LESSON E5_EN. INTERNET ADRESSES AND INTERNET ADDRESSING. SUBNETTING.

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:

- Why network segmentation must be achieved,
- How to achieve network segmentation,
- How to use the subnet mask,
- How to multiply the Addresses,
- How the NAT and PROXY procedures function.

<u>CONTENT OF THE LESSON</u>

<u>LEARNING OBJECTIVES:</u>

After learning this lesson you will accomplish the abilities to:

- understand and apply network segmentation,
- understand the advantages of network segmentation and the possible weaknesses of the segmentation.
- learn how to use subnet masks.
- understand the NAT and Proxy procedures and to multiply addresses.

1. SUBNETWORKS AND THE GENERATION OF SUBNETS.

<u>1.) Sub-networks (subnets).</u>

The Internet is a network of networks… of networks… .
At lower levels, the Internet is supported by the under-networks of lower levels.

Practically, the Internet basically relies on thousands of under-networks. The under-networks are the basic bricks of the Internet.
A network connected to the Internet is always, except the large and very fast backbones, an under-network.
The sub-net may have more under-networks, some of which have other under-networks, and so on, through other steps, to the networks of the lowest rank.
The RFC 950 offers the possibility to create sub-nets through the division of the network IP Address in multiple IP addresses of smaller networks.
The procedure of dividing the IP Address into IP Addresses of smaller sub-nets is equivalent to the allocation of binary positions from the HOSTID to the NETID.

In creating the network segment it is advisable to work with IP Addresses under binary representation.

The IP procedure of addressing through the mask of the sub-net constitutes the basic stage in achieving and accomplishing the subnets (under-networks).

The distribution mode of the IP addresses between the sub-nets is very important for communication, namely for the mode in which the Data Packets find their path.
As it is illustrated in fig. 1.1., in order to efficiently deliver the Data Packets, it is more convenient that the Data Packets should be sent (inside a large and complex network of networks) directly to part of the space segment of the IP addresses.

In this way, the following are achieved:

- Sending the Data Packets toward that subnet which includes the IP Addresses of interest (the IP Destination Address).
- The division of the network in convenient subnets with positive effects on troubleshooting and security.

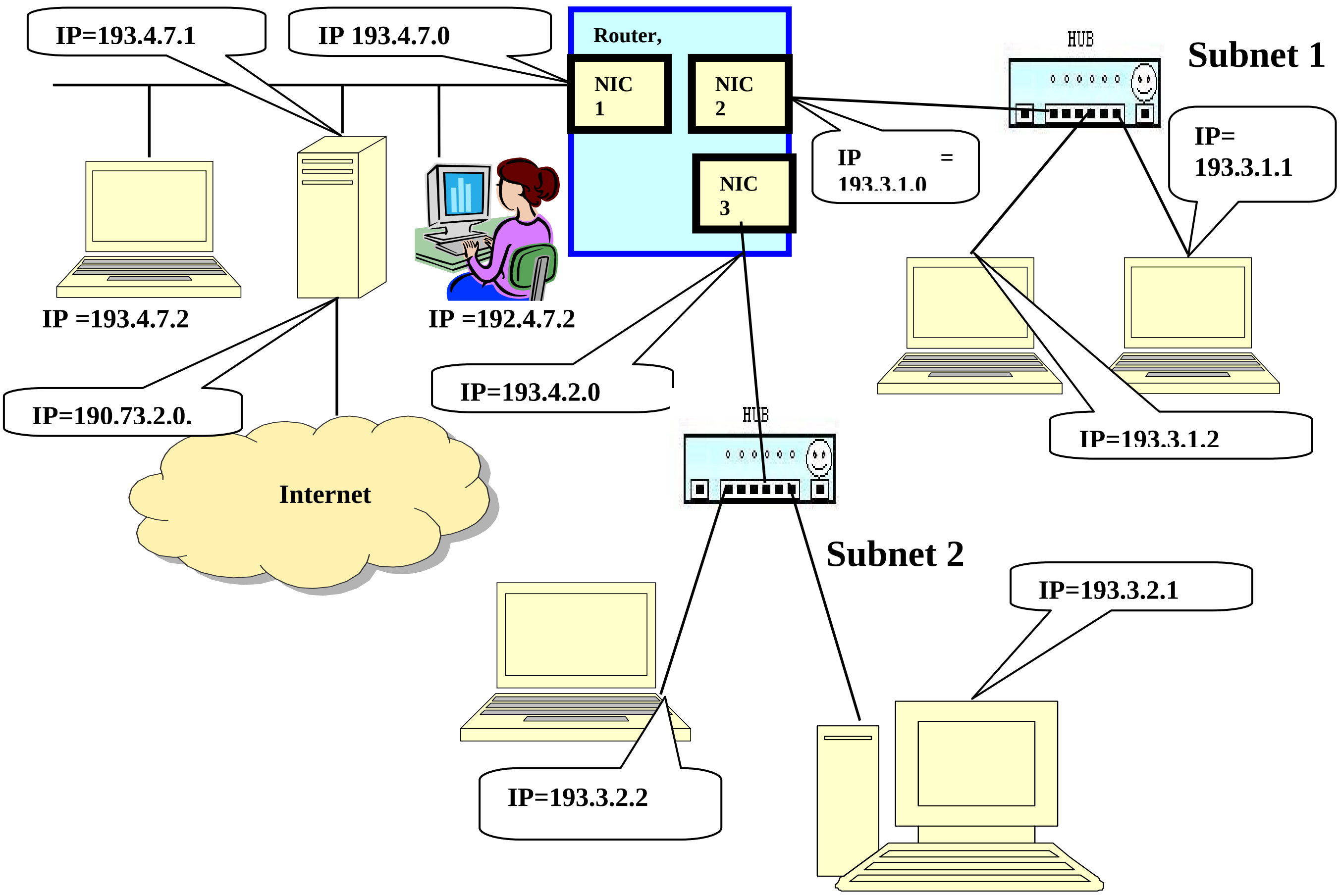


Fig. 1.1 Class C network 193.3.3.0. was divided into two Class C subnets, subnet 193.3.1.0 and subnet 193.3.2.0. Subnet 1 communicates through NIC 2 and Subnet 2 communicates through NIC 3.

The ideas presented in fig.1.1 are summarised as an example in fig. 1.2.

For instance, in fig. 1.1 the Data Packets having the IP Destination Address 193.3.1.1 in the header will travel to the device with this IP Address, 193.3.1.1, without entering subnet 193.3.2.0. or subnet 193.3.3.0. In this way, the traffic and isolation (for troubleshooting and security) in the sub-nets, as well as the networking efficiency will improve.

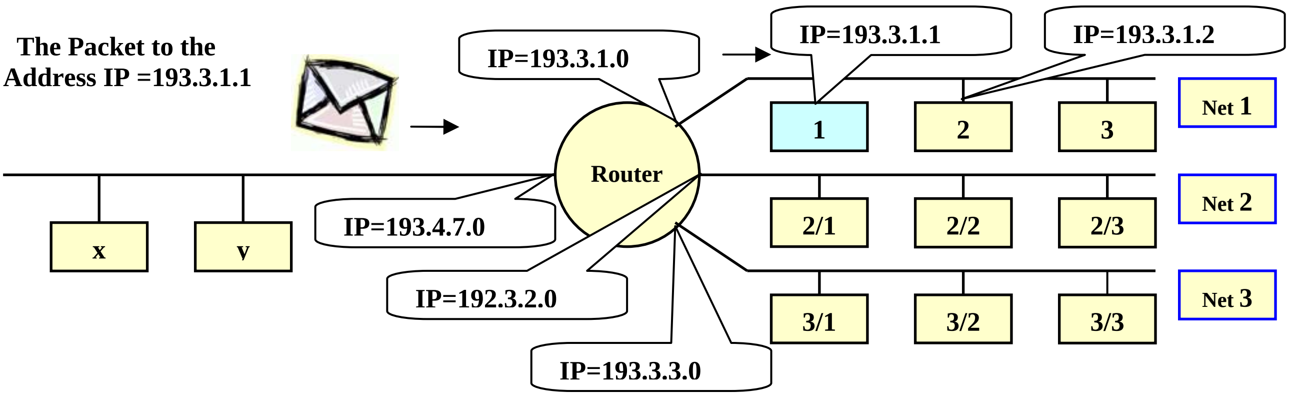


Fig. 1.1 The filtration of the packets sent toward the segmented addresses.

2.) Solutions for segmenting the networks.

The solution of constructing of the Internet architecture consists in:

- A. the hierarchical organization of the network with the sub-netting, respectively, the division into under-networks (RFC 917, RFC 950 and other) and the use of sub-networks as **Separate Networks.**
  The classical division of the NETID and of the HOSTID into octets (respectively, with the NETID and respective HOSTID formed from entire numbers of octets) may be used in these cases.

- B. Using **the subnet mask.** This method allows the allocation of some rank positions of bits inside the octet. In these cases, the NETID includes not only octets but also fractions of octets (taken from the HOSTID). Thus, new values of NETIDs are generated and from the initial IP Address multiple sub-nets are defined.

2. SUBNET MASKS.

The subnet masks are the basic tools for creating the under-networks.

The mask of the subnet is similar to the IP Address, i.e. a 32-bit binary word.

Each bit from **the under-network** (subnet) **mask** corresponds to the respective bit (rank) of the IP address.

The **subnet mask** is equivalent to a tool for reading and deciphering the structure of the IP Address, for “illuminating” with value 1- bits the bits of the IP Address used for the NETID.

Bits **1** of the **subnet mask** indicate part of the NETID of the IP Addresses; bits **0** of the **subnet mask** indicate the ranks of bits allocated for the HOSTID of the IP Addresses.

The **mask of a subnet** is the same for the all participants (for all the computers) connected to the respective under-network.

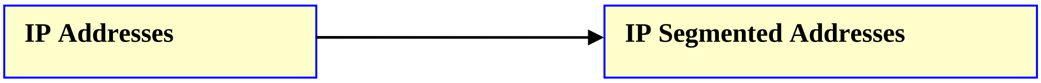
In practice, creating an under-network implies dividing an IP Address allocated for a network in multiple IP Addresses for multiple sub-nets.
Bits of the HOSTID may be transferred to the NETID to create the NETID of each subnet.

The element which indicates the bits involved in the NETID is the subnet mask.

The sub-network masks indicate (with their own bits in position 1) which bits of the IP Address are included in the NETID (with their own bits in position 0) and which bits remain for the HOSTID.

1.) Dividing sub-networks (into under-networks).

Dividing the



is based on the use of the **sub-network masks** which indicate which bits of the HOSTID are transferred to the NETID with a view to define the sub-network address.

With a view to transfer part of the HOSTID bits to NETID’s bits, binary positions of the HOSTID are consumed and the number of the addressed Hosts diminishes. Therefore, the sub-net will allow a smaller number of Hosts.

2.) The information offered by the subnets mask.

The **under-network** (sub-net) **mask** offers the following information:

- A. - information about the network class (through the number of octets occupied by binary values 1);
- B. – which are the bits of the IP Address allocated for the NETID of the respective sub-net.
- C. - which are the bits of the IP Address allocated for the HOSTID.

That means that the **subnet mask** may indicate some bits which are usually allocated for the HOSTID and transferred through the “highlighting” created by the subnet mask to the bits of the NETID.

The case in which the **subnet mask** is formed of octets, where each octet is formed only of values **‘1’** or only of values **‘0’.**

In many situations, the **mask of the under-network** has octets of value 11111111 or 00000000.
This situation leads to the instant conversion of the binary **subnet mask** into dotted-decimal under-network mask.

For instance, for a Class C IP Address, the binary **mask**:

11111111 11111111 11111111 00000000

leads to the dotted decimal value of the **subnet mask** of value **255.255.255.000** (class C network).

The following Table 2.1.illustrates the way in which the mask of the sub-net indicated the class of network.

Class	The subnet mask for the NETID part of the IP Addresses (binary)	The subnet mask for the NETID part of the IP addresses (Dotted-decimal) .
A	**11111111 HOSTID HOSTID HOSTID**	**255. HOSTID.HOSTID.HOSTID**
B	**11111111 11111111 HOSTID HOSTID**	**255.255.HOSTID.HOSTID.**
C	**11111111 11111111 11111111 HOSTID**	**255.255.255.HOSTID.**

The way in which the sub-net mask indicates the network class is summarised in the following Table 2.2. :

The network Class of	The correspondent mask (Without using the segmenting procedures)
Class A	**255.xxx.xxx.xxx**
Class B	**255.255.xxx.xxx**
Class C	**255.255.255.xxx**

The case in which the **subnet mask** also occupies (with value 1) fractions of octets.

In this case, the conversion is done in the following way:

The binary octets which include only value **1** will be directly converted to the decimal value **255**.
The binary octets which include only value **0** will be written as decimal value **0**.

The octets which include both value 1 and value 0 will be converted from binary to decimal as illustrated in the previous lessons (the conversion of IP addresses from binary to dotted-decimal, but only for that specific octet).

In this way, it is possible to use the following under-network masks (octets including a number of 1’s and a number of 0’s):

255.255.220.000

Therefore, the under-network mask:

- allows the selection of that part of the HOSTID bits to be converted to NETID bits, in order to be used as a sub-net address,
- indicates / highlights the bits allocated to the NETID.

Actually, according to the following example in Table 2.3., the **subnet mask** indicates / highlights which bits of the entire word of the IP Address are allocated to the NETID in order to generate the subnet IP Address.

Table 2.3.

Positions of bits in IP Address	**32**	**31**	**30**	**29**	**28**	**27**	**26**	**25**	**24**	**23**	**22**	**21**	**20**	**19**	**18**	**17**	**16**	**15**	**14**	**13**	**12**	**11**	**10**	**9**	**8**	**7**	**6**	**5**	**4**	**3**	**2**	**1**
IP Address	**NETID**																								INITIAL HOSTID							
IP Address																									**SEGMENTS taken by the NETID from the**		FINAL POSITIONS FOR HOSTID					

																									HOSTID							
IP Ad-dress	**1**	**1**	**0**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**0**	**1**	**x**	**x**	**x**	**x**	**x**	**x**
Mask	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**x**	**x**	**x**	**x**	**x**	**x**

Remember the functions of the NETID and HOSTID and of **the subnet mask:**

- The part called NETID of the IP Address is used to find the network,
- The part called HOSTID of the IP Address is used to identify the computer of the respective net,
- The subnet mask “highlights” (through positions “1” of the bit) the bits of the IP Address which belong to the NETID, including bits taken from the HOSTID and allocated to the NETID.
- Through this conversion, the sub-net mask may divide the initial IP Addresses poll and generate the sub-nets.

The subnet mask allows the extension of the NETID.
The subnet mask extends the value of a network IP Address by “highlighting” the bits of the IP Address used for the NETID with its own value “1“ bits.

The subnet mask may be considered “as a lantern” which “illuminates” (through value “1“ bits) all the bits of an IP Address which are used for the creation of the NETID.

The subnet mask has only value 1 bits in the newly accomplished (extended) NETID of the IP Address.

The subnet masks divide the IP addresses in three zones.

INITIAL NETID	ZONE OF THE HOSTID, TAKEN FOR THE NETID AND INDICATING SEGMENTS OF ADDRESS	REMAINED ZONE OF THE HOSTID INDICATING THE ADDRESS OF THE HOST.

Example:

The **sub-network mask:**

11111111.11111111.11111111.11100000

respectively, in dotted-digital **255.255.255.224** indicates (“highlights “) the binary positions:

8	7	6	5	4	3	2	1
128	64	32	-	-	-	-	-

8, 7, 6 of the rightmost octet of the IP Address of the **initial** HOSTID of a net of Class C network.
Because the subnet mask has illuminated bits 8, 7,6 with its own “1” bits, these ranks become binary positions of the NETID.

In this case, 3 bits in positions 8, 7, 6 are destined for segmentation.

The binary positions indicating the segments of the IP Address consume, in this example, 3 supplementary binary positions of the HOSTID.
After this, a maximum [(16 + 8 + 4+ 2+ 1)- 2] IP Addresses per each segment of addressing will remain for Hosts and 30 (instead of 32) addresses per each sub-segment.

In this example, 2 IP Addresses, out of 32 are used up for:
a.) - an IP Address (with the bits 8, 7, 6, on “0” logic) is used for the backbone of sub net,
b.) - an IP Address (with the bits 8,7,6, on “1” logic) is used for permitting the broadcasting to all the addresses of the respective network.

The number of possible sub-networks depends on:
-the Class of the IP Address,
-the number of supplementary bits taken from HOSTID with the view to define the NETID – (value 2),

Table 2.4.Example for the class C, the most used class of IP Addresses, (according also to [3.]):

The number of bits allocated	The number of possible	The number of possible	The sub-network mask

to HOSTID for segmenting the IP address	**sub-networks**	**machines (Hosts) on each sub-network**	
2 bits	2 (not 4 because 2 positions are used for the broadcasting respective reserved for the net's backbone IP Address)	62 (and not 64 because 2 positions are used for the broadcasting reserved for the net's backbone IP Address)	255.255.255.192 11111111.11111111.11111111.11000000
3 bits	6 (not 8)….	30 (not 32)	255.255.255.224 11111111.11111111.11111111.11100000
4 bits	14 (not 16)	14 (not 16)	255.255.255.248 11111111.11111111.11111111.11110000
5 bits	30 (not 32)	6 (not 8)	255.255.255.252 11111111.11111111.11111111.11111000
6 bits	62 (not 64)	2 (not 4)	11111111.11111111.11111111.11111100

The number of possible binary positions (taken from the HOSTID to NETID) for segmenting is minimum two.

The segmenting with only 1 binary position (on position 128 of a Class C IP address, for instance) is not possible because this situation generates only two numbers:
"0" which is reserved for the IP Address of the backbone of the sub-net and "**1**" which is reserved for broadcasting.

3. THE PRACTICAL USE OF THE SUBNET MASK.

1.) How to know the subnet mask of your machine?.
By using the diagnosis command (with the computer connected to Internet):

C:/>**IPConfig /All** [Enter]

2.) Who provides your subnet mask and when is it set?

The ISP provider provides the subnet mask.
The subnet mask is set according to the configuration and setting of the computer parameters inside the network configuration.

3.) If you are an ISP, how do you use the subnet masks?
As in the above chapters: 1, 2 and as in chapter 4.

4. THE NETWORK ADMINISTRATOR PRACTICE: PRACTICAL SEGMENTING OF THE NET THROUGH THE USE OF THE SUBNET MASK

Initial Data.
In one example, an administrator intends to create two segments of IP Addresses, respectively, two sub-networks of a Class C network.
Therefore, the IP pallet of accomplished IP Addresses must be divided into two separate segments.
Each segment will have, in accordance with the possibilities offered, in accordance with Table 2.4 above by:

- segmenting the Class C IP Addresses,
- using two binary positions of HOSTID (position 7 and position 8 of the HOSTID indicated in the rightmost octet and from right to left) which will be transferred to the NETID, for the segmenting process, into sub-networks having a maximum of 62 IP Addresses per each segment (as in the above Table 2.4., row 2).
  These 2 positions of the HOSTID, which becomes NETID, will be used as following:

Position 8 of the previous HOSTID	Position 7 of the previous HOSTID	Comment
0	0	Not used for segmentation, Used for the IP Address of the backbone of the subnet
0	1	To be used to the NETID of one subnet.
1	0	To be used to the NETID of second subnet.

1	1	Not used for segmentation, Used for the IP Address of broadcasting

The situation is illustrated in figure 4.1. (initial situation) and fig. 4.2. (after segmenting):

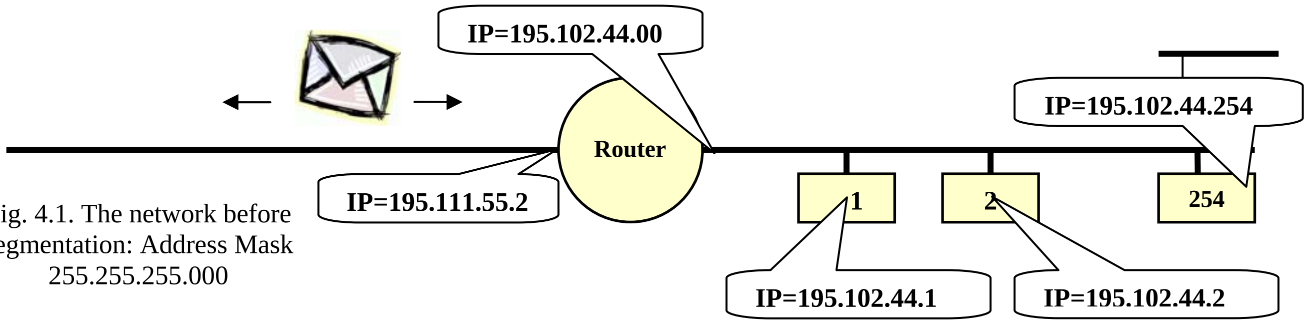


Fig. 4.1. The network before segmentation: Address Mask 255.255.255.000

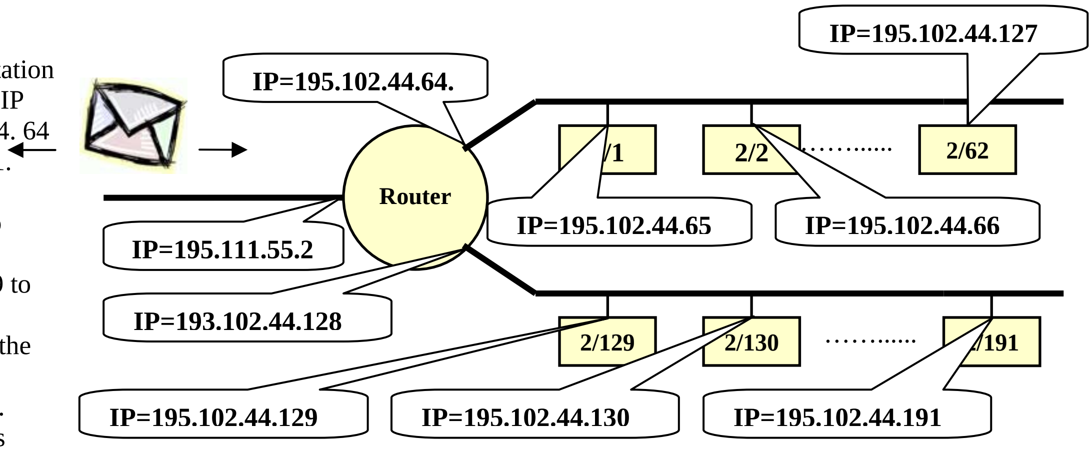


Fig. 4.2. The segmentation of the spectrum of IP Addresses 195.102.44. 64 to 195.102.44.191. into 2 segments: 195.102.44.65 to 95.102.44.127, and 195.102.44.129 to 195.102.44.191 through the use of the subnet mask 255.255.255.192. The IP Addresses 195.102.44. 64 and 195.102.44. 128 are addresses of each of the new buses (NICs of the Gateway).

In the configuration from the fig. 4.2., the sub-net mask: 255.255.255.192 is the same for the both sub nets: Subnet 1 and Subnet 2.
The mask of sub-network illuminates with value “11” the bits (of the position 8 and 7) taken from the HOSTID.
This allows that the position 8 and 7 of the lowest significance octet of the IP Address to be used to create the two subnets:
In this example the IP address of the initial network (which will be segmented), a network which is of the Class C is:
In dotted decimal from: 195.102.44.0 respectively I binary form: 11000011.01100110.00101100.00000000.

Based on the considerations that:

1.)- it is a case of Class C network and IP address and
2.)- two binary positions of the HOSTID will be used for the “lighting“ of the two binary position of the IP address (position 8 and 7),

the subnet mask will result as: 11000011.01100110.00101100.11000000.

Using 2 binary positions for the segmenting results the two possible sub-networks

FIRST PART OF THE NETID	**THE PART OF THE NETID TAKEN FROM HOSTID** (binary positions)	**HOSTID FOR THE COMPUTER ADDRESSING** (binary positions)
11000011.01100110.00101100	**10**	**xxxxxx**
11000011.01100110.00101100	**01**	**xxxxxx**

Part of the subnet mask	Part of the subnet mask	Part of the subnet mask
11111111 11111111 1111111	**11**	**000000**

The two subnets which are formed through the use of the subnet mask have the following IP addresses of the backbone of each subnet:
11000011.01100110.00101100.01000000 that is 195.102.44.64 and maximum 62 machines between 195.102.44.65 and 195.102.44.126
and
11000011.01100110.00101100.10000000 that is 195.102.44.128 and maximum 62 machines between 195.102.44.129 and 195.102.44.191.

The backbone of the initial network is:

11000011.01100110.00101100.00000000, that is 195.102.44.0.

Finally, three networks have resulted all in all:

1. basic network and backbone and
2. sub-networks, respectively, backbones

Each of the two networks may to have maximum 62 machines (Hosts).

The IP addresses of the machines, connectable within each of the two sub-networks will be:

Address number	**For network: 195.102.44.64**	**For network: 195.102.44.128**
1	195.102.44.65	195.102.44.129
2	195.102.44.66	195.102.44.130
3	195.102.44.67	195.102.44.131
4	195.102.44.68	195.102.44.132
………	………	………..
62	195.102.44.127	195.102.44.191

One has to be sure that near the initial backbone **195.102.44.0** the Internet IP addresses may be used:
195.102.44.64 to 195.102.44.127 and **195.102.44.129 to 195.102.44.191**

Because between the IP Address of the basic network, the backbone, and IP **195.102.44.0**, respectively, and the IP address of the first segment of the network, **195.102.44.64,** respectively, an interval of 63 addresses is not used, it is recommendable that this interval also must be used as the 3rd segment of addresses.

From the ISP of the superior rank one space of IP addresses is normally required (in the previous example from: **195.102.44.0** to **195.102.44.191**), respectively, of about **192** IP Addresses.

The creation of the network segments does reduce the number of usable IP Addresses.

5. THE IP ADDRESSES SEGMENTATION HELPING REPAIRABILITY, MAINTENANCE, AVOIDANCE OF CONGESTION AND IMPROVEMENT IN THE NETWORK SECURITY.

The division into sub-networks allows a better management of the network and of the IP addresses.

The division of the IP addresses in segments allows better maintenance, manageability and also improvement of the network security and of the hosted computers on the respective network.

By dividing the net into subnets, the different net points become accessible more quickly (a diminished number of positions of the Routing Tables will be evaluated on the Router and the bifurcation ways toward different computers, respectively).

6. VARIABLE-LENGTH SUB-NET MASKS (VLMS).

The VLMS is innovatively developed in order to create segments of IP Addresses with the different dimensions.

With the previous procedures, passing from established segments of IP addresses to subnets of other dimensions leads to time-intense processes.

In 1987, the RFC 1009 added improvements which facilitate the use of subnets of different dimensions (different number of allocated IP addresses).

The solution consists in dividing the initial network into subnets with a different number of permitted addresses following in-situ requirements and using the subnet masks with different compositions.

The different compositions of the subnet masks refer to the number of binary positions used to "illuminate" the binary positions of the HOSTID which are granted to the NETID.

In these cases, the notation of an IP Address of the backbone (the network) may be used under the form (for instance):

195.102.44.0/2

where the value after the slash indicates the number of binary positions GRANTED by the HOSTID to the NETID.

7. CIDR-CLASSLESS INTERDOMAIN ROUTING. ADDRESS SPACE. AGGREGATION.

Innovative developed in 1990, published in the RFC 1517, 1518, 1519, 1520, 1817, the CIDR operates by using a CIDR IP Address of the form:

195.102.44.2/22

where
1.)- 195.102.44.2 indicates the IP Address and
2.)- /22 indicates that there are 22 bits totally allocated for the NETID, respectively, from the left part of the binary representation of the IP Address.

Through this procedure:
1).- the length of the NETID becomes variable and consume diminished space of the total length of the IP Address. Therefore, there is additional space left inside the HOSTID for addressing the computers and additional IP Addresses, respectively;

2.)- bits from the left part of the IP Address word are left aside, a part which consume substantial addressing space in IP Address Classes.
For instance, for class C in the address:

11000011.01100110.00101100.00000000.

the three bits in red on the right indicate Class C. This indication is cancelled in the CIDR systems.
The RFC 1518 describes a domain as a group of "resources under the control of a single administration"[4].

The CIDR is to be used especially in inter-domains.
The CIDR is meant to cover group of addresses which have been lost, because they are placed inside inter-domains of IP Addresses groups.
For instance, the Class B IP Addresses lose a significant number of IP Addresses.
Class B IP Addressing is very rarely used.

One action of the CIDR, called **address space aggregation**, consists in replacing the Class B IP Addresses (which are very rarely used) with a group of Class C IP Addresses which are accessed in a different way (compared to the normal IPv4 standard).

Following the **address space aggregation**, some class B IP addresses are saved.

There are some problems related for instance to the single character of the IP Addresses used which may be generated to the CIDR uses.

Today, despite the arrival of the CIDR, the classic formation of the IP Addresses according to IPv4 remains the basis of the world IP addressing.
The aspect includes the situation of the networks with small pallets of IP Addresses.

The CIDR which works around IPv4, also works well in smaller networks.

Generally, the CIDR may work only if the Router supports this type of operation, these types of IP Addresses, respectively: (IP Addresses include the slash followed by the number of bits of the subnet mask).

8. MULTIPLICATION OF IP ADDRESSES. NAT SERVERS.

NAT Network Address Translation.

The NAT, also called (in UNIX) IP Masquerade hides the computers of a LAN behind a public, legally registered IP Address [9.]. The LAN has only the legal registered IP Address of the NAT. The NAT software is normally supported by the same server which also achieves the functions: Proxy (for instance from www.analog.com) and Firewall.

In order to be able to communicate with the Internet, a computer from a LAN -Local Area Network must have its own IP registered (and consequently unique) Address.

In the NAT systems, only one computer of the NAT local space, the computer functioning as a Gateway between the Internet and the Intranet, has its own IP registered Address.

An example of NAT (Network Addresses Translation) system is illustrated in Fig. 8.1.

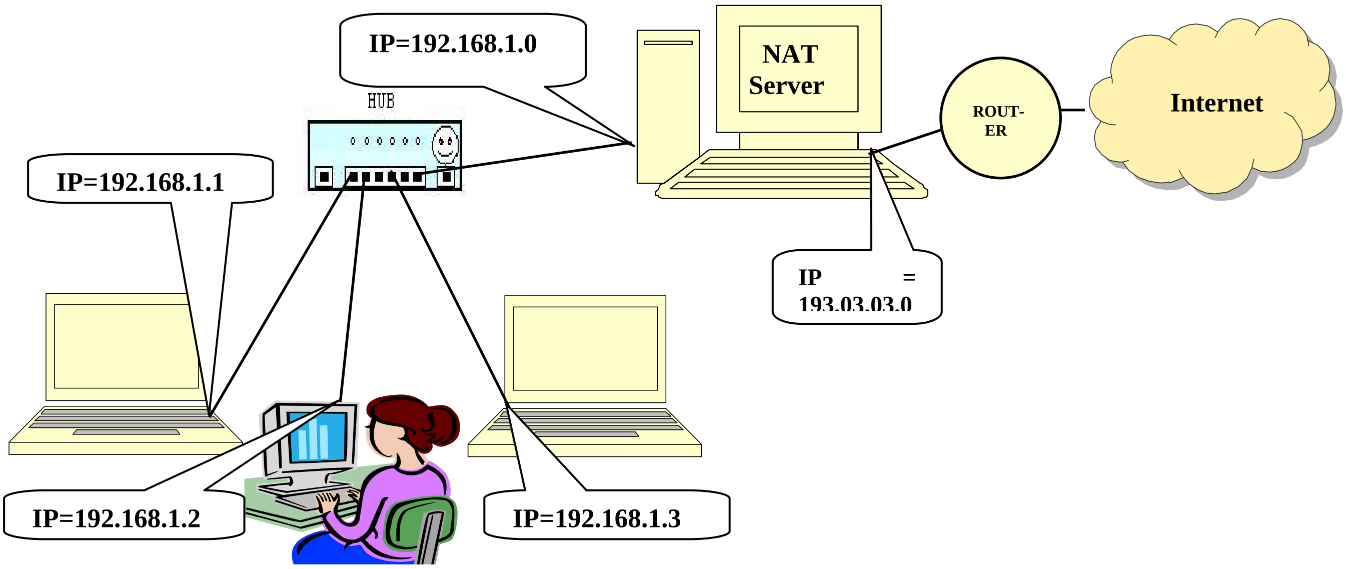


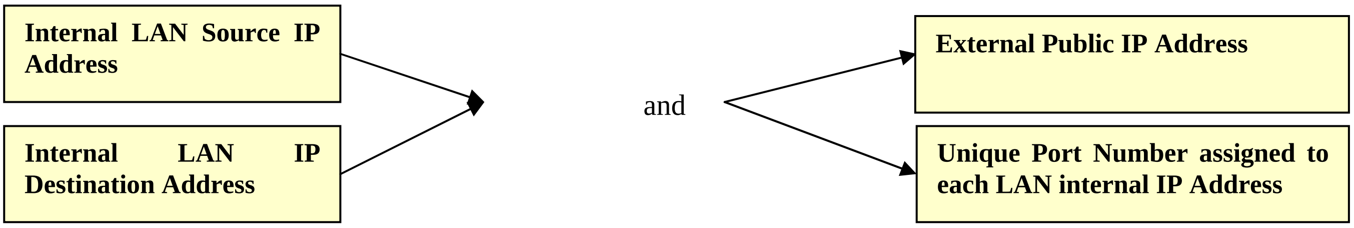
Fig. 8.1. Translation of Addresses by using the NAT.
In this example, only the IP 193.03.03.0 is a registered IP Address.

In the configuration illustrated in figure 8.1 above, only the IP 193.03.03.0 is a registered IP Address. The Addresses 170.5.04.x are LAN internal IP Addresses which are not visible from the Internet side but even in this case they may communicate with the Internet through the NAT procedure of IP Address translation.

The device which helps this process is called NAT Router and all the conversations of the Internet with the Intranet are achieved through the NAT Router.
The NAT Router (which includes the Gateway) ensures the correspondence between the Intranet private, non registered IP Addresses and the IP registered Addresses from the Internet.

After the NAT, on the Intranet side (the LAN – local network), the registered Internet IP Addresses cannot not be used (except the public registered IP Addresses of the Gateway configured in LAN).

The NAT Router creates one Table which associates, prepares and stores for each session of Internet dialogue the association between :


Internal LAN Source IP Address
Internal LAN IP Destination Address
and
External Public IP Address
Unique Port Number assigned to each LAN internal IP Address

The Public IP Address is the IP Address assigned to the NAT Server and the registered IP Address of the system.

The Port number (which, in this case is a type of software identifier which works inside the software of the NAT Server) is the key to ensuring the correspondence between the LAN internal IP Addresses and the external IP Addresses.

The NAT service maintains an Internal Table of correspondence between:
a.)- the internal (inside the LAN) source addresses which are not registered IP addresses,
b.)- the Internet registered IP Addresses from the Internet registered space of addresses.

The process is running as follows:

1.)- When a computer of the Intranet (the LAN) wants to communicate with the Internet, the NAT Router establishes the connection,
2.)- When Data Packets arrive from the Internet, the NAT addressing scheme provides the delivery of the Data Packet to the local Intranet computer.
For this target, the NAT ensures the correspondence between:
the external addresses and the internal addresses plus the assigned NAT port.
(The internal IP Address + the assigned NAT port form one specified socket).
3.)- The NAT Router achieves all the necessary monitoring actions to achieve the translation of addresses, respectively, of the representation of the computers in communicating with the Internet.
4.)- Some registered IP Addresses may also remain inside the LAN, and these have to be taken into consideration as normal IP Addresses,
5.) – In some configurations, the special IP Addresses are preferred as internal, hidden LAN addresses which are not used by the Internet by means of convention.

These IP Addresses are the following [1.], [9.]:
10.xxx.xxx.xxx; with the subnet mask 255.0.0.0; (Class A network),
172.16.xxx.xxx; with the subnet mask 255.255.0.0; (Class B network)
172.31.xxx.xxx; with the subnet mask 255.255.0.0; (Class B network)
192.168.xxx.xxx, with the subnet mask 255.255.255.0; (Class C network).

9. THE PROXY SERVER.

The use of PROXY servers technology is largely applied and has the following advantages:

- the multiplication of network addresses,
- the possibility to create a barrier between the part of the network which is not trusted and that part of the internal network,
- the possibility to introduce the protection elements such as Firewalls and other.

The Proxy Server operates as a “go-between” between the Internet and the Intranet [1.].

The Proxy Server acts as a separator between the Internet and the LAN.

On the Intranet side the Proxy Server may work with non registered IP Addresses (as is the case of NAT addressing schema from the spectrum of addresses for the spectrum of addresses: 10.xxx.xxx.xxx; 172.16.xxx.xxx; 172.31.xxx.xxx; 192.168.xxx.xxx.) or with other types of addresses of the Intranet machines.

Proxy Servers include NAT technology.

The operation mode of the Proxy Server is illustrated in fig. 9.1.

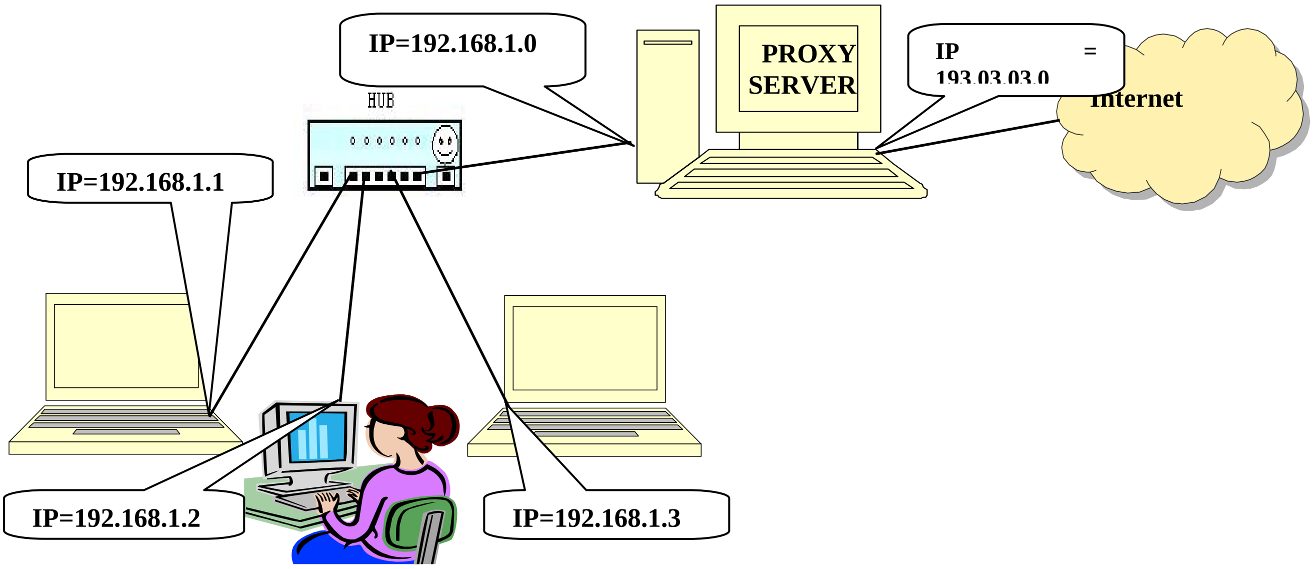


Fig. 9.1 The Proxy Server includes the NAT procedure and ensures the translation of the non-registered LAN internal IP Addresses, the multiplication of addresses, and creates one level of protection of the machines.

The Proxy server operates as follows [1.]:

1.)- One Intranet computer informs the Proxy Server about the desire to communicate with a destination of the external (outside the Intranet) network, with the Internet for instance, with the view to receive a Web page.

For instance, the computer with **the internal LAN** IP Address **172.16.4.305** (invisible from the Internet) intends to access the Internet Server with the registered **IP Address 195.102.44.0**

2.)- The Proxy Server assigns to the Intranet device:
2.1.) - its public IP Address (registered and its own address of the Proxy Server), for example, in this case: **193.03.03.0** and
2.2.) - a unique port number (inside the software of the Proxy Server) allocated for this connection, in this case: Port number 8001.
By assigning its own IP Address with the unique port number, the Proxy Server creates one **socket:**
(Server Address + Port Number = Respective **Socket**).

3.) - The Proxy Server writes the above generated **socket** inside one own Table of correspondences.
For instance:

"**Socket 193.03.03.0,8001** generated by machine **172.16.4.305** is temporarily assigned at the IP Address **195.102.44.0**"

4.)- When the response and the Data Packet from the Internet network arrive at the Proxy Server, in this case from the IP Address **195.102.44.0,**
the Proxy Server analyses the temporary Tables written as in point 3.) above - and may take the decision to direct the content of the arrived Data Packet inside the LAN-Local Network to the machine with an IP local address **172.16.4.305** , according to with the Table inside the Proxy Server previously noted.

The Proxy server hides the Addresses of the LAN's machines, against the possibility that they could be viewed from the Internet side and, by this, improves the level of security of the LAN partners.

The Proxy Severs may be a software part of the same device: the server of the LAN.

10. DNS ADDRESSES.

DNS addresses were a result of the following:

- The need to make the IP addresses more "humane". The IP Addresses are formed by the concatenation of four groups of decimal values, each having a maximum value of 255. This form is not very friendly for the human party.

- The need to increase the ON-LINE VISIBILITY of the respective site and to add contributions to marketing and promotion,
- The improvement of the entity brands,
- The need to allow the possibility to remember the addresses of the site quickly and easily,
- Etc.

For each DNS alphanumeric address there is a matching IP Address.

Not all IP addresses have a corresponding DNS address:

- Normally, only the hosts (for instance web pages) have a DNS address,
- Ordinary work stations (PCs, laptops etc) do not have a DNS.

The DNS features are presented in the following Lessons.

11. THE E-MAIL ADDRESSES.

E-mail addresses such as ecic@ipa.ro are formed of 2 parts:

1.) – what is placed left of '@', where elements related to the owner of the workstation may be introduced and established,
2.) – what is placed right of '@', which includes elements related to the DNS Address of the host which manages the network.

12. ADDRESSING VIRTUAL PROTOCOL ELEMENTS.

The software running into the operation system of the machine, including the TCP/IP protocol part, ensures the addressing of the protocol elements which are called **Ports**.

The IP Address together with the **Port Number** forms the **Socket.**

The aspects are illustrated in the following lessons related to the operation mode of the TCP/IP Protocols.

13. THE IPv6 PROTOCOL.

The new protocol: IPv6 was developed and launched under the pressure of exhausting all useable IPv4 protocol addresses.

IPv4 uses the well-known IP Addresses of 32 bits.
These addresses are presented as dotted-decimals divided into four groups.

The new Internet addressing protocol, IPv6, uses addresses on 128 bits divided into 16 dotted-decimal groups.

The IPv6 may also use the hexadecimal representation.

The hexadecimal representation is divided into 8 hexadecimal groups.
Between these groups are introduced the signs **:**
Therefore, one IPv6 address may be written hexadecimally as:

0005:1222:C432:00FF:0000:000E:AD12:BA1E

Additionally, the first zeroes of each hexadecimal groups are suppressed.
Therefore, using the presentation from the previous example, the above IPv6 address turns into:

5:1222:C432:FF::E:AD12:BA1E.
Also, if the words between the signs '**:**' include only zeroes, they are replaced by the **:** , as in the example above.

The IPv6 stresses the possibilities to prioritize the transmission of some Data Packets, to meet the requirements of Internet transmission speed for video, audio, multimedia.

The essential aspect related to the IPv6 is the possibility for the IPv6 to function and cohabitate with the IPv4.
That signifies that the IPv4 must be very well known.

The last bytes on the right of the IPv6 may be used as bytes of the IPv4.

Key Point Summary Conclusions and Recommendations

The subdivision of the nets into subnets represents an important aspect for the efficient use of IP Addresses. The consequences include improving the traffic, improving the troubleshooting possibilities, accomplishing the isolation and the convenient level of reliability.
The subnets must be achieved with a minimum IP Address loss through the use of the subnet mask.
The subnet mask, which "highlights" the bits of the IP Address, may contribute to structuring the networks into subnets.
The division into subnets does not lead to a multiplication of addresses.
The NAT and Proxy procedures may to lead to the multiplication of addresses, including the occasion of extending the networks. At the same time, the Proxy procedure helps improving the security level.

Study Guide

ESSENTIAL QUESTIONS TO EVALUATE THE ACQUIRED KNOWLEDGE

1. Why is the network segmentation necessary?
2. How is the network segmentation achieved?
3. What is the subnet mask?
4. How is the subnet mask constructed?
5. How can the subnet mask be used for network segmentation?
6. Does the network segmentation lead to the multiplication or the loss of IP addresses?
7. How it is possible to multiply the Addresses?
8. Which are advantages of using the PROXY procedure?
9. How do the NAT and PROXY procedures operate?
10. Describe the steps in starting and implementing a network inside an entity.

BIBLIOGRAPHY. REFERENCES.

As in the previous lesson

IMPORTANT SUPPLEMENTARY BIBLIOGRAPHY. REFERENCES. (www)

As in the previous lesson.

SUPPLEMENTARY GUIDANCE ABOUT THE CONTENTS OF THE LESSON

Also consult : www.cisco.com; www.cramsession.com; www.ietf.org RFCs; www.rfc-editor.org RFCs.

ANSWERS TO QUESTIONS

1. The network segmentation improves the network speed, the traffic, ensures a good monitoring of networks, improves the level of troubleshooting, manageability, security, the distribution of IP addresses between different clients.
2. The network segmentation is achieved either by dividing the initial network, based on the assessment of the accomplished block of addresses, in different convenient networks and by using the subnet mask.
3. One word of 32 bits of the same length as the IP Address and which illuminates the bits used in the IP Address for the NETID.
4. The subnet mask is constructed with bits "1" to "highlight" the NETID and "0" the bits of HOSTID. The subnet mask extends the NETID over the bits of the HOSTID which receives the NETID meanings of the new segments.
5. By supplementing the bits of the NETID with most significant bits of the HOSTID.
6. The addresses are not multiplied; moreover, a few addresses are lost.
7. The Addressed may be multiplied by using the NAT and the PROXY Servers. This multiplication is done without viewing these new addresses directly from the Internet side.
8. The PROXY procedure ensures the multiplication of the LAN addresses without these addresses.
The PROXY procedure includes the NAT procedure and is based on the translation of the LAN internal IP Addresses
9. The classical relevant steps to start a network inside an entity include [2.]:

- The preliminary design of the LAN based on the existent machines,
- Purchasing a switch, possibly some hubs and, according to configuration, one router,
- Accomplishing a pallet of addresses from the IPS,
- Constructing the Ethernet LAN- local area network through the use of one switch and some hubs.
- Distributing the IP Addresses;
- Tests with Ping, Tracert and other tools.
- Improving the speed of the network through segmentation,
- Introducing the monitoring and management tools,
- Solving troubles generated by segmentation,
- Implementing the NAT.
- Introducing the Firewalls and other security devices,
- Installing the DNS- Domain Name System addresses and making the DNS server operate,
- Introducing the VPN- Virtual Private Network, in order to reduce the cost of communication with the other network.
- Monitoring, management and improvement.

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