-

UD 09. NETWORK ARCHITECTURE AND COMPONENTS

Computer Systems
CFGS DAW

Borja Salom
b.salomsantamaria@edu.gva.es
2022/2023

Version:230126.1040

Licence

Nomenclature

Throughout this unit different symbols will be used to distinguish important elements within the content. These symbols are:

 Importante

 Atención

 Interesante

TABLE OF CONTENTS

UD09. NETWORK ARCHITECTURE AND COMPONENTS

1. Characteristics of computer networks.

Networks are everywhere, and computer networks are part of the increasingly widespread global connection system known as the Internet. As a future professional in the IT sector, one of the things you should know is: how computers work, and how they are connected to each other to form larger systems that, in most cases, use networks of different characteristics.

In this work unit you will see the principles of computer networks, to later be able to apply them.

We define a computer network as two or more devices connected to share the components of their network, and the information that may be stored on all of them.

If we take the definition given by Andrew S. Tanenbaum as a reference, a computer network is a set of computer equipment connected to each other by means of physical devices that send and receive electrical impulses, electromagnetic waves or any other means for the transport of data, with the purpose of sharing information and resources.

This last definition is the one that will serve as a starting point for the development of the work unit, since, as you will see, in order to work with computer networks we need to know the most used communication systems, the architecture that makes them possible, the associated protocols, the way to connect them and their components.

Although in the development of the unit we will see different characteristics of computer networks, and we will give a broader explanation, it is convenient to start by citing some of the most important, and that have contributed to its generalization:

- **Connectivity:** the possibility of connecting different devices with each other in order to share own or external resources, both in local and remote environments.
- **Scalability:** a computer network can easily expand its possibilities, in addition this network can connect with other networks, and thus provide greater benefits.
- **Security:** this characteristic is desirable and necessary, although it is not always taken care of enough. In some cases, networks increase security against data loss, since they duplicate information, and in other cases, they decrease the security of that data, since it is more available. It is convenient to consider this characteristic as one of the most important.

- **Cost optimization:** if we can share resources, and these resources give us greater productivity, in addition to making our work easier, we are optimizing costs and getting a better return on our investment.

1.1 Communication system.

According to the Dictionary, system, in one of its meanings, is the set of rules or principles on a subject rationally linked to each other. In this same dictionary we can search for the word communication, and we find that it can be defined as the transmission of signals by means of a common code between the sender and the receiver.

Therefore, we can define a communication system as a set of elements that, following certain rules, intervene in the transmission of signals, allowing the exchange of information between a sender and a receiver.

From this definition we can infer the components of a communication system, which will be:

- **Transmitter:** element that transmits the information.
- **Receiver:** element that receives the information.
- **Channel:** means by which information is transmitted, using properly coded signals.

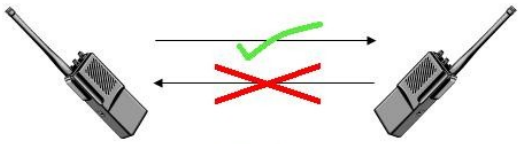
As we can deduce, it is necessary for the sender and receiver to encode the information in such a way that both understand each other, therefore they need to create a set of rules that regulate the communication between them, this set of rules is what we know as communication protocol.

Considering that the transfer of information between sender and receiver is carried out through of the communication channel, we can define the latter as the physical means by which transports the information conveniently encrypted, following established protocols.

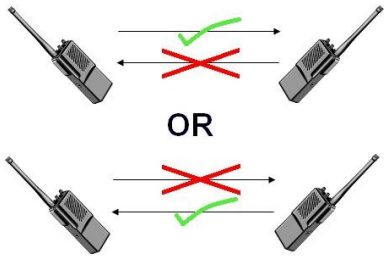
Thus we can classify communication systems according to different points of view. If we take into account the transmission medium, we can have online or wired systems and wireless systems.

On the other hand, if the criterion we use is the directionality of the transmission, communication systems can be classified as:

- **Simplex:** When the communication is carried out in only one direction. Sender emits, receiver receives. Example: When we listen to music on the radio, we only receive.



- **Semiduplex (half duplex):** When communication is carried out in both directions, but not simultaneously. Emitter emits, receiver receives, receiver becomes emitter, and emitter becomes receiver. Example: Talking on the walkie-talkie.



- **Duplex (full duplex):** When communication is carried out in both directions simultaneously. Both are emitters and receivers at the same time. Example: Computer networks often work this way.

Other criteria used to classify communications are:

- According to the way of synchronizing the signals: thus we have synchronous and asynchronous communications.
- According to the nature of the signal: this criterion leads us to use the terms of analog and digital communications. This last classification is more used in the field of communications, so for us it will be more appropriate to talk about analog or digital transmissions. This is so because computers are systems that are based on the use of digital signals.

In addition to these criteria, there are also two concepts related to communications that we must know, one of them is the term Data Terminal Equipment (ETD), which will be all the equipment, whether they are transmitters or receivers of information. The other term is that of Data Communication Equipment (ECD) which is any device that participates in the communication but that is neither the original sender nor the final receiver.

1.2 Computer networks.

Computer network or computer network: it is a set of computer equipment connected to each other by means of physical devices that send and receive electrical impulses, electromagnetic waves or any other means for the transport of data with the purpose of sharing information and resources.

The main purpose for creating a computer network is to share resources and information, ensure the reliability and availability of information, increase the speed of data transmission and reduce the overall cost of these actions.

If we connect two computers to each other we already have a network, if we connect more computers, add printers, and connect to devices that allow access to the Internet, we are getting our network to grow and have more resources, since the Individual resources can be shared. This is the main idea of networks, since as we connect more devices and they share their resources, the network will be more powerful.

Therefore, the main advantages of computer networks will be:

- ✔ The possibility of sharing resources.
- ✔ The possibility of sharing information.
- ✔ Increase the possibilities of collaboration.
- ✔ Facilitate centralized management.
- ✔ Reduce costs.

If we analyze some of these advantages, it is clear that using computer networks to work is better than doing it in isolation.

When it comes to sharing resources, most of us have the Internet connection in mind. It is obvious that a single shared Internet connection is cheaper than having one connection for each computer. This has been one of the main reasons why computer networks have been so successful. But we must not forget other no less important resources, such as the use of shared peripherals such as: printers, network hard drives, scanners, etc. In this section of shared resources, we should also mention the possibility of sharing software. Shared software is growing, and in some work environments it is essential.

Related to the possibility of sharing resources, we have the possibility of sharing information. In this way we will be able to use shared databases, documents that can be read, and even elaborated by several different users.

The latter links with another of the advantages, which is the possibility of collaboration. When we share resources and information, the possibilities for collaboration increase. In addition, this collaboration can occur between people who are in the same office or institute, but it can also occur between people who are so far apart that they do not even get to know each other. The latter is very fashionable; Surely you have heard of the concept of cloud computing to refer to the possibility of offering computer services over the Internet. This concept is closely linked to the use of computer networks and the Internet.

Regarding the centralized management of resources, comment that it improves the security of the systems, It usually optimizes network performance and is cheaper.

Finally, we can say that the main objective of any association, corporation or person is that when making an investment, it is not excessive. If a good planning of the network is carried out, and a good design of it is made, surely implementation and maintenance costs will be reduced.

1.3 Network classification

Networks can be classified according to different concepts, we will focus on the most used concepts.

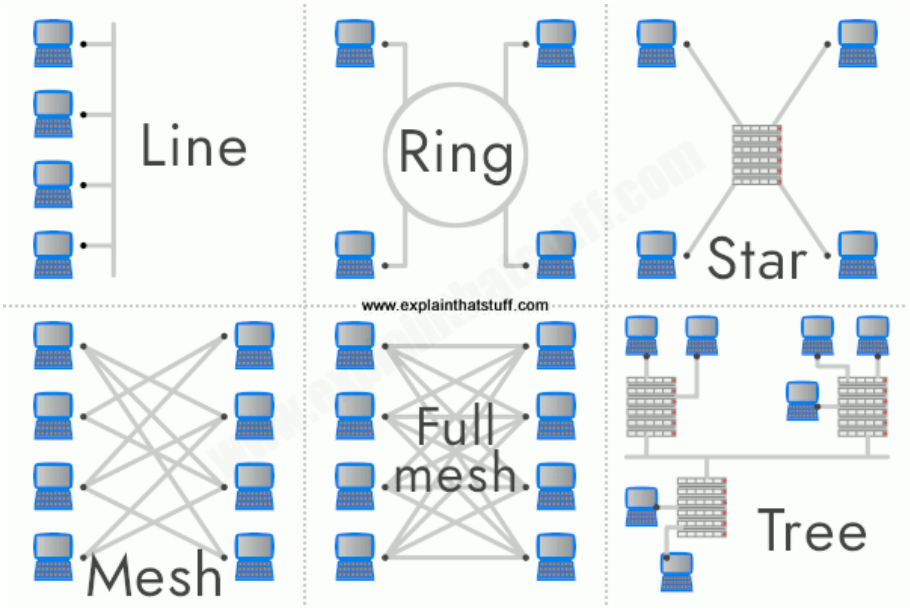
By scope or extension we have:

- **Personal area network or PAN (personal area network)** is a computer network used for communication between computer devices near a person.
- **Local area network or LAN (local area network)** is a network that is limited to a special, relatively small area, such as a room, a classroom, a single building, a ship, or an airplane. Local area networks -6-Developing Web Applications Topic 3 tend to have the highest speeds, and are considered the essential building block for the creation of larger networks.
- **A campus area network or CAN** is a computer network that connects local area networks throughout a limited geographic area, such as a college campus or military base. This term is usually used as an extension of LAN, since what you really have are local networks connected to each other to cover a larger area.
- **Metropolitan area network or MAN (metropolitan area network)** is a high-speed network (broadband) that provides coverage in a large geographical area. This concept is used to define networks that cover relatively large extensions, and that need additional resources to those that a local network would need.
- **Wide area network or WAN (wide area network)** are computer networks that extend over a large geographical area. Within this classification we can find the telecommunications networks that allow the use of the Internet, and the Internet itself, which can be considered as a gigantic WAN network.

Según las funciones de sus componentes:

- **Peer-to-peer or peer-to-peer networks**, also known as peer-to-peer networks, are networks where no computer is in charge of running the network. Each computer controls its own information and can function as a client or server as needed. The most used operating systems include the possibility of working in this way, and one of its most outstanding characteristics is that each user controls their own security.
- **Client-server networks**, are based on the existence of one or several servers, which will serve the rest of the computers that are considered clients. This type of network facilitates centralized management. To create networks of this type we need server-type operating systems, such as Windows 2008 server or GNU-Linux. It should be noted that in principle any Linux distribution can act as a server, although there are distributions specially recommended for this purpose, such as Debian, Ubuntu server, Red Hat enterprise, etc.

The way to connect the computers gives us another widely used classification, which is what is known as topology. In this section we will only cite some topologies since in this unit we will dedicate a section to explain them in more detail. Among the connection topologies we can cite: bus, ring, star, tree, mesh, double ring, mixed and fully connected.



Depending on the type of connection we can have:

- **Wired networks:** In this type of network, different types of cables are used to connect computers, later we will study what is related to the most used types of cables.
- **Wireless networks:** These are networks that do not need cables to communicate, there are different wireless technologies that we will study later.

Another interesting classification is taking into account the degree of diffusion, in this classification we distinguish two types of networks:

- **Intranet** is a computer network that uses some network technology for commercial, educational or other private use, that is, it does not share its resources or information with other networks, unless they authenticate, or comply with certain measures certain security.
- **The Internet** is a decentralized set of interconnected communication networks that use the TCP/IP family of protocols, guaranteeing that the heterogeneous physical networks that comprise it function as a single, worldwide logical network. It is precisely this characteristic that has made the use of the Internet more widespread and that all networks work using TCP/IP protocols.

1.4 WAN networks

We have seen that WAN networks (wide area networks) are computer networks that extend over a large geographical area. Within this classification we can find the telecommunications networks that allow the use of the Internet, and the Internet itself, which can be considered as a gigantic WAN network.

WAN networks are capable of covering distances from about 100 to about 1000 km, providing service to a country or a continent. An example of this type of network would be the Internet or any network with similar characteristics.

There are WANs built by and for a particular organization or company and are for private use, others are built by internet providers (ISP) to provide connection to their customers.

Today, the Internet provides high-speed WAN, and the need for private WAN networks has been drastically reduced, while virtual private networks that use encryption and other techniques to make that network dedicated are continually increasing.

Usually the WAN is a point-to-point network that uses packet switching. WAN networks can use satellite or radio communication systems.

WAN networks base their operation on switching techniques. We can define switching techniques as the way in which one user and another establish communication. These techniques are:

- **Circuit switching:** it consists of the establishment of a physical link for the transmission between two nodes, which will be released when the communication ends in the case of using a switched network, or will remain if a dedicated network is used (Example: data transmission to through the switched telephone network).
- **Message switching:** it is a method based on the treatment of blocks of information, endowed with a source address and a destination address, in this way the network stores the messages until verifying that they have correctly reached their destination and proceed to retransmission. or destruction. It is a technique used with the telex service and in some of the email applications.
- **Packet switching:** consists of dividing the message into packets. Communication between two computers involves the transmission of packets. Each packet is sent from one node on the network to the next node. When the receiving node fully receives the packet, it stores it and re-broadcasts it to the following node. This process is repeated until the packet reaches the final destination. Two types of techniques have been defined for the use of packet switching: datagrams and virtual circuits. The Internet is a datagram-based packet-switched network.

Wide area networks are usually supported by public telecommunications networks that are the ones we all know and that we usually use to connect to the Internet. Examples of these networks will be:

- The basic telephone network or switched telephone network (RTB or PSTN)

allows us to talk on the phone, but if we use a modem we can transmit data at low speed.

- The asymmetric digital subscriber loop, better known as ADSL, telephone operators offer the possibility of using a data line independent of the telephone line, taking advantage of the available bandwidth above that required by the telephone service up to the limit allowed by the line itself.
- Mobile telephony through UMTS or 3G telephony, provide the possibility of transferring both voice and data (a telephone call or a video call) and non-voice data (such as software downloads, email exchange, and instant messaging).
- Internet by cable, using cable modems or routers, cable networks offer the possibility of using fiber optic cable combined with coaxial cable, to give high speed Internet access.

2. The network architecture.

When we talk about network architecture, we may think about how the network is built, the cables, the equipment, etc. But it is not like that, the concept of network architecture is broader and includes issues related to the hardware and software of a network.

Before defining the concept of network architecture, it is convenient for you to understand that one of the most important problems when designing a network is not that the computers connect with each other, but rather that these computers can communicate, understand each other, share resources , which, after all, is what we want. For this we have already mentioned that communication protocols are needed. Due to the complexity involved in considering the network as a whole, it was considered opportune to organize the networks as a series of layers, where each layer would take care of some function. In this way, the complexity of network design and of the applications used in it would be reduced.

Therefore we can define network architecture as the set of layers or levels, along with the protocols defined in each of these layers, that make it possible for a computer to communicate with another computer regardless of the network in which it is located.

This definition implies that the specification of a network architecture must include enough information so that when a program is developed or a device is designed, each layer responds appropriately to the appropriate protocol.

From all this we can conclude that the network architecture will have to take into account at least three important factors such as:

- The way in which the nodes of a network are connected, which is usually known as topology, in addition to the physical characteristics of these connections.

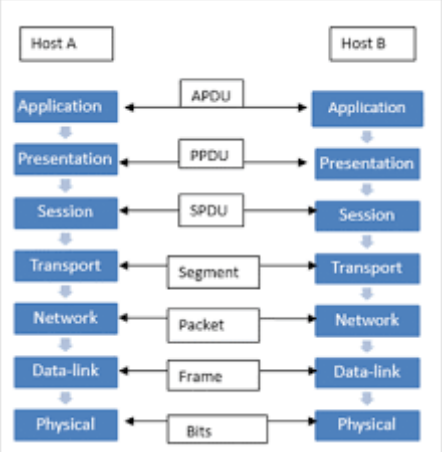
- The way to share information on the network, which in some cases will require choosing a method of access to the network and some rules to avoid loss of information.
- Some general rules that not only promote communication, but also establish, maintain and allow the use of information, these rules will be the communication protocols.

Next we will study in more detail how the architectures based on levels work, the protocols and most importantly, we will see the two most important models in the development of networks, the OSI reference model and the TCP/IP protocol stack, which we can Consider it as the base architecture for Internet communications.

2.1 OSI model and TCP/IP protocols.

We have already commented previously that the network architecture was divided by levels or layers to reduce the complexity of its design. This division by levels implies that each one of these levels has associated one or more protocols that will define the communication rules of the corresponding layer. For this reason, the term protocol stack or protocol hierarchy is also used to define the network architecture that uses certain protocols. We will see this more clearly when we explain the TCP/IP protocol suite.

But how does a tier-based architecture work? In order to explain this we will use different graphics that we believe can better illustrate the explanation.



In the above graphic, we can see the schematic of a seven-tier network architecture. We can see two computers that will have the architecture implemented, as we have seven levels, each level will have its protocols, so we can say that communications between equal levels is done through the corresponding protocols. But the actual flow of information, with the data that we want to transmit, will go from one computer to another, passing through each of the levels. This implies that in reality the data is not transferred directly from one layer to another of the same level, but that each layer passes the data and control information to the adjacent layer. In this way, the information will go

through all the layers, it will be transferred to the appropriate transmission medium and later the same thing will happen, but in the opposite direction, in the other computer. In this way, the information will reach its destination and each level will only deal with the data and control information it needs, according to the protocol used, without worrying about what the other levels do or need.

It is worth mentioning that with this way of working, each layer has some assigned services, in addition the layers are hierarchical and each one has some functions, in this way the levels are independent from each other, although the necessary data is passed from one to another.

In order to do this, the adjacent layers have what is called an interface. In this context, the interface will define the operations and services that the lower layer offers to the upper one.

When designers, designers, or manufacturers want to make compatible products, they must follow the network architecture standards, for this it is important to define clear interfaces between levels and that each level has its services well defined.

All of this implies that for the proper functioning of the network, certain rules must be respected, such as: that the services are defined by means of standard protocols, that each level only communicates with the upper or lower level, and that each lower level provides services. to its higher level.

It should be noted that this type of architecture by levels implies that each level generates its own set of data, since each layer passes the original data together with the information that it generates, in order to control the communication by levels. This information for the lower levels is treated as if it were data, since it will only be used by the corresponding level of the destination computer. Later we will see the different names that these data have depending on the architecture used.

Finally, it should be noted that layer-based network architectures facilitate compatibilities, both software and hardware, as well as future modifications, since it is not necessary to change all the layers when we want to improve the system. It would be enough to modify the protocols by levels and we could achieve improvements in the system.

2.2 Communication protocol.

As we have seen previously, a communications protocol is a set of standardized rules for the representation, signaling, authentication, and error detection necessary to send information through a communication channel.

Among the protocols necessary to establish communication, we need protocols for:

- Identify the sender and the receiver.
- Define the medium or channel that can be used in communication.
- Define the common language to be used.

- Define the form and structure of the messages.
- Set the speed and timing of messages.
- Define the encoding and encapsulation of the message.

The protocols used in the networks are adapted to the characteristics of the sender, the receiver and the channel, in addition the protocols must define the details of how to transmit and deliver a message.

If we focus on computer networks, we can define some issues that network protocols must resolve, these issues will be:

Routing: In computer networks there can be different routes to reach the same destination, therefore one of them must be chosen, it being desirable that the best or fastest one is always chosen. Therefore, network architectures must have protocols that serve this purpose, we will see what they are and at what level it is resolved.

Addressing: Since a network is made up of many nodes connected to each other, there must be some way of knowing which is which. For this we need to define network addresses that allow us to determine which computer I want to connect to or where I must connect to reach a destination. In order to achieve this, network architectures define addressing protocols, from a logical and physical point of view, which are defined at appropriate levels so that communication is possible and duplication does not occur.

The need to share a means of communication: It may be the case that the same means of transmission is shared, therefore mechanisms must be established to control access to the medium and the order in which it is accessed.

Saturation: Protocols of any level must be able to prevent the receiver of the message, or the intermediate devices that act in the transmission of the message, from being saturated. This is usually a problem, and it is not always easy to solve, but a good design and the adaptation of the network to the needs help.

Error control: It is desirable that network protocols have error control mechanisms. As we will see when we analyze network architectures, this control can be done from different points of view and at different levels.

We have mentioned some issues, but it is clear that the protocols solve many more, the important thing to keep in mind is that thanks to some standardized protocols, and a good network design, we can get computers from all over the world to communicate with each other.

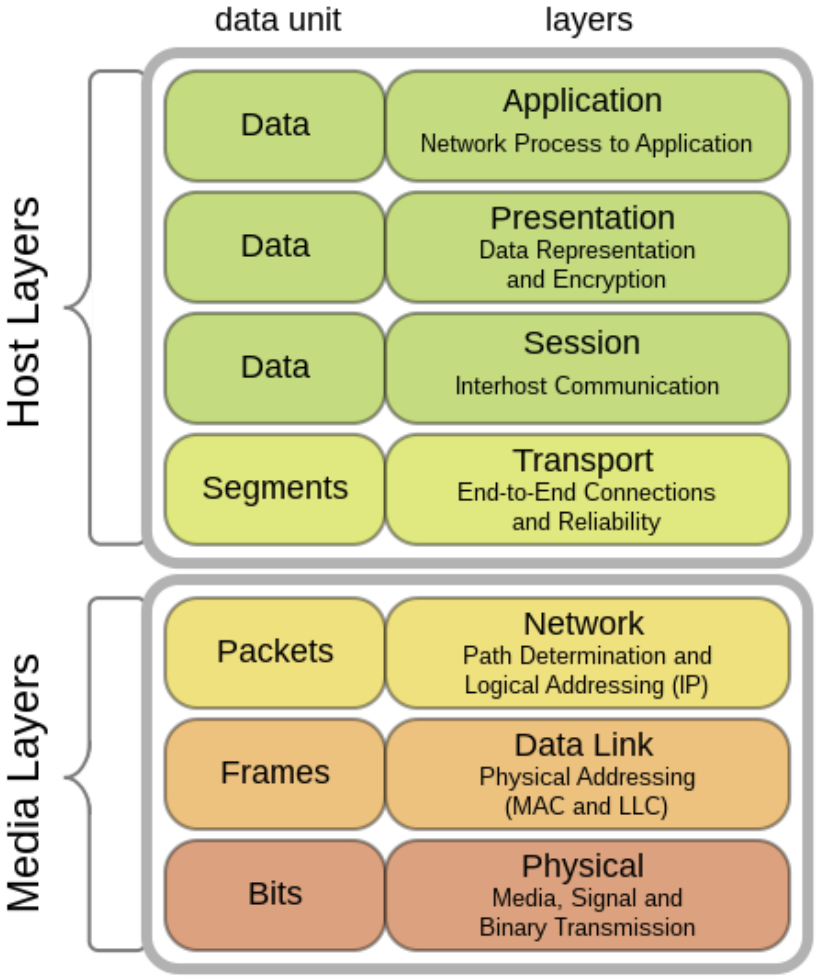
2.3 Operation of a level-based architecture.

The OSI model, acronym in English for Open System Interconnection or translated, Open Systems Interconnection, is the network model created by the International Organization for Standardization (ISO) in 1984. This model defines a reference framework for the definition of interconnection architectures of communication systems. It should be noted that the OSI model simplifies

network activities, since it groups communication processes into seven layers that perform different tasks. It is convenient to take into account that the OSI model is not an architecture developed in any system, but a reference to develop network architectures, so that the protocols that are developed can be known by all.

Although the OSI model is not really developed in any system, it is convenient to know and apply it, since it helps us to understand the communication processes that occur in a network, and it can also be used as a reference to perform error detection or a maintenance plan.

The graphical representation of the OSI model is usually done as a stack, where application layer 7 would be at the top and layer 1 or physical at the bottom.



It is convenient to mention that sometimes reference is made to the fact that layers 1, 2 and 3 of the model are related to hardware and layers 5, 6 and 7 are related to software, layer 4 being an intermediate layer between hardware and software. . This is usually the case because the devices and network components usually work at levels 1 to 3, with the programs working at the higher levels.

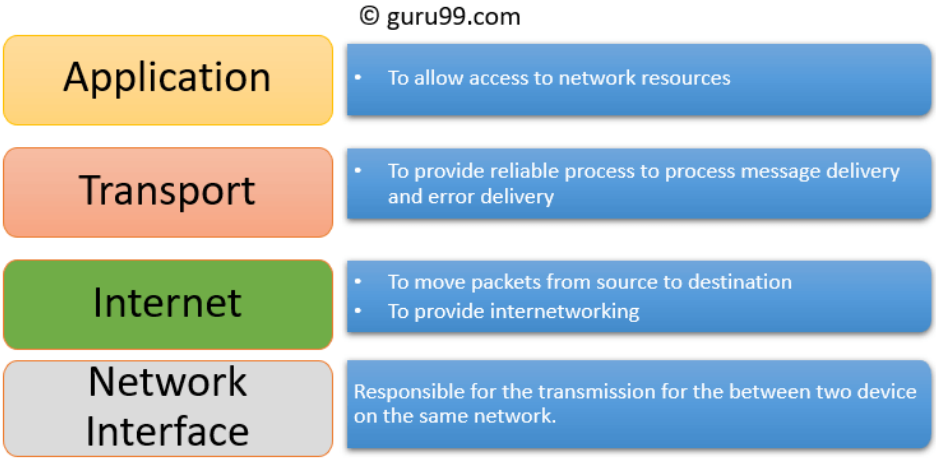
2.4 TCP/IP

When talking about TCP/IP protocols, one is actually referring to the network architecture that includes several network protocols, among which two of the most prominent are the TCP protocol (Transmission Control Protocol) and the protocol IP (Internet Protocol).

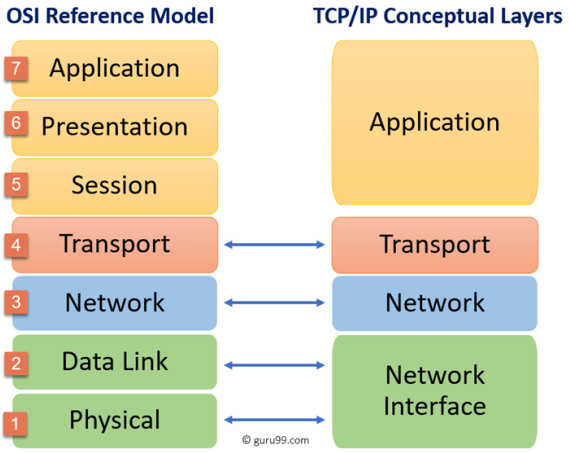
Therefore, it would be convenient to consider this model as an architecture in itself, being the most widely used, since it is the basis of Internet communications and modern operating systems.

When we refer to the TCP/IP architecture or TCP/IP model, we are referring to a set of general rules for the design and implementation of network protocols that allow computers to communicate. As we will see in more detail during this unit, there are protocols for different types of network services.

The TCP/IP architecture is composed of four layers or levels that are:



A comparison of this architecture with the OSI model can be seen in the following graph.



The TCP/IP architecture is structured in hierarchical layers and is used on the Internet, so in some cases you will hear about the Internet Protocol Family referring to this architecture when working on the Internet.

It should be remembered that in some cases the network access layer is divided into a hardware or physical layer and a data link, so that the architecture would have five levels instead of four. This is usually done in reference to the OSI model. Actually this can be done and would not change the structure of the architecture.

2.5 The level of access to the network.

The TCP/IP architecture in its original standardization did not care too much about the physical level itself, in fact, at first it only cared about standardizing the protocols related to the data link, hence the name of this level.

Subsequently, with the rise of networks of all kinds, it was seen that the standards that already existed from a physical point of view, increasingly had to be taken into account, and for this reason some authors, developers and designers consider that the TCP architecture /IP actually consists of five layers, with the first being the physical or hardware layer and the second being the data link layer, as recommended by the OSI model.

For us it is enough to consider it as one, as referred to in RFC 1122, a document that defines the TCP/IP model.

The main function of this level is to convert the information provided by the network level into signals that can be transmitted by the physical medium. The inverse function is to convert the signals that arrive through the physical medium into information packets that can be handled by the network level. At this level, issues related to physical connections must be taken into account, which in local networks are defined by the Ethernet standard. This standard defines the physical layer cabling and signaling characteristics, and the data link layer data frame formats. Ethernet is the basis for the IEEE 802.3 standard, which is an international standard that has potential for use in both local and wide area networks.

Another important aspect of this level is related to physical addressing. This concept comes from what is considered a sublayer of the data link layer, and is called media access control, whose acronym in English, MAC, is used to define what are known as MAC addresses.

The MAC address is a 48-bit identifier, usually represented as hexadecimal numbers, in a format of 6 blocks of two hexadecimal numbers, divided by colons. The format is as follows:

FF:FF:FF:FF:FF:FF

The 24 most significant bits (those on the left) determine the manufacturer and are known as the Organizational Unique Identifier, and the 24 least significant bits (those on the right) identify a specific interface. In this way no network card

has the same physical address.

At this level there is a protocol related to physical addressing. This protocol is ARP.

ARP stands for Address Resolution Protocol, this protocol works at the data link level and is responsible for finding the physical or MAC address that is related to the corresponding logical address, which, as we will see in the next section, corresponds to the IP address. What ARP does is translate logical (IP) addresses to physical (MAC) addresses. There is its inverse, RARP, which stands for reverse address resolution protocol, it does the inverse function of the ARP protocol but it is not widely used.

2.6 The internet or network layer.

The network layer of the TCP/IP model is considered the most important architecture layer, since it allows stations to send information to the network in the form of packets. These packets travel through the network independently, being able to cross different networks and without an established order. This is one of the main advantages of this architecture and that is why it is the basis of the Internet.

The main objective of the network layer will be to route the packets from the source node to the destination node.

In the TCP/IP architecture, the network layer is almost completely comparable to the network layer of the OSI model, but in the case of the TCP/IP architecture, the network layer is not concerned with the tasks of ordering the packets when they arrive. to his destiny. This is what is known as a connectionless service. When the packets are treated independently, each containing the destination address, it is said that the datagram technique is used, therefore the Internet is a datagram-based packet-switched network.

Among the functions of the network layer are:

- **Addressing:** Allows the unique identification of each node in the network. When we talk about addressing at this level, we are talking about logical addressing, to distinguish it from the physical addressing that we have already seen before.
- **Connectivity**: Getting the nodes of a network to connect, regardless of the network to which they belong.
- **Routing**: Also called routing, the protocols of this layer must be able to find the best path between two nodes.
- **Congestion control**: It is convenient to control the traffic, since if a node receives more information than it can process, saturation occurs and this problem can spread to the entire network.

To perform all these functions, the network level uses different protocols, among the most prominent protocols of this level we have:

- **IP**: Internet Protocol, or Internet Protocol provides connectionless routing of packets and is used by both the source and destination for data communication.
- **ARP and RARP**: They are also used in the data link layer and serve to relate IP addresses to MAC addresses and vice versa.
- **ICMP**: Internet Control Message Protocol, provides message sending and control capabilities. It is also considered a transport layer protocol, and tools such as ping and tracert use it to function.
- **OSPF**: It is a routing protocol that finds the shortest path between two nodes on the network.
- **RIP**: Routing Information Protocol, like OSPF, also seeks the shortest path, but using other routing techniques.

As can be seen, this level has several functions and several protocols, but we can say that the most important of all, in fact, gives its name to the architecture, is the IP protocol.

The IP protocol, in addition to what is mentioned above, also provides IP addresses. An IP address is a number that logically and hierarchically identifies an interface within a network that uses the Internet protocol. Later you will learn more about IP addressing, but now it is convenient for you to know that there are two versions: IPv4 (IP version 4) and IPv6 (IP version 6). They differ in the number of bits they use, version 4 uses 32-bit addresses and version 6 uses 128-bit addresses.

Example IP addresses are:

- IP version 4: 192.168.1.11 (Using decimal values).
- IP version 6: 2001:0DB8:0000:0000:0000:0000:1428:57AB (Using values in hexadecimal and can be simplified as: 2001:0DB8::1428:57AB)

2.7 The transport level.

It fulfills the function of establishing the rules necessary to establish a connection between two remote devices. Like the previous layers, the information that this layer handles has its own name and is called a segment.

Therefore, the transport layer must be in charge of joining multiple segments of the same data stream. Since the network layer in the TCP/IP architecture is not concerned with packet order or errors, it is at this layer that these details must be taken care of.

The transport level of the TCP/IP architecture is fully comparable to the transport level of the OSI model, therefore we can say that this level is responsible for the error-free transfer of data between the sender and the receiver, although it is not are directly connected, as well as maintaining the flow of the network. The task of this layer is to provide reliable data transport

from the source machine to the destination machine, independent of physical networks.

Several protocols work at this level, but the two most important are TCP and UDP.

TCP is a reliable, connection-oriented protocol, specifically designed to provide a reliable end-to-end stream of bytes over unreliable networks. That is why it is so useful on the Internet, since unlike traffic on a single network where we will know its characteristics, the networks that make up the Internet could have different topologies, bandwidths, delays, packet sizes, etc. But TCP has a design that dynamically adapts to the properties of these networks and allows connection in many types of situations.

UDP is a connectionless and unreliable protocol, this protocol provides everything necessary for applications to send encapsulated IP datagrams without having an established connection. One of its uses is in the transmission of audio and video in real time, where it is not possible to carry out retransmissions due to the strict delay requirements in these cases.

When an application process wants to establish communication with another remote application process, it must specify which one to connect to. The method that is normally used is to define transport addresses on which processes can listen for connection requests. These end points are called ports.

Therefore a port will be the transport addresses in which the processes can listen for connection requests. The term port is used on the Internet, the generic term is Transport Service Access Point, whose acronym in English is TSAP.

Port numbers are used by TCP and UDP to identify the sessions that different applications establish. Some ports are:

- **20**: FTP (File Transfer Protocol) data.
- **21**: FTP control.
- **53**: DNS (Domain Name Service).
- **80**: http (Protocol used to serve and download web pages)

2.8 The application level.

The application level contains the user programs (applications) that allow our computer to create texts, chat, read mail, visit web pages, etc.

This level includes all the high-level protocols that programs use to communicate.

In the TCP/IP architecture this level includes the session, presentation, and application levels of the OSI model.

Some of the application layer protocols are:

- **FTP**: Protocol used to transfer files between one computer and another.
- **DNS**: Domain Name Service, is the system used on the Internet to convert the names of network nodes into network addresses.

- **SMTP**: Simple text-based Mail Transfer Protocol used for exchanging email messages. It is based on the client-server concept, where a client sends a message to one or more servers.
- **POP**: Post Office Protocol, is used by mail clients to retrieve mail messages stored on a server.
- **SNMP**: Network Management Protocol, allows you to monitor and control network devices and manage settings and security.
- **HTTP**: Hypertext Transfer Protocol, is the protocol used in web page transactions. Defines the syntax and semantics used by web architecture software elements (clients, servers, proxies) to communicate. It is a transaction-oriented protocol and follows the request-response scheme between a client and a server. It has a secure version that is HTTPS.

Once we know the different levels of the architecture we can define the concept of socket. A socket is a connection that is formed by the union of the IP address plus the port that is used for the connection. Since each port is associated with an application, we can say that no two connections will be the same at the same instant of time. Example: 192.168.1.11:80, this means that the computer whose address is 192.168.1.11 is using port 80, which is associated with the application layer http protocol, therefore this may mean that the computer is visiting a web page or serving a web page. This concept will surely be useful to you later when you program web services or applications that use the Internet.

3. Network topologies and connection modes.

The network topology is defined as the communication chain used by the nodes that make up a network to communicate. Topology can refer to both the physical path and the logical path. Usually we will use topology from the physical point of view and therefore we will consider it as the way in which the computers of a network are connected. Among the connection topologies we can cite: bus, ring, star, tree or hierarchical, mesh, double ring, mixed and fully connected. When doing a network installation, it is convenient to make a network diagram that shows the location of each computer, each interconnection equipment and even the wiring. This is usually done using the plans of the building or plant, where the network is located and is a useful tool when it comes to maintenance and updating.

The logical topology or logical scheme, shows us the use of the network, the name of the computers, the addresses, the applications, etc. In these diagrams a group of computers can be represented with a single icon. In the next unit you will use these types of schemes.

As an example, we show you a graph that shows a computer network that will have an Internet connection thanks to a router. The network is represented by an oval with the network address inside and the network name outside. This type of logical schemes can be more or less complex but they serve to give us

an idea of how a network is connected. There are programs that allow you to make these diagrams, but they can be done using any drawing program, as long as all the elements that are represented in the graphic are made clear.

If we take into account the physical topologies, they can also have more or less detail in their representation, but the fundamental idea is to show how the devices are connected from a physical point of view, as we will analyze later.

Another concept related to how to connect computers in a network is that of connection mode, this concept is related to wireless networks, it represents how computers can be connected to a network wirelessly. Two wireless connection modes are defined, which are:

- Infrastructure mode: Usually includes an access point.
- Ad-hoc mode: No access point required.

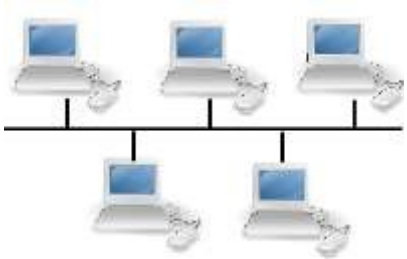
A little later we will see more details about these two connection modes. Just comment that these connection modes are used mainly in the design of wireless local networks or Wi-Fi networks.

Es conveniente que sepas diferenciar las topologías y los modos de conexión, las primera están más relacionadas con las conexiones físicas y el diseño, y las otras tienen relación con el diseño de redes inalámbricas.

3.1 Bus and ring

The bus topology uses a single backbone cable with terminations at the ends so that computers on the network connect directly to the backbone. The first Ethernet networks used this topology using coaxial cable.

Variants of the bus topology are currently used in cable television networks, in the trunk connection of fiber optic networks, and in the installation and operation of machines and industrial equipment used in production processes.

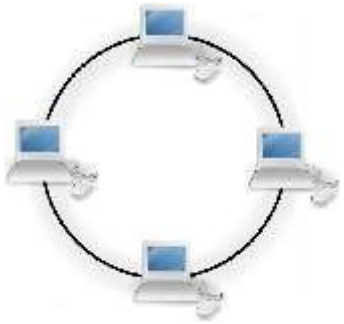


The ring topology connects each computer or node to the next and the last to the first, creating a physical connection ring. Each station has a receiver and a transmitter that acts as a repeater, passing the signal to the next station. In this type of network, communication is given by the passage of a token, in this way eventual loss of information due to collisions is avoided. Token-ring local networks use a ring topology even though the physical connection is star.

Dual ring topologies exist where two rings allow data to be sent in both

directions. This configuration creates redundancy (fault tolerance).

This topology is used in FDDI or Fiber Distributed Data Interface networks, in Spanish Fiber Distributed Data Interface, which can be used as part of a backbone network that distributes data over fiber optics. In some server configurations this type of topology is also used.



3.2 Star

The star topology connects all computers to a central node, which can be: a router, a switch or switch, or a hub or hub. Modern local area networks based on the IEEE 802.3 standard use this topology.

The central interconnection equipment channels all the information and all user packages pass through it. This central node will carry out distribution, switching and control functions. It is important that this node is always active, since if the entire network fails it will be without service.

Among the advantages of using this topology we have that this topology is fault tolerant since if a computer disconnects it does not harm the entire network, it also facilitates the incorporation of new computers to the network as long as the central node has connections, and allows preventing conflicts of use.

An extension of the star topology is the spanned star or tree where star networks are connected to each other.

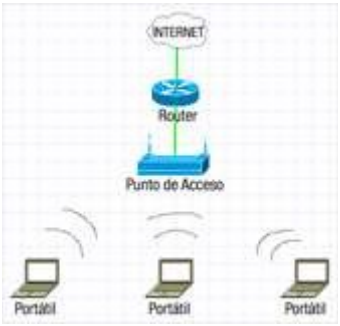
When the extended star has an element from which it starts, we will talk about the hierarchical star topology, where from star-connected networks we get a broader network that maintains a hierarchy of connections, since we have a node that is the beginning of the hierarchy. This node is usually a router and from it a local area network is created that allows services to be provided to smaller local area networks.

This type of topology is very typical in local area networks where the beginning of the hierarchy will be the router that connects to the Internet, usually the one provided by the telecommunications company, and the rest are the switches that serve different classrooms, rooms computers, offices, etc.

This topology has the advantage that from a single Internet connection, for example, we can provide service to several local networks or subnets, thereby saving costs. Its main disadvantage is precisely in the hierarchy, if the highest hierarchy interconnection equipment fails, the network no longer provides the services for which it was designed.

3.3 Infrastructure mode and ad-hoc mode.

As we have seen, there are several ways to connect computers in a network that we call topologies. These topologies, in principle, would serve as the basis for any type of local area network, whether wired or wireless. But in wireless networks that follow the IEEE 802.11 standard, a different concept is introduced, which is the connection mode.



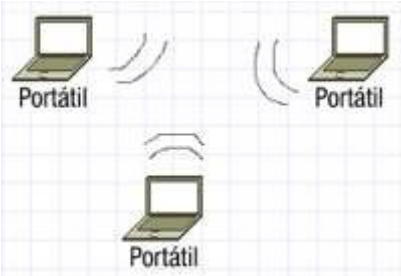
In wireless networks with the IEEE 802.11 standard, also called Wi-Fi networks, two connection modes are specified, which are infrastructure mode and ad-hoc mode. It is worth mentioning that sometimes you will hear about connection mode or connection topology in reference to the way of connecting wireless devices, and mode of operation referring to the operation of the equipment. In our case we prefer to use the term connection mode.

The infrastructure mode is usually used to connect wireless equipment to an

existing wired network, its main characteristics is that it uses an interconnection equipment as a bridge between the wireless and wired network. This interconnection equipment is called an Access Point and it can be equipment specially designed for this purpose that only performs this function, or it can be a router with access point characteristics. It is usually used as an access point to the cable infrastructure that allows the Internet connection, the wireless router installed by the telecommunications company.

In infrastructure mode, all wireless network traffic is channeled through the access point, and all wireless devices must be within the coverage area of the access point in order to establish communication between them.

Ad-hoc mode allows you to connect wireless devices to each other, without the need to use any equipment as an access point. In this way, each device on the network is part of a peer-to-peer network (Peer to Peer).



This type of connection allows information to be shared between computers that are in a certain place in a timely manner, for example a meeting, it can also be used to connect gaming devices to play with each other.

A third possibility is to combine both connection modes, to take advantage of both.

4. Components of a computer network.

At this point we will review some of the most important components that make up a computer network. As we have already seen, a computer network, or computer network, is a set of computer equipment connected to each other by means of physical devices that send and receive electrical impulses, electromagnetic waves or any other means of transporting data, with the purpose of sharing information and resources and offer services. This term also encompasses those technical means that allow the sharing of information.

Therefore, we can consider network components to be the computers themselves with their operating systems that allow them to be used, and all the hardware and software that help the network to function. At this point we will focus on the hardware, since you will study the software in the following units.

Some of these components will be:

- **The network cabling and its connectors**, which allow the transmission of the signal.

- **The rack or connection cabinet** is a frame designed to house electronic, computer and communications equipment.
- **The patch panel,** connection panels that serve as cable terminators and help to organize it.
- **The network cards**, which will allow the connection of the computer, either by cable or wirelessly.
- **The switches or switch,** which allow the connection of different computers to each other and of network segments to each other.
- **Routers or routers,** also known as routers, which allow you to connect different networks, such as a local area network with the Internet.
- **Access points,** which allow the interconnection of wireless devices with each other, and/or the connection of wired devices with wireless ones.
- **Firewalls,** which can be hardware devices with specific software to block unauthorized access to the network, or specific software that is installed on computers and/or servers to prevent unauthorized access.
- **Servers,** which are nothing more than computers with a specific operating system to act as a server, or with non-server operating systems but with server software.

In addition to these components, we also consider the computers that will work on the network, which in many cases are called workstations, as part of the network. Any device that can be connected to the network to provide a service, such as printers, network hard drives, or any peripheral that is connected to a computer on the network, is also a component of the network and is often called nodes. grid.

Before developing any of the concepts explained, it is worth mentioning that among the network servers that will serve the network, we can find: file servers, mail servers, web page servers, print servers, etc.

4.1 Classification of transmission media.

The transmission medium constitutes the channel that allows the transmission of information between two terminals in a transmission system. Therefore, in computer networks they will be the channels that transmit information between the nodes of the network, be they computers, servers, etc. Transmissions are usually made using electromagnetic waves that propagate through the channel.

Sometimes the channel is a physical medium and other times it is not, since electromagnetic waves are susceptible to being transmitted through a vacuum. For this reason we can classify the means of transmission as:

- **Guided media:** conduct electromagnetic waves through a physical path.
- **Unguided media:** provide a support for the waves to be transmitted, but not the direct.

Therefore, when we talk about guided media, we are referring to the different

types of cables that can be used. Among the most used types of cables we find twisted pair, coaxial and fiber optics. We will give more details about them later.

When we refer to unguided media, we are referring to the possibility of transmitting electromagnetic waves, through air or vacuum. This particularity makes it possible to set up wireless networks and have wireless telecommunications systems, such as mobile phones or Internet connections via mobile phones.

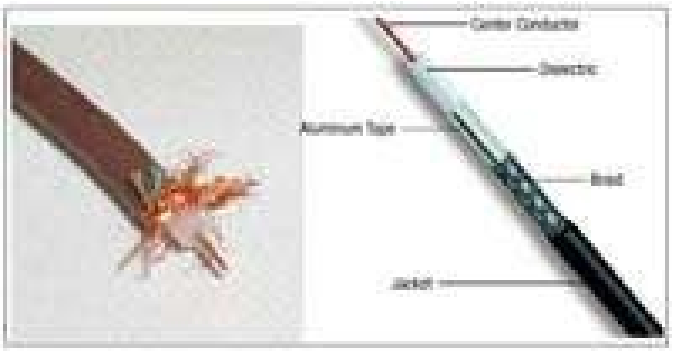
Wiring and connectors.

At this point we are going to make a summary of the types of cables most used in the connection of computer networks and the most used connectors.

The most widely used cable in local area networks is the eight-wire twisted pair. It consists of eight wires with different colors and is used in computer networks under the IEEE 802.3 (Ethernet) standard.

The colors are: white-orange, orange, white-green, green, white-blue, blue, white-brown and brown. The distribution of these colors when connected to the connector is standardized, so that network connections are easily recognizable.

The connector used with this wiring is RJ-45, having a male and a female.



Coaxial cable is also used in computer networks. This cable is composed of a conducting wire, called the core, and an external mesh separated by a dielectric or insulator.

The connectors that are usually used are the BNC and the N type. Within the coaxial cable there are different standards, depending on its use. Currently the coaxial cable is not used to set up computer networks, but rather for the distribution of television signals, cable Internet, etc.

In the distribution of the Internet signal by cable, the coaxial cable is used to connect the Internet distribution center that reaches the street or neighborhood with the subscriber's house. In this case, RG6 type cable is usually used, which allows different configurations to include telephone connections and data transmission.

4.2 Structured cabling.

The telecommunications infrastructure necessary to connect a building or a group of buildings is called structured cabling. This infrastructure includes both

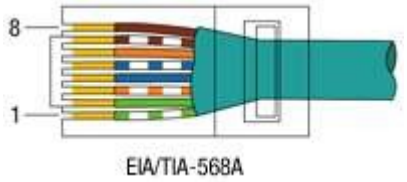
cables and pipes, power strips, cabinets, devices, specific spaces, etc. Structured cabling defines some subsystems to organize cabling installation. The structured cabling subsystems are:

- Campus cabling or building interconnection.
- Building entrance, point where the exterior cables are connected to the interior ones.
- Equipment room, room where all the connections of the building are distributed.
- Trunk cabling or backbone, vertical distribution cabling between plants.
- Distribution cabinets, where the cables come together and where the control equipment is mounted.
- interconnection, using rack and patch panels.
- Horizontal wiring, plant wiring.
- Work area.

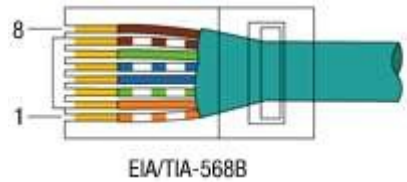
There are structured cabling standards that specify how to organize the cabling installation. These standards specify the type of cable, the connectors, the maximum lengths of the sections, the organization of the interconnection elements, the location of the devices, etc. For example, in horizontal cabling, a maximum of 100 meters is recommended from the distribution cabinet or rack to the work area.

Another standard to take into account is the ANSI/EIA/TIA 568 A and B, which among other things defines the distribution of colors in the connection of the twisted pair cable with the RJ-45 connectors. The 568 A and B distributions are:

Conexions 568A and 568B		
Pin	568-A	568-B
1	white-green	white-orange
2	green	orange
3	white-orange	white-green
4	blue	blue
5	white-blue	white-blue
6	orange	green
7	white-brown	white-brown
8	brown	brown



EIA/TIA-568A



EIA/TIA-568B

In the network connections we will use direct cables, which means that the two ends will have the same standard. It is recommended to use the 568B. In case of wanting to make a crossover cable we will use the 568A standard at one end and the 568B standard at the other. Crossover cables are used to connect two

pieces of equipment of the same type, for example, computer to computer.

4.3 Interconnection elements.

When we talk about interconnection elements, we refer to all the elements that allow equipment to be connected in a network. Normally we will refer to the interconnection elements of a local area network, although the interconnection elements can belong to any type of network.

One way to classify the interconnection equipment is taking into account the level at which they work using the OSI model as a reference. Therefore we are going to make a classification taking this model as a reference.

At the physical level we have:

- Network cards: they can be wired or wireless. Network cards allow computers to connect to the network.
- Concentrators also known as hubs: they allow the signal to be distributed to different computers without discriminating between them.
- Repeaters: they can be local or remote, and their function is to repeat the signal to regenerate and/or amplify it.

At the data link level we have:

- Commutators or switch: they are in charge of connecting network segments, and computers among themselves, but in a more efficient way than a hub, since it only sends the information to the computer that needs it.
- Bridges or bridges: connect subnets, transmitting non-local generated traffic from one to another.
- Access points: they can be considered as data link level elements, they are responsible for connecting wireless elements to each other, and allowing wireless device access to wired networks.

At the network level:

- Router or router: is responsible for connecting different networks. Its main use is in the Internet connection, since it allows local area networks to connect to the Internet. It is based on the use of the IP protocol, so it needs to be assigned at least two IP addresses, one for the Internet and one for the local network. It also handles routing and network control protocols. It can provide wireless service and therefore provide access point service.

At higher levels:

- Gateways: Interconnection equipment that works at higher levels of the OSI model is often referred to as gateways. There are different types of gateways, we can have those that are in charge of connecting networks with different technologies, those that facilitate access control to a network, those that control unauthorized access. Depending on their

function, they can also be servers, firewalls, etc.

It should be remembered that a piece of equipment that works at one level is usually capable of providing service to the lower levels, a well-known example is the case of the router. Unrouter works at the network level, but it can act as a switch since it has several RJ-45 connections incorporated and provides service to several computers, and in the case of being wireless, it can act as an access point so that the wireless computers have a connection to Internet through you.

4.4 Network cards and MAC addressing.

We have already explained something about network cards, now we will explain some of its most important features.

A network card or network adapter allows communication with devices connected to each other and also allows resources to be shared between two or more computers. Network cards are also called NIC from the English network interface card or in Spanish network interface card.

Its main function is to allow the connection of the computer to the network, the necessary protocols are recorded on the card for this to happen. All network cards have the corresponding MAC address recorded. As we have already seen, the MAC address is made up of 48 bits and allows the card to be identified at the data link level. This address is known as the physical address and is unique.

Network cards can be connected to the computer using one of the internal buses, such as PCI, using the external USB bus, or be integrated on the board.

The card must determine the speed of the transmission, the amount of information to transmit, which protocols to use, and all the physical parameters of the transmission. Once it does that, it must transform the information that arrives through the connection with the computer, in order to be transmitted, it does so by converting the information into a serial sequence of bits, conveniently coded, to form a suitable electrical signal. to the transmission medium.

Most of the cards have the same components, we highlight:

- The main processor.
- A transceiver that is the device in charge of accessing the medium.
- A wake on LAN connector that allows the computer to boot from another computer on the network.
- Status indicators to know if you are connected and if you are sending or receiving data.
- Depending on whether the card is for wired or wireless networks, we will have a female RJ-45 connection or an antenna connection, either internal or external.

The installation and configuration of the card will depend on the operating system, but in general, we will need it to have an IP address configured, a netmask configured and a gateway defined. You can practice this in the

following units of the module.

Thanks to the relationship established between the card's IP MAC address and the address assigned to it, a computer can be identified on the network

4.5 Switches.

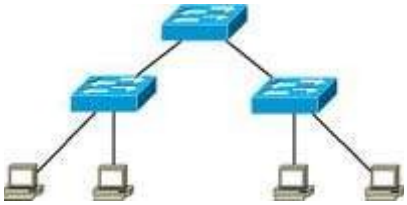
The commutator or switch is an interconnection element that works at layer 2 or data link level, allowing two or more network segments to be connected. The switch allows us to connect different computers so that they can connect with each other, and that they have access to other network segments. The switch works by storing the MAC addresses of the computers that are connected to it and the devices that are on each segment. Thanks to this, it is capable of connecting one computer to another efficiently, without the need to send the information to the entire network.

This characteristic is what makes it the central connection element in local area networks with star topology.

Using a switch has some advantages such as getting high connection speeds and allowing multiple simultaneous transmissions, so more than two computers can be connected at the same time.

The drawback of using switches is that they can only connect networks with the same topology, although they can work at different speeds.

An example of connecting segments can be seen in the following image.



There are layer 3 or layer 3 switches, which have the advantages of switches in terms of speed and can also choose the best route between different devices. One of the most important applications of Layer 3 switches is the ability to define virtual local area networks, or VLANs. VLANs are logically independent networks within the same physical network.

4.6 Routers.

The router or router is the network interconnection equipment that is responsible for connecting two different networks.

It is a layer 3 interconnection equipment or network level. Routers direct network traffic, looking for the best path to reach the destination. They work with packets that contain the information of the source and destination IP addresses, as well as the message data itself.

Given the popularity of the name in English, we will use router, router, or router interchangeably, to make it easier for you to familiarize yourself with the term.

It should be noted that each port or interface of the router will be connected to a different network, therefore all routers must have at least two IP addresses since they will belong to at least two different networks. It must be remembered that a router, in addition to the functions of connecting different networks and routing functions, is capable of filtering, address transfer, linking and acting as a switch. To carry out its functions, a router needs to store information on the networks it can access, this is done through the routing table, which is nothing more than a table where it is stored how to get from one network to another, using which Interface.

The routing algorithms that are used allow working with static routes and with dynamic routes. We talk about static routes when the router keeps the information permanently and without changing the routes that the packets can follow. Static routes are useful when there is only one way to connect to the Internet since the packet will always follow the same path. Dynamic routes will be useful when we have several possibilities to connect to another network, in this case it is convenient that the router can collect information from the network in order to choose the best possible path.

Routers need to be configured to work properly, in the configuration the IP addresses of each of the interfaces are usually defined, information on the subnet masks is included, it is specified if a gateway is going to be used, which DNS servers are used are going to be used, if the IP address assignment service is going to be provided through DHCP, etc. In some cases it is possible to configure which ports will be open, and in the case of wireless routers the configuration characteristics of wireless networks, which we will see a little later.

Most of the time we will use a router to connect to the Internet, either by ADSL or by cable. In these cases, the routers are usually configured by Internet service providers, and we will not have to configure much, these routers are called ADSL routers or cable routers.

On some occasions you will hear about a neutral router, this is a terminology used to differentiate the router that joins two local networks from the one that allows you to connect to the Internet.

Usually, when you use a router as part of your home or work network, this will be the one that allows you to connect to the Internet, therefore in the computer configuration, you will have to put the address of the router as the gateway, since that the computer will send to this gateway all the packets that are not typical of the network and therefore it will be the "gate" to go out to the Internet. In these cases, routers use the NAT or network address translation

mechanism that allows packets to be exchanged between two networks that mutually assign incompatible addresses. You will see these concepts and the configuration of the necessary parameters in the operating system in successive units of work.

4.7 IDS

In computer networks we have seen that we can have different devices to make them work. In addition to the interconnection equipment, we can have servers that perform different functions, as we have previously mentioned. Well, all these teams need to maintain security measures, to prevent unauthorized users from making use of the network or obtaining unauthorized information.

To a greater or lesser extent, all the equipment implement more or less complex security measures, but there is the possibility of implementing an intrusion detection system that complies with these security premises.

This is precisely what IDS does, since IDS stands for Intrusion Detection System or Intrusion Detection System, which we can define as an application used to detect unauthorized access to a computer or network.

There are usually two types of IDS:

- N-IDS: which are responsible for detecting unauthorized network access.
- H-IDS: which are responsible for detecting unauthorized computer or host access.

N-IDS need exclusive hardware as they need to be able to analyze all network traffic. One solution is to integrate the N-IDS into the firewall, in this way the IDS is responsible for detecting possible unauthorized access and the firewall to prevent access.

H-IDS can be integrated into the computer's own system, and can also be combined with the firewalls installed on each computer.

It is important to establish the differences between IDS and firewalls since they are not the same. The IDS detects intrusions but does not prevent them, and the firewall limits traffic to prevent intrusions but does not detect them, hence the combination of both is a good option for a network.

This concept of detection/prevention is the one that inspires a more current trend that is that of the so-called IPS. An IPS is an Intrusion Prevention System, in this case not only the intrusion is detected but it is also prevented from accessing it. There are IDS and IPS type software and/or hardware solutions.