Ministry of Higher Education and Scientific Research
Mohamed Khider university of Biskra
Faculty of Exact Sciences Natural and Life Sciences
Computer science department

2nd Licence year

Installation and configuration of local networks using TCP/IP protocols

Pr. Abdelhamid DJEFFAL
Web site : www.abdelhamid-djeffal.net

Year 2025/2026

1 Introduction

The purpose of a local network is to allow a large number of users, in the same area, to communicate with each other, without an intermediary, to exchange any type of information.

Connecting computers in the same area allows very interesting possibilities :

- Copying files,
- Allow different views of data on different workstations,
- Peripheral sharing (printers, HDDs, servers,...)
- Internet access sharing,...

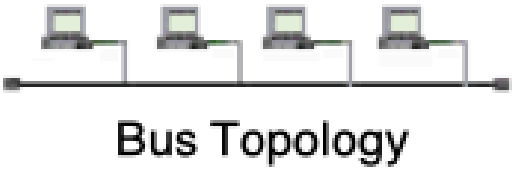
In this course, we will describe the equipment, and the software necessary for the installation of such networks using the TCP/IP protocols.

2 Hardware installation

The hardware required for the implementation of a local area network depends on the architecture to be adapted : bus, star or wireless.

2.1 Bus topology

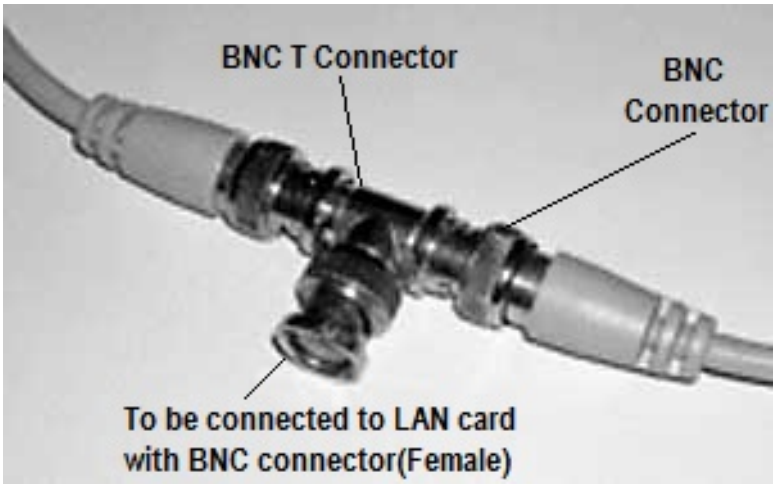
This topology generally uses coaxial cables, the computers are simply connected one after the other on a central line of this type.



Each PC must be equipped with a network card called "Ethernet" integrated or mounted on one of its ports.

Network adapter (bus)

We must also have for each station a T connector which will allow to connect the network card to the coaxial cable using BNC connectors (British Naval Connector).

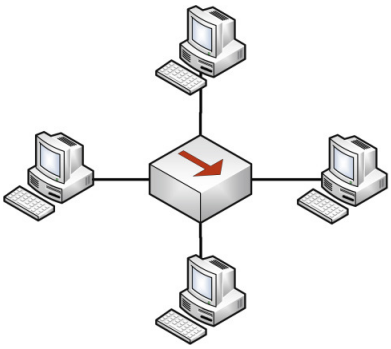


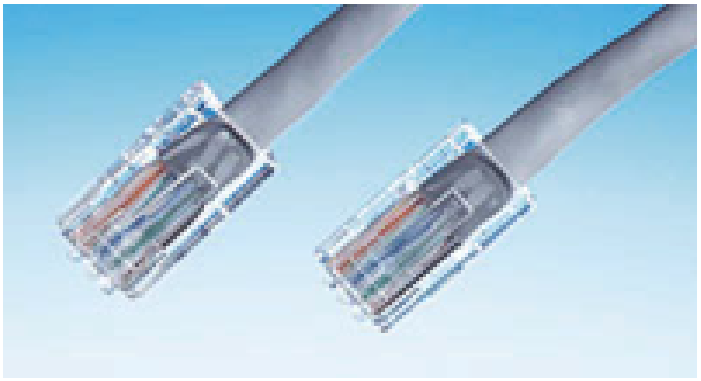
For cards at the ends of the bus, a specific connectors (Ethernet Terminator) are placed on the unconnected part.

Ethernet Terminator

2.2 Star Topology

In this topology, an Ethernet network card and RJ45 Twisted Pairs (TP) cables equipped with RJ-45 (Registered Jack) connectors are used on each PC.

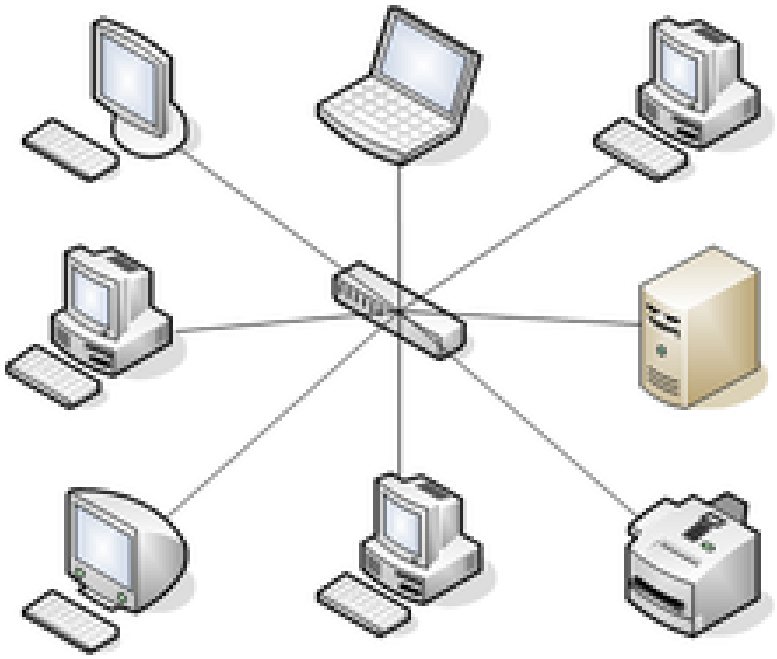




UTP cables and RJ45 connectors

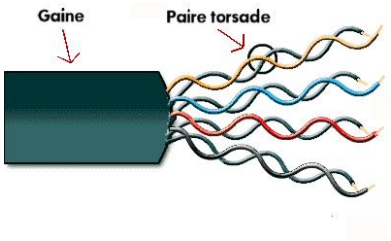
RJ45 Network adapter

The device which allows to play the role of the central node of the star is the Hub (core) :



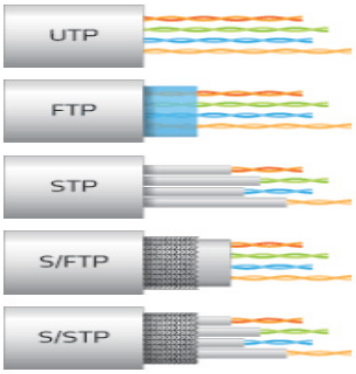
2.2.1 Composition of cables RJ45

RJ45 cables contain 4 twisted pairs :



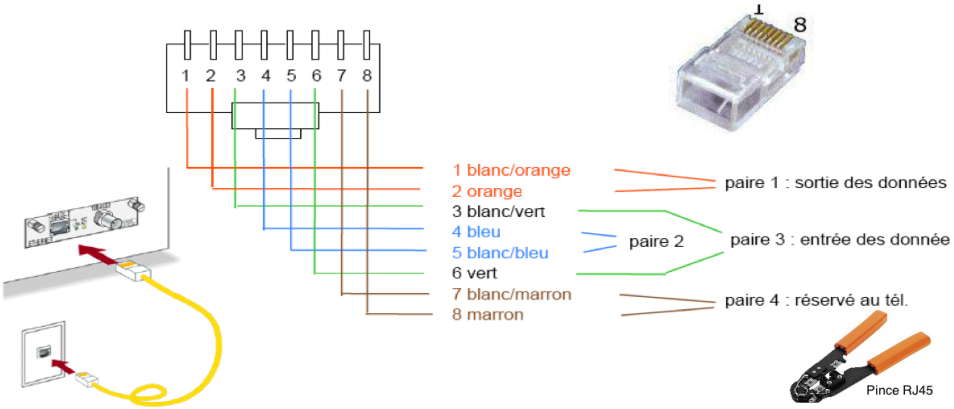
Depending on the shielding used, there are several types of cables :

- UTP (Unshielded Twisted Pairs) : unshielded and unscreened twisted pair cable. Sometimes used for telephony, not recommended for computing.
- FTP (Foiled Twisted Pairs) : twisted pairs surrounded in their entirety by an aluminium foil (screen). This is the standard type.
- STP (Shielded Twisted Pairs) : twisted pairs each surrounded by an aluminium foil.
- SFTP (Shielded Foiled Twisted Pairs) and SSTP (Shielded Shielded Twisted Pairs) : shielded FTP or STP cables. To be used in rooms with strong electromagnetic disturbances.



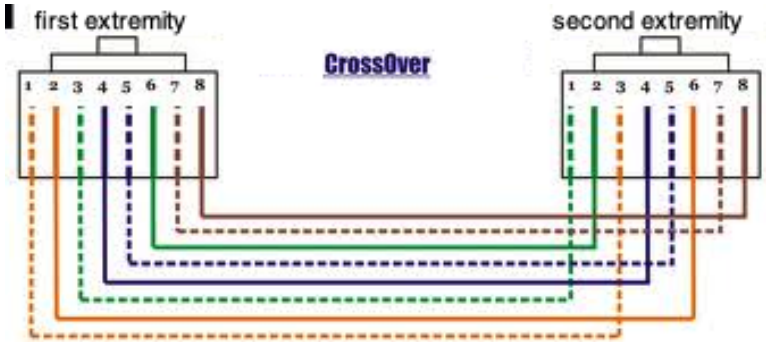
2.2.2 Manufacture of RJ45 cables

The connection of the RJ45 cables is made through the RJ45 connectors allowing the wires to be connected according to the following diagram :



The manual manufacture of RJ45 cables is done by a special clamp called "RJ45 clamp". This type of cable is called a straight cable, it is used to connect a PC to a HUB or Switch.

Another type of cable is called a crossover cable, it is made by reversing wires 1 and 2 with 3 and 6 respectively.



The use of straight and crossover cables is summarized in the following table :

	Hub	Switch	Router	Workstation
Hub	Crossover	Crossover	Straight	Straight
Switch	Crossover	Crossover	Straight	Straight
Router	Straight	Straight	Crossover	Crossover
Workstation	Straight	Straight	Crossover	Crossover

2.3 Wireless LAN

A WLAN (Wireless Local Area Network) is a network that covers the equivalent of a corporate local area network, i.e. a range of approximately one hundred meters using radio-electric waves.

Two modes are possible.

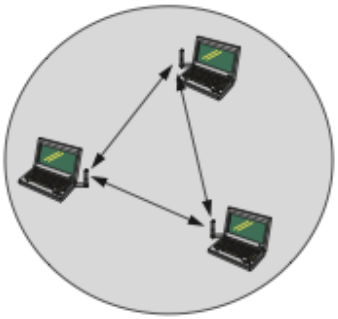
2.3.1 Infrastructure mode

Uses an access point and wireless network cards. It suffices, therefore, to have an access point, to mount the network cards and to proceed to the software configuration.

Equipment and connection of a WLAN

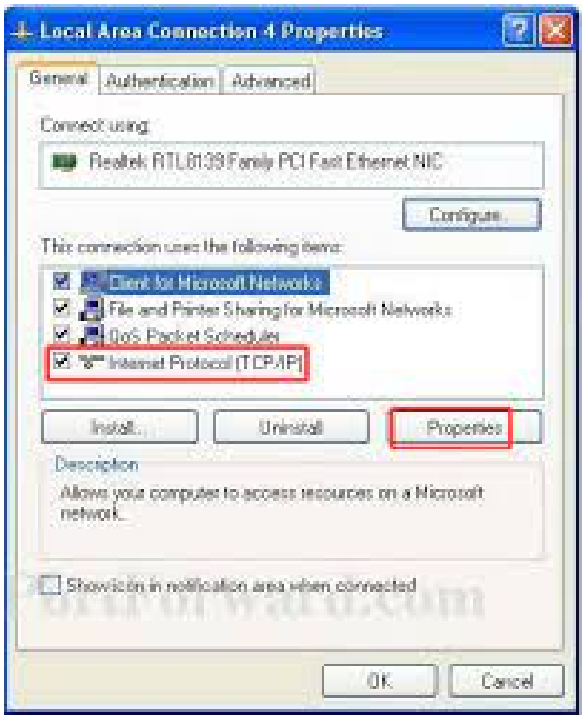
2.3.2 Mode ad hoc

The "Ad-Hoc" mode allows computers equipped with a Wi-Fi card to be connected directly to each other



3 Software installation

The TCP/IP protocols make it possible to connect machines equipped with different systems such as Windows, Linux or MAC-OS.



The TCP/IP protocols must be installed to be able to connect a LAN (Local Area Network) to the Internet, but of course nothing prevents installing TCP/IP anyway ; even without the Internet, this flexible protocol has many very interesting characteristics for a network administrator.

To use TCP/IP protocols on Windows, in :

"Control Panel → Network Connections → Local Area Connections"

Add the TCP/IP protocol (by clicking on add, then protocol).

For the configuration of the TCP/IP protocols, only three points are of interest to us :

3.1 Allocation of IP addresses

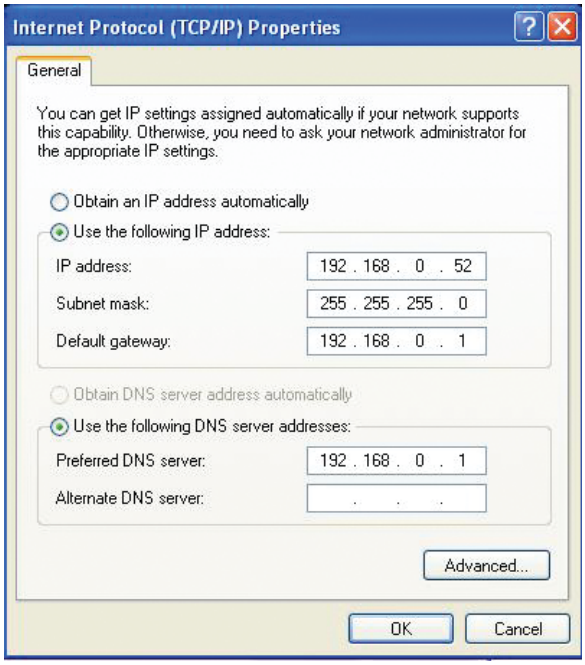
In fact, if a network is completely isolated from the rest of the world, we can put the IP addresses that it likes. On the other hand, if a computer on the network can "communicate further", for example if it is equipped with a modem and can access the Internet, we have no choice but to use any IP addresses. In principle, in the absence of a routing system, we could put any IP address, because the information circulating on the LAN cannot "leave" the network anyway. However, for security reasons, we always use the following IP addresses :

from 10.0.0.0 to 10.255.255.255, from 172.16.0.0 to 172.31.255.255 , from 192.168.0.0 to 192.168.255.255

These addresses have been "reserved" by INTERNIC and will never be routed by Internet providers. For local networks, the IP addresses 192.168.0.1, 192.168.0.2, 192.168.0.3, etc. are generally used.

3.2 The subnet mask

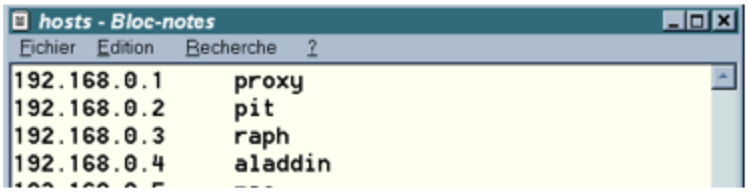
We use the default mask for class C local networks : 255.255.255.0



3.3 A host-like naming system

This system is used to give names to machines that are easier to use than IP addresses. On each machine, we must create a hosts file (without extension!) which establishes a

relationship between the IP address and a name, easier to remember. Here is an example of a file of this type (to be done with notepad for example) :



Do not forget the carriage return (enter) after the last entry in the file. The file must imperatively reside in the c :\windows\ directory, on all the computers on the network.

For a local network connected to other networks by a router or which uses a shared Internet connection, the address of the gateway and the DNS server must be indicated for each machine : The gateway is the address where packets are sent that are destined for computers outside the local network. It is therefore necessary to put the address of the router or the PC which has the software for sharing the Internet connection generally 192.168.0.1

The DNS is used to convert addresses in the form of names (www.yahoo.com) into a numerical IP address. You must therefore put the address of the PC sharing the Internet connection (probably 192.168.0.1)

For the PC that shares the Internet connection, these parameters are provided by the Internet access provider automatically on connection. It is therefore necessary to leave "automatically obtain an IP address" on the interface in connection with the Internet (modem) and configure only the IP address and the mask (192.168.0.1/255.255.255.0) for the other interface (network card).

The network is now installed, we must reboot all the machines, and carry out the tests.

3.4 Tools for testing TCP/IP protocols

To check the network connections of the different machines, or for solving a management problem in the network, there is a set of software tools available on most systems. To run these tools, they must be run on the MSDOS command line.

– **Ping** :

Allows you to test IP level connectivity and the presence of a machine and the response time on the network.

Examples.

ping 192.168.0.1

ping http ://www.yahoo.fr/ if you are connected to the Internet.

ping cathy

C :\ WINDOWS>ping 192.168.0.1

Pinging 192.168.0.1 with 32 bytes of data :

Reply from 192.168.0.1 : bytes=32 time=2ms TTL=128

Reply from 192.168.0.1 : bytes=32 time=2ms TTL=128

Reply from 192.168.0.1 : bytes=32 time=2ms TTL=128

Reply from 192.168.0.1 : bytes=32 time=2ms TTL=128

C :\ WINDOWS>

- **Ipconfig /all**

  Gets a detailed configuration report for all host computer interfaces.

- **Tracert**

  Allows you to see the route to another machine on the network. Useful especially on the public Internet network.

  Exemple :

  tracert http ://www.yahoo.fr/.

- **Arp**

  Address Resolution Protocol (ARP) allows a host to look up the physical address of a host on the same network, given the host's IP address. For this protocol to be effective, each computer stores IP to physical address mappings in memory to eliminate repetitive ARP broadcast requests.

  The arp command is used to view the ARP table and troubleshoot address resolution issues.

- **Netstat** View protocol statistics and TCP/IP connections.

  Examples :

  netstat -a to show all connections.

  netstat -r to display the routing table

  netsaat -p [protocole] to display the connections of a given protocol such as TCP, UDP,...