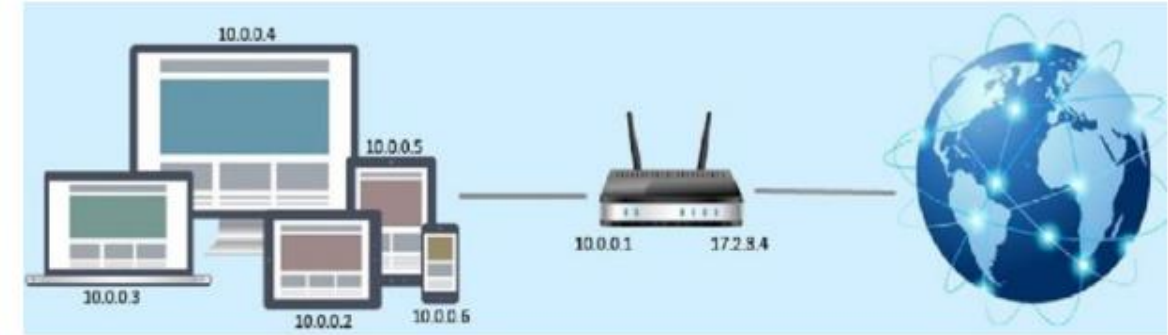
NAT: I will now mention a concept that might sound difficult to some of you, but which nowadays is used in almost all networks. The word NAT stands for “Network Address Translation”. But what does it actually mean? I will try to be as clear as possible. When you surf the Internet from home, several things will happen: the first one is that your PC will receive a private IP address, usually belonging to class C (192.168.1.0/24). However, as you already know, this is not enough to browse on the Internet. You need a public IP address, and this is where your router and NAT come into play. The router will automatically translate the private IP address into a public address and therefore you will be able to navigate without any problems. PRIVATE IP ADDRESS -> to verify your private IP type the "ipconfig" command. PUBLIC IP ADDRESS -> to check your public IP click on the following link: https://www.whatsmyip.org/. Let’s imagine that the IP address of your personal PC is 192.168.1.10. When you try to access the outside network, the router will automatically translate that IP address into a public one, like for example 34.34.23.12. The peculiarity of this mechanism is that, if you had ten devices at home each with its own private IP address, they would all be associated with the same public IP address 34.34.23.12.



For now, I will not go into detail regarding this process. You just need to understand the concept of a port to achieve the same result I have just mentioned. In corporate networks, companies try to reduce the number of public IPs assigned. For this reason, few of these IPs tend to correspond to many private IP addresses for each of the PCs in the network. There are several reasons why this happens: 1. The number of IPs is limited and only few of them are still available. This leads to higher prices for each IP address. 2. Using this NAT mechanism allows you to create a first layer of network protection. This means that nobody from outside knows your private IP address. Instead, potential attackers might only be seeing your public IP address without knowing the table of private IP–public IP associations. This is not enough for them to trace us. One final comment, in corporate networks the firewall usually performs the NAT. Besides, there are several types of NATs and you can refer directly to Wikipedia (https://it.wikipedia.org/wiki/Network_address_translation) if you want to learn more about each one of them