LESSON E4_EN. BRICKS OF THE TCP/IP. INTERNET ADDRESSES AND INTERNET ADDRESSING.

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:
- The main types of addresses used in Internet and practising these addresses.
- The concepts of TCP/IP addressing and their practical use. Applying the Physical / MAC Addresses.
- Understanding the practical network configuration and design from the point of view of addressing.
- Working with binary, hexadecimal and dotted decimal addressing modes and related conversions.
- Network structures from the point of view of addressing. Other essential aspects.

CONTENT OF THE LESSON

LEARNING OBJECTIVES:

After learning this lesson, you will accomplish the ability to:
- Practically understand, work with and use the types of network addresses.
- Apply the TCP / IP elements to problems regarding addressing aspects in networks.
- Practically understand and use the conversion of the network addresses and the conversion application in the configuration and design of the networks,
- Classic networks structures from the point of view of addressing.
- How to achieve a network from the point of view of addressing.

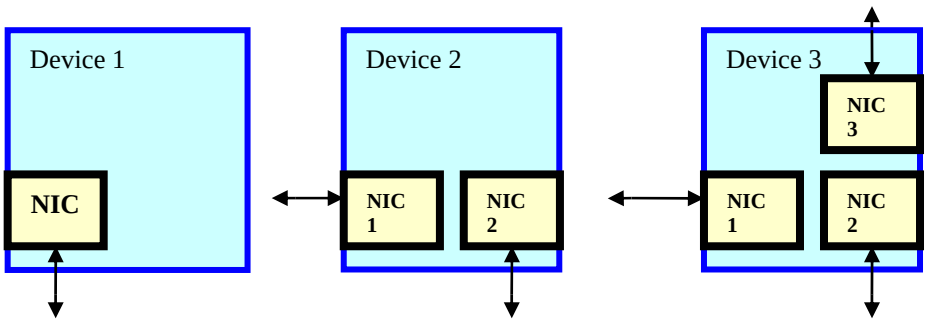
1. IMPORTANT BRICKS FOR UNDERSTANDING THE TCP/IP.

In the previous lessons you have practically experimented the travelling of Data Packets on the pathways and the testing of connectivity. These are the bricks of the Internet. The tests are also conducted through an intensive use of Internet addresses.

Other important bricks of the Internet technology consist in:
- Internet communication based on switching / commutation of Data Packets and on the transfer of Data Packets, respectively, through different paths of the world networks.
- The Internet functions based on a robust suite of IP protocols.
- The Internet functions based on an efficient use of virtual addresses: IP and physical addresses: MAC.
- The IP addressing permits finding the destination network and also the network segmentation, separation and isolation. The MAC addressing permits the communication with the computer from the final network, the LAN.
- The End to End technology is a technology in which Data Packets travel from Source to Destination Hop by Hop (Device by Device).
  The Data Packets are processed in Hops (Servers, Routers, etc) and sent from each Hop to the destination.
  The selection of the NIC (the Network Interface Card) of the Hop (the Hop where the Data Packet has arrived) through which the Data Packet will be sent to the Destination is achieved through a cooperation between the Data Packet and the software placed inside the Hop:
    - The Data Packet offers the Destination Address (and other information) and
    - The Hop evaluates the new direction of the Data Packet based on the Destination IP Address and the tables (including algorithms) present in the Hop.

The networks may rely on devices with:
1 NIC or equivalent,
2 NICs or equivalents,
more NICs or equivalents.

Fig. 1.1. Different devices connected to the network.
According to the number of the NICs (or equivalent) of the device, the device may to be connected to multiple networks and consequently ensure the transfer of the Data packets among different networks.



The devices with two or more NICs (or equivalents) (Routers, Gateways, etc) may direct the information (Data Packets) to different networks or transfer the information (Data Packets) to both directions, from one network (for instance, from one LAN) outside the respective network (for instance, to the Internet).

Devices with more than one NIC – Network Interface Card (or equivalent) achieve the transfer of the Data Packets from one network to another. They may be Routers, Gateways, Bridges or other inter-network connection devices.

- The entire processing is in compliance with the TCP/IP protocols and is achieved by the software programs present in the each device connected to the network, including your machine.
  The software of the OS-Operation System of your machine (PC or Laptop) runs programmes in compliance with TCP/IP protocols.
  The machines that function inside the TCP/IP network must be personalized (with your name, etc.) and configured [with the IP Address, Implicit Gateway Address (from the LAN side), the IP Addresses of the DNS servers, etc.] in order to comply with the network framework. The new systems allow an automatic configuration.

- The Internet is based on a virtual mode of addressing constructed through IP Addresses. The IP, a virtual addressing mode, has been decisive for the success of the Internet. It is a virtual mode because it is not set in the structure of the machine and can be changed and accessed all around the world.

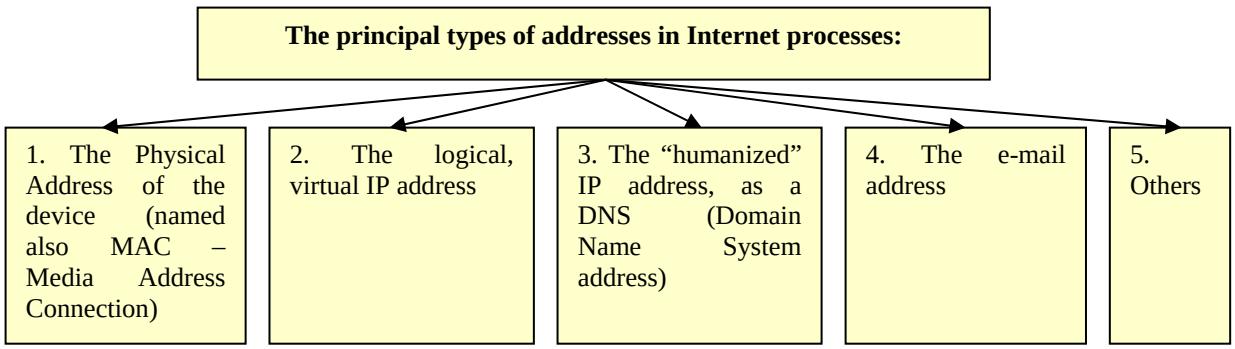
2. THE INTERNET AS A GAME OF ADDRESSES.

Sending the Data Packet from one place (source) to another (destination), from one computer (or other device) to another is first a problem of addressing.

Much of the Internet theory and practice focus on the processing and management of addresses.

The understanding of the IPv4 (IP Addressing version 4 is essential for knowing and monitoring the networks. This is true when your network:
- is connected to the Internet, or
- is not connected to the Internet.

The main addresses used on the Internet are the following:



The concept of addressing in Internet takes into consideration the fact that all the devices which can be connected to a network have been provided with an address by the factory producing the respective equipment:

the Physical Address of the device, or the MAC (Media Address Connection).

The Physical Addresses is the address placed (burned) on the NICs (Network Interface Cards) or on equivalent interfaces.

The Physical Addresses are the addresses that are visible from the local network (frequently Ethernet) toward the device.

In order to help the Internet Data Packets to find the right End to End path to the network of destination, it is not the Physical Addresses that are used.
The IP Addresses are used in order to find the path Hop by Hop to the destination network.

The IP addresses are the King of the Internet, one of the essential principles of the functioning and success of the Internet.
All the devices connected to the Internet have at least one IP address.

For instance, the construction and presentation of the IP Addresses as:

193.22.4.15

Offers a low and unfriendly degree of comfort.

Therefore, along the years, a supplementary form of addressing, DNS (Domain Name System) addressing was introduced.
DNS Addresses are alphanumeric addresses, such as:

www.altavista.com

with an improved degree of friendly, " humanized " presentation and contributions to the On-Line Visibility.

3. PHYSICAL ADDRESSES.

Each workstation, host, router or any device which may be connected to a network (which can or cannot be connected within the Internet) is provided with its own Physical Address also called MAC- Media Access Control.

These addresses are usually found (burned) in the PROM- Programmable Read Only Memory of the respective interfacing to the net device called NIC.
In order to avoid troubles, the Physical Address of each device within a net must be unique.

The Physical Address of a device (burned on the NIC – Network Interface Card) is used to communicate with the device connected to a network which is plugged or not to Internet.

In either of the cases, when the device works within a separate (isolated) LAN (Local Area Network) or when the devices work inside one LAN connected to the Internet, the Data Packets are taken over by these devices based on the uses of the Physical Address.

When the device works inside a network connected to Internet and when the device inside the LAN-Local Area Network is accessed, the Data Packets from the Internet use the Physical Address (through mapping by one device of the respective LAN, for instance by the Gateway, and of the IP address in the Physical Address).

For the Data Packet to find the final LAN (which has the IP Address of destination) the IP addressing is used.
To access the device inside the LAN, the Physical Address of the respective device is used.

The access of the Data Packet inside each device (partner of the network) is achieved by using the Physical Address.

The Physical Address is not present in the Header of the Data Packet, emitted at the Source through the Internet to one Destination.
Only the logical, virtual IP Address of the Destination (and also the IP Address of the Source) is present, in order to monitor the correct arrival of the Data Packets to the Destination and to re-send the Data Packets in case of errors or Data Packet losses.

The ARP and RARP protocol, procedures and tests permit the automatic finding and mapping (through broadcasting methods) of the Physical Address when the IP Address is known and vice-versa.

The path of the Data Packet between the Source and the Destination can be found based on the IP Address.

<u>The MAC structure:</u>
Inside the net, all devices must have a Physical Address in order to achieve communication.

All the NICs (the Network Interface Cards) of the connected devices (machines) inside a network (for instance, LAN), have their own MAC. At the time of manufacturing, the MAC is burned or selected with hardware jumpers inside the NIC.

The MAC structure is formed of 6 bytes (48 bits), where:

- the first 3 bytes contain a hexadecimal ID (identifier) in connection with the manufacture code and based on the IEEE organization instructions. This manufacture code is assigned by the IEEE.
- the second group of 3 bytes in hexadecimal contain a unique number assigned to each individual device by the manufacturer.

The length of 48 bits corresponds to the length used for addressing by the Ethernet type standards and networks.

The hexadecimal representation.

Besides 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, the hexadecimal representation also includes the following values:

The Hexadecimal value	A	B	C	D	E	F
The decimal value	10	11	12	13	14	15

The table of conversion from the hexadecimal code in the binary numbers goes as follows:

1	**0001**
2	**0010**
3	**0011**
4	**0100**
5	**0101**
6	**0110**
7	**0111**
8	**1000**
9	**1001**
A= decimal 10	**1010**
B= decimal 11	**1011**
C= decimal 12	**1100**
D= decimal 13	**1101**
E= decimal 14	**1110**
F= decimal 15	**1111**

Example:
The hexadecimal value C2 represents the decimal value for the following binary presentation:

Values of each rank	128	64	32	16	8	4	2	1
Resulted binary value for the Hexadecimal value C2	**1**	**1**	**0**	**0**	**0**	**0**	**1**	**0**

The resulted binary value of the hexadecimal value C2 results from concatenating value 2 placed to the right part, which is represented by binary as:

0	0	1	0

with the left part of the conversion and with the conversion of the hexadecimal value C, respectively, with the following binary representation:

1	1	0	0

Taking into consideration the above binary positions for value C2 indicated in the Table above, the following decimal value of the hexadecimal value C2 results:

1x128 + 1x64 + 1x2= 194. Therefore, C2 in hexadecimal represents 194 in decimal.

The same value results through the direct conversion from hexadecimal to the decimal:

Cx16 + 2x1 = 12x16 + 2= 194

As it is can be noticed, in only 2 characters (2 hexadecimal positions), the hexadecimal number represents a decimal number which requires 3 decimal positions. The hexadecimal presentation is a more compact representation of the values.

Example of MAC / Physical Address:

For instance, the MAC may be: **00 0A 52 F0 C2 01** where
IEEE has indicated to the manufacturer the ID: 00 0A 52
and the manufacturer has additionally assigned the number for the respective NIC: F0 C2 01.

This MAC address complies with the Ethernet standard for address representation.
The Ethernet standard for address representation uses 48 binary positions.

If the above hexadecimal address

00 0A 52 F0 C2 01

is represented as binary, the following Ethernet address will result (the high level ranks are placed to the left of the representation) :

0	0	0	0	0	0	0	0	0	0	0	0	1	0	1	0	0	1	0	1	0	0	1	0	1	1	1	1	0	0	0	0

1	1	0	0	0	0	1	0	0	0	0	0	0	0	0	1

How to quickly detect the MAC / Physical Address of your machine?

You may quickly know the Physical Address of your computer (only if you are connected to the Internet) by using the MS-DOS diagnosis tool and command:

IPConfig (Enter), or **IPConfig /All** (Enter),

That have been practiced in the previous practical lessons. The computer must be connected to the Internet.

How can the other network devices identify the MAC / Physical Address of your computer when the IP Address of your computer is known?

By using (with your computer connected to the network) the above-mentioned ARP protocol (and practical automatic procedure) of the TCP/IP succession of protocols.
The ARP protocol and the corresponding procedure supported by the software of your computer sends to all the LAN partners a questioning packet which require the MAC Address corresponding to the IP address that is the object of inquiry.

In the broadcasting address this transmission includes all the MAC Addresses (the address is 111…., with 48 bits of 1, which corresponds to all possible addresses of the LAN-Local Area Network).

The NICs of all network partners find their address in the combination of 111…, which defines all network MAC addresses.
Consequently, all the partners take over the questioning Data Packet and the software (of the targeted computer and of the computer whose IP corresponds to the respective MAC) will reply with a Data Packet to the computer which sent the Questioning Data Packet.
This response Data Packet includes the MAC of the respondent computer.

How can the other devices connected to the same network identify the IP Address of your computer when they know its MAC Address?

By using (with your computer connected to the network) the above-mentioned RARP (Reverse ARP) protocol (and practical automatic procedure) of the TCP/IP succession of protocols.

The functioning mode is similar to that of the ARP:

- The computer that needs to know the IP Address of the other computer in the network sends a questioning Data Packet to all computers.
- All computers in the network read the Data Packet (because the data packet is sent to all the Physical Addresses / MAC addresses) and
- the computer of the LAN which has a correspondent between the MAC of the questioning Data Packet and its own MAC address responds with a Packet, indicating its own IP address.

Because your computer is supposed to know the MAC of the respective computer in order to identify the IP, the RARP may be also performed straight to the targeted computer (in which the known MAC corresponds to the desired IP Address) no transmission being necessary.

The MAC can send Data Packets to the specific MAC Address in order to find the IP Address.

In networking, IP Addresses are the kings because they direct the Data Packets from the Source to the Destination.

In LANs, the MAC / Physical Addresses are the kings because only the MAC addresses may be taken over by the devices connected to the LAN.

4. THE IP (INTERNET PROTOCOL) ADDRESSES. CLASSES OF IP ADDRESSES. USING THE IP ADDRESSES.

4.1. IP ADDRESSES.

The IP addressing procedure is important to operating, creating, using and troubleshooting of the Internet systems and under-systems and to Internet applications. The IP Addressing is described in the RFC 793 ([Supp. 5.], [Supp. 4.] www.ietf.org RFCs).

The IP addressing allows the network segmentation, separation and isolation.

Network segmentation, separation and isolation are essential procedures focusing on troubleshooting, accomplishing the network speed, reliability and systematization.

The IP Address is a logical address related to, and unique for, addresses across the world (if that specific network is open to the Internet and if procedures for the substitution of the addresses are not used).

Example of a Class C IP Address: **193.22.1.2**, where (in Class C):
- the left part **193.22.1** is the NETID, the network address (the network ID -identifier) and
- **2** is the HOSTID address (the host ID-Identifier) of the computer in this network.

The IPv4 and IPv6.
The present chapter tackles the uses of the IPv4 version of the standards related to IP Addressing.
Despite the development and application of the new IPv6 standard (also related to IP addressing), the IPv4 technology and applications still remain in wide use.
Also, the IPv4 functions in parallel with the IPv6 (the IPv4 functions in some subnets, the IPv6 in other subnets, in a parallel and interoperable way).

The addressing architecture based on the IPv4 allows in theory over 4.000.000.000 of IP Addresses.

The IP Addresses were not economically used. For instance, sub-nets take up more addresses than they actually use.
The pool of IPv4 IP addresses is almost exhausted.

Formats of IP Addresses.

IP Addresses are presented and used in two formats: binary and dotted decimal.

a) The IP Address in binary format.

If the decimal numerical system uses numbers from 0 to 9, the binary numerical system has only 2 valid numbers: 0 and 1.

The bites positions inside the binary number are generated based on the power of two.

For each rank of the bits with value one in the binary octet from right to left, there are generated correspondent decimal values.

Therefore, each power of two from power value between 0 and 7 generates a correspondent (to the respective rank of the binary position of the bite) decimal value.

For instance, inside the binary number: 11111111,

the power of the position of each bit (when the respective bit exists - i.e. its value is 1- on the respective rank position) is illustrated for a word which is one octet/byte long, as in the following table:

Binary number	The decimal value corresponding to the binary position of bit 1 inside the octet, and the decimal value of the binary number from the left column	The rank of the position in which the value is 1
00000000	0	**0**
00000001	1	**1**
0000001**0**	2	**2**
000001**00**	4	**3**
00001**000**	8	**4**
0001**0000**	16	**5**
001**00000**	32	**6**
01**000000**	64	**7**
10000000	128	**8**

Total	**255**	

Also, taking into consideration the table above, the binary number 11011111 has the following decimal value:

1x128 + 1x64 + 1x0 + 1x32 + 1x16 + 1x8 + 1x4 + 1x2 + 1x1 = 223.

The IP Address may be presented as a binary number of 32 bits and of 32 binary positions, respectively.
The IP Address is divided into four segments, each of eight bites and four bytes, respectively.
Each segment covers 1 byte.

Each segment (byte) of the binary format may have values ranging from
00000000 to 11111111.

Example: **01111111.10011000.0000010.0000001**
There is one IP address in binary format. In describing addresses, the bytes are concatenated and form a continuous string of bits. The most significant bits are placed to the left part of the string.

b) The IP Address in the dotted-decimal format

In order to improve the ways of monitoring the IP Addresses, these IP Addresses are converted into a dotted decimal format. The IP Address in dotted-decimal format (decimal with dot) consists in dividing the address in four groups (the four bytes) and generating a decimal value from the each byte. The separation between the decimal groups is done with dots.

Therefore, this format is presented as four-decimal values separated by one dot.

Each octet may represent a decimal number between **0** and a maximum value of **255**.

Example: the numeric representation 193.23.40.5 represents an IP Address illustrated as a decimal form.

The maximum value of each decimal group is **255** because this value is a maximum decimal value corresponding to the binary octet/ byte:
11111111 (with the bigger rank to the left of the number).

This byte, the full "1" byte, results in the following when converted to the decimal value:

1x1 + 1x2 + 1x4 + 1x8 + 1x16 + 1x32 + 1x64 + 1x128 = 255

The lower IP Address in the dotted decimal is **0.0.0.0** and the larger IP address is **255.255.255.255** .

In networking, it is essential that the relation between binary and decimal IPO Addresses numbers should be used

4.2. THE PROCESSING OF IP ADDRESSES AS BINARY EXPRESSIONS AND AS DOTTED DECIMAL EXPRESSIONS

1.) The conversion of the binary IP Addresses in the dotted decimal format.

For the conversion:
- the IP address in binary form on 32 bits is divided in four octets of eight bits each.
- Each octet is separately converted into decimal value and based on the conversion table:

Position 8	Position 7	Position 6	Position 5	Position 4	Position 3	Position 2	Position 1
128	64	32	16	8	4	2	1

- The rank of the decimal octets are in the table below:

Rank 4	Rank 3	Rank 3	Rank 1
The octet generated by the 4th binary segment to the left	The octet generated by the 3rd binary segment to the left	The octet generated by the 2nd binary segment to the left	The octet generated by the 1st segment to the left

In order to convert the binary to dotted decimal, the following steps must be followed:

- Step 1: the accomplished four digital segments are placed (annexed) following the order of the above ranks from left to right..

Example:
The binary IP 01001111000110001100011000101011 Address is converted to dotted-decimal as follows:

- the binary value is separated in four octets:

01001111 00011000 11000110 00101011

- Step 2: each octet is converted to the decimal value as follows:

  - Step 2.1:

The first octet from the left side 01001111 will generate taking into consideration the power of two from the table above

0x128 + 1x64 + 0x32 + 1x16 +1x8 + 1x4 + 1x2 + 1x1 = 164+8+4+2+1= 79

The procedure is similar for the second, third and forth octet (starting numbering from the left):

  - Step 2.2:
    16+8 = 24

  - Step 2.3:
    128+64+4+2=198

  - Step 2.4:
    32+8+2+1=43

- Step 3: the resulted decimal values are arranged in dotted form taking into consideration the order of the binary octets which have each generated the decimal value per octet; the resulted dotted digital value is:
  79.24.198.43 .

Therefore, the dotted decimal value of the binary number **01001111000110001100011000101011** is **79.24.198.43** .

This is the way the dotted digital value of the IP Address is obtained when the binary value of the Address is known.

2) The conversion of the dotted decimal IP Addresses in binary format.
The conversion procedure of the dotted decimal values to binary values is the reverse of the conversion method from binary to dotted decimal values. The conversion includes the following steps:

- Step 1: Each decimal segment of the dotted decimal value is converted to binary value.

- Step 2: The resulted binary segments and octets, respectively, are concatenated according to their ranks.

How is achieved the conversion of the decimal values (between 0 and 255), included in the dotted decimal values, into binary values?

First, it is emphasized that only the conversion per octets and per maximum decimal value 255 is achieved.

Step 1.1.: The conversion is achieved by comparing the decimal values with the binary values of the power of two indicated in the table above, starting with the biggest value, 128, respectively:

THE TABLE OF THE POWERS OF TWO FOR ONE OCTET

2 to the power 7	2 to the power 6	2 to the power 5	2 to the power 4	2 to the power 3	2 to the power 2	2 to the power 1	2 to the power 0
128	64	32	16	8	4	2	1

Step 1.2.:

Step 1.2. A. If the value of the decimal number proposed for conversion is bigger than or equal to a value in the table above (looking from left to right),

- then:
  - this number from the above table is subtracted from the number proposed for conversion,
  - at the position corresponding to the rank of the reduction number on the binary converted number place bit 1
  - the rest of the above subtractions is stored in order to continue the conversion process.

Example:

The decimal value 217 is converted to binary as follows:

a.) Is 217 > or equal to 128? (Where " > " means "bigger").
Yes.
In this case, consider that the decimal value to be converted includes the binary value 128.
Consequently, value 1 is introduced in the following table on a position corresponding to 128.

128	64	32	16	8	4	2	1
1							

If the initial decimal number equals 128, bit 1 is introduced corresponding to position 128.

128	64	32	16	8	4	2	1
1							

Because in this example the number value is over 128, 128 is subtracted from the number proposed for conversion, 217: 217-128 = 89
1 is inserted in the 128 position of the converted number.
The remaining value 89 is kept to continue the conversion operations.

Step 1.2.B. If the value of the decimal number to be converted is lower than the value selected initially from the TABLE OF THE POWERS OF TWO FOR ONE OCTET

 then:
on the binary rank of the converted number corresponding to the rank of the number selected from the above TABLE OF THE POWERS OF TWO FOR ONE OCTET

- insert value 0.
- selects the new, lower value of the power of two from the TABLE OF THE POWERS OF TWO FOR ONE OCTET
- continue the iteration with a new iteration which uses the newly selected value and rank from the TABLE OF THE POWERS OF TWO FOR ONE OCTET

Continuing the example
b.) the iteration continues with the new value under 128 and the rest value, namely 89.
It is compared with the values from the TABLE OF THE POWERS OF TWO FOR ONE OCTET and it is compared with value 64,

New Step 1.2.: Is the remaining value: 89 > or equal to the value 64?
Yes, it is.
In this case, consider that the decimal value to be converted includes the binary value 64.
Consequently insert 1 under the position of value 64.

128	64	32	16	8	4	2	1
1	1						

Because the value of the number to be converted is 64, perform the subtraction 89 – 64= 25

c.) Is the remaining value 25 bigger than 32?
No, it isn't.
Insert value 0 under the position corresponding to 32.

128	64	32	16	8	4	2	1
1	1	0					

d.) Is the remaining value 25 bigger than 16 ?
Yes, it is.
Insert 1 in the position corresponding to value 16 and diminish the value 25 by 16. Do the subtraction 25-16 = 9

128	64	32	16	8	4	2	1
1	1	0	1				

e.) Is the remaining value bigger than 8?
Yes, it is.

Insert 1 in the position corresponding to 8 and diminish the value 9 by 8: 9-8 = 1

128	64	32	16	8	4	2	1
1	1	0	1	1			

f.) Is the remaining value bigger than 4?
No, it isn't.
Insert 0 in the rank position corresponding to value 4 (rank 3, respectively).

g.) Is the remaining value bigger than or equal to value 2?
No, it isn't.
Insert 0 in the position corresponding to 2.

128	64	32	16	8	4	2	1
1	1	0	1	1	0	0	

h.) Is the remaining value bigger than or equal to value 1?
Yes, it is.
Insert 1 in the position corresponding to 1.

128	64	32	16	8	4	2	1
1	1	0	1	1	0	0	1

Therefore, the decimal value **217** corresponds to the binary value: **11011001**

In the same way, the binary octet is obtained for each of the four decimal values of the dotted decimal word.
After the individual conversion of each octet, the binary octets are concatenated into the correspondent binary word/string and with the most significant bits to the left side.

4.3. CLASSES OF IP ADDRESSES. THE NETID AND THE HOSTID.

The **NETID** (NET Identifier).
The NETID is a segment of a pre-established numbers of bits, to the left of the IP Address.
The NETID identifies the sub-network (the lowest level of the network, the final net) which the IP Address refers to.

The **HOSTID** (HOST Identifier).
The HOSTID is a segment of a pre-established number of bits, to the right of the IP Address.
The HOSTID identifies the host (the computer) within the network indicated by the NETID.

The NETID is similar to the name of a street while the HOSTID is similar to the number of the house on that street. The IP Address indicates: the "street"/ the net and the "house on the street" / the host.

The main classes of IP addresses.

The main classes of IP addresses are:
-Class A
-Class B
-Class C

1.) Class A of IP Addresses and networks.

With class A, the NETID occupies the first byte from the left side of the IP Address.
With class A, the HOSTID occupies the rest of the 3 bytes to the right side of the IP Address.
The most significant ranks are always to the left side (for the NETID and separately placed for the HOSTID).

NETID BYTE: IV	**HOSTID BYTE: III**	**HOSTID BYTE: II**	**HOSTID BYTE: I**

The class A networks are few, only 0 to 255 networks or to a maximum of 256 (actually to a maximum of 127 because the first LEFT bit of the NETID of Class A always has value 0).

The networks of class A may have many bifurcations to the under-networks or hosts, indicated by one word made of 3 bytes and more than 16 000 000 of hosting possibilities, respectively.

The networks of class A may have many hosts or a maximum number of hosts offered by the number:

1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1

one binary value generated by 24 binary positions, respectively.

Two positions of addressing possibilities of class A are reserved:
The HOSTID made of all 1s reserved for broadcasting;
The HOSTID made of all 0s reserved for the net basic structure (Gateway IP Address of the respective LAN) as in the example in figure 4.1.

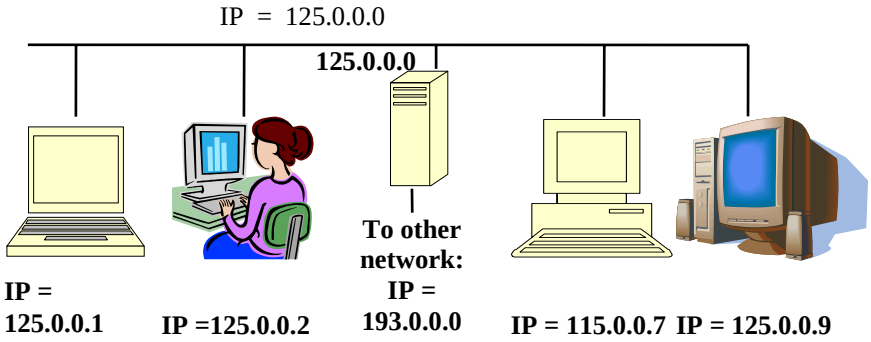


Fig. 4.1. The IP Addresses of a network where the value of the HOSTID (in dotted decimal) in the network basic structure is 125.0.0.0.
This is only one example given to understand the basic structure addressing with the HOSTID = 0.0.0.
Normally, class A does not include Hosts but bifurcations / Routers / Gateways etc. to other networks.

2.) Class B of IP Addresses and networks.

With the IP addresses of class B the first 2 bytes from the left side are occupied by the NETID, while the rest 2 bytes are taken by the HOSTID.

NETID BYTE: IV	NETID BYTE: III	HOSTID BYTE: II	HOSTID BYTE: I

Actually, the NETID of Class B may define (taking into consideration the number of addresses lost by the class identification) about 16382 class B networks. Each network can have 65534 unique host addresses.

Two of the addressing possibilities of class A are preserved:

a.) The address with the HOSTID in which the value of all bits is 1; the form of the HOSTID is as follows:

1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1

This addressing format is used for the broadcasting emission within the respective network.
Because the above address includes all combinations of addresses, this broadcasting emission is performed to all of the addresses.

b.) The address with the HOSTID in which the value of all bits is 0; the form of the HOSTID is as follows:

0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

This is a format which is used for the identification of the respective network (of the basic structure of the respective network, as in the example in fig. 4.1).

3.) Class C of IP Addresses and networks.

With the IP addresses of class C the first 3 bytes from the left side and from the high ranks which are placed to the left side, respectively, are occupied by the NETID, while the rest of only 1 byte is taken by the HOSTID.

NETID BYTE: IV	NETID BYTE: III	NETID BYTE: II	HOSTID BYTE: II

Just as with the previous two classes A and B, class C has the addresses reserved:

1.)- The address with all the bits of the HOSTID of value 1 and the form of the HOSTID as: 11111111,
a format which is reserved for the broadcasting emission within the respective network,

2.)- The address with all the bits of the HOSTID of value 0 , and the form of the HOSTID as: 00000000,
a format which is reserved for the identification of the respective network (or the basic structure of the respective network, as in the example from fig. 1.5.1.).

Class C networks are numerous, over 16.000.000, with a maximum of 256 (0 to 255, respectively, and actually only 254 because the classes
- with the HOSTID=0
- and with the HOSTID= 11111111 in binary, respectively 255 in decimal,

are reserved: the first for the basic structure of the network and the last for the broadcasting to all network addresses, partners machines on each network of class C). Class C is the class most often used of the IP Addresses.

Normally, your computer is connected within a network of type C, with a maximum of 244 values of HOSTID, and 254 computers connected to this network, respectively.

Other types of IP Addresses and of networks:
The D and E network type are for a special use.

For instance, D is used for the multicast and for the IGMP protocol (Internet Management Protocol, which is a protocol hosted in Layer 2, called Internet, of the pile of the TCP /IP protocols); thus communication with the D type addresses is achieved.
The E addresses are used for the experimental activities.

By means of convention, the following rules apply for the IPv4:

Special bits which indicate the Class	**Class**	**The most significant octet has the decimal value between**	**Excluded addresses [2], with the view of creating the private networks.**
If the binary address on 32 bits begins with value **0** (at the most significant bit of the 32-bit expression, namely the leftmost bit)	**A**	0 to 127	10.0.0.0 to 10.2555.255.255 and 127.0.0.0 to 127.255.255.255
If the binary address on 32 bits begins with value **10** (at the most significant bit of the word of the 32 bits, respectively, the 2 bits situated furthest to the left)	**B**	128 to 191	172.16.0.0 to 172.31.255.255
If the binary address on 32 bits begins with value **110** (at the most significant bit of the word of the 32 bits, respectively, the 3 bits situated furthest to the left)	**C**	192 to 223	192.168.0.0 to 192.168.255.255
If the binary address on 32 bits begins with value **1110** (at the most significant bit of the word of the 32 bits, respectively, the 4 bits situated furthest to the left)	**D**	224 to 239	
If the binary address on 32 bits begins with value **11110** (at the most significant bit of the word of the 32 bits, respectively, the 5 bits situated furthest to the left)	**E**	240 to 247	

The design and the creation of the IP Addresses inside the classes of IP Addresses are illustrated in the table below:

The class	**The first compulsory bits**	**Highest Octet = Octet at the right part .** Octet 4 or the leftmost side of octet 4 (placed to the left side of the word of IP Address). The first bits (from the left side) of this octet define the IP Class	**Octet 3**	**Octet 2**	**Lowest Octet = Octet to the right side of the concatenated octets Octet 1**	**Remarks**
CLASS A	**0**	0 NETID	HOSTID	HOSTID	HOSTID	
CLASS B	**10**	10 NETID	NETID	HOSTID	HOSTID	
CLASS C	**110**	110 NETID	NETID	NETID	HOSTID	
CLASS D	**1110**	1110				Used for the multicast .
CLASS E	**11110**	11110				For research

The above table is synthesized in the following table:

CLASS	**First compulsory bits (to the left side of the address word)**	**Bits used with the indication of the class of address**	**NETID** **bits**	**HOSTID** **bits**	**Total number of bits of the word of the IP address**
A	0	1	7	24	32
B	10	2	14	16	32
C	110	3	21	8	32

Losses of addresses and non-economy in the IPv4 space of addresses.

These IPv4 rules, imposed at the point of launching the Internet networks, including the Internet IP addressing, have resulted in losing an amount of possible addresses.
The division of the Internet addresses in classes has led to the non-economic use of a big number of IP addresses, especially by the incomplete use of the interval of addresses allocated to different entities / clients.

These entities which have received part of the addressing spectrum do not use the complete allotted interval / poll of the IP Addresses.

At the same time, through the pre-established allocation of the IP Addresses,
- achieved according to the possibilities of dividing the IPv4 addresses,
- following the mode of division into Classes,
- following the allocation of a big spectrum of addresses to specified entities (where the received addresses are not used entirely)
- where the addresses from the allocated addresses to one entity may not be used as their own IP Addresses by other entities,

some part of the spectrum (a number of addresses) is lost.

Example:
One company needs 400 addresses of Class C. Two groups are allocated, each of 254 addresses, a single group of 256 addresses is not sufficient).
In this case the following are lost:

(2x256) – 400 = 112 addresses , respectively, about 20 % from the addressing spectrum is lost.

In conclusion, by offering addressing space/ spectrum to the entities without verifying the real needs of the IP addressing spectrum of the respective entity has led to a substantial lost because:
- the addresses were not used in their own network,
- those addresses could not be used by other entities.

Other reasons for IP Addresses losses.

Other reasons for losing addresses consist in the fact that some segments of the pallet of IP Addresses are prohibited, being used for the special applications.

By giving a Class B address to one entity there are thousands of addresses lost.
On the other hand, Class B of the IP addresses was not used for along time: "no one has been assigned a Class B address since 1992" (said Scott Brander, cited in [4]).

Solutions when IP Addresses are lost.

The above negative situations may be ameliorated, for instance, by the following procedures:

- through the extensions offered by the using of the masks of the under-networks,
- through the using of the procedure: Variable Length Subnet Masks - VLMS,
- through the using of the procedure: Classless Inter-Domain Routing - CIDR,

and, also through the use of the new rules for the IP Addresses and IP addressing offered by the IPv6.

In applying specific rules, IPv6 may coexist with IPv4. For instance, a network (connected to the Internet) is achieved with the addressing in compliance with IPv4 while other networks (connected to the Internet) are achieved in compliance with IPv4.

4.3. SPECIAL IP ADDRESSES.

1.). **The IP Address of the backbones of the network and the IP Addresses of the backbones of the possible sub-nets (under-networks)**.

The IP addresses of the networks, the under-networks (as the addresses of basic structure of the respective networks or under-networks) and of partners for each respective network (fig. 4.1.) are:

- essential elements of the Internet design,
- decisive elements for a reliable Internet functioning.

In many cases, the networks' (backbones) and the subnets' / under-networks' (sub-backbones) IP Addresses have names in which all the bits of the HOSTID value are 0.
The partners on the same network or on the same subnet (under-network) have the same NETID. In a net, the HOSTIDS have different values.

Figure 4.2. illustrates two classes C networks and one subnet (under-network) (compulsory also of class C, because the hierarchical network is of class C), where the addresses of the networks and of the under-networks backbone are, for example, as follows:

The IP Address of the backbone of the first C class network is: **192.150.22.0 .**
The IP Address of the backbone of class C subnet: **192.150.25.0**

The IP Address of the backbone of class C second network: **200.40.10.0**

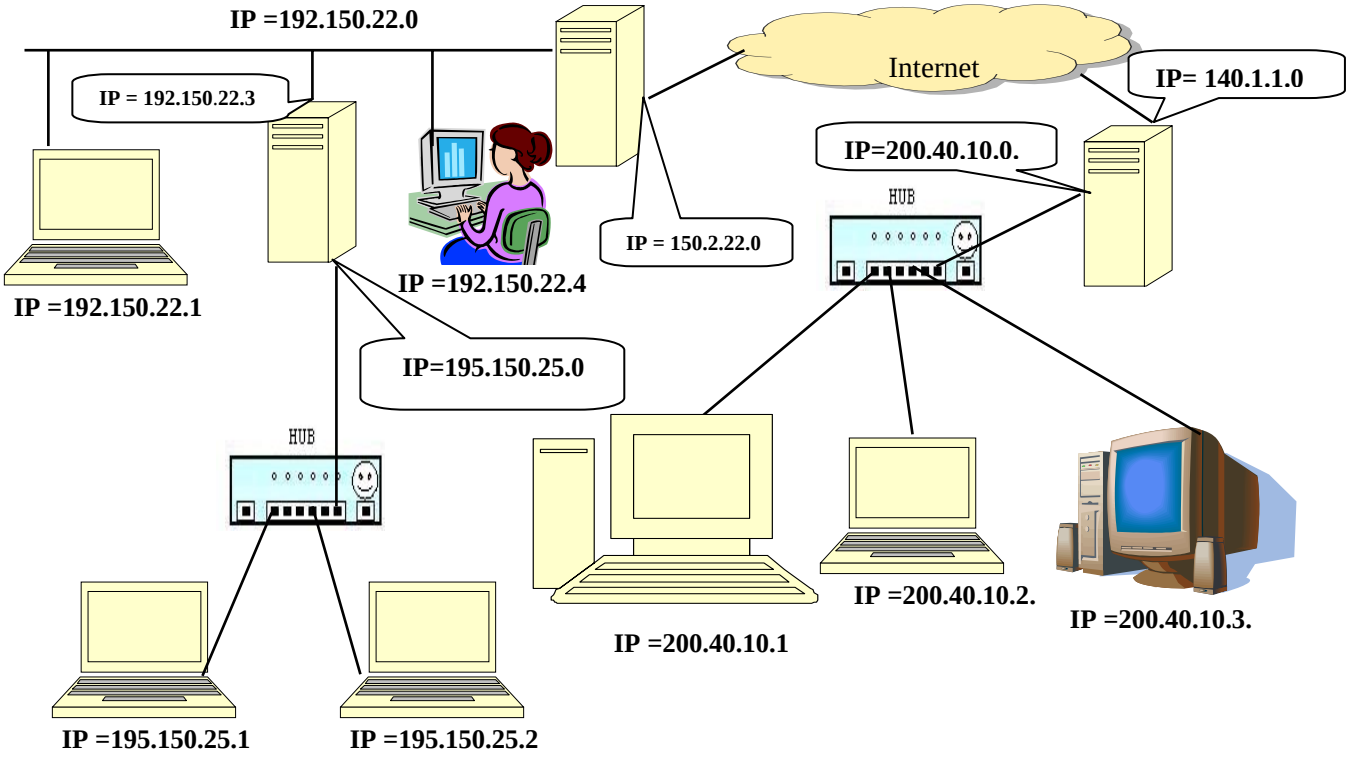


Fig. 4.2 Two nets interconnected through the Internet and a sub-net, and the example of the possible IP Addresses

In the picture above, fig. 4.2., it can be noticed that:

- the networks and subnets (under – networks) are in this case of class C (the IP addresses include value 110 on the first bits to the left of the NETID) and,
- being of class C, the nets and the subnets usually, but not compulsorily, have the HOSTID of the back-bone (of the node) of a binary value 00000000, that is of decimal value 0.

2). IP Addresses for broadcast.

The **broadcast** Packet (message) is a Data Packet which may be sent to the IP Addresses or inside the LAN to the IP addresses or to Physical addresses / MAC addresses.

The broadcast addresses may be IP Addresses which cover all of or part of addresses of the world IP Addresses..

Examples:
a.) On one sending (the sending of a Data Packet) in which all the bits of the HOSTID of the IP Address of Destination in one network of Class C has the following value:

11111111 , respectively, the addressed HOSTID is 255.255.

The combination of bits **11111111** covers all the addresses of the Hosts (computers) connected within the respective network.

Because the NETID (the Address of the Network in this case) remains the same, all the Hosts of the net with the respective NETID are broadcast.

Consequently, all the computers of this network can usually receive, take over and process the Data Packet.

In practice, the emission inside the LANs is based on the MAC addresses (is achieved toward the MAC addresses), the only type of addresses which may to be taken over by each NIC of each computer.

On one sending in which the NETID of the Data Packet has, for instance, for class C the following value

1	1	0	1	1	1	1	1

(the first bits **110** from the left side of the NETID indicate that it is the case of addresses and class C network).
Because the value of all the other bits of the NETID (excluding the firs 3) is "all 1", all word nets of class C are targeted.
If additionally the HOSTID has the form:

1	1	1	1	1	1	1	1

the result is that all the word's Hosts (computers) of all class C networks are broadcasted.

If, for instance, in the class C network from the previous figure with the **back-bone** address **192.150.25.0,**
It is necessary to send a **broadcast Packet** / message, then this message will be sent to the address:

192.150.25.255,

where 255 on the rightmost side signifies the address **11111111** which includes all the possible addresses of the partners connected to the backbone IP Address **192.150.25.xxx..**

The IP address: **255.255.255.255**

may be used for broadcasting to all the Internet addresses.

3.) **IP Addresses for the loop back**.

The IP addresses for the **loop back** are self addresses of the TCP / IP implementation of the respective system.

Some addresses start with 127; especially the IP Address **127.0.0.1** are **loop back addresses** and serve, firstly, for internal testing; for instance, with the software diagnosis tools **ping, tracert** and other of the TCP / IP implementation .
The good response (in MS-DOS) to the

C:\>**Ping 127.0.0.1** [Enter]

and to the:

C:\>**Tracert 127.0.0.1** [Enter]

offers the first indications (which are not complete) that the installation and configuration of the TCP/IP is correctly performed on that computer.

4.) **IP Addresses reserved (not used) by the Internet**.

By convention there are fields of addresses which are not used by the Internet.
These addresses cannot be registered as Internet addresses.

The fields of the above mentioned addresses, called **addresses in the private IP address blocks,** are the following (in dotted decimal):

10.xxxx.xxxx.xxxx

172.16.xxxx.xxxx

172.31.xxxx.xxxx

192.168.xxxx.xxxx

Key Points Summary. Conclusions and recommendations.

The IP Addresses, virtual addresses working at Internet level which ensure the End to End transfer of the Data Packets and the Physical Address /MAC- Media Address Control which work at LAN level and offer the possibility to take over the Data Packets inside LANs are essential elements of the Internet and of the TCP/IP protocols.
The practical tools for the identification of the addresses, such as the ARP and RARP protocols of the TCP/IP suite of protocols, constitute one of the procedures and diagnosis tools extremely important.
The Internet is in fact one Game of Addresses and of continuous exchange and mapping between IP Addresses and MAC Addresses.

Study Guide

ESSENTIAL QUESTIONS TO EVALUATE THE ACQUIRED KNOWLEDGE

1. Which addresses are used for guiding the Data Packet from the Hop to Hop: MAC Addresses or IP Addresses ? Why?
2. Which addresses are used for taking over the Data Packet from the NIC entry: MAC Addresses or IP Addresses? Why?
3. Who offers for use the MAC Addresses and who offers the IP Addresses?
4. How is the MAC address formed?
5. Which is the decimal value of the following hexadecimal values: C4, AA, FA?
6. How is the IP Address obtained?
7. Who does the transfer of the Data packets from one network with a NETID to a network with another NETID?
8. Which are the normal special addresses?
9. Which are the addresses which the broadcast can be directed to?
10. For a network from Class C of IP Addresses, which is the value of HOSTID, in order to ensure the broadcasting to all the partners in that specific network?

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.] Craig Hunt: *TCP/IP Network Administration*, O'REILLY, Sebastopol, CA, 2002, 0-596-00297-1.
[9.] Joe Habraken: *Absolute beginer's Guide to Networking*, Que Publishing, Indiana, USA, 2004, 0-7897-2911-3

IMPORTANT SUPPLEMENTARY BIBLIOGRAPHY. REFERENCES. (www

[Supp. 1.] http://www.prenhall.com/tanenbaum, Prentice Hall, Andrew S. Tanenbaum
[Supp. 2.] www.cisco.com/univercd/cc/td/doc/cisintwk/idg4
[Supp. 3.] www.cramsession.com
[Supp. 4.] www.ietf.org RFCs.
[Supp. 5.] www.rfc-editor.org RFCs.

SUPPLEMENTARY INDICATIONS ABOUT THE CONTENTS OF THE LESSON

It is advisable to also check: www.cisco.com; www.cramsession.com; www.ietf.org RFCs;www.rfc-editor.org RFCs.

ANSWERS TO QUESTIONS

1. The IP addresses. The IP addresses are used because the Routers / Hops evaluate the direction of the path based on the tables with IP Addresses.
2. The MAC Addresses. The MAC Addresses are used because only the MAC Addresses may be identified by the NIC- Network Interface Card.
3. The MAC Addresses are implemented in the NIC for good (or equivalent of the NIC), by the manufacturer of the NIC or equivalent. The IP Addresses are virtual addresses which are delivered by the ISP – the Internet Services Provider or by the automatic distribution of the IP Addresses (the DHCP protocol).
4. The MAC Address is similar or even identical with the Ethernet address used in LANs, an address of 48 bits. The MAC address is constructed from 6 hexadecimal numbers, each having 2 hexadecimal ranks / positions.
5. 196, 170, 250.
6. The IP Address may be expressed in the dotted decimal form (from 4 decimal independent groups, each group up to a maximum value of 255) or in the binary form in strings of 32 bits.
7. The devices with more than 1 NIC and with an adequate software and local configuration. These devices may be bridges, Gateways, routers and other.
8. The normal special IP addresses are: a.) the IP Address or Addresses for broadcasting; b.) the IP Addresses for computer diagnosis such as : 127.0.0.1..; c.) the reserved IP Addresses: 10.xxxx.xxxx.xxxx; 172.16.xxxx.xxxx; 172.31.xxxx.xxxx; 192.168.xxxx.xxxx .
9. To the IP Addresses and within the LANs, to the IP Addresses and to the Physical addresses.
10. HOSTID: 255.255.

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