Sistemas Informáticos (Computer Systems)

Unit 11. Computer networks - Part 01

Authors: Sergi García, Alfredo Oltra

Updated January 2023

Licencia

Nomenclatura

A lo largo de este tema se utilizarán diferentes símbolos para distinguir elementos importantes dentro del contenido. Estos símbolos son:

📖 **Important**

❕ **Attention**

💬 **Interesting**

INDEX

Unit 11. Computer networks - Part 01

1. INTRODUCTION

Undoubtedly, one of the elements that most has contributed to the evolution of computing in recent years has been the ability to connect computers to exchange information.

All communication between two parts consists of a series of elements:

- ***Message***: the information to transmit.
- ***Sender/Receiver***: the device that sends/receives the message. They are usually called host.
- ***Channel***: it is the medium that transmits the message.
- ***Transducer***: the device which converts the message in a signal to be transmitted. For instance, in a human, the vocal cords or the ears or, in a computer, the network card.
- ***Accessory elements*:** elements that help make communication better: a telephone, an antenna or, in computer networks, a hub, a router, a repeater…
- ***Protocols***: the sets of rules that control the data flow and define physical parameters of the other components in the communications system. For instance:
    1. We dial a number.
    2. The phone rings.
    3. Someone picks it up.
    4. Says "hello".
    5. The other person says, “hello, it’s me”.

2. TYPES OF NETWORKS

There are many ways to classify a network, although the most used are:

2.1 By geographic area

LAN (Local Area Network): The main feature that the distance between computers should be small (from a room to a few kilometres).

They are widely used to connect personal computers and workstations in company and factory offices in order to share resources (printers, etc.) and exchange information.

WAN (Wide Area Network): It is a type of network that covers distances of between 100 and 1,000 kilometres, which allows it to provide connectivity to several cities or even a whole country. They are usually implemented by a company or an organization for private use, or even by an Internet Service Provider (ISP), to provide connectivity to all its customers.

📖 **Important:** This classification can be extended with many other types such as MAN (Metropolitan Area Network) or CAN (Campus Area Network) depending on the breadth and connectivity

2.2 By services

- **Client-server**: some computers (clients) demand services and others, the servers, offer them.
- **Peer to peer:** all computers can work as both clients and servers.

2.3 By type of communication

- **Simplex**: the channel only allows communication in one direction. An example could be the radio broadcast.
- **Half-duplex**: the channel allows communication in both directions, but not simultaneously. An example could be the use of "walkie-talkie".
- **Duplex**: the channel allows communication in both directions simultaneously. An example could be a phone call.

3. ARCHITECTURE

The network architecture is a concept that aims to define all the formal aspects of the implementation of a network. Its study encompasses the topology and communication protocols.

3.1 Topology

The topology refers to the physical form in which the network hosts are connected.

3.1.1 Wired Network Topologies (the media is a wire)

Bus: all computers are connected to the same media. To avoid *echoes* (that the signal rebound and return to the media), terminators are necessary. The problems are that if you break the wire the entire network fails and that they have a low speed because only one computer can use the media at the same time.

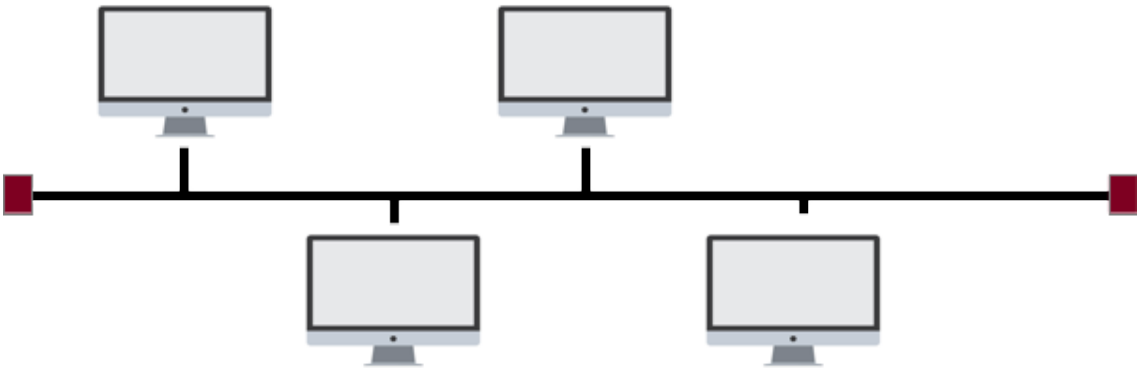

Figure 1 - Bus

Star: each network host is connected to a central hub with a point-to-point connection. All traffic that traverses the network passes through the central hub. The star topology is considered the easiest topology to design and implement, because it is very easy to add additional nodes. The main disadvantage of the star topology is that if the hub fails, the whole network fails.

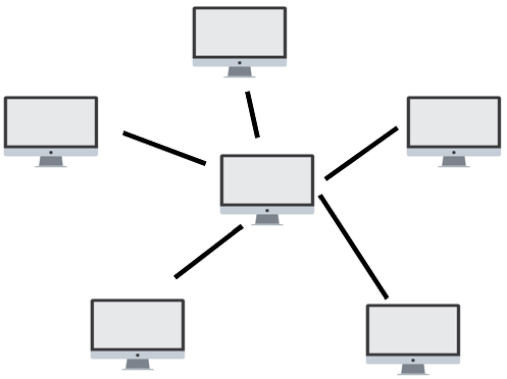

Figure 2 - Star

Ring: similar to the typology in bus, but forming a loop. The data is sent in one direction and until it reaches the destination host.

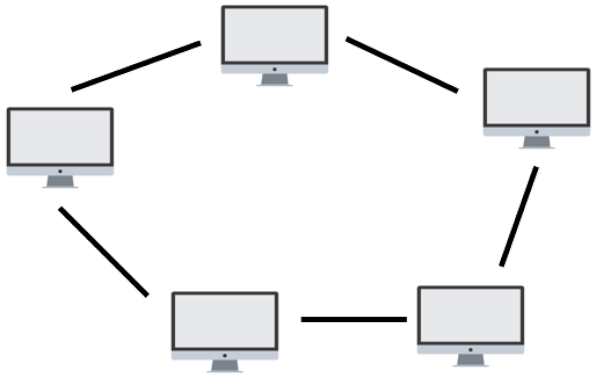

Figure 3 - Ring

Mesh: each computer is connected point to point with all other computers. The big advantage is that if a node falls, the rest of the net is still working.

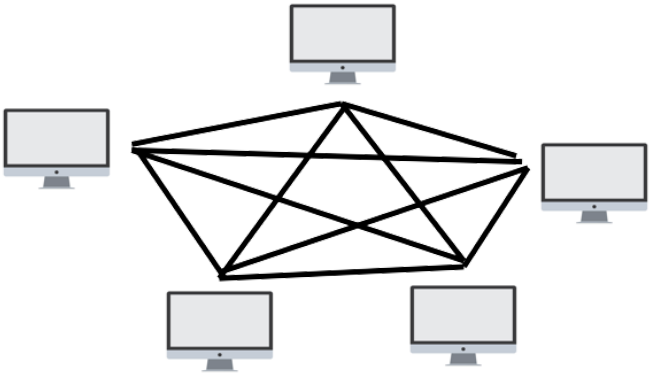

Figure 4 - Mesh

Tree: it is a mixture between the star technology and the bus topology: several bus lines are connected to another bus line. This connection is made by auxiliary elements such as hubs, routers or switches.

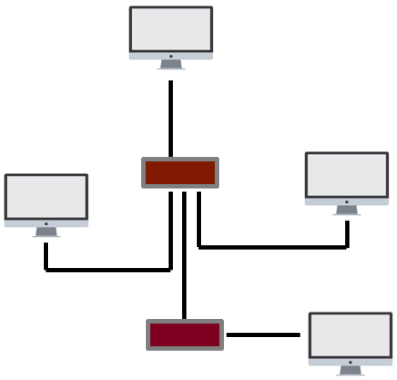

Figure 5 - Tree

3.1.2 Wireless Network Topologies

Ad-hoc: ad-hoc networks do not require an access point. In this mode of operation, the devices interact with others, allowing direct communication between devices. They are sometimes called *peer to peer* wireless networks.

Figure 6 - Ad-hoc

Infrastructure: this topology is made up of an access point connected to a network cabling segment. It is the habitual one that we have in the homes or in the organizations.

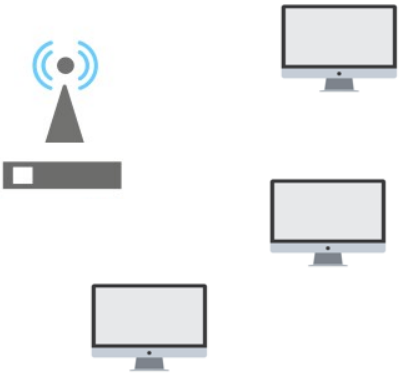

Figure 7 - Infrastructure

3.2 Layers and protocols

In the beginning of the networks, the different solutions to enable the connection between computers were independent, that is, it was only possible to connect computers that came from the same manufacturer. Over time, and looking for interoperability, it was decided that it was necessary to create a standard that would allow all machines to interact with each other, as long as they followed that standard or model.

The general idea of the standard is to work by dividing the communication process into small phases, phases that, executed sequentially, allow the sending and receiving of messages. In the sender, the execution of these phases in order ends with leaving the message in the media. Once this reads the receiver, it executes these sequential phases, but in a reverse way.

Each of these phases is called layers, and each layer only understands the information coming from the same layer of the opposite computer. In order to communicate with each other, each of these layers use one or several protocols, that is, several procedures to receive or send the information.

📖 **Important:** The set of all the layers with their respective protocols is called *a protocol stack*.

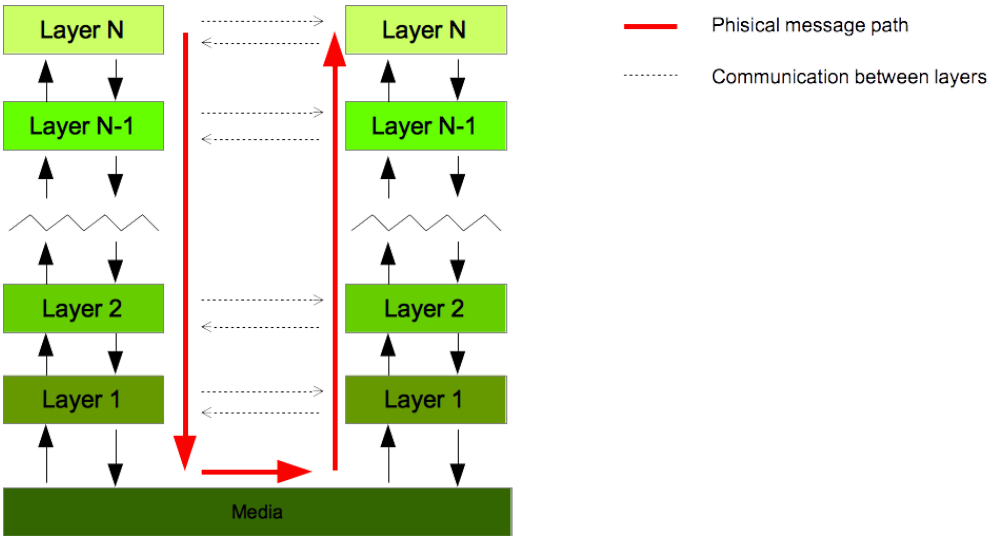

Figure 8 - Sending a message between computers

Initially, the first model adopted was the called OSI model, that differentiated seven layers. Although this model was initially implemented to achieve standardization, over time it has been replaced by a different model used today by the vast majority of computers. This model is the so-called TCP IP model that groups several layers of the OSI model, leaving it only in 4 layers

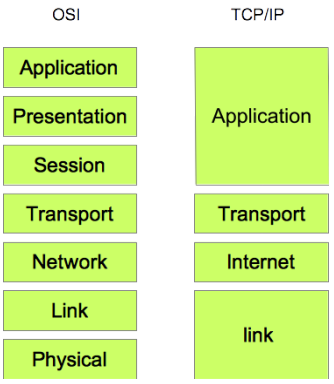

Figure 9 - OSI vs TCP/IP

3.2.1 Link layer

It is the set of protocols that network interface cards use to exchange data. The protocols of this layer depend on the technology of the network and are usually stored in a built-in ROM memory of the networking card. One of its functions is to convert the bits into electrical impulses that must be transmitted through the medium, The most important protocols are: Ethernet (used in LAN), DOCSIS (for cable-modem networks) and xDSL (such as the ADSL).

3.2.2 Internet layer:

The protocols in this layer find paths to let any package reach its destination node. One of its function is to define how to identify the network nodes. To do it, it uses protocols like *IPv4* and *IPv6*.

3.2.3 Transport layer:

It divides the information that the upper layer (application), trying to send in small blocks called packets and, besides, makes sure that the packets arrive at the destination. The most important protocols of this layer are:

TCP: It is a connection oriented protocol that provides a reliable transmission of information using an unreliable channel.

- The applications that send and receive the packets are identified by their port numbers. Servers have fixed port numbers (the web server is port 80) but client programs can have a random port number.
- Each packet has a different sequence number. When a computer sends a TCP packet, the receiver sends a confirmation message with the same sequence number back to the sender.
- If a confirmation is not received after a predefined time interval, the sender will assume that its packet was lost, and it will send it again.
- The receiver will use the sequence numbers to sort the packets and build the original message again

UDP: It is a connection-less protocol useful for streaming.

- This protocol identifies the client and server computers using port numbers like TCP
- Unlike TCP, the computer that sends the packets does not wait for any confirmation from the computer that receives the packet. The receiver will ignore the packets with a wrong sequence number

📖 **Important:** This protocol is used when receiving the data in time is more important than receiving all the original data, so it is used to broadcast audio and video on the Internet. Nobody will care if a frame is lost from time to time while watching a video. However, if they are downloading a file and a packet is lost, the file will be corrupted, so this protocol is not used for data transmission.

3.2.4 Application layer

It handles the communication of user applications such as a web server and an Internet browser which are being executed in different machines. The most known protocols are:

- **HTTP**: to request web pages.
- **FTP**: to upload and download files.
- **SMTP, POP3, IMAP:** to send mails from server to server, download the email to an email client and to read the email directly from the server.
- **DNS**: to translate URL's (such as google.com) in IP addresses (such as 45.24.28.55).
- **DHCP**: to configure automatically the IP addresses of the computers in a given network.

A very simplified example of the operation of a communication between two computers (a client and a server) to make a request for a web page would be:

1. From the client's application layer of the client, the protocol and the URL of the page to be displayed are indicated.
2. This information is divided into small packages of the size required by the standard.
3. In the Internet layer, to each of these packets is added information regarding the IP address of the destination computer.
4. Finally, in the link layer, each one of those packets is converted into electrical impulses that are sent to the media.
5. In the server, the link layer receives those impulses and converts them into packets.
6. In the Internet layer of the server, the IP address of the packet is checked to test if this packet belongs to this computer
7. The packets with addresses that match the address of the server that are sent to the transport layer to join, forming the message. (Transport layer)

8. That message will be processed by the server application server to get the correct page. (Application layer)

4. INTERNET LAYER

Although all layers have their importance, in this course we will focus only on the internet layer, where it is done in addressing and routing of packets (datagrams).

4.1 IP Address

Each of the computers in a network have a unique IP address, or rather, in the same network there can not be two computers with the same IP address.

In fact, to speak properly, each of the network interfaces (each of the network cards) must have a unique IP address. For example, a computer with a wired and Wi-Fi network would have two interfaces and, therefore, would have two IP addresses associated with it.

4.2 The IP address format

An IP address is a 32 bits number grouped from 8 to 8. Each of the groups separated by a point. For instance:

10101010.10001101.11110000.00001111

or, in decimal mode

170.141.240.15

The number of numbers that we can represent with 8 bits is 2^8=256 (from 0 to 255), therefore, the range of IP addresses goes from 0.0.0.0 to 255.255.255.255.

4.3 Classes of addresses

Just as a postal address consists of several elements (street name, number, city, ...) an IP address is also composed of several parts, in this case, 2 parts:

- The network ID, that is, the part which identify the network
- The host ID, that is, the part which identify the computer (the interface)

The difference is that just in the postal address each element is clearly differentiated, but in an IP address the two parts are mixed and may not be obvious to locate them. In fact, in order to locate each of these parts, it has to use another number, with the same format as the IP address, called the *network mask.*

The network mask is a number that has 1 in the part of the IP address that belongs to the network and 0 in the part that identifies the computer. For example:

11111111.11100000.00000000.00000000

Performing an AND operation between the IP address and the net mask, we can locate the part of network identifier:

```
    10101010.10001101.11110000.00001111 -> IP (170.141.240.15)
AND 11111111.11100000.00000000.00000000 -> network mask (255.224.0.0)
    10101010.10000000.00000000.00000000  = 170.128.0.0  -> Network ID
```

As you can see, all the network masks make up a sequence of ones followed by a sequence of zeros. For this reason, it is quite common to define the mask only with a number that indicates the number of ones. This notation is called CIDR. For instance 170.141.240.15/11

Obviously, doing a NOT operation of the mask and performing an AND with the IP address, we can obtain the part that identifies the host.

```
    10101010.10001101.11110000.00001111 -> IP (170.141.240.15)
AND 00000000.00011111.11111111.11111111 -> NOT network mask (0.31.255.255)
    00000000.00001101.11110000.00001111 = 0.13.240.15  -> host ID
```

4.4 IP address classes

It is possible to classify IP addresses into 5 classes:

- **A class:** the first bit of the address is 0 (that is, the range goes from 0.0.0.0 to 127.255.255.255) and its network mask is "255.0.0.0" or "/8". For instance: 25.124.200.200
- **B class**: the first two bits of the address are 10 (that is, the address range goes from 128.0.0.0 to 191.255.255.255). The network mask is 255 255.0.0 or /16. For instance: 165.124.200.200
- **C class**: the first three bits of the address are 110 (that is, the address range goes from 192.0.0.0 to 223.255.255.255). The network mask is 255 255.255.0 or /24. For instance: 192.168.20.20
- **D class:** the first four bits of the address are 1110 (that is, the address range goes from 224.0.0.0 to 239.255.255.255).
- **E class:** the first five bits of the address are 11110 (that is, the address range goes from 240.0.0.0 to 247.255.255.255).

> ! **Attention:** D and E classes are very special because they are used for multicasting and research purposes.

It may seem shocking that in the previous section we have put an example whose network mask was /11, that is, a network mask that does not exist in any of the previous network classes. The explanation has two reasons:

- This classification is simply a formal classification, that is, no one prevents me, for example, in an isolated way that I can use an address that has the first bit to 0 (class A) with a network mask /12. But if I want to connect my network to other networks, it is very likely I had problems.
- These types of non-formal networks are created internally to divide a network into other networks and gain efficiency and security. We will see it in the subnettig section.

4.5 Public and private Addresses

Such as an IP address is defined, the possible number of devices connected to a network can be up to 256 * 256 * 256 * 256. This number, although it is very high, is already clearly surpassed in networks as Internet. That is why a first solution to be able to optimize the number of addresses available is to separate the addresses in public addresses and private addresses.

- Public addresses are which one that are unique and can not be repeated
- Private addresses are those that can not be used publicly, but internally, so that the same private address can be used by several computers from different organizations. In this way, if these addresses can be used by several computers, the number of possible devices connected to the Internet increases.

The ranges of private addresses are:

- **A class:** from 10.0.0.0 to 10.255.255.255
- **B class:** from 172.16.0.0 to 172.31.255.255
- **C class:** from 192.168.0.0 to 192.168.255.255

That is, if you want to use an internal IP address for your organization, you have to use one of them in function of the class that you are using. Otherwise, your IP can collide with any public address

But the question is: how can there be two equal directions in the same network? The solution is given by the use of techniques such as NAT, which we will talk about later.

4.6 Special addresses

Within a network segment, there is a set of special addresses, that have a specific function.

Loopback: Address 127.0.0.1 is used to make internal checks of the network interface itself.

> **Attention:** This address is associated with the name *localhost.*

> **Attention:** You might think that testing the IP address assigned to that NIC would be the same as using the loopback, but this is false. If the IP is used, the package leaves and comes back. In the case of the loopback, it does the internal tests.

Broadcast: Sending a packet to this address will get the packet to reach all the hosts on the network. It is calculated by setting to 1 all the bits of the host. For instance, the broadcast address of a network 170.141.240.15/11 is (red colour network ID, green colour host ID):

170.141.240.15/11 → 10101010.10001101.11110000.00001111 → 10101010.10011111.11111111.11111111 → 170.159.255.255 (broadcast address)

Gateway: It is not a specific address like the previous ones, but it is very important. Indicates the address of the device that will allow sending packets to the outside of the local network segment[1]. Usually the second network address is used as a gateway (the first is usually used as the network name), for instance 192.168.20.1

4.7 Subnetting

As mentioned before, the number of IP addresses is finite and not very large, so it is necessary to be efficient in its allocation. That means optimizing its use and to avoid wasting directions. For this, one of the techniques to use is the *subnetting*. The best way to understand the process is with an example.

Suppose that our IP address assigner provides the network ID 192.168.40.0/24 for our organization. This network is a private network of type C, so its network mask is 255.255.255.0 and therefore the number of possible hosts is 256 (from 0 to 255).

The organization has five departments. In each department, there are 30 devices that may require connection to the network. It could use the entire range of addresses (the 256) to distribute among all departments, but a better idea would be from the assigned network to create five networks, one for department. In this way would make a more optimal use of the directions and would also get five networks, which would improve the isolation, security and minimize possible traffic problems.

[1] In the next sections we will study what is a router and NAT

For this, the technique of subnetting is used. The process consists of including in the network address (in addition to the ID network and the host ID) another element, the subnet ID, which is obtained by "stealing" bits to the host ID

The process is:

1. We calculate the number of bits needed to represent the 5 networks. In our case, we want 5 networks, then 3 bits are needed ($2^3 = 8$).
2. We check that we have enough bits to address all hosts. In our case, the network mask is /24, so we have 8 bits for the host. Of them we are going to dedicate 3 to the subnet, reason why we have five bits free for each subnet. The host number will be $2^5 = 32$, greater than the 30 that is needed.
3. We calculate the addresses of the subnets (the first address of each subnet). For this, we perform all combinations of 0 and 1 on the bits stolen from the host, leaving the rest to 0

Net (192.168.40)	Subnet	Host	Subnet address
11000000.10101000.00101000.	000	00000	192.168.40.0
11000000.10101000.00101000.	001	00000	192.168.40.32
11000000.10101000.00101000.	010	00000	192.168.40.64
11000000.10101000.00101000.	011	00000	192.168.40.96
11000000.10101000.00101000.	100	00000	192.168.40.128
11000000.10101000.00101000.	101	00000	192.168.40.160
11000000.10101000.00101000.	110	00000	192.168.40.192
11000000.10101000.00101000.	111	00000	192.168.40.224

Attention: In our case, we only need the first 5 networks

4. We calculate the network mask of each of the subnets. This mask will be the same for all subnets. For this, we only add to the initial mask the number of bits we have stolen from the host. In our case, it will be 24 + 3.

Net (192.168.40.)	Subnet	Host	Subnet address
11000000.10101000.00101000.	000	00000	192.168.40.0/27
11000000.10101000.00101000.	001	00000	192.168.40.32/27
11000000.10101000.00101000.	010	00000	192.168.40.64/27
11000000.10101000.00101000.	011	00000	192.168.40.96/27
11000000.10101000.00101000.	100	00000	192.168.40.128/27

5. We calculate the range of addresses of each network, indicating the broadcast address (the last one) and the gateway address (the second one). In our case we have 5 bits to define the hosts, ($2^5 = 32$) host, therefore the range of addresses will go in blocks of 32.

Subnet	Range	Broadcast	Gateway
192.168.40.0/27	192.168.40.0 - 192.168.40.31	192.168.40.31	192.168.40.1
192.168.40.32/27	192.168.40.32 - 192.168.40.63	192.168.40.63	192.168.40.33
192.168.40.64/27	192.168.40.64 - 192.168.40.95	192.168.40.95	192.168.40.65
192.168.40.96/27	192.168.40.96 - 192.168.40.127	192.168.40.127	192.168.40.97
192.168.40.128/27	192.168.40.128 - 192.168.40.159	192.168.40.159	192.168.40.129

In figure 10 the drawing of the topology of the resulting subnets can be observed. For simplicity, only two hosts per subnet have been drawn

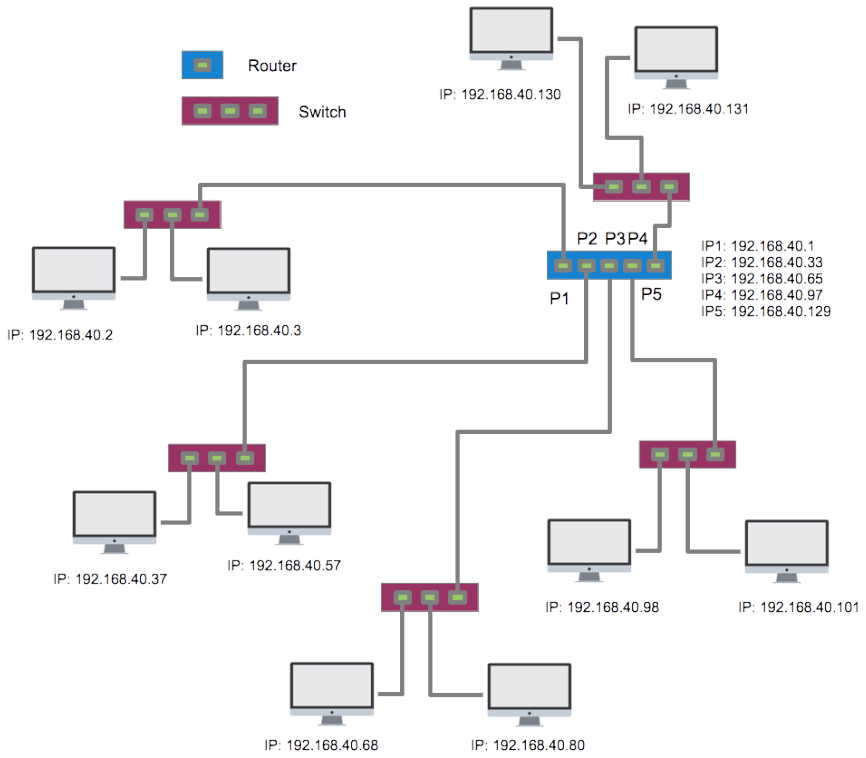

Figure 10 - Subnetting result

4.8 Routing

Routing is the technique that allows you to move a package from one computer to another, even if they belong to different networks. This process is performed by the router through so-called routing tables. In a very simplified way, this table is composed of 2 columns: target and interface

The target column refers to who will be the receiver of the package. It can be an IP, a network address or the default route (indicated with 0.0.0.0). The interface column refers to the interface of the router[2] through which the packet will have to be sent to that destination address. For instance, the router of the previous figure has the next routing table:

[2] A router is a device that has as many interfaces as networks interconnected.

Target	Interface
192.168.40.0	P1
192.168.40.32	P2
192.168.40.64	P3
192.168.40.96	P4
192.168.40.128	P5

4.9 NAT

Given the scarcity of IP addresses, the NAT technique allows the information to be transmitted from a public IP to private IPs and vice versa transparently for the user.

Thanks to this technique, from a public address, the user can configure the private network (with private IP addresses and subnetting) as large as desired. The router is responsible for adding information about the public IP and an indicator to which of its local hosts it sends to the packet that goes to the external network. The response to that packet will arrive at the router that will be in charge of directing it to the corresponding local host.

4.10 IPv6

Even with techniques such as subnetting and NAT, the number of devices continues to grow, and IP addresses are running out. To resolve this problem, the organizations have created several solutions to the problem. One of these solutions is IPv6. Unlike IPv4, which uses 32-bit addresses, IPv6 uses 128-bit addresses, which offer enough IP (2^{128}) addresses.

In this case, the notation is based on hexadecimal numbers grouped in blocks of 16 bits (from 0000 to ffff) separated by:. The zeros to the left in each group can be deleted and a set of zeros can be replaced by: :: only once per address.

For instance, the IPv6 address:

de34:0000:0000:0000:045e:0000:0000:0ffa

To simplify, it would be as:

de34::45e:0:0:ffa

As in the traditional (IPv4) format, the address stores the network ID as well as the host ID. The only difference is that in IPv6 the network is always identified by the first 64 bits, while the host does it with the last 64.

Network ID: de34::
Host ID: 45e:0:0:ffa

5. HARDWARE NETWORK COMPONENTS

5.1 Network Interface card

The network interface card (NIC) is the hardware component that connect the computer with the media. All devices connected to a network must have at least one[3]. There are two types, wired and wireless.

> ! **Attention:** It works in the link layer

[3] Each of them connects a different network

It is physically identified by ID called the MAC address (Media Access Control), a unique number that is assigned by the manufacturer and that is independent of the protocol stack to be used. An example could be 00:35:AA:28:5F:69

📖 **Important:** Today the importance of network connection is so great that most devices have one (computers, mobiles, printers, televisions ...)

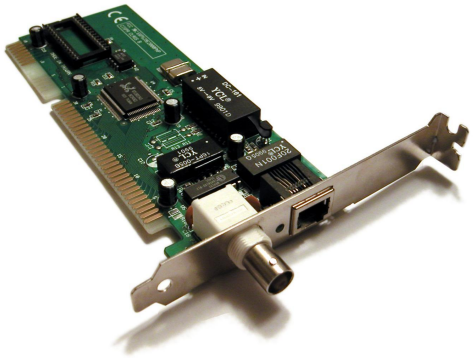

Figure 11 - NIC

5.2 Media

❕ **Attention:** They work in the link layer

5.2.1 Guided media

They are those in which the medium guides the signal. There are three types: twisted pair, coaxial and fibre optical.

Twisted pairs

They are formed by two copper wires. They are twisted to avoid interferences. There are 3 types:

- ***UTP (Unshielded Twisted Pair)***: They don't have any extra protection against interferences.
- ***FTP (Foiled Twisted Pair)***: It has a single protection mesh that covers all twisted pairs.
- ***STP (Shielded Twisted Pair)***: Each pair has an independent conductive cover that is connected to the grounding of the computer and improves protection against interferences.

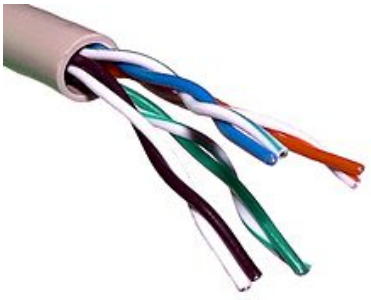

Figure 12 - UTP

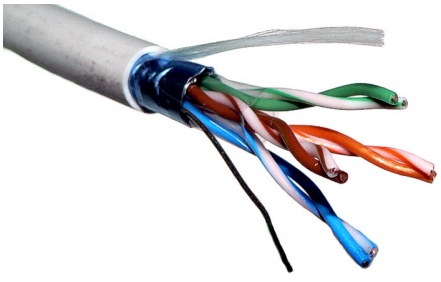

Figure 13 - FTP

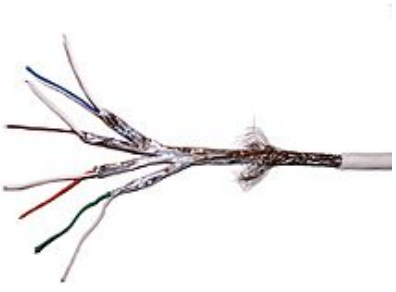

Figure 14 - STP

📖 **Important:** Actually it is possible to find more types of cabling like S/UTP, S/FTP, S/STP or F/UTP. These name indicates the type of shield that covers all the wires, being F foiled and S braided[4].

In addition, these types of cables are also classified by categories, from 1 to 7 depending on the quality of the same: to more quality greater distances and higher speed, but, obviously, more expensive.

There are two types of connectors associated with this type of media, RJ-11 (used in telephone and xDSL connections) and rj-45 (used in Ethernet networks)

Figure 15 - RJ-11 and RJ-45

Coaxial

Widely used in MAN networks (although it is increasingly being replaced by fibre optics). It has a central conductor which transports the electrical signals, an external conductor which works as a shield protecting the inner conductor against interferences and a dielectric isolating both wires.

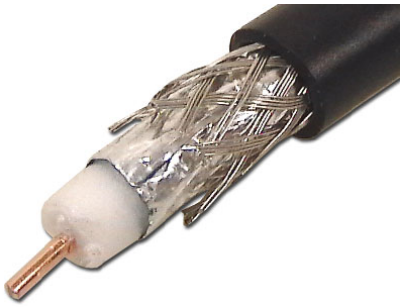

Figure 16 - Coaxial

Figure 17 - BNC connector

The connector type used is called BNC.

Fibre optical

The electrical signal is replaced by light signals emitted by a laser, which makes them immune to electromagnetic interference. They are composed of a jacket (a cover that isolates from external light), strength members (added to the fibre optic cable to prevent the breakage of the fibre glass during installation), cladding and a core.

[4] The braided shields offer better protection than foil shields.

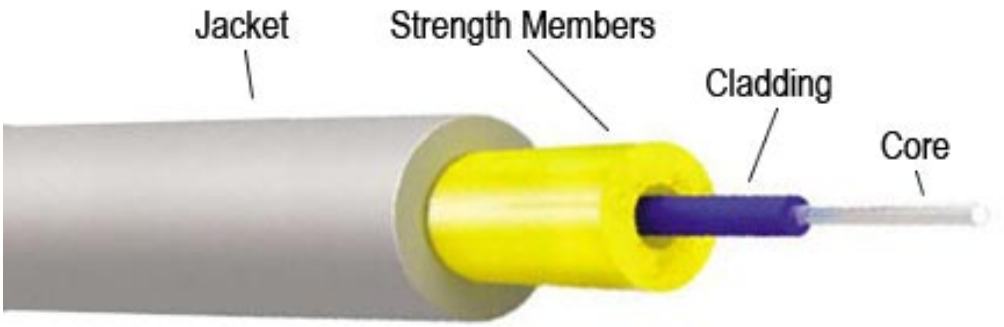

Figure 18 - Coaxial

There are a lot of connectors: FDDI, LC, FC, SC, etc.

Figure 19 - FC connector

Figure 20 - FDDI connector

5.2.2 No guided media

The information is sent by electromagnetic signals that are propagated by air or in the space.

Its great advantage is the ease of installation and its scalability. On the other hand, its main drawback is that they are very affected by the atmospheric conditions and that its speed is much smaller than in the guided media.

Microwaves

Typical examples are Wi-Fi and Bluetooth, which work at frequencies around 2.4GHz, TV broadcasts work in the range from 50MHz to 900MHz or Cellphones work at the frequencies of 900MHz, 1800MHz and1900MHZ

Infrared signals

They are designed for communication between devices very close to each other and are very much affected by external light. Typical examples are remote controllers for TV.

5.3 Modem

Modem is an acronym for **MO**dulator/D**EM**odulator. When the signal is sent through a medium to travel long distances, it has to be modulated[5]. When this signal reaches the receiver, the reverse process must be performed, that is, it must be demodulated.

In general, it is the device that allows the connection of our LAN with the WAN or MAN that provides the service. In this way and depending on the type of connection, there are, for example, cable modem, ADSL modem, telephone modem, etc.

> ! **Attention:** It works in the link layer

[5] https://en.wikipedia.org/wiki/Modulation

5.4 HUB

A Hub is a device with several connection ports and whose task is to forward the packet received by one of the ports to the rest, previously amplifying it. Although they are now being replaced by switches, they have been widely used since their use allowed the creation of Ethernet network segments[6].

> **Attention:** If works in the link layer

Its biggest problem is that, even if the sender is only a computer, the information is sent back to everyone, therefore, the traffic increases and the speed decreases. Besides, all the network cards in the segment have to work at the speed of the slowest one.

5.5 Switch

A switch is an intelligent HUB. The switch stores a table with the MAC address of the computer connected to each port. When a packet (message) is sent from a computer to another, the switch re-transmits the packet only to the destination port. The advantages of a switch compared to a hub are that it avoids unnecessary packet replication and helps to reduce the network traffic and increases the speed, and besides each device can work at a different speed.

Externally a hub and a switch are very similar, in fact can only be differentiated by the label itself.

Figure 21 - HUB

Figure 22 - Switch

> **Attention:** Although it has some intelligence, it works at the link layer level, since it does not modify or redirect the package, it only "opens or closes the door" depending on its address.

5.6 Router

A router is a device much more intelligent than a switch. It works on the Internet layer, so it understands IP addresses. So, it can determine the path that a packet must follow to reach a computer that is not included in any segment of the local network. That is, the router is able to decide whether the packet is directed to a computer in the local network or to one of the external network and to route it correctly (adding the necessary information to the packet so that the recipient knows who to respond to). To do it, it has at least two NIC connected to different networks (local and external).

[6] Two or more computers can not be connected in a tree if at least there is no central element, which was either a computer with multiple NICs or a hub, much cheaper

Figure 23 - Router

📖 **Important:** Note that the MAC address is a data that comes from the factory, while the IP address is a data that is assigned to the NIC depending on how it is connected to the network. The MAC will always be the same, the IP can change.

📖 **Important:** It is very common that in a home environment, the modem and the router (and even the switch) are together in the same component.

6. BIBLIOGRAPHY

[1] Computer networks. S. Tanenbaum Andrew. Pearson. 2010