime permits the use of other facilities, such as **Configuring**, which permits the opening of a **Trouble-shooter**. The **Trouble-shooter** offers the information for the troubleshooting in the existent situations, at the respective time.
  - The item used by the above connection and the elements involved in the above connection, such as (only examples):
    - TCP / IP Internet Protocol,
    - NWLink NetBios,
    - NWLink IPX/SPX NetBios Compatible Transport Protocol…
    - Client for Microsoft Network
    - File and Printer Sharing for Microsoft Network,
    - QoS Packet Scheduler
    - And other.

A part of the above protocols and regimes may be opened by clicking on **Properties** (in the **Network Connections** page**,** on the mini-screen describing the features of the type of connection).

For instance, in the **View status of this connection → Properties** regime, the opening of the following line (by click) may be achieved:
- **Internet Protocol TCP / IP**, where the present TCP/ IP settings can be viewed.

2.) – The **My Network Places** menu (in the left column of the **Network Connections** page).

Clicking on **My Network Places** opens on the screen the page: **My Network Places**.
On the **My Network Places** page**,** on the right side of the screen, under the title: **Local Network**, (usually numerous) Icons are illustrated, related to the Public documents, of the different partners (machines) of the Local network.

In the **Details** section (of the vertical column on the left side of the screen), details about the connection are indicated. These details are indicated by the activated (roll-over) Icon (the Icon changes its colour when the arrow of the mouse is on the respective Icon, signalling that it has the attention of the human operator).

Simultaneously with the opening of the **My Network Places** page, new lines will appear inside the menu, in the column on the left side of the page.

At this step, special attention must be given to the Icon and the line of the left menu named:
**View workgroup computers**.
(The Icon is formed from a triplet of machines, where each machine is connected to the same LAN).

The **View workgroup computers** regime presents a special importance. It permits the dynamical viewing of the machines which are connected, respectively which connect (and these machines are illustrated on the screen), or are disconnected, where the images of the disconnected machines disappear from the screen.

A workgroup signifies any network which does not use a centralized Server for user authentication [21.].
In fact, the Workgroup is a LAN without a centralized Server.

After clicking on the Icon (the triplet):
**View workgroup computers**,
the system (the machine and the network) works intensively:
the machine (your machine, for instance) sends broadcasting messages, questioning the network about all the machines connected in the respective group or subnet and about their status.

The valid machines respond with adequate Data Packets towards the questioning machine.

These responding machines have the possibility to send their packets, because the address of the machine which questions is present in the questioning packet.

All the operations are solved by the software packages which support TCP /IP protocols.
Normally, the ARP protocol of the TCP/IP suite of protocols is automatically launched and brings the responses from the different Ethernet LAN machines.
This test detects the machines which are “live” and are connected to the subnet.

The intense activity and dialogues may be seen within the **View workgroup computers** menu, on the Icon on the left side of the screen.
For instance, the image indicating the machines connected to the respective group of Ethernet LAN (the group may represent the entire LAN, a segment of addresses or another configuration) is illustrated, only as an example, in the following image (the image is normally generated by the Microsoft ® XP software; in the figure, only one example is created to suggest the Microsoft ® software running results).

The machines connected to the net, but with the **power off** will **not** be indicated on the screen.

At the respective time, these powered-off machines are not considered partners of the net, despite the fact that these machines have the net cable connectors plugged in the NIC.
The situation is generated by the fact that the un-powered machines do not have the possibility to respond to the requesting Data Packets.

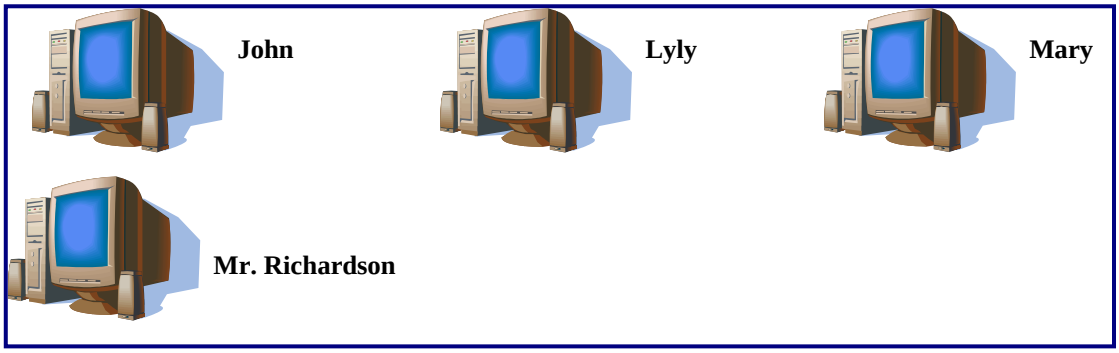


Fig. 3.1. In the **View workgroup computers** regime, the Microsoft ® software assures that the machines connected to the LAN dynamically appear and disappear, according to their powered and un-powered status. A new powered machine will be automatically signalled on the **View workgroup computers** screen (Fig. 3.1. is only an illustrative figure).

New machines connected to the network. The test about the presence of the machine inside the net.

The good integration of a new machine inside the Ethernet network is also detected and globally tested by the above described regime, in the regime:

**View workgroup computers**.

Each newly connected and powered machine will automatically appear on the screen.
In the **View workgroup computers** regime, the presence of the new comers may be seen.

Other possibilities to view the network behaviour offered by the MS © XP **My Network Places** page

From the **My Network Places** page, by using the left column of menus, the following steps are possible:

| **Click on:** | **Look to:** |
|---|---|
| **View workgroup computers** | Partners of the group connected to the network (as explained above). |
| **Microsoft Windows Network** | Displays on the right side of the screen: all the groups, in the form of Icons (as triplet Icons), and indicating the name of the respective group. |
| **Click** on the selected **Icon** of the above groups (indicated in the left side of the above row). | The Machines of the respective group are selected and displayed in the form of Machines Icons. |
| Click on the selected **Icon** of the above **Machines Icons**. | Many possibilities are generated:<br>- If public documents exist, they can be selected and viewed (with or without password, depending on the case).<br>- If the access is prohibited, the respective indication about the prohibition will be displayed. |

# 4. MS® ELEMENTS OF THE TROUBLESHOOTING OF THE LAN

Important aspects related to the troubleshooting are illustrated in the above and below lessons.
The aspects include:

- 1.) THE MICROSOFT® MS © XP **PAGE**: **"NETWORKING PROBLEMS"** which first of all helps by generating numerous explanations.
  The explanations are delivered based on the use of the word **Search** regime (at the top of the page, on the left). The words for which one may search to receive explanations may be found with the **Index** command**,** on the top horizontal menu .
  The MS © XP **NETWORKING PROBLEMS** page includes 2 categories of aspects:
  - "**Fix a problem**" and
  - "**Pick a task**".

- 2.) THE MICROSOFT® MS © XP **NETWORK DIAGNOSIS**.
  The MS © XP Network Diagnosis is opened on your machine in the following way (succession of clicks):
  **Start** (1 click) → **Settings** → **Control Panel** (1 click ) → **Network and Internet Connections** → ( in the column on the left side ) (under **Troubleshooters**) → **Network Diagnosis** (1 click).

**The MS © XP NETWORK DIAGNOSIS** achieves the diagnosis of the respective machine related to the status and life of this machine within the net. The diagnosis is accomplished based on the consistent number of automatic tests.

The tests of this automatic diagnosis offer important results, such as:

- **the fact that the NIC – Network Interface Card has passed or not the diagnosis test**,
- Information about the Internet Explorer web Proxy:
  - IEProxyPort (number)
  - IEProxy IPAddress): the results of the Ping test, towards the Proxy IP Address. The presentation of the complete manner in which the Ping test has evolved.
  - The port at which the Server of the LAN is running and other Data.

The resulted aspects, indicated with + in the left rectangles, of the displayed results may be extended (by clicking on the +) to:

- supplementary information or
- about the manner in which the Ping test has evolved.

- 3.) TESTING THE SIMPLE ETHERNET LAN.

a. -Testing the connectivity of the personal machine with different other machines of the LAN.The testing of the connectivity within a very simple Ethernet LAN, without a Server, is possible through the use of the Ping tools (described in the previous lessons).

b. **- Net view command** http://www.computerhope.com/nethlp.htm#03

The testing of the list of resources which are being shared (with other machines connected to the respective Workgroup / LAN) is achieved with the MICROSOFT® MS © XP tool: **Net view.**

The Net View command permits the testing of the list of resources which are shared on the machine (computer).

The Net View command lists the respective workgroup which shares resources on the screen of the computer.

The syntax of the command may be:

Case 1.

**NET VIEW** [\\computer] [/YES]

Where **computer** specifies the name of the computer whose shared resources will be listed.

For it to be used, it is necessary to know the name of the machine. The name of one's own machine may be immediately obtained with the **Hostname** command (presented in the previous lessons).

For a machine with the name Sand, the MS-DOS commands are:

**C:\>Net view \\sand**,

and the exemplified response of the machine may be:

**Shared resources at Sand**
**Sand**

| **Share name** | **Type** | **Used as** | **Comment** |
|---|---|---|---|
| **pub** | **Disk** | | |
| **SharedDocs** | **Disk** | | |

**The command completed successfully**

If there are no entries in the list, the machine will write: **There are no entries in the list.**

Case 2.

**NET VIEW [/WORKGROUP:wgname] [/YES]**

Where **WORKGROUP** indicates that the computer where the shared resources will be presented is in another workgroup.

**Wgname** specifies the name of the workgroup for which the shared resources are desired to be viewed.

c.)- The Results of the **Network Diagnosis** achieved with the MS © XP NETWORK DIAGNOSIS, as mentioned in the above point.

# 4. THE SECOND STEP. THE EXTENSION OF THE ETHERNET LAN BY INCLUDING A SERVER. THE DOMAIN BASED NETWORKS.

2 types of networks generate the basic elements:

- A. - Workgroups,
- B. - Domain Environments.

The small collection of computers connected together for information and resource sharing is named Workgroup.

Larger environments, respectively larger LANs, have surpassed the level of Workgroup and become Domain Environments. They use a centralized administration, achieved by one or more Servers (for instance Window Servers).

1.) The Server within the LAN. **The Workgroup**.
In the above chapters, the manner of creating the most simple Ethernet LAN, **the Workgroup**, the democratic LAN, in which all the partners have equal rights, is described.
Also, all the machines have 1 NIC (Network Interface Card), through which the connection to the network is achieved.
The **Workgroup** solution is destined for a small group of machines (normally under 20) which may create an isolated LAN.

It is possible to introduce a Server within the initial LAN workgroup.

The Server of the LAN may accomplish supplementary rights and tasks. For instance, it may achieve the cooperation with the DHCP (Dynamic Host Configuration Protocol) or achieve the NAT (Network Address translation), respectively accomplish the function of representing the LAN, through an IP Address visible on the Internet, and, possibly, received through the DHCP procedure.

Also, this Server may offer important functions to the isolated network: it may deliver materials from its own Data Base, for instance, multimedia, etc., or materials from CD-ROMs or DVDs to the local partners.

When one of the network partners has become a Server, it is possible to discuss about 2 situations:

A. If the Server also has only 1 NIC, that means that this Server may be connected only to the respective network.
B. If the Server has 2 NICs, that means that the Server may be connected, through the second NIC, to the other network, usually to the Internet. B. is the normal solution.

The Server connects the initially separate net to the exterior of the net, normally towards the Internet.

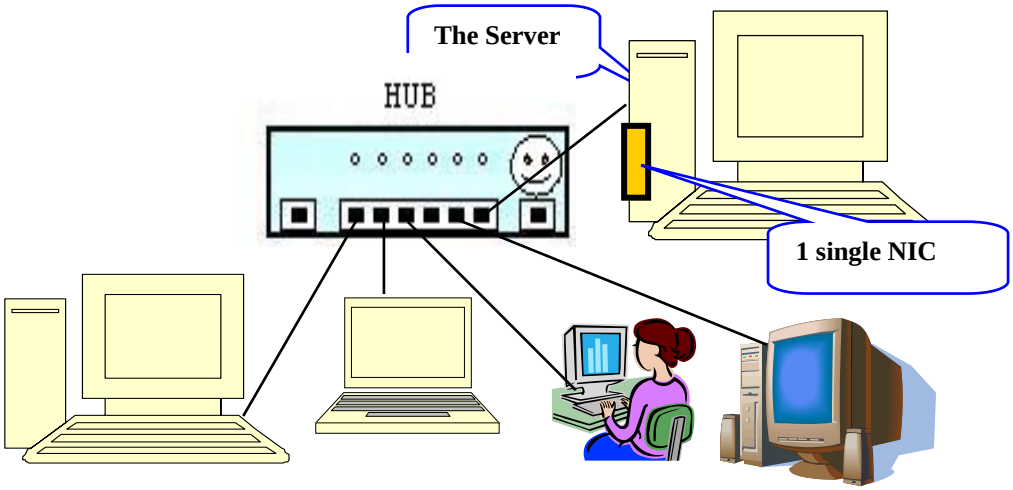


Fig. 4.1. An isolated Ethernet network, achieved in star configuration.

2.) The Domain Based Network.

In the Domain Environment, the central server verifies the password and the user name for the respective Domain.

The Windows domain, for instance, provides the following benefits [21]:

- improved security: the Active Directory of Windows XP offers security features such as:
  - digital certificate authentication,
  - IP security.
- Organization, centralized administration and control (the maintenance and the control of the users and of resources, management of permissions, etc.),
- Domain extensibility: the possibility to grow the number of machines,
- Domain flexibility: delegation of the management to another machine, grouping in organisational units: in tree, forests, etc.

For the more extended LANs, with many machines, the second solution may be applied, consisting in the creation of the Domain-Based Network.

The Domain Server is a Server destined to administer one domain. A Domain controller, normally the same Server, assures the user authentication of the network users and the communication with other domains [21.].

In conclusion, the LAN:

- may not have a Server, the situation being known as a **workgroup**, for a small number of interconnected computers,
- may have a Server, not connected to other networks, but which performs functions within the network (authentication, the delivery of information, such as multimedia, lessons etc., supervises the security) and this configuration is named **Domain environment.**
- may have a Server (including, for instance, the domain server) which connects to other servers (below the third step, Chapter 5.), normally to the Internet.

# 5. THE THIRD STEP. THE EXTENSION OF THE ETHERNET, BASED ON THE GATEWAY SERVER (OR ROUTER), TOWARDS THE INTERNET. NAT. DHCP.

## 5.1. THE NON-ISOLATED LAN.

1.) The equipments which have minimum 2 NICs.

The solution to connect the LAN to other networks, especially to the Internet, consists in the use of a Gateway which connects the LAN to the Internet.

The connection of the LAN to the Internet amplifies the LAN power by thousands or millions of times.
At the same time, it may create big problems of security.

The Gateway which connects the LAN to the Internet has a minimum number of 2 NICs, one for the connection to the LAN, and the second for the connection to the other network, for instance to the Internet.
The equipment which connects the (first) LAN to the other network may be a bridge or a very intelligent Gateway, also named Router.

The Server with the Router functions may also:

- Achieve the NAT functions (Network Translations Functions),
- Achieve DHCP (Dynamic Host Configuration Protocol) functions,
- Permit the accomplishment of the DHCP functions, inside the LAN, through the use of the DHCP facilities and protocol offered by another DHCP Server, anywhere in the Internet space.

Having 2 NICs, fig. 5.1., the server with the Router function, with one input and one output, will also have 2 IP addresses:

- 1 IP Address inside the initial LAN, which is nothing but the Default Gateway and
- 1 IP Address in the configuration of the exterior network and which connects the Gateway to the Internet.

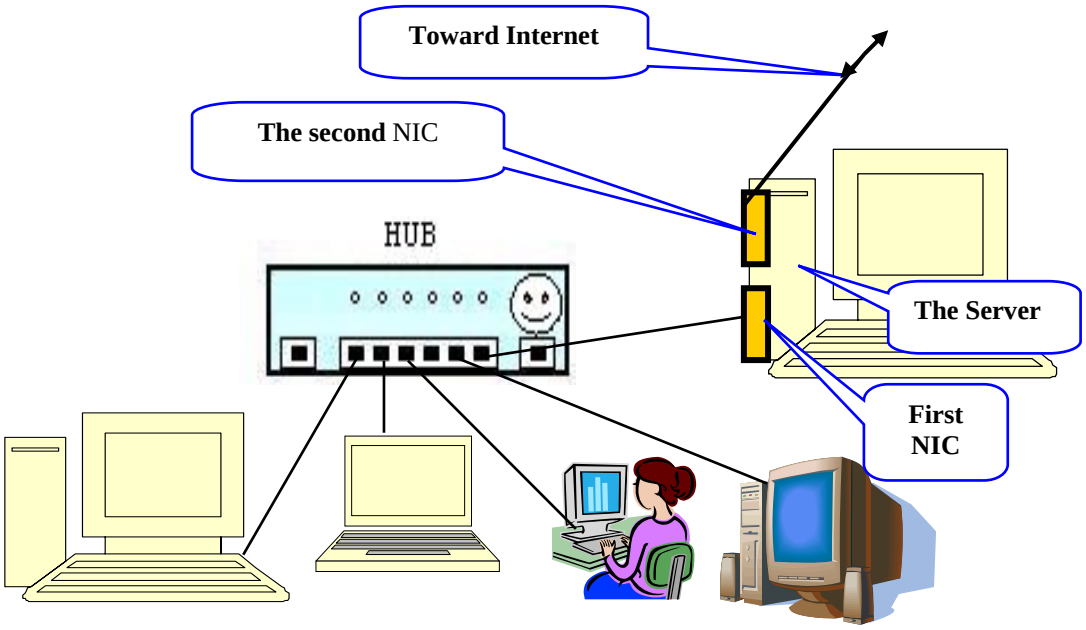


Fig. 5.1. Opening an isolated Ethernet network to the Internet.

2) The multiple possibilities to connect the Router to the Internet.

In fig.5.1., different possibilities are illustrated through which the machine, which may be a Server with the function of Gateway, respectively Router, connects the LAN to the new network which permits the connection to the Internet.

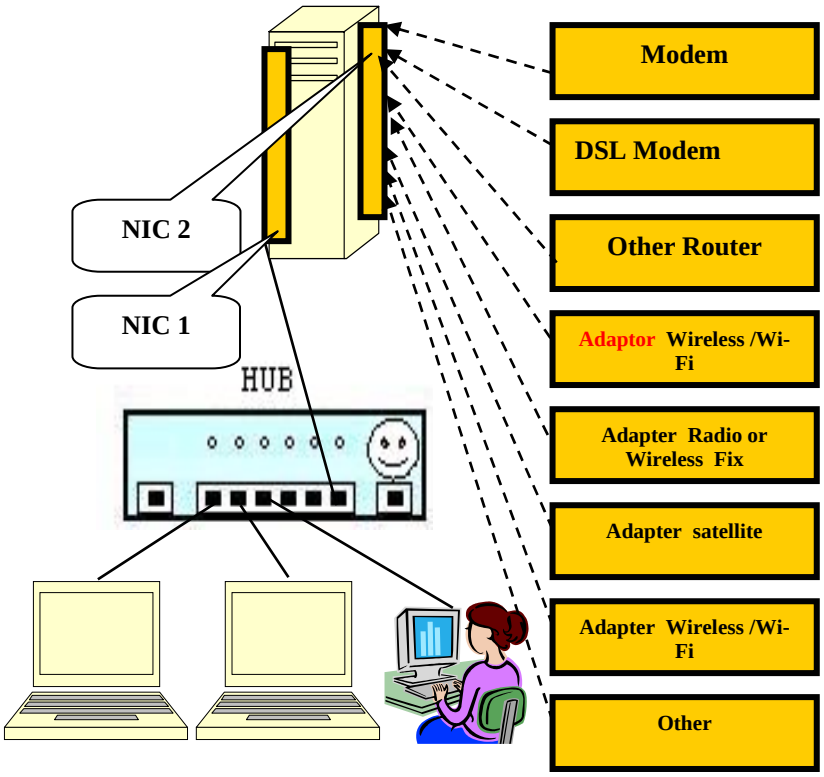


Fig. 5.2. Different possibilities for connecting the Ethernet LAN to the Internet.

## 5.2. NAT.

NAT – Network Address Translation procedure provides transparent **IP- level access** to the Internet from a host internal to a LAN and also with **a private (unofficial/ non-registered) address** [22].
Through **NAT – Network Address Translation**, the machines of a LAN, machines which do not have officially registered IP Addresses, may use the IP Addresses (of the NAT Server).

The NAT technology ensures that the hosts from the LAN side which do not have official IP Addresses may be active at the level of the IP Addresses.

Based on the NAT, the LAN may have a single connection to the Internet and a single (or multiple) official / legal IP Address, named the G (global) IP Address for communications with the Internet.

The NAT software is implemented within the NAT Server /Gateway.

From the Internet side, the Internet partners view only the Gateway Internet Address. [The Internet machines view only the IP Address of the NAT Server (IP Address on the Internet side of the NAT Server) and not the addresses inside the LAN].
For the Internet partners, the IP Address (or Addresses) of the NAT Server, from the Internet side, represents the LAN's IP (temporary official) Address (or Addresses).

The NAT Server ensures the monitoring of the LAN's internal IP Addresses (non-registered addresses of the Hosts of the LAN) and the correspondence between:
- the LAN's internal Addresses and
- the Internet IP Address of the NAT Server.

With this target, the LAN partners share the same IP Address of the NAT (the IP Address from the Internet side) in correspondence with the external communications needs.

The NAT software placed inside the NAT Server (Gateway), notices, maps, stores and translates all the requirements of communications of the Addresses (machines) from the LAN.
In the second phase of the process, the NAT Server uses these notations (about the LAN partners) for directing the responses arrived in the NAT Server towards the LAN internal addresses.

**The LAN addresses (IP Addresses) are not visible from the Internet side.**

**Only the NAT's IP Address is representing (using supplementary NAT's notations) all the LAN's addresses.**

These internal LAN's addresses are interpreted by the NAT Server, which uses the internal NAT addresses and its own notations to help the communication of the Hosts of the internal LAN (and which do not have official registered IP addresses) to and from Internet.
Certain simplifications and an economy of IP Addresses result.

The operation of the NAT.
The NAT translates the addresses in both directions: for the outgoing and for the incoming Data Packets.

- For the outgoing Data Packets (from the machines of the LAN), the Source address of the host is replaced with the G named IP Address.
- For the incoming Data Packets (from the Internet), the Destination IP Address is replaced with the private address of the respective host.

From the Internet point of view, all the Data Packets from NAT use the NAT IP Address. Only the NAT address is viewed from the Internet side.

From the internal (inside LAN) host point of view, the NAT Server is viewed as a Router.

To summarize:
A. When a machine of the LAN launches a request, the NAT Server offers its IP Address (named G) to the requester (the station of the LAN which has launched the request) and notices the situation (maps inside the Table of correspondences).
Through this process, the Source IP Address inside the Data Packet is replaced with the NAT's IP Address (named G).

B. The NAT Severe / Router transmits to the Internet (under its own IP Source Address, named G) the request of the machine of the LAN.

C. The corresponding appealed machine of the Internet responds by transmitting the Data Packets towards the leased IP Address (named G), offered by the NAT Server / Router to the machine from the internal LAN.

D. When the response from the Internet returns to the NAT Router (or Server), the NAT Router achieves the inverse procedure: **it changes the Destination Address, from the header of the coming Data Packet, with the private Address of the respective machine of the LAN** (which has launched the requirement).

Therefore, the Data Packet of response arrives, through the personal NIC, at the private address of the machine of the LAN, machine which has launched the request.

How does NAT know which internal host should receive a Data Packet arrived from the Internet?
The solution is based on the fact that the NAT Server constructs tables of correspondence.
In the Table of correspondence, 2 or more items are written for each established communication:

A.- which internal IP Address (unofficial address) of the LAN has required the communication with the
B.- IP Address from the Internet world.

The above information is used for directing the responses from the Internet, passing through the NAT Server, toward the right, internal addresses of the LAN.

The initiation of the Table of correspondence is normally achieved by the outgoing Data Packets (the Data Packets arrived at the NAT Server from the internal LAN), when these Data Packets pass through the NAT Server and support the replacement of the source address with the G address (respectively, the IP address of the NAT Server).

The NAPT. There are different variants of the NAT, such as NAPT.

An example of the translation table used by NAPT is the following [22]:

| Private Address | Private Port | External IP Address | External Port | Nat port | G Address= IP Address of the NAT viewed from Internet side | Protocol Used |
|---|---|---|---|---|---|---|
| 10.0.0.5 | 386 | 192.10.2.3 | 80 | **14005** | 192.168.1.1 | tcp |

At the outgoing (from internal LAN) of the Data Packet, the Source IP Address is replaced: 10.0.0.5 with the G (NAT) IP Address: 192.168.1.1.
At the reception of the Data Packet from the Internet, the destination IP Address: 192.168.1.1 is replaced with the Host IP Address: 10.0.0.5.

The NAPT uses in translation several elements for identification (of the host from the LAN):
1.)- a NAT port,
2.)- external address (IP Address, respectively the address from the Internet, to which the Data Packet must be sent),
3.)- external port to be accessed,
4.)- G address (the IP Address of the NAT Server from the Internet side).

The 4-tuples identify completely the owner (the Host from the internal LAN) which communicates in the respective time interval.

Instance of 4-tuple: [ G= 192.168.1.1 ; NAT PORT = 14001; External Address: 128.1.2.4; External port (the port of the Internet web site, from which the Data is intended to be taken)].
The element which avoids the confusions (when many hosts access the same destination address) is the NAT PORT.

The NAT PORTs are allocated by the NAT protocol, one for each machine for each communication.
The NAT PORT number avoids the potential conflicts when 2 machines internal to the LAN communicate with the same Internet machine.

## 5.3. DHCP.

The DHCP permits a computer to accomplish the information necessary to operate without manual intervention, including the IP Address and the network mask.

The DHCP (Dynamic Host Configuration Protocol) automatically assigns the IP Addresses and the subnet masks to the machines which request an IP Address.
The work is achieved by the DHCP Servers in the world.

Many operating systems of the machines are configured to automatically accomplish, DHCP based, an IP Address by default. Example: Windows XP Professional. This aspect may be viewed by looking at the screen: **Internet Protocol (TCP/IP) Properties** (where the following may also be set manually: the IP Address, Subnet mask, Default gateway.

The steps of operation of the DHCP are the following:

a. When the computer is turned on (power on), the machine, named client computer, does not have an IP Address and requires an IP Address from the DHCP Server (or Servers, through broadcasting).
The requirement is called: "DHCP discover message", respectively DHCPDISCOVER, and includes:
- The host name of the client computer which requires an IP Address,
- The Physical Address (MAC) of the client computer which requires an IP Address.

Normally, this requirement is sent (by the machine which is powered and does not have an IP Address) in the form of a broadcast. The broadcast is sent repeatedly until a response is received.

b. The DHCP Servers from the world respond with the message DHCPOFFER.
Because the client machine does not have an IP Address, the DHCPOFFER message is also broadcasted. It is broadcasted by the DHCP Servers.

The client computer takes the first offer and acknowledges, through broadcasting, this acceptance by broadcasting the message DHCPREQUEST. This message informs the DHCP Servers that a DHCP Server was selected.

At the same time, the other DHCP Servers terminate the offers (based on the conversation), respectively they retract the offers.

c. The respective selected DHCP Server sends (also broadcasting) to the Client machine the DHCPACK message:
The client computer accomplishes, through the DHCPACK, in leasing (or permanently), after automatic "negotiations" with a DHCP Server:
- an IP Address,
- a subnet mask,
- a time interval, in hours, of leasing the IP Address.

d. The client machine changes the regime of the granted IP Address to a permanent IP Address.
From this moment on, the client computer has an IP Address and may work normally inside the Internet network.

## 5.4. THE POSSIBLE JOINT WORKS OF NAT and DHCP [4.].

For the general configuration, illustrated in fig. 5.1., the NAT and DHCP procedures may work together.
The same Server / Gateway may be, for the machines of the LAN, a NAT router and also a DHCP Server.
The NAT and the DHCP may work together, for instance, as follows:

The Gateway Server (the Server of the LAN, which connects to the exterior of the LAN) acts, in this example simultaneously, as:
- NAT Server. The NAT Server has its official IP Address (received from ISP). The NAT Server ensures the translation of IP Addresses, based on its own registered IP Address,
- DHCP Server, offering dynamic IP Addresses to the machines of the LAN.

For instance, the DHCP Server, destined to achieve the DHCP procedure only to the LAN, receives from the ISP, for itself, the IP Address 192.168.1.1 and leases IP addresses to the computers of the LAN house, such as, for instance:
192.168.1.2; 192.168.1.3, etc.

## Key Point Summary Conclusions and Recommendations

- The achievement of the LANs consists in 2 steps: the creation of the workgroup connection or Domain environment and the extension of these LANs towards the Internet. In the second step, advanced procedures may be used, such as the use of the NAT Server in combination with the DHCP Server.
- The design of the Ethernet LANs takes into consideration the selection of the network topology, wire limitations and constraints, physical constraints, the possibilities of extension, costs and the required bandwidth.
- The TCP / IP also present advantages at the use inside the LAN and also within the LAN which is not connected to the Internet. The use of the TCP / IP within the isolated LAN permits the self-recognition of the partners and the dynamic monitoring. Also, it is possible to view the workgroup connections (MS ®), the presence of the machines inside the LAN and the entry (connecting) of new machines inside the LAN.

- The NAT Server procedure, combined with the DHCP Server, adds supplementary advantages to the Ethernet LANs.

## Study Guide
### ESSENTIAL QUESTIONS FOR THE VERIFICATION OF THE ACQUIRED KNOWLEDGE

1. What are the components of the Ethernet Data Packet?
2. What are the components which influence the design of an Ethernet LAN?
3. Why is it necessary for an Ethernet LAN to use the TCP /IP protocols and IP Addresses, even if it is an isolated workgroup LAN?
4. How is NAT working?
5. Which are the functions of the NAT server + DHCP Server joint procedure?
6. Can the above 2 Servers (NAT and `DHCP for Local LAN) be placed as software packets inside a single Server which monitors the LAN?
7. Where, on your machine, may you find more information about the networks and the networking?
8. With which tool or procedure can you see, from one machine of the work group, the putting into service of a new machine in the LAN?
9. The MICROSOFT® MS © XP procedure. Does **viewing workgroup connections** represent a powerful, dynamic test and tool about the situation of the connection of a new machine within the LAN?
10. Which other tools are recommended to test the status and the availability of the new partner inside the LAN?

### 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.
[11.] Gilbert Held: *Ethernet network. Design, Implementation, Operation and Management* .Fourth edition. John Wiley and Sons Ltd, England, 2003, 0-470-84476-0.
[12.] Terè Parnell: *LAN Times Guide to Wide Area Networks.* Osborne McGraw-Hill, Berkeley, California 94710, USA, 1997, 0-07-882228-9.
[13.] IEEE Standard 802.1 - LANs: General concepts and architecture.
[14.] IEEE Standard 802.3- ETHERNET.
[15.] IEEE Standard 802.8- Optical fiber.
[16.] IEEE Standard 802.9 - LANs for the real time applications.
[17.] IEEE Standard 802.10-Virtual LANs and the security.
[18.] IEEE Standard 802.11- Wireless LANs
[19.] IEEE Standard 802.15- Bluetooth
[20.] IEEE Standard 802.16- Wireless BB ( Broad Band ).
[21.] Curt Simmons, James Causey: *Microsoft® Windows ® XP Networking. Inside Out.* Microsoft Press, Redmond Washington, 2003, 98052-6399.
[22.] Douglas E. Comer: *Networking with TCP/IP*, 5-th edition, Pearson Prentice Hall, 2006, 0-13-187671-6.

### 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
[ Supplem. 4. ] http://uga.edu/~ucns/lans/docs/ethernet/faq Ethernet Network Questions and Answers. Summarized from UseNET group… .

### SUPPLEMENTARY INDICATIONS ABOUT THE CONTENTS OF THE LESSON

It is also recommended to consult the documentations from: www.cisco.com; www.cramsession.com; http://www.computerhope.com/nethlp.htm#03 and other.

### ANSWERS TO QUESTIONS

1. The Ethernet Packet looks (in general) as follows:

| 62 bits | 2 bits | 6 bytes | 6 bytes | 2 bytes | 46 bytes to 1500 bytes | 4 bytes |
|---|---|---|---|---|---|---|
| A<br>The Preamble **to accomplish the synchronization** | B<br>The delimiter which indicates the Start of the Frame | C<br>The Ethernet Address of the Source: 6 bytes, respectively 48 bits | D<br>The Ethernet Address of the Source: 6 bytes, respectively 48 bits | E<br>types of Data, in the IEEE 802.3. | F<br>- Data. | G<br>Control of the Data integrity |

2. The elements which influence the design phase of the Ethernet LAN are the necessary speed (bandwidth, estimated throughput) of the Ethernet LAN,
   - the initial physical topology and the estimated maximum partners of the LAN network; the repartition of the Hub or Hubs,
   - type of topology: dispersed (machines at some distances), multi-segment (machines in different segments connected through bridges),
   - the wired limitations (single-room, multi-room, permitted cables trajectories, cable economy etc.),
   - physical constraints (heat, noise, access to power outlets) at the placement of the equipment,
   - the location features,
   - taking into consideration the future extensibilities,
   - other.

The above elements influence: the initial repartition of the IP Addresses based on the clearly pre-established pallet of IP addresses; the types of cables, the types of components and interfaces,

3. Because the use of the TCP / IP protocol (including the IP Addressing) offers many important facilities, such as: the possibility for the partners of the LAN to recognize each other, for the TCP /IP troubleshooting possibilities to be applied, for a quick connection to the Internet to be assured.

4. When a machine of the internal LAN launches a request, the NAT Router leases its IP Address (and notes that) to the requester. The NAT Router transmits to the Internet the request of the machine of the internal LAN. The corresponding appealed machine from the Internet responds, transmitting the Data Packets towards the leased IP Address, temporarily offered by the NAT Server / Router to the LAN machine.When the response from the Internet returns to the NAT Server / Router, the NAT Server / Router achieves the inverse procedure: it changes the Address from the header of the coming Packet with the Address of the LAN machine and sends the Data Packet within the local LAN.

5. The NAT + DHCP procedures offer the translation of addresses by the NAT server together with the accomplishment of the DHCP Addresses to the machines of the LAN.

6. Yes.

7. With the MICROSOFT® MS © XP PAGE: "NETWORKING PROBLEMS" which firstly helps by generating numerous explanations, the **Search** regime (at the top part of the page, on the left). The MS © XP page **NETWORKING PROBLEMS** includes 2 categories of aspects: **"Fix a problem"** and **"Pick a task".**

8. **View workgroup computers.** From the page MICROSOFT® MS © XP PAGE **Network Connections → My Network Places → View workgroup computers**, you enter the page **View workgroup computers**, which dynamically displays the entry or disappearance of the network partners.

9. Yes.

10. THE MICROSOFT® MS © XP **NETWORK DIAGNOSIS**. **Start** (1 click) → **Settings** → **Control Panel** (1 click) →**Network and Internet Connections** → ( in the column on the left side ) under **Troubleshooters** → **Network Diagnosis**.
Also**: Ping, ARP, TRACERT, NETSTAT, NBTSTAT** and other.

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