

Networks

Introduction

- Networks were born from a need to exchange information simply and quickly between machines.
- At the beginning, we worked on the same machine, all the information necessary for the work was centralized there, it is the autonomous mode.
- Almost all users and programs needed this information, so, for reasons of cost and performance, we came to multiply the number of machines.
- The information then had to be duplicated on different machines on the same site.
- This duplication was more or less easy and did not always provide consistent information.
- We therefore managed to first connect these machines together; this was the appearance of local networks.
- These networks were often proprietary networks. Later we felt the need to exchange information between distant sites. Medium and long distance networks began to emerge.
- Today, networks are found on a global scale. The need for information exchange evolved more and more, and this was the appearance of the global Internet network.

Definition

Telecomputing

- it is the association of processing and transport of information.
 - Processing: IT field.
 - Transport: field of telecommunications.

Network

- A (data) network is any telecomputing system made up of equipment linked together by communication channels through which these various elements can communicate. (equipment: computers, peripherals (printer, scanner, switches, etc.)

Purpose

➤ A network allows:

- Sharing files and applications
- Communication between people (through email, live chat, etc.)
- Communication between processes (between industrial machines)
- Guarantee of uniqueness of information (databases)

➤ Today, the trend is towards the development of wide area networks (WAN) deployed nationwide, or even worldwide. So there are multiple interests, whether for a company or an individual.

Types of computer networks

- The type of network to install depends on the following criteria:
 - Size of the company
 - Necessary level of security
 - Type of activity
 - Administrative skill level available
 - Network traffic volume
 - Network user needs
 - Budget allocated to network operation

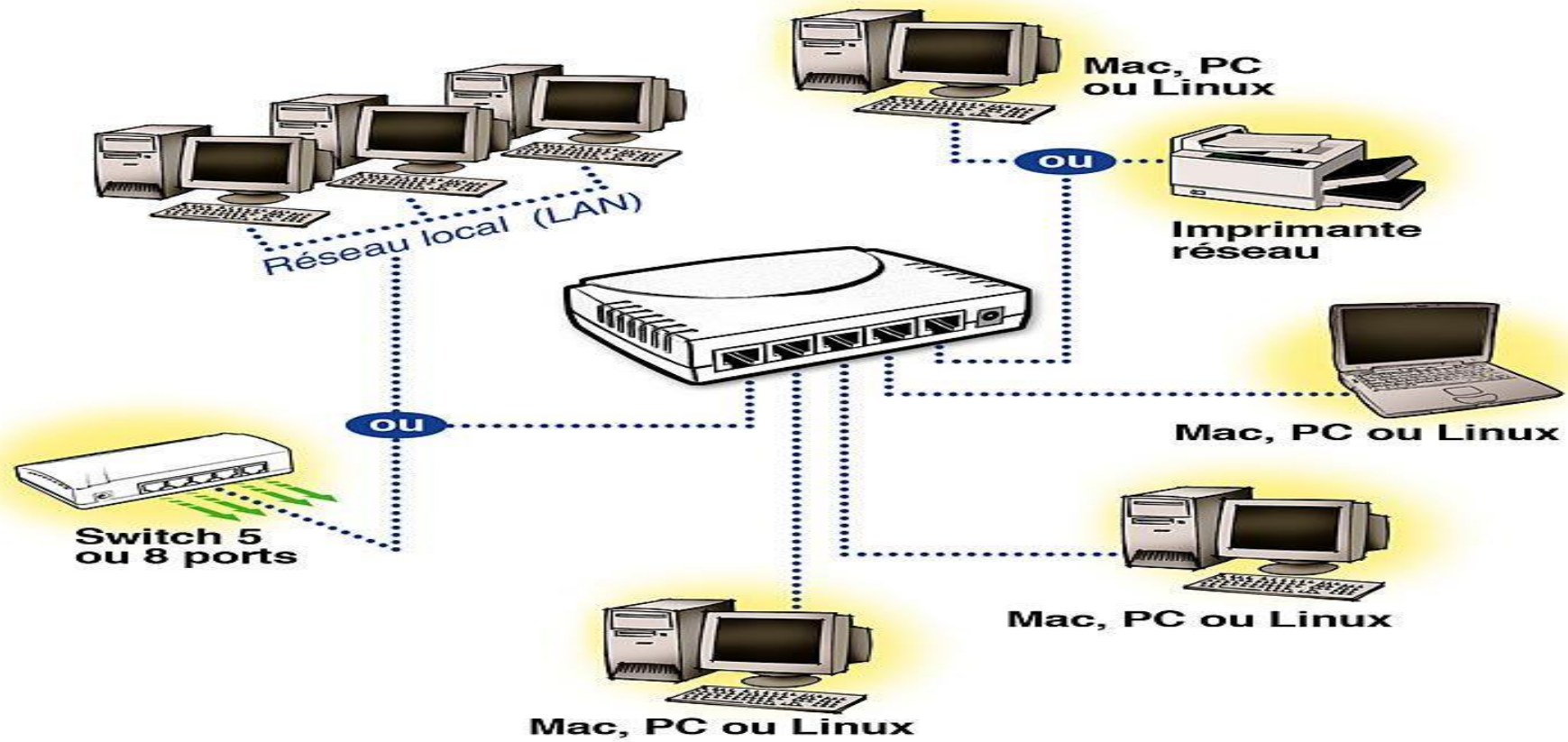
Types of computer networks

- There are generally six categories of networks:
 - PAN (Personnel Area Network)
 - LAN (Local Area Network)
 - TAN (Tiny Area Network) identical to LANs but less extensive (2 to 3 machines)
 - MAN (Metropolitan Area Network)
 - CAN (Campus Area Network) identical to the MAN maximum bandwidth between all LANs in the network).
 - WAN (Wide Area Network)

Local Area Networks (LAN)

- If several computers need to be brought together on a network, this is generally done in the form of a local area network or LAN.
- Such a network can connect two computers in a home or several hundred devices within a company. But also networks in public institutions such as administrations, schools or universities are generally implemented in the form of a LAN.
- If more than two computers are nested together in a local network, additional components such as a hub (or concentrator), bridge (bridge) or switch (network switch) are necessary and then act as coupling elements and distribution nodes .
- A LAN is designed to allow rapid transfer of large amounts of data. Depending on the network structure and the transmission medium used, a data rate of 10 to 1000 Mbit/s is common.

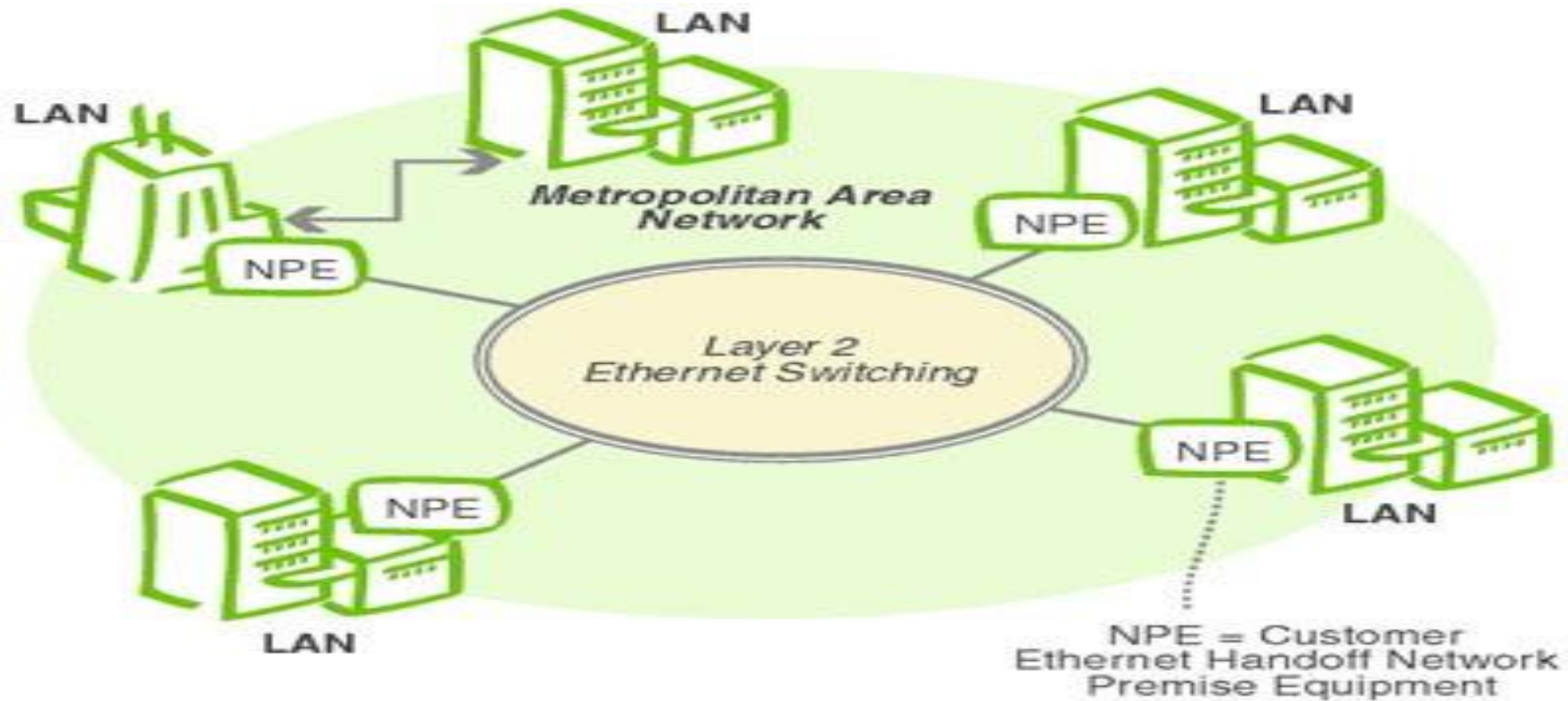
Local Area Networks (LAN)



Metropolitan Area Networks (MAN)

- A Metropolitan Area Network allows users and computing resources to be interconnected across a larger geographic area or region than that covered by a LAN
- The term applies to the interconnection of city-wide networks to form a single, enlarged network (which can then also provide an efficient connection to a WAN).
- It also designates the interconnection of several local networks by means of basic lines, called backbones. This latter usage is sometimes also called a campus network.

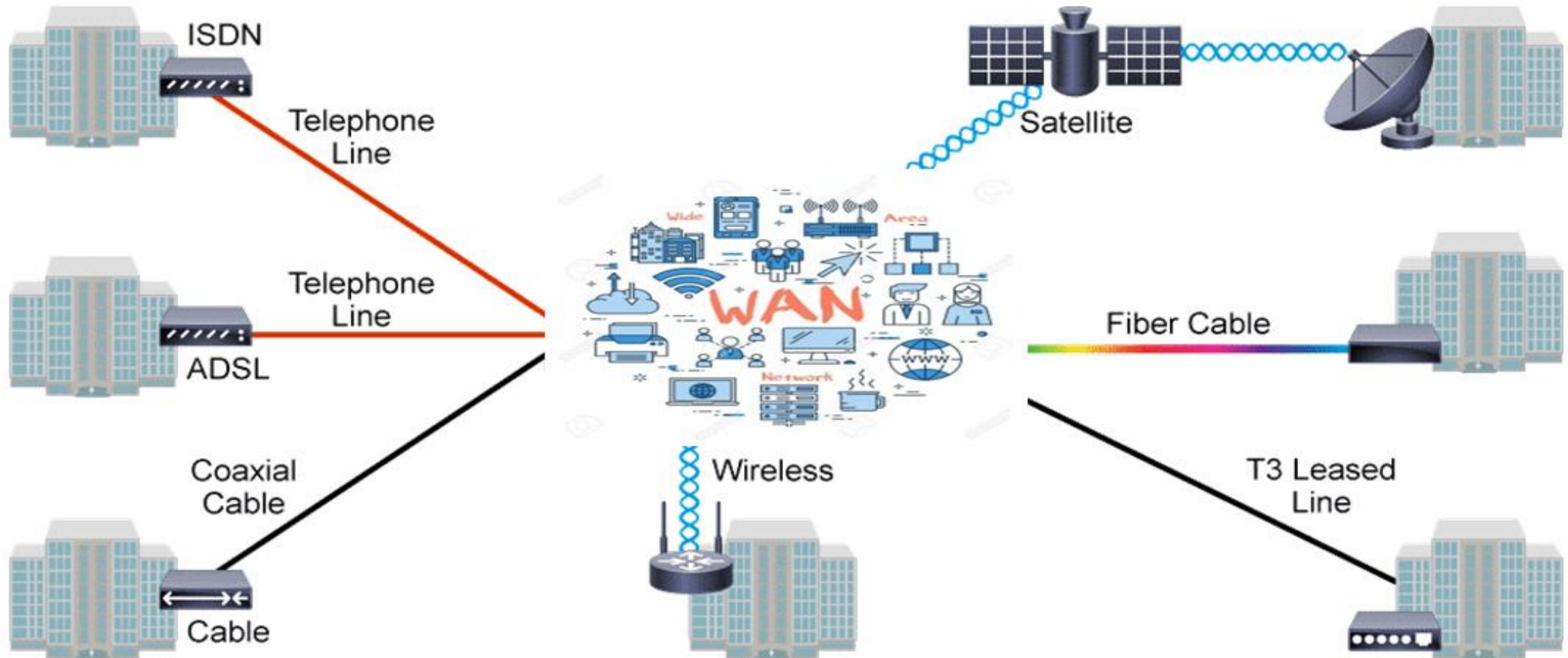
Metropolitan Area Networks (MAN)



Wide Area Networks (WAN)

- Metropolitan area networks connect areas that are close to each other in rural or urban areas while WAN cover large geographic areas on the scale of a country or continent.
- The number of local networks or computers connected to a wide area network is unlimited.
- Networks (LAN) and MAN can be achieved due to the geographical proximity of connected computers or networks on the basis of Ethernet, wide area networks use techniques like:
 - IP/MPLS (Multiprotocol Label Switching),
 - PDH (Plesiochronous Digital Hierarchy),
 - SDH (Synchronous Digital Hierarchy),
 - SONET (Synchronous Optical Network),
 - ATM (Asynchronous Transfer Mode)
 - X.25

Wide Area Networks (WAN)



Network topologies

- A computer network topology corresponds to its architecture (physical or logical), defining the connections between network equipment and a possible hierarchy between them.
- It can define the way in which equipment is interconnected and the spatial representation of the network (physical topology).
- It can also define the way in which data passes through communication lines (logical topologies).

Physical topologies

- We generally distinguish the following physical topologies:
 - Bus topology
 - Star topology
 - Ring topology
 - Tree topology
 - Hybrid Topology
 - Mesh topology

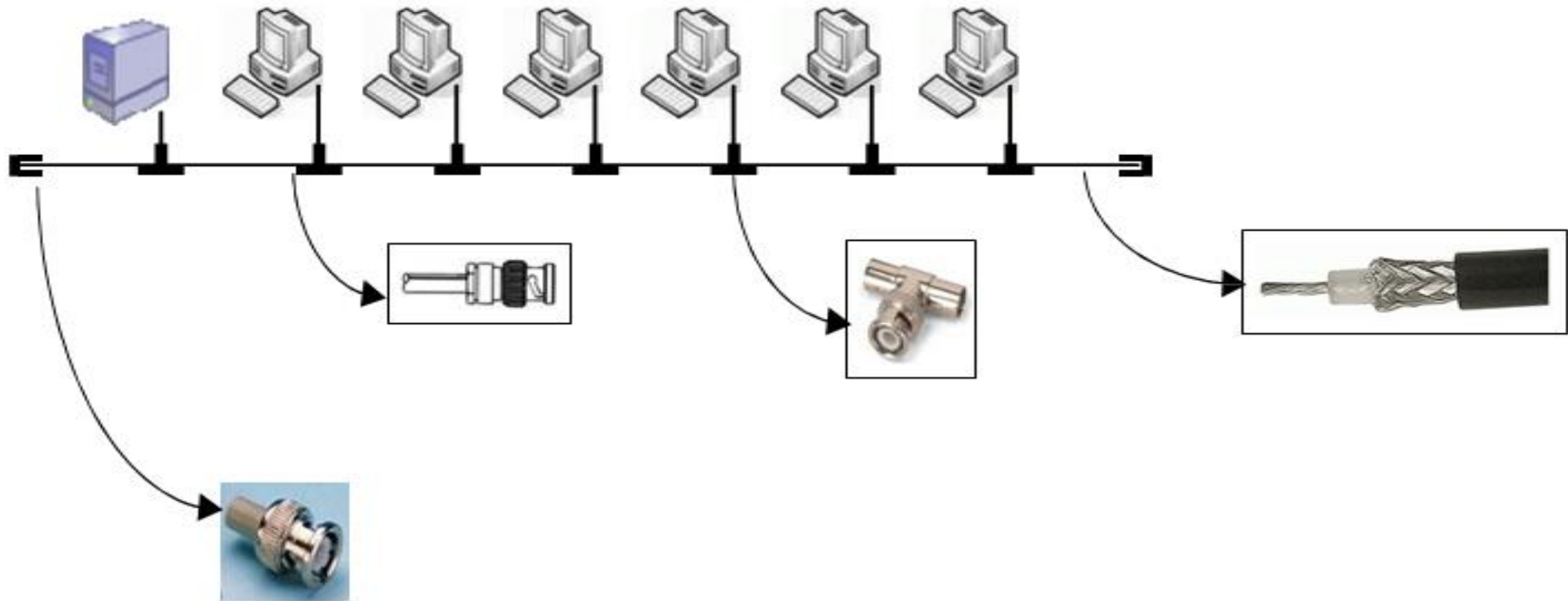
Bus topology

- The bus network (computer) topology is represented by a single cabling of the network units.
- It also has a low deployment cost and the failure of a node (computer) does not split the network into two subnetworks.
- These units are connected passively by electrical or optical bypass.

Bus topology

- The characteristics of this topology are as follows:
 - When a station is faulty and no longer transmitting on the network, it does not disrupt the network.
 - When the support is down, the entire network no longer works.
 - The signal emitted by a station propagates in one direction or in both directions.
 - If the transmission is bidirectional: all connected stations receive the signals transmitted on the bus at the same time (within propagation delay).
 - The bus, in the case of coaxial cables, is terminated at its ends with impedance adapters (“caps”) to eliminate signal reflections.
 - All stations are directly connected to a single segment (limited by cable length).

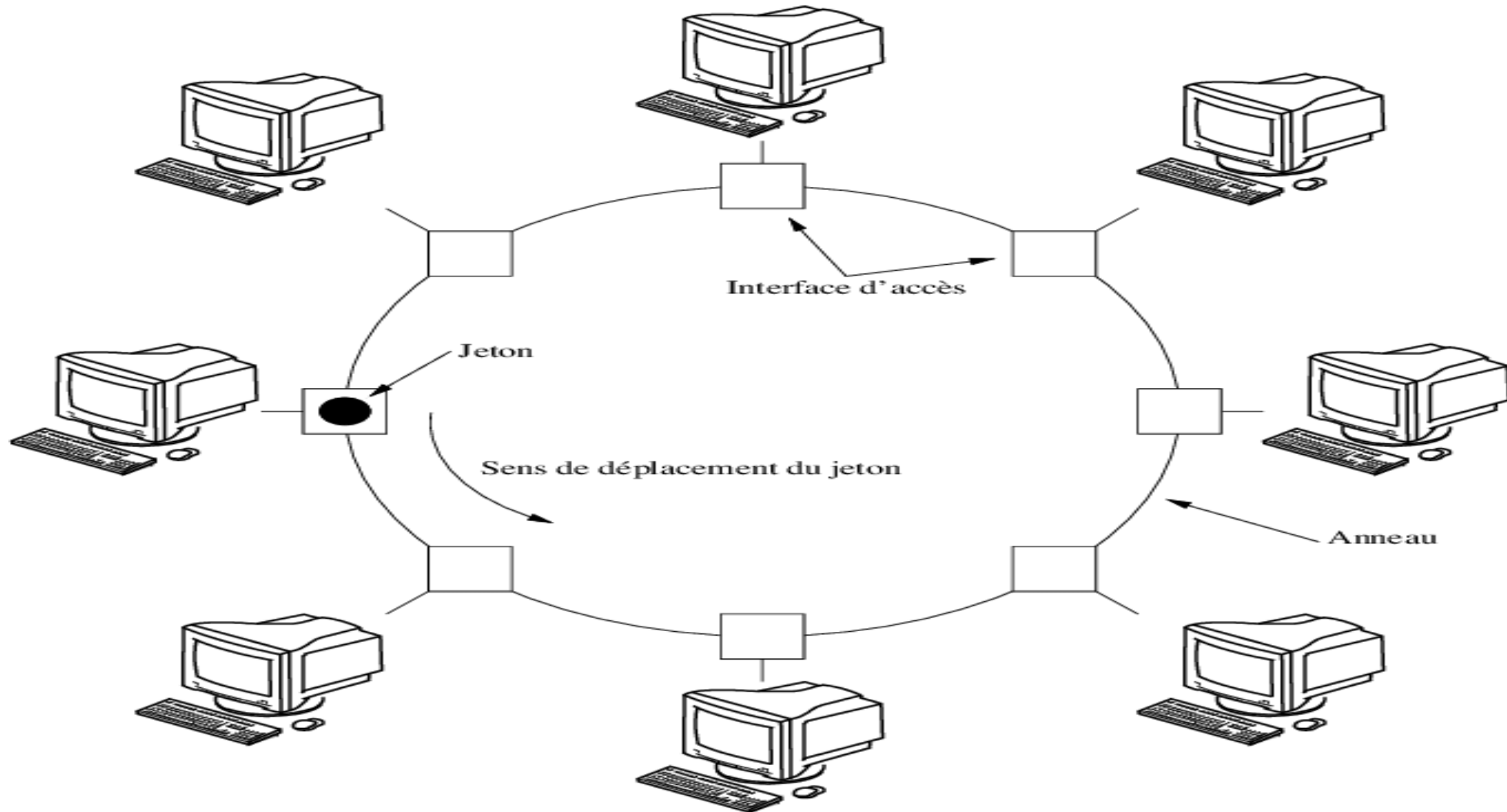
Bus topology



Ring topology

- A network has a ring topology when all its stations are connected in a chain to each other by a two-point link from the last to the first.
- Each station plays the role of an intermediate station.
- Each station that receives a frame interprets it and retransmits it to the next station in the loop if necessary.
- Host failure breaks the structure of a ring network if communication is unidirectional
- In practice, a ring network is often composed of 2 counter-rotating rings.

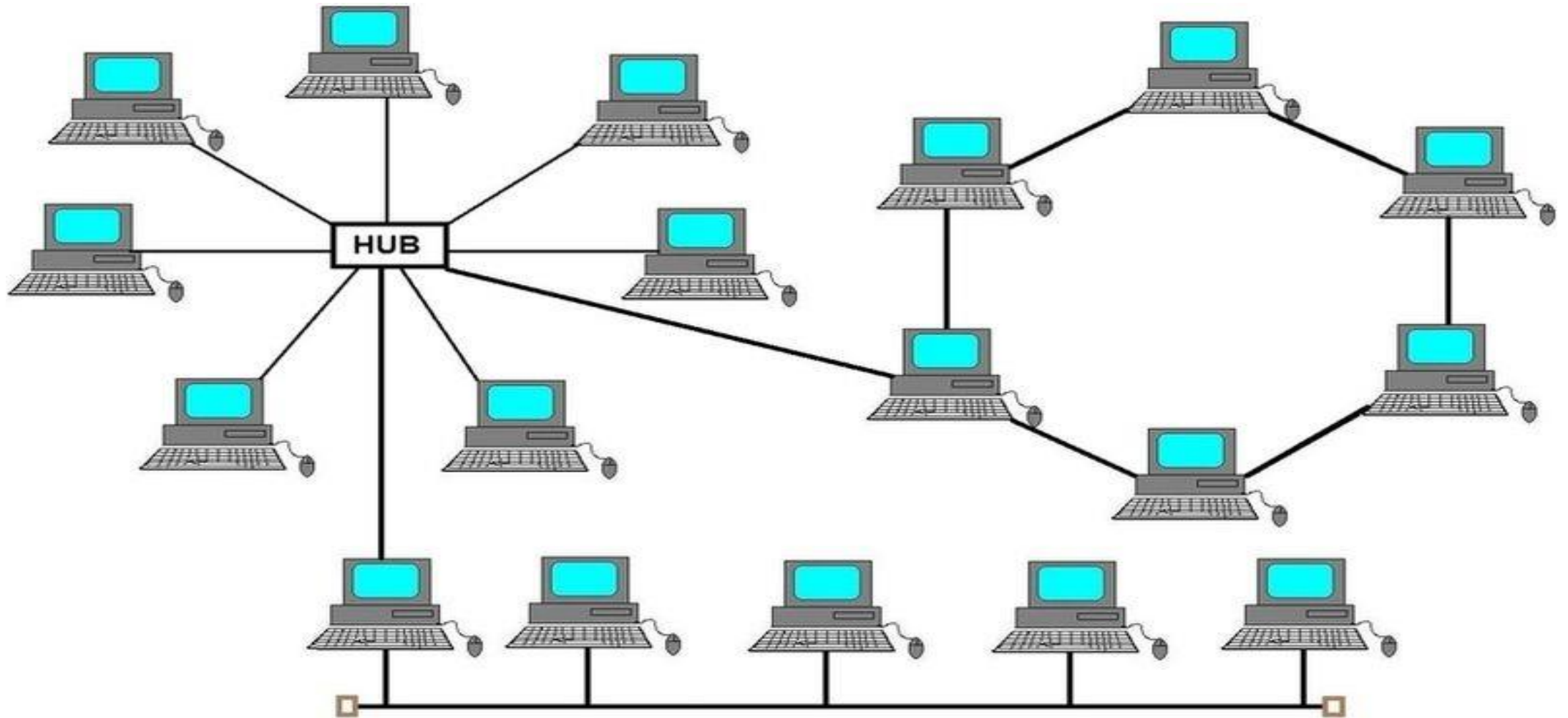
Ring topology



Star topology

- The star topology is by far the most common.
- Each unit is connected to a central node (HUB or SWITCH) via twisted pair cable.
- The connectors are RJ45 type.
- The HUB is also called a concentrator.
- The SWITCH is also called a Commutator.
- HUBS or SWITCHES can be cascaded to form more complex structures

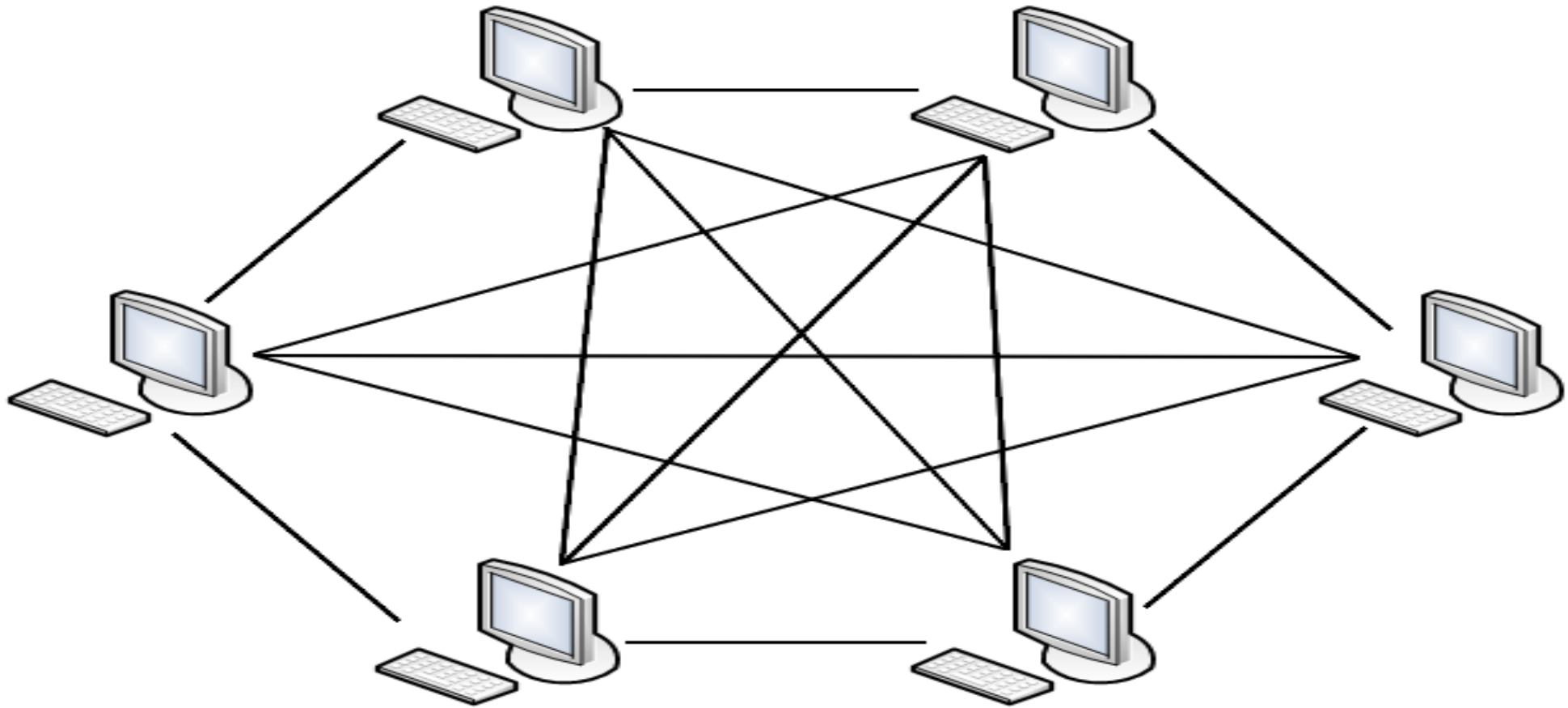
Star topology



Mesh topology

- The principle of mesh topology is to connect all computers together (full mesh), or at least a large number.
- There is no risk of a general breakdown if a machine breaks down, but if you get caught in cables, since they are everywhere!
- If we want to connect all the machines together, the formula for knowing the number of cables is $n(n-1)/2$, with n the number of computers. So just with 8 computers for example, that will give us $8(8-1)/2$, or up to 28 cables!
- In practice, we almost never use full mesh networks, but only partially meshed.
- This topology remains little used given the difficulty in setting up such an infrastructure.

Mesh topology



Hybrid topology

- A hybrid topology combines one topology with another.
- Hybrid topologies come in several types. For example, part of a network may be a physical ring, while another part of the network may be a physical star.
- Another type of hybrid topology is the physical-logical hybrid topology. In this case, you have a network that physically resembles in one sense or physically resembles a topology, but operates like a different technology.

Les topologies logiques

- Se réfèrent plus à la façon dont les données se déplacent via le réseau
- La topologie logique fait référence au modèle du flux de données dans un réseau.
- Le même réseau peut avoir une topologie physique très différente de la topologie logique.
- Les topologies logiques les plus courantes sont:
 - Ethernet
 - Token Ring
 - FDDI.
 - Arcnet

Ethernet

- Est un protocole de réseau local à commutation de paquets.
- C'est une norme internationale : ISO/IEC 802-3.
- Depuis les années 1990, on utilise très fréquemment Ethernet sur paires torsadées pour la connexion des postes clients, et des versions sur fibre optique pour le cœur du réseau.
- Cette configuration a largement supplanté d'autres standards.
- Depuis quelques années, les variantes sans fil d'Ethernet (normes IEEE 802.11, dites « Wifi ») ont connu un fort succès, aussi bien pour les installations personnelles que professionnelles.
- Ethernet n'offre pas de garantie de bonne livraison des données, ce qui est laissé aux couches protocolaires supérieures.

Ethernet

Sigle	Dénomination	Câble	Connecteur	Débit	Portée
10Base2	Ethernet mince (thin Ethernet)	Câble coaxial (50 Ohms) de faible diamètre	BNC	10 Mb/s	185m
10Base5	Ethernet épais (thick Ethernet)	Câble coaxial de gros diamètre (0.4 inch)	AUI	10Mb/s	500m
10Base-T	Ethernet standard	Paire torsadée (catégorie 3)	RJ-45	10 Mb/s	100m
100Base-TX	Ethernet rapide (Fast Ethernet)	Double paire torsadée (catégorie 5)	RJ-45	100 Mb/s	100m
100Base-FX	Ethernet rapide (Fast Ethernet)	Fibre optique multimode du type (62.5/125)		100 Mb/s	2 km
1000Base-T	Ethernet Gigabit	Double paire torsadée (catégorie 5e)	RJ-45	1000 Mb/s	100m
1000Base-LX	Ethernet Gigabit	Fibre optique monomode / multimode		1000 Mb/s	550m /10km
1000Base-SX	Ethernet Gigabit	Fibre optique multimode		1000 Mbit/s	550m
10GBase-SR	Ethernet 10Gigabit	Fibre optique multimode		10 Gbit/s	500m
10GBase-LX4	Ethernet 10Gigabit	Fibre optique multimode		10 Gbit/s	500m

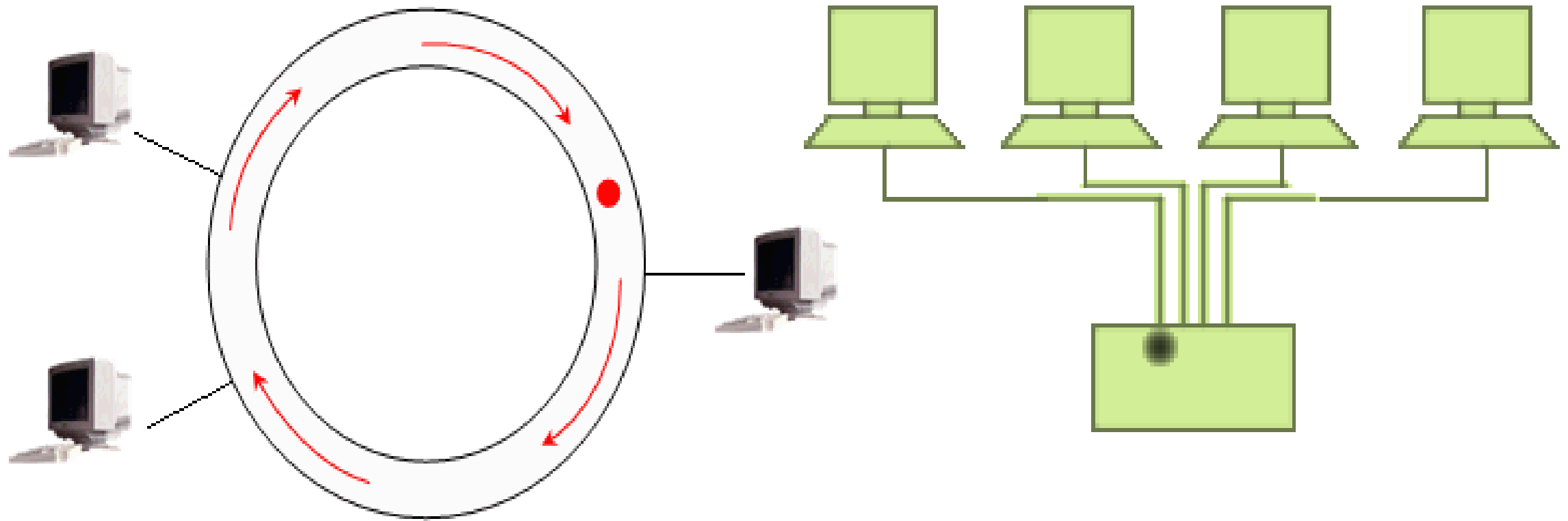
Le token ring

- C'est une topologie de réseau associée à un protocole de réseau local qui fonctionne sur la couche « liaison » du modèle OSI.
- Le protocole utilise une trame spéciale de trois octets, appelée jeton, qui circule dans une seule direction autour d'un anneau.
- Les trames token ring parcourent l'anneau dans un sens qui est toujours le même.
- Le paradigme est celui du « rond-point », qui se montre généralement capable d'écouler un débit plus grand qu'un « carrefour », toutes choses égales par ailleurs.
- En contrepartie, on créait des contraintes topologiques : l'Ethernet est concevable sur n'importe quel support, y compris par radio ou en théorie par infrarouge sur un plafond blanc ; le token-ring ne peut fonctionner que sur une « boucle ».

Le token ring

- Une boucle typique de token ring pouvait faire 6 km. Cette technologie a permis à IBM de résister à la concurrence de nouveaux constructeurs développant une informatique décentralisée.
- Le « jeton » matérialise le « droit de transmettre ».
- Chaque station le passe (le « répète ») sur l'anneau, à la station qui lui a été prédéfinie station suivante.
- Une station désirant transmettre le garde le temps nécessaire à transmettre une trame, puis envoie le jeton à la suite de cette trame pour indiquer que la voie est libre.
- Si une station tombe en panne, une interaction se fait afin de bloquer l'accès au jeton pour la station qui est en panne.
- Un anneau de token ring était limité à 250 stations en raison de considérations liées à la fréquence de transmission.

Le token ring



FDDI

- La technologie LAN FDDI (Fiber Distributed Data Interface) est une technologie d'accès au réseau sur des lignes de type fibre optique.
- Il s'agit en fait d'une paire d'anneaux (l'un est dit "primaire", l'autre, permettant de rattraper les erreurs du premier, est dit "secondaire").
- Le FDDI est un anneau à jeton à détection et correction d'erreurs (c'est là que l'anneau secondaire prend son importance).
- Le jeton circule entre les machines à une vitesse très élevée. Si celui-ci n'arrive pas au bout d'un certain délai, la machine considère qu'il y a eu une erreur sur le réseau.

ARCnet

- ARCnet est un acronyme anglais (Attached Resource Computer NETwork).
- C'est un protocole de réseau local (LAN) similaire à Ethernet ou Token Ring.
- Il a été développé par Datapoint Corp. en 1976 pour mettre en cluster des terminaux (par exemple les Datapoint 2200).
- ARCnet fut inventé afin de permettre à ces machines de communiquer. Il fut annoncé dès 1975 (disponibilité début 1977), soit 6 ans avant la sortie aux États-Unis du premier IBM PC
- ARCnet fonctionne à 2,5 Mb/s, utilise du câble coaxial, et une topologie logique à base de bus ou d'étoile à jeton.

Les supports d'interconnexion

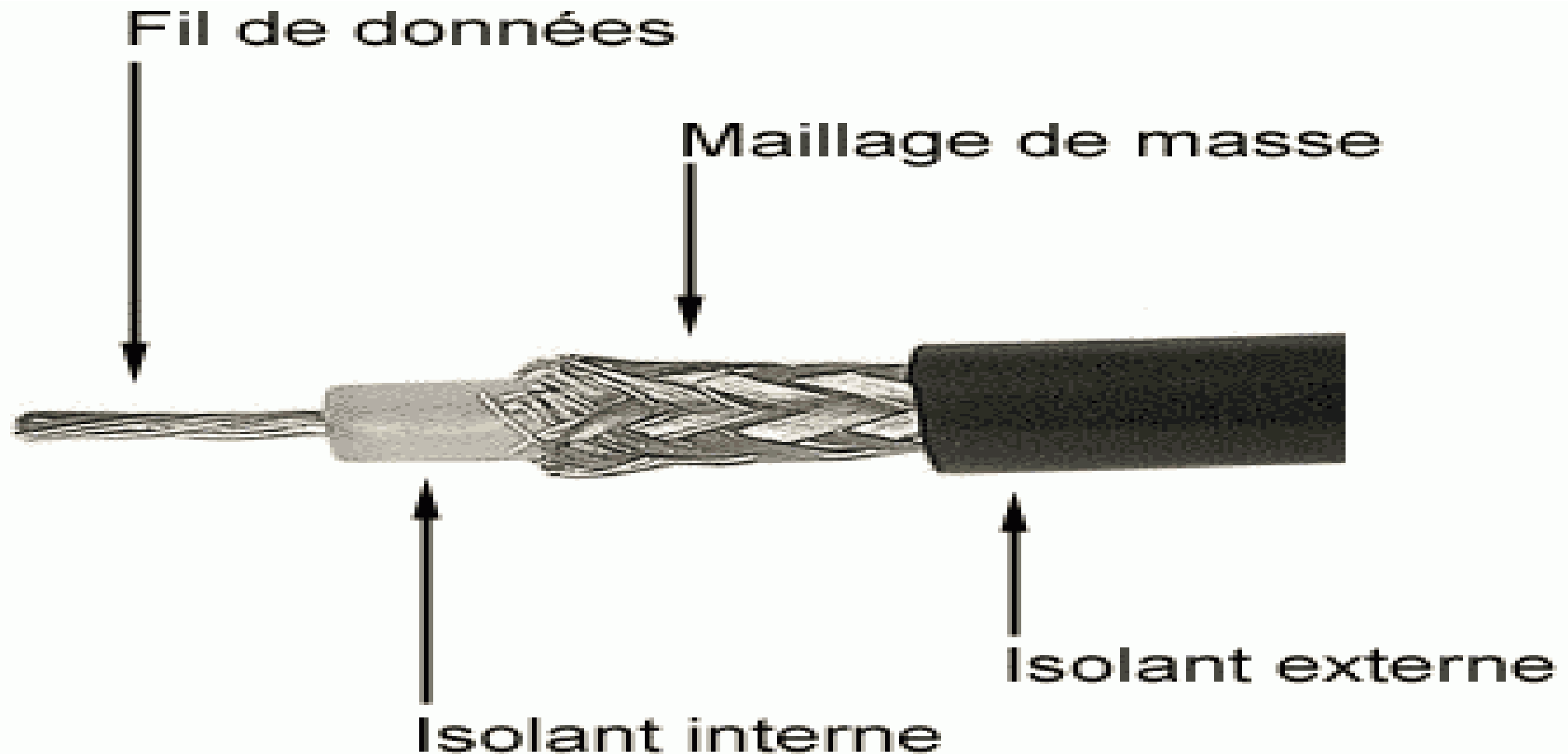
Le câble coaxial

- Le câble coaxial est un câble à deux conducteurs de pôles opposés séparés par un isolant.
- Il est utilisé pour la transmission de signaux numériques ou analogiques par fréquences hautes ou basses, notamment entre les antennes TV et les téléviseurs.
- Il a été élaboré par l'Américain Herman Affel qui a obtenu le brevet de cette invention en 1931.
- Le câble se compose d'un conducteur central appelé l'âme, généralement en cuivre, qui est enrobé dans un matériau diélectrique isolant.

Le câble coaxial

- Ce dernier est lui-même entouré par un blindage qui fait office de second conducteur.
- Ce blindage peut être une tresse de cuivre ou une feuille d'aluminium.
- Le tout est protégé dans une gaine isolante.
- Cette configuration est pensée pour que les conducteurs ne produisent et ne subissent aucune perturbation vers et depuis l'extérieur.
- La moindre détérioration d'un câble coaxial altère son fonctionnement et ses performances.

Les supports de transmission: Le câble coaxial



Le câble coaxial

➤ Il est possible de trouver un câble coaxial dans :

- Entre une antenne TV (TNT ou parabole satellite) et un récepteur de télévision ;
- Dans les réseaux câblés urbains (télévision par câble et accès à Internet) ;
- Entre un émetteur et l'antenne d'émission, par exemple une carte électronique Wi-Fi et son antenne ;
- Entre des équipements de traitement du son (microphone, amplificateur, lecteur CD...);
- Dans les réseaux de transmissions de données tels qu'Ethernet dans ses anciennes versions : 10BASE2 et 10BASE5 ;
- Pour les liaisons inter-urbaines téléphoniques et dans les câbles sous-marins ;
- Pour le transport d'un signal vidéo, exemple caméra de surveillance filaire déportée, sur des distances significatives (plusieurs dizaines de mètres).

Le câble à paires torsadées

- Le câble à paire torsadée (TWISTED-PAIR CABLE) est composé de plusieurs éléments :
 - Des brins de cuivre entrelacés (torsadés)
 - Une enveloppe isolante
- Le câble à paire torsadée a été largement diffusé parce qu'il est à l'origine utilisé pour les lignes téléphoniques et qu'il était jusqu'en 1983 systématiquement pré installé dans tous les nouveaux bâtiments américains. Le câble à paire torsadée est le support le plus utilisé à l'intérieur d'un bâtiment.
- L'entrelacement des brins de cuivre permet de limiter les interférences extérieures (moteur, relais, transformateur, ...), toutefois la protection d'un blindage est bien plus efficace pour diminuer les risques d'interférences.

Le câble à paires torsadées

➤ Les qualités de la paire torsadée sont les suivantes :

- Répond aux spécifications de la norme « 10 base T »
- Très utilisé pour les réseaux locaux
- Une longueur maximale de 100 mètres
- Un débit de 10 à 100 Mb/s
- Un câblage peu coûteux, c'est le moins cher
- Une installation et des connexions simples
- La plus grande flexibilité du câble
- La plus grande vulnérabilité aux interférences
- Un choix fiable, mais qui ne garantit pas l'intégrité des données transmises sur de longues distances et à des débits élevés

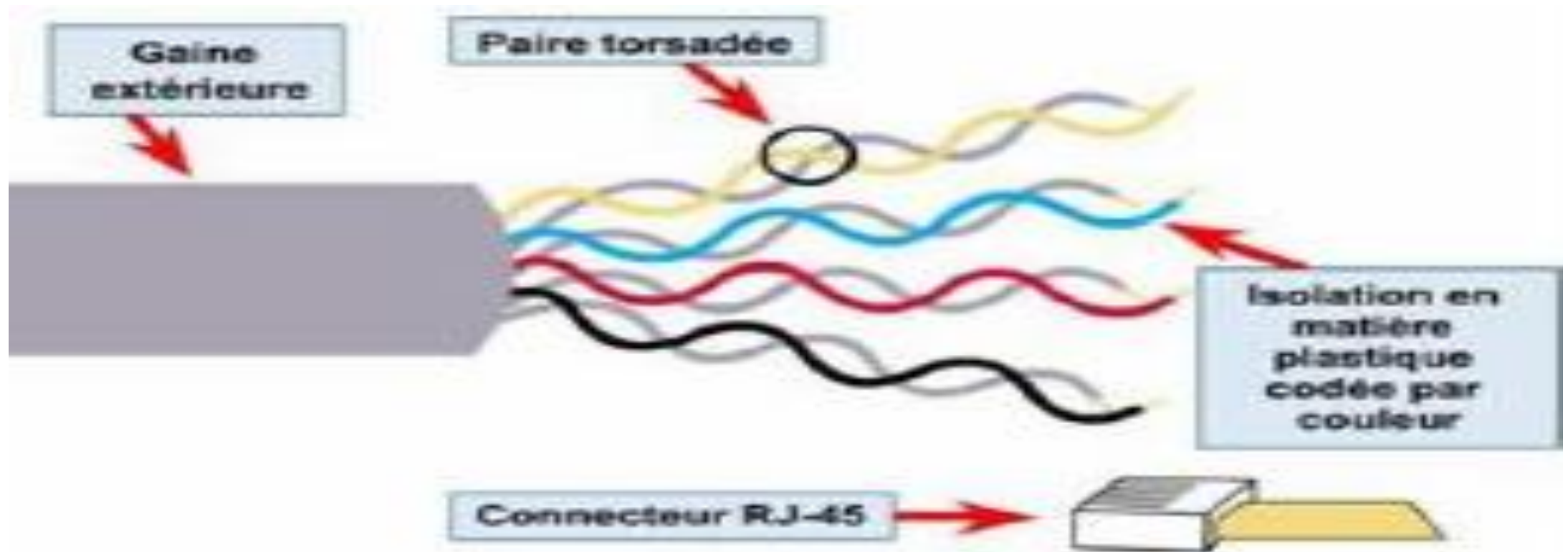
Le câble à paires torsadées

- Il existe deux types de câbles à paires torsadées :
 - Le câble à paire torsadée **non blindée** (UTP pour UNSHIELDED TWISTED-PAIR)
 - Le câble à paire torsadée **blindée** (STP pour SHIELDED TWISTED-PAIR)

Le câble à paires torsadées (UTP)

- Il comporte deux ou quatre paires de fils.
- Ce type de câble compte uniquement sur l'effet d'annulation produit par les paires torsadées pour limiter la dégradation du signal due aux interférences électromagnétiques et aux interférences de radiofréquences.
- Le câble UTP est le plus fréquemment utilisé pour les réseaux Ethernet.

Le câble à paires torsadées (UTP)



Le câble à paires torsadées (UTP)

- Les composants d'un câble à paire torsadée non blindée :
 - Deux ou quatre brins de cuivre entrelacés (torsadés)
 - Une enveloppe isolante
- Les caractéristiques du câble à paire torsadée non blindée (UTP) :
 - Utilisé à l'origine pour les lignes téléphoniques
 - Réponds aux spécifications de la norme « 10 base T » des réseaux ETHERNET
 - Très utilisé pour les réseaux locaux
 - Une longueur maximale de 100 mètres

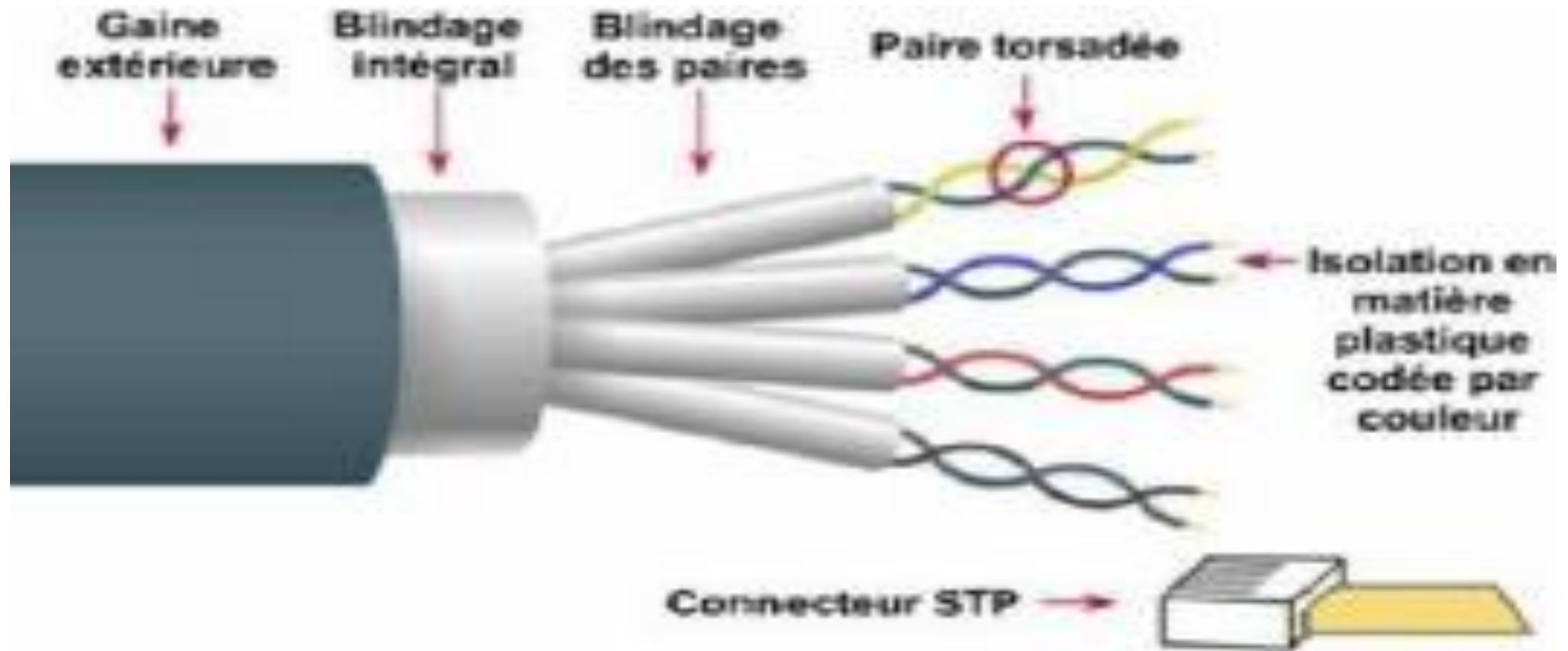
Le câble à paires torsadées (UTP)

Catégorie	Fonction	Vitesse	Nombre de paires torsadées
1	La voix analogique		
2	Les données numériques	4 Mb/s	4
3	Les données numériques	10 Mb/s	4
4	Les données numériques	16 Mb/s	4
5	Les données numériques	100 Mb/s	4

Le câble à paires torsadées (STP)

- allie les techniques de blindage, d'annulation et de torsion des fils.
- Chaque paire de fils est enveloppée dans une feuille métallique afin de protéger davantage les fils contre les bruits. Les quatre paires sont elles-mêmes enveloppées dans une tresse ou une feuille métallique.
- Le câble STP réduit le bruit électrique à l'intérieur du câble, mais également à l'extérieur du câble (interférences électromagnétiques et interférences de radiofréquences).

Le câble à paires torsadées (STP)

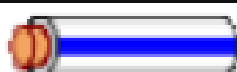
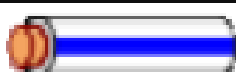
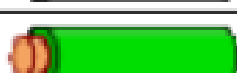


Les connecteurs

- C'est le connecteur RJ45 (Registered Jack) qui est le plus couramment utilisé en terminaison d'un câble à paires torsadées.
- Il comporte 8 broches de connexion électrique.
- Il est souvent associé au standard TIA/EIA-568-B qui décrit le brochage de terminaison du câble, Utilisé très couramment dans les réseaux informatiques câblés en étoile (type Ethernet), on le retrouve également en téléphonie.

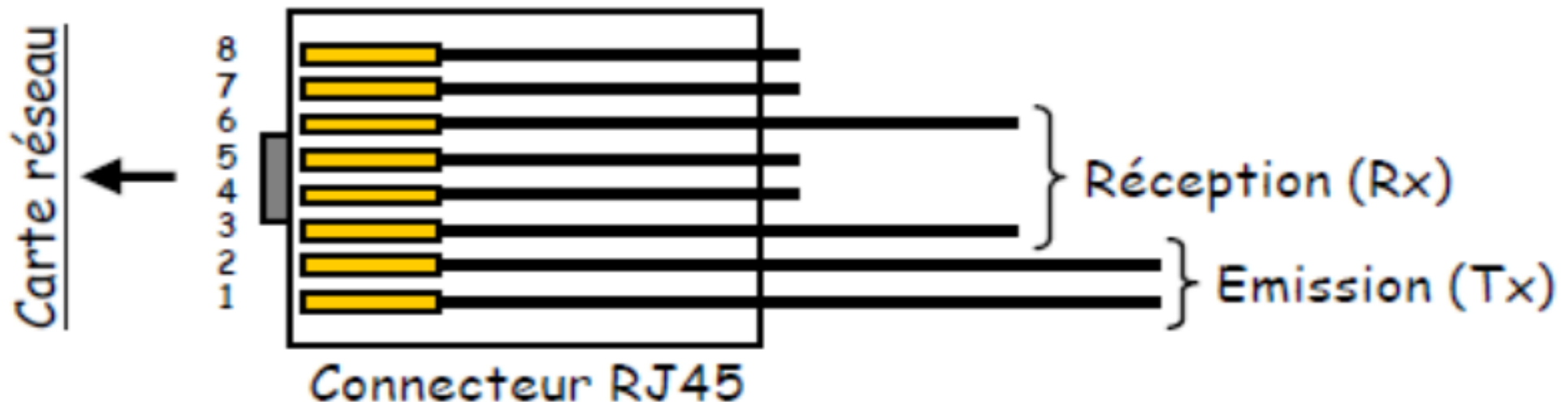


Les connecteurs

Norme T568A			Norme T568B		
pin	couleur	paire	paire	couleur	pin
8	 marron	4	4	 marron	8
7	 marron-blanc			 marron-blanc	7
6	 orange	2	3	 vert	6
5	 bleu-blanc	1	1	 bleu-blanc	5
4	 bleu			 bleu	4
3	 orange-blanc	2	3	 vert-blanc	3
2	 vert	3	2	 orange	2
1	 vert-blanc			 orange-blanc	1

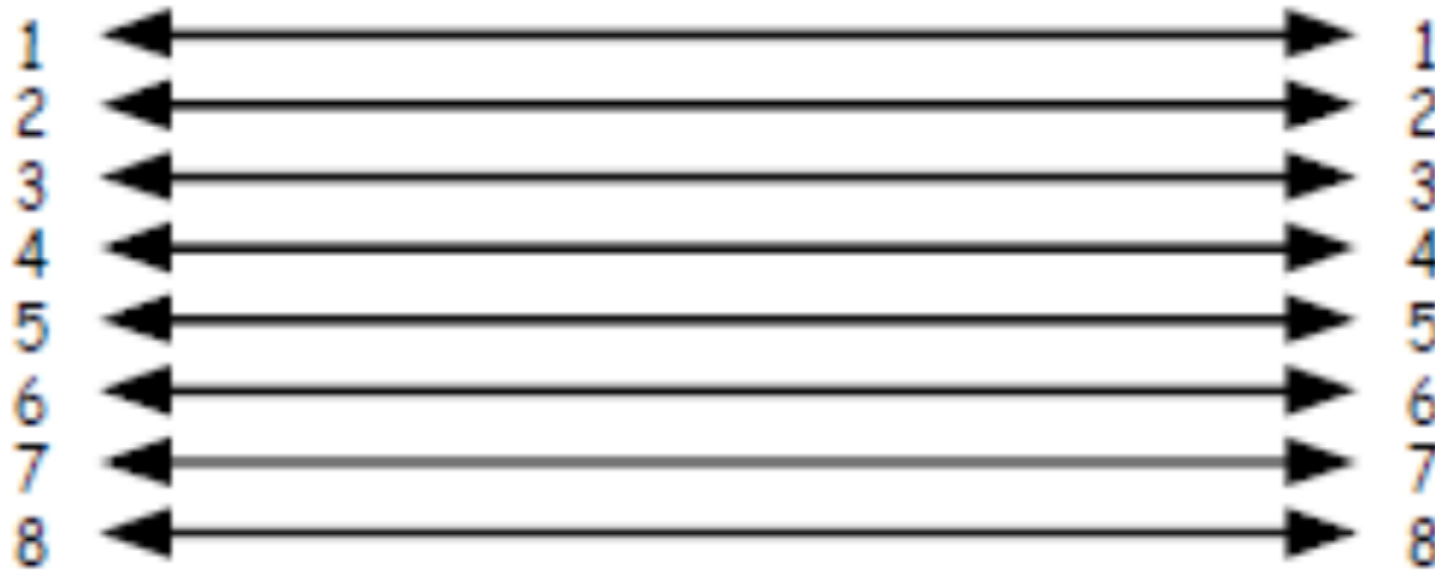
Les connecteurs

- Lors d'un câblage informatique en 10base-T ou 100base-T seules 2 paires torsadées sont utilisées : contacts 1-2 et 3-6.
- Une paire en émission (Tx) et une en réception (Rx).
- Lors d'une utilisation en 1000base-T, les 4 paires sont utilisées (8 contacts utilisés) en émission et réception.



Les connecteurs

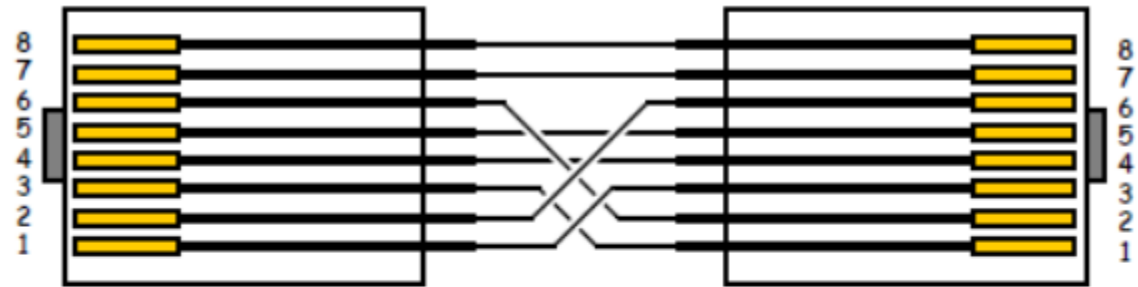
- Lorsqu'un poste de travail est connecté à un HUB (concentrateur) ou un SWITCH (commutateur), il faut utiliser un câble droit.



Les connecteurs

- Lorsque deux postes sont reliés directement, il faut utiliser un câble croisé.
- Certains équipements réseau récents sont toutefois capables de faire du (dé)croisement automatique en fonction du type de câble (MDI/MDI-X).

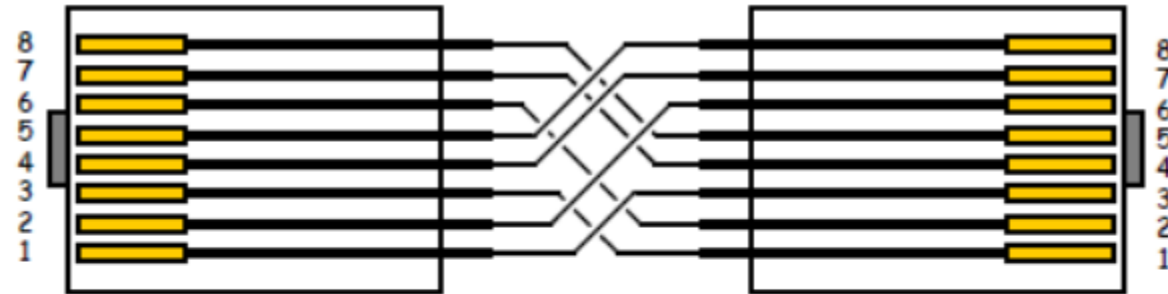
Les connecteurs



8	 marron	marron 	8
7	 marron-blanc	marron-blanc 	7
6	 orange	vert 	6
5	 bleu-blanc	bleu-blanc 	5
4	 bleu	bleu 	4
3	 orange-blanc	vert-blanc 	3
2	 vert	orange 	2
1	 vert-blanc	orange-blanc 	1

câble croisé en 10 base-T et 100base-Tx

Les connecteurs



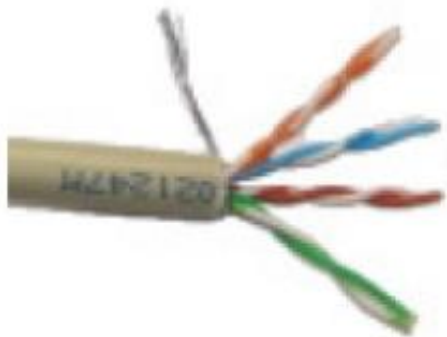
8		marron	bleu-blanc		8
7		marron-blanc	bleu		7
6		vert	orange		6
5		bleu-blanc	marron		5
4		bleu	marron-blanc		4
3		vert-blanc	orange-blanc		3
2		orange	vert		2
1		orange-blanc	vert-blanc		1

Câble croisé en 1000base-T

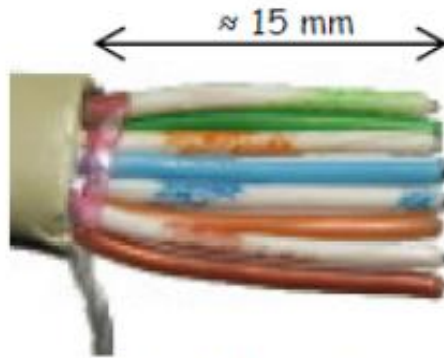
Les connecteurs

- La fabrication d'un câble réseau n'est pas très fréquente, elle peut rendre service dans certains cas
- C'est une opération minutieuse et quelques règles doivent être respectées.
- Les outils indispensables sont la pince coupante et la pince à sertir (RJ45).

Les connecteurs



Dénuder la gaine du câble.



Dépaire, trier les conducteurs selon le câblage désirer (ici 568A) et recouper.



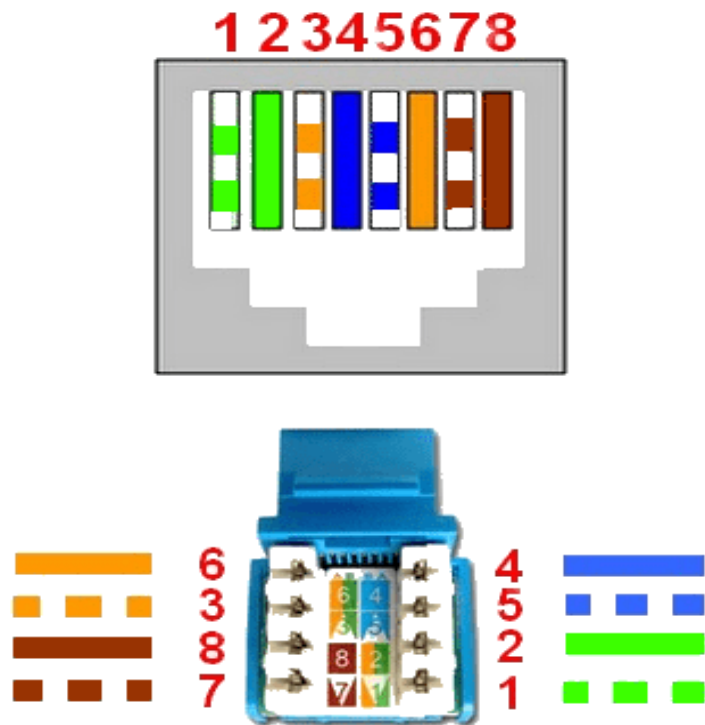
Insérer à fond dans le connecteur RJ45



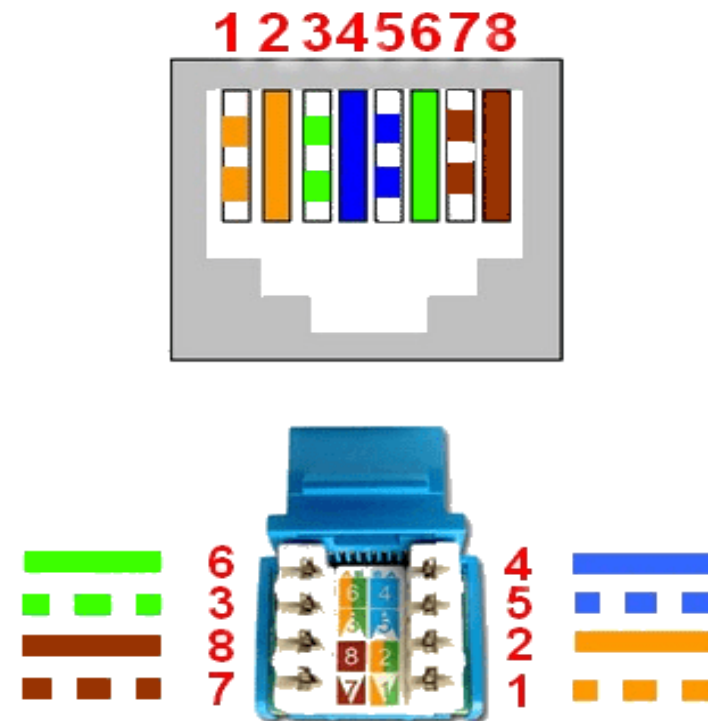
Sertir à l'aide de la pince

Les connecteurs

Norme T568A



Norme T568B



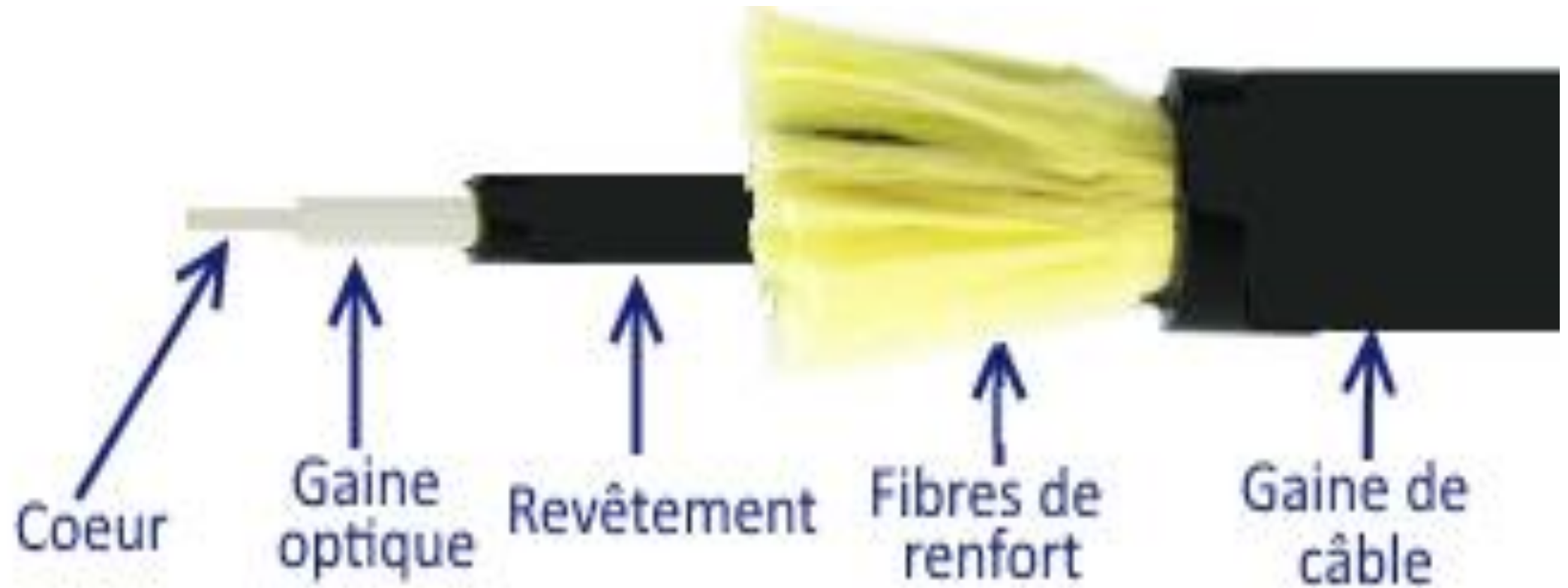
La fibre Optique

- Une fibre optique est un fil dont l'âme, très fine, en verre ou en plastique (250 micromètres), a la propriété de conduire la lumière et sert pour la fibroscopie, l'éclairage ou la transmission de données numériques.
- Elle offre un débit d'information nettement supérieur à celui des câbles coaxiaux et peut servir de support à un réseau « large bande » par lequel transitent aussi bien la télévision, le téléphone, la visioconférence ou les données informatiques.
- Entourée d'une gaine protectrice, la fibre optique peut être utilisée pour conduire de la lumière entre deux lieux distants de plusieurs centaines, voire milliers, de kilomètres.
- Le signal lumineux codé par une variation d'intensité est capable de transmettre une grande quantité d'information. En permettant les communications à très longue distance et à des débits jusqu'alors impossibles

La fibre Optique

- Le record actuel de débit de transmission a été établi par Les chercheurs de l'University College London (UCL) en septembre 2020 qui affirment avoir atteint la vitesse Internet de 178 térabits par seconde (Tbps).
- Selon eux, cette vitesse permettrait de télécharger la totalité du catalogue Netflix en moins d'une seconde.
- Pour y parvenir, les chercheurs ont utilisé des gammes de bande passante différentes de celles habituellement utilisées dans les systèmes optiques commerciaux.
- Les infrastructures de fibre optique classiques utilisent une bande passante de 4,5 THz, mais la bande passante de 9 THz est de plus en plus disponible dans le commerce.
- Pour leurs expériences, les chercheurs de l'UCL ont utilisé une bande de 16,8 THz.

La fibre Optique



La fibre Optique

- Il existe 2 types de fibre optique, chacune avec des caractéristiques déterminant un usage particulier.
- Les fibres de type multimode sont privilégiées sur de courtes distances pour des débits moins importants.
- Son fonctionnement permet de transporter plusieurs trajets lumineux.
- Conséquence ; un impact direct sur les performances de la fibre. Les fibres monomodes possèdent un seul canal de propagation qui permet un débit plus important.

La fibre Optique

- Il existe 4 catégories de réseaux qui correspondent au type de raccordement:
- **FTTH (Fiber To The Home):** Le client est raccordé au réseau par une fibre tirée entre le nœud de raccordement optique et l'intérieur de son local.
 - **Le FTTLA (Fiber To The Last Amplifier):** la fibre s'arrête à un nœud optique, les données sont acheminées par câble coaxial.
 - **FTTB (Fiber To The Building) et FTTC (Fiber To The Cabinet):** Dans ces deux cas, la fibre optique ne va pas jusqu'au local, les données sont alors transmises via le réseau téléphonique.

La fibre Optique

Avantages:

- Une plus grande bande passante et une vitesse plus élevée.
- Contrairement à ce que l'on pourrait croire, la fibre optique est bon marché.
- Les fibres optiques sont aussi plus minces et plus légères.
- Une capacité de charge plus élevée.
- La fibre optique offre moins de dégradation du signal.
- Les données sont transportées par des signaux lumineux.
- La fibre optique a une meilleure durée de vie

La fibre Optique

Inconvénients:

- L'utilisation de la fibre optique est limitée
- Fragilité : la fibre optique est plutôt fragile et plus vulnérable aux dommages par rapport aux fils de cuivre
- Distance : la distance entre l'émetteur et le récepteur doit rester courte.

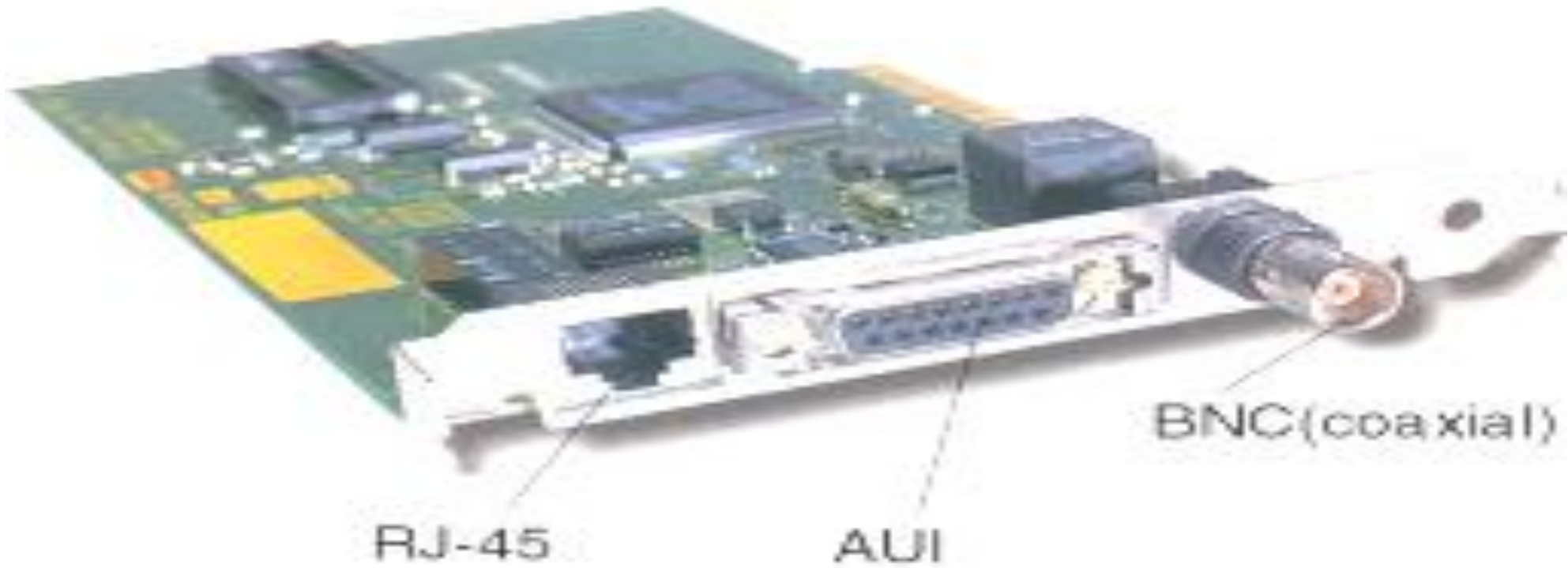
Tableau comparatif des spécificités des câbles					
	Le câble coaxial		La paire torsadée		La fibre optique
	Coaxial fin	Coaxial épais	Non blindée (UTP)	Blindée (STP)	
Norme	10 base 2	10 base 5	10 base T	10 base T	
Réseau	Ethernet fin	Ethernet épais			
Longueur	185 mètres	500 mètres	100 mètres	100 mètres	2 kilomètres
Connecteur	BNC	BNC, AUI	RJ45	RJ45	
Débit	10 Mb/s	10 Mb/s	10 à 100 Mb/s	10 à 100 Mb/s	0,1 à 1 Gb/s
Blindage	Oui	Oui	Non	Oui	Non
Installation	Simple	Simple	Simple	Simple	Complicquée
Flexible	Assez flexible	Peu flexible	Très flexible	Assez flexible	Pas du tout
Atténuation	Oui	Oui	Oui	Oui	Non
Interférences	Peu sensible	Peu sensible	Très sensible	Sensible	Pas du tout
Sécurité	Faible	Faible	Très faible	Assez Faible	Importante
Site	Moyen	Backbone	Petit	Token Ring	Excellence
Coût	Peu cher	Assez cher	Le moins cher	Pas cher	Le plus cher

Les équipements d'interconnexion

La carte réseau

- La carte réseau assure l'interface (la connexion) entre l'équipement ou la machine dans lesquels elle est montée et les machines connectées sur le même réseau.
- Aujourd'hui on peut trouver des cartes réseau un peu partout, dans les ordinateurs, imprimantes, téléphones portables, consoles de jeux, télévisions, etc.
- On n'utilise le terme « carte réseau » que dans le cas d'une carte électronique autonome prévue pour remplir ce rôle d'interface réseau.

La carte réseau



Le répéteur

- Dans une ligne de transmission, le signal subit des dégradations et un affaiblissement d'autant plus importants que la distance qui sépare deux éléments actifs est longue.
- Généralement, deux nœuds d'un réseau local ne peuvent pas être distants de plus de quelques centaines de mètres, c'est la raison pour laquelle un équipement supplémentaire est nécessaire au-delà de cette distance, appelée souvent répéteur.
- Un répéteur (en anglais repeater) est un équipement simple permettant de régénérer un signal entre deux nœuds du réseau, afin d'étendre la distance de câblage d'un réseau.
- Le répéteur travaille uniquement au niveau physique (couche 1 du modèle OSI), c'est-à-dire qu'il ne travaille qu'au niveau des informations binaires circulant sur la ligne de transmission et qu'il n'est pas capable d'interpréter les paquets d'informations.
- D'autre part, un répéteur peut permettre de constituer une interface entre deux supports physiques de types différents, c'est-à-dire qu'il peut par exemple permettre de relier un segment de paire torsadée à un brin de fibre optique.

Le répéteur



Le concentrateur (HUB)

- Le concentrateur est un élément matériel permettant de concentrer le trafic réseau provenant de plusieurs hôtes, et de régénérer le signal.
- Le concentrateur est ainsi une entité possédant un certain nombre de ports (il possède autant de ports qu'il peut connecter de machines entre elles, généralement 4, 8, 16 ou 32).
- Son unique but est de récupérer les données binaires parvenant sur un port et de les diffuser sur l'ensemble des ports.
- Tout comme le répéteur, le concentrateur opère au niveau 1 du modèle OSI, c'est la raison pour laquelle il est parfois appelé répéteur multiports.

Le concentrateur (HUB)

- Il est possible de connecter plusieurs hubs entre eux afin de concentrer un plus grand nombre de machines, on parle alors de connexions en cascade (parfois appelé daisy chains en anglais).
- Pour ce faire, il suffit de connecter les hubs à l'aide d'un câble croisé, c'est-à-dire un câble reliant les connecteurs de réception d'une extrémité aux connecteurs de réception de l'autre.
- Les concentrateurs sont en général dotés d'un port spécial appelé "uplink" permettant d'utiliser un câble droit pour connecter deux hubs entre eux.
- Il existe également des hubs capables de croiser ou de décroiser automatiquement leurs ports selon qu'il est relié à un hôte ou à un hub.

Le concentrateur (HUB)



Le commutateur (SWITCH)

- Un commutateur (en anglais Switch) est un pont multiports, c'est-à-dire qu'il s'agit d'un élément actif agissant au niveau 2 du modèle OSI.
- Le commutateur analyse les trames arrivant sur ses ports d'entrée et filtre les données afin de les aiguiller uniquement sur les ports adéquats
- il utilise un mécanisme de filtrage et de commutation consistant à diriger les flux de données vers les machines les plus appropriées, en fonction de certains éléments présents dans les paquets de données,
- il inspecte les adresses de source et de destination des messages, dresse une table qui lui permet alors de savoir quelle machine est connectée sur quel port du switch.

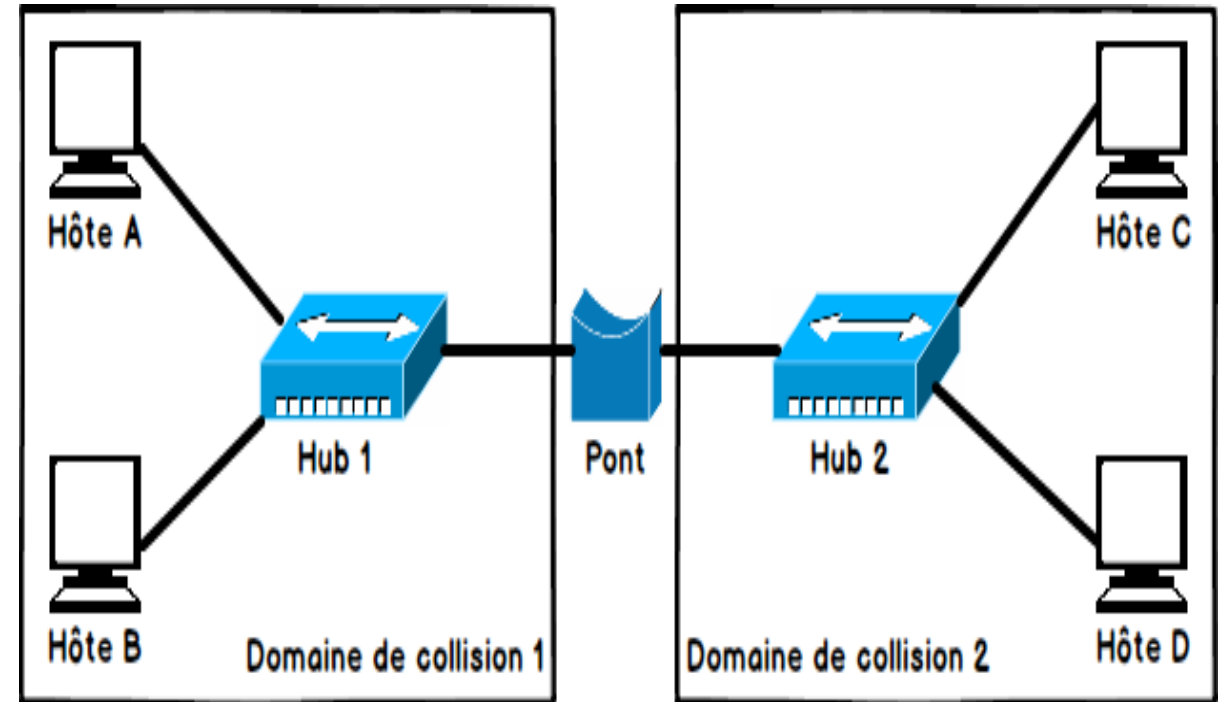
Le commutateur (SWITCH)



Le pont

- Un pont est un dispositif matériel permettant de relier des réseaux travaillant avec le même protocole.
- Ainsi, contrairement au répéteur, qui travaille au niveau physique, le pont travaille également au niveau logique (la couche 2 du modèle OSI),
- Il est capable de filtrer les trames en ne laissant passer que celles dont l'adresse correspond à une machine située à l'opposé du pont.
- En contrepartie, l'opération de filtrage réalisée par le pont peut conduire à un léger ralentissement lors du passage d'un réseau à l'autre, c'est la raison pour laquelle les ponts doivent être judicieusement placés dans un réseau.

Le pont



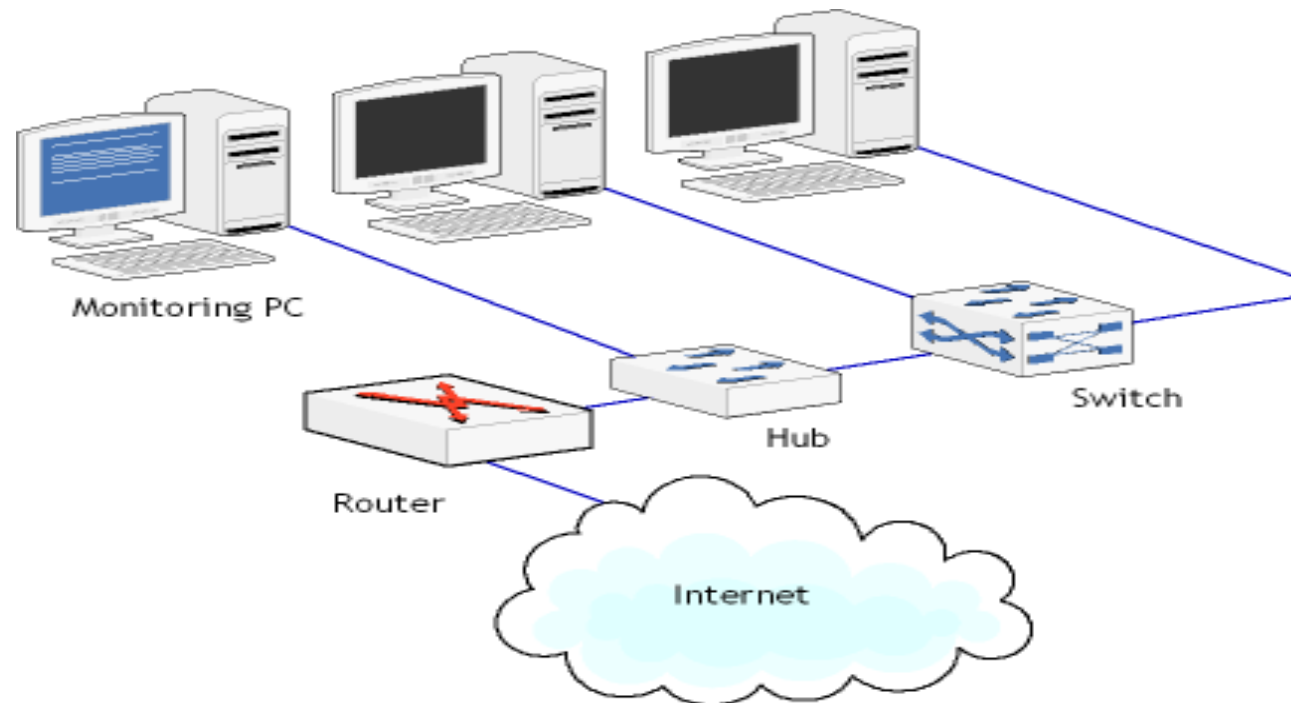
Le routeur

- Un routeur est un équipement d'interconnexion de réseaux informatiques permettant d'assurer le routage des paquets entre deux réseaux ou plus afin de déterminer le chemin qu'un paquet de données va emprunter.
- Lorsqu'un utilisateur appelle une URL, le client Web (navigateur) interroge le serveur de noms (DNS), qui lui indique en retour l'adresse IP de la machine visée.
- Son poste de travail envoie la requête au routeur le plus proche, c'est-à-dire à la passerelle par défaut du réseau sur lequel il se trouve.
- Ce routeur va ainsi déterminer la prochaine machine à laquelle les données vont être acheminées de manière à ce que le chemin choisi soit le meilleur.

Le routeur

- Les routeurs tiennent à jour des tables de routage, véritable cartographie des itinéraires à suivre en fonction de l'adresse visée.
- En plus de leur fonction de routage, les routeurs permettent de manipuler les données circulant sous forme de datagrammes afin d'assurer le passage d'un type de réseau à un autre.
- Dans la mesure où les réseaux n'ont pas les mêmes capacités en termes de taille de paquets de données, les routeurs sont chargés de fragmenter les paquets de données pour permettre leur libre circulation.
- Un routeur sans fil est le même que celui d'un routeur classique, si ce n'est qu'il permet à des dispositifs sans-fil (stations Wifi par exemple) de se connecter aux réseaux auxquels le routeur est connecté par des liaisons filaires (généralement Ethernet).

Le routeur



Le modem

- Est le périphérique utilisé pour transférer des informations entre plusieurs ordinateurs via un support de transmission filaire (lignes téléphoniques par exemple).
- Les ordinateurs fonctionnent de façon numérique, ils utilisent le codage binaire (une série de 0 et de 1), mais les lignes téléphoniques sont analogiques.
- Les signaux numériques passent d'une valeur à une autre, il n'y a pas de milieu, de moitié, c'est du « Tout Ou Rien » (un ou zéro). Les signaux analogiques par contre n'évoluent pas « par pas », ils évoluent de façon continue.
- Le modem convertit en analogique l'information binaire provenant de l'ordinateur, afin de le moduler par la ligne téléphonique. On peut entendre des bruits étranges si l'on monte le son provenant du modem.
- Ainsi, le modem module les informations numériques en ondes analogiques. En sens inverse, il démodule les données analogiques pour les convertir en numérique. Le mot « modem » est ainsi un acronyme pour « MOdulateur/DEModulateur ».

Le modem



Le modem

- La vitesse de transmission du modem est généralement exprimée en bauds, en hommage à Emile Baudot (11 septembre 1845 - 28 mars 1903), un célèbre ingénieur français ayant œuvré dans les télécommunications.
- Cette unité de vitesse de transmission d'informations caractérise la fréquence de (dé)modulation, c'est-à-dire le nombre de changements d'état que le modem fait subir au signal par seconde.
- Le débit en bauds n'est pas tout à fait égal au débit en bits par secondes, car plus d'un changement d'état du signal peut être nécessaire pour coder un bit.

Le modem

- La multiplication des modems a nécessité une standardisation des protocoles de communication par modem afin qu'ils parlent tous un langage commun.
- Deux organismes ont mis au point des standards de communication :
 - Les laboratoires BELL, précurseurs en matière de télécommunication ;
 - Le Comité consultatif international de téléphonie et de télégraphie (CCITT), renommé depuis 1990 en union internationale des télécommunications (UIT).
- L'UIT a pour but de définir les standards de communications internationaux.
- Les standards des modems peuvent se diviser en 3 catégories :
 - Les standards de modulation (par exemple CCITT V.21)
 - Les standards de correction d'erreurs (par exemple CCITT V.42)
 - Les standards de compression des données (par exemple CCITT V.42bis)

Les architectures des réseaux informatiques

Type de réseaux

- Il existe 2 modes de fonctionnement des réseaux :
 - poste à poste ou égal à égal (en anglais peer to peer), dans lequel il n'y a pas d'ordinateur central et chaque ordinateur a un rôle similaire exemple du partage de fichier sous Windows.
 - client/serveur, dans lequel un ordinateur central fournit des services réseaux aux utilisateurs exemple des serveurs FTP.

L'architecture poste-à-poste

- Chaque ordinateur dans un tel réseau joue à la fois le rôle de serveur et de client.
- Cela signifie notamment que chacun des ordinateurs du réseau est libre de partager ses ressources.
- Les réseaux poste à poste ne nécessitent pas les mêmes niveaux de performance et de sécurité que les logiciels réseaux pour serveurs dédiés.
- Tous les systèmes d'exploitation intègrent toutes les fonctionnalités du réseau poste-à-poste.
- Chaque utilisateur administre son propre poste. D'autre part tous les utilisateurs peuvent partager leurs ressources comme ils le souhaitent (données dans des répertoires partagés, imprimantes, cartes fax etc.)

L'architecture poste-à-poste

- La mise en œuvre d'une telle architecture réseau repose sur des solutions standards :
 - Placer les ordinateurs sur le bureau des utilisateurs
 - Chaque utilisateur est son propre administrateur et planifie lui-même sa sécurité pour les connexions, on utilise un système de câblage simple et apparent
- Il s'agit généralement d'une solution satisfaisante pour des environnements ayant les caractéristiques suivantes :
 - Moins de 10-30 utilisateurs
 - Tous les utilisateurs sont situés dans une même zone géographique
 - La sécurité n'est pas un problème crucial
 - Ni l'entreprise ni le réseau ne sont susceptibles d'évoluer de manière significative dans un proche avenir

L'architecture poste-à-poste

Avantages:

- Un coût réduit.
- Très simple à réaliser (la gestion et la mise en place du réseau et des machines sont peu compliquées).
- Il est facile de mettre en réseau des postes qui étaient au départ isolés.
- Chaque utilisateur peut décider de partager l'une de ses ressources avec les autres postes.
- Dans un groupe de travail, l'imprimante peut être utilisée par tous.
- Cette méthode est pratique et peu coûteuse pour créer un réseau domestique.

L'architecture poste-à-poste

Inconvénients :

- Ce système n'est pas du tout centralisé, ce qui le rend très difficile à administrer ;
- La sécurité est moins facile à assurer, compte tenu des échanges transversaux ;
- Aucun maillon du système ne peut être considéré comme fiable.
- Ainsi, les réseaux d'égal à égal sont préférentiellement utilisés pour des applications ne nécessitant pas un haut niveau de sécurité ni une disponibilité maximale (il est donc déconseillé pour un réseau professionnel avec des données sensibles).

L'architecture poste-à-poste

Inconvénients :

- Chaque utilisateur a la responsabilité du fonctionnement du réseau.
- Les outils de sécurité sont très limités.
- Si un poste est éteint ou s'il se "plante", ses ressources ne sont plus accessibles.
- Le système devient ingérable lorsque le Nombre de postes augmente.
- Lorsqu'une ressource est utilisée sur une machine, l'utilisateur de cette machine peut voir ses performances diminuer

L'architecture client/serveur

- De nombreuses applications fonctionnent selon un environnement client/serveur, cela signifie que des machines clientes (des machines faisant partie du réseau) contactent un serveur.
- Un serveur est une machine généralement très puissante en termes de capacités d'entrée-sortie, qui leur fournit des services.
- Ces services sont des programmes fournissant des données telles que l'heure, des fichiers, une connexion, etc.

L'architecture client/serveur

- Les services sont exploités par des programmes, appelés programmes clients, s'exécutant sur les machines clientes.
- On parle ainsi de client (client FTP, client de messagerie, etc.) lorsque l'on désigne un programme tournant sur une machine cliente, capable de traiter des informations qu'il récupère auprès d'un serveur (dans le cas du client FTP il s'agit de fichiers, tandis que pour le client de messagerie il s'agit de courrier électronique).

L'architecture client/serveur

Avantages:

- Le modèle client/serveur est particulièrement recommandé pour des réseaux nécessitant un grand niveau de fiabilité.
- **Des ressources centralisées** : étant donné que le serveur est au centre du réseau, il peut gérer des ressources communes à tous les utilisateurs, par exemple une base de données centralisée, afin d'éviter les problèmes de redondance et de contradiction
- **Une meilleure sécurité** : car le nombre de points d'entrée permettant l'accès aux données est moins important
- **Une administration au niveau serveur** : les clients ayant peu d'importance dans ce modèle, ils ont moins besoin d'être administrés

L'architecture client/serveur

Avantages:

- **Un réseau évolutif** : grâce à cette architecture, il est possible de supprimer ou rajouter des clients sans perturber le fonctionnement du réseau et sans modification majeure
- Les serveurs sont conçus pour le partage de ressources et ne servent pas de station de travail.
- Il suffit de les dimensionner en fonction de la taille du réseau et du nombre de clients susceptibles de s'y connecter.
- Les systèmes d'exploitation de serveurs proposent des fonctions avancées de sécurité que l'on ne trouve pas sur les réseaux "peer to peer".

L'architecture client/serveur

Avantages:

- Ils proposent également des fonctions avancées à l'usage des utilisateurs par exemple les profils itinérants qui permettent à un utilisateur (sous certaines conditions) de retrouver son environnement de travail habituel, même s'il change de poste de travail.
- Les serveurs étant toujours en service (sauf en cas de panne), les ressources sont toujours disponibles pour les utilisateurs.
- Les sauvegardes de données sont centralisées, donc beaucoup plus faciles à mettre en œuvre.
- Un administrateur gère le fonctionnement du réseau et les utilisateurs n'ont pas à s'en préoccuper.

L'architecture client/serveur

Inconvénients:

- Le serveur est le seul maillon faible du réseau client/serveur, étant donné que tout le réseau est architecturé autour de lui ! Heureusement, le serveur a une grande tolérance aux pannes (notamment grâce au système RAID)
- La mise en place d'un tel réseau est beaucoup plus lourde qu'un cas simple de "poste à poste".
- Elle nécessite impérativement la présence d'un administrateur possédant les compétences nécessaires pour faire fonctionner le réseau.
- Le coût est évidemment plus élevé puisqu'il faut la présence d'un ou de plusieurs serveurs.
- Si un serveur tombe en panne, ses ressources ne sont plus disponibles. Il faut donc prévoir des solutions plus ou moins complexes, plus ou moins onéreuses, pour assurer un fonctionnement au moins minimum en cas de panne

L'architecture à plusieurs niveaux

- **L'architecture à deux niveaux** (aussi appelée architecture 2-tier, tier signifiant rangé en anglais) caractérise les systèmes clients/serveurs pour lesquels le client demande une ressource et le serveur la lui fournit directement, en utilisant ses propres ressources. Cela signifie que le serveur ne fait pas appel à une autre application afin de fournir une partie du service.
- **L'architecture à 3 niveaux** (appelée architecture 3-tier), il existe un niveau intermédiaire, c'est-à-dire que l'on a généralement une architecture partagée entre :
 - Un client (l'ordinateur demandeur de ressources), le serveur d'application (appelé également middleware), chargé de fournir la ressource, mais faisant appel à un autre
 - Serveur: le serveur de données, fournissant au serveur d'application les données dont il a besoin. Il peut y avoir plusieurs serveurs de données.

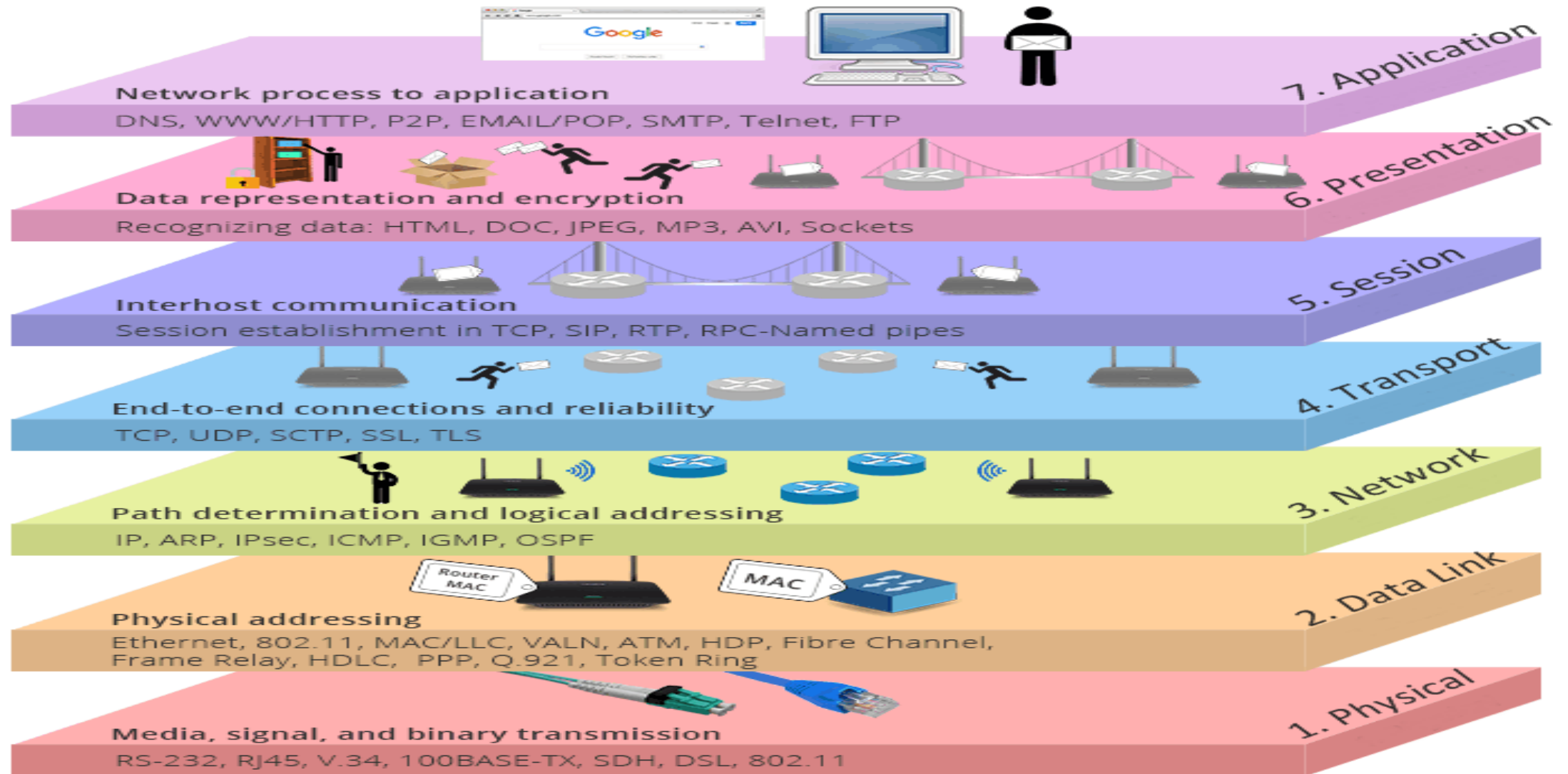
Les normes de communication TCP/IP et OSI

- Les communications de données entre différents réseaux ne sont pas possibles s'il n'existe pas de règles communes pour la transmission et la réception des paquets de données.
- Ces règles sont connues sous le nom de protocoles, parmi lesquels le protocole de contrôle de transmission (TCP) / protocole Internet (IP) est l'un des plus utilisés.
- Le modèle TCP/IP est couramment utilisé dans la description du réseau et est plus vieux que le modèle OSI.
- Ils ont tous deux plusieurs couches.

Couches du modèle de référence OSI

- Le modèle OSI est un modèle conceptuel qui caractérise et normalise la façon dont différents composants logiciels et matériels impliqués dans une communication réseau doivent diviser le travail et interagir les uns avec les autres.
- Il contient sept couches:
 - Couche 7 : Couche d'application,
 - Couche 6 : Couche de présentation,
 - Couche 5 : Couche de session,
 - Couche 4 : Couche transport,
 - Couche 3 : Couche réseau,
 - Couche 2 : Couche de liaison de données,
 - Couche 1 : Couche physique.

Couches du modèle de référence OSI



Couches de modèle TCP/IP

- Le modèle TCP/IP est également un modèle de référence en couches, mais c'est un modèle à quatre couches.
- Il est également connu sous le nom de "suite de protocoles Internet".
- Il est généralement appelé TCP/IP parce que les protocoles de base sont TCP et IP, mais ce ne sont pas les seuls protocoles utilisés dans ce modèle.

Couches de modèle TCP/IP

Couche d'Application

- La couche d'application du modèle TCP/IP permet aux applications d'accéder aux services des autres couches, et détermine les protocoles que les applications utilisent pour échanger des données.
- Les protocoles de couche d'application les plus connus sont HTTP, FTP, SMTP, Telnet, DNS, SNMP et Routing Information Protocol (RIP).

Couches de modèle TCP/IP

Couche de Transport

- La couche transport, également connue comme la couche transport hôte-à-hôte, est chargée de fournir à la couche application des services de communication de session et de datagramme.
- Les protocoles de base de cette couche sont TCP et UDP.
- TCP fournit un service de communication fiable de dispositif à dispositif et axé sur la connexion. Il est responsable de la séquence et reconnaissance de réception des paquets envoyés, et récupération des paquets perdus en transmission.
- UDP fournit un service de communication sans connexion et peu fiable de dispositif à dispositif ou dispositif à plusieurs dispositifs. UDP est généralement utilisé lorsqu'il y a une faible quantité de données à transférer (par exemple, lorsque les données peuvent tenir dans un seul paquet).

Couches de modèle TCP/IP

Couche Internet

- La couche Internet est responsable des fonctions d'adressage, du conditionnement et de routage des hôtes.
- Les principaux protocoles de la couche de protocole Internet sont:
 - IP: un protocole routable responsable de l'adressage IP, du routage, de la fragmentation et du réassemblage des paquets. Il existe maintenant une adresse IPv4 (32 bits) et une adresse IP Ipv6 (128 bits).
 - Protocole de résolution d'adresse (ARP): ARP est responsable de la découverte des adresses de la couche d'accès au réseau telles que les adresses matérielles associées à une couche d'accès Internet déterminée.

Couches de modèle TCP/IP

Couche Internet

- Protocole de message de contrôle Internet (ICMP): chargé de fournir des fonctions de diagnostic et de signaler les erreurs provoquées par une mauvaise livraison de paquets IP.
- Protocole de gestion de groupe Internet (IGMP): responsable de la gestion des groupes de multidiffusion (Multicast) IP.

Couches de modèle TCP/IP

Couche Accès Réseau

- La couche d'accès réseau (ou couche de liaison) est responsable de placer et de recevoir les paquets TCP/IP dans et en dehors du support réseau.
- TCP/IP est conçu pour être indépendant de la méthode d'accès au réseau, du format de trame et du support.
- En d'autres termes, il est indépendant de toute technologie de réseau spécifique.
- De cette façon, TCP/IP peut être utilisé pour connecter différents types de réseaux, tels que l'Ethernet, Token Ring, et Asynchronous Transfer Mode (ATM).

OSI Model

Application Layer

Presentation Layer

Session Layer

Transport Layer

Network Layer

Data Link Layer

Physical Layer

TCP/IP Model

Application Layer

Transport Layer

Internet Layer

Network Access Layer

TCP/IP Protocol Suite

H
T
T
P

S
M
T
P

T
e
l
n
e
t

F
T
P

D
N
S

R
I
P

S
N
M
P

TCP

UDP

ARP

IP

IGMP

ICMP

Ethernet

Token
Ring

ATM

Frame
Relay

Le DNS

- Tout d'abord, DNS veut dire "Domain Name System" ou système de nom de domaine.
- Pour mieux comprendre, le rôle et le fonctionnement d'un serveur DNS, voici l'exemple suivant :
 - Vous souhaitez appeler quelqu'un dont vous ne connaissez pas le N° de téléphone ?
 - Que faites-vous ?
 - Vous utilisez un annuaire !

Le DNS

- Un serveur DNS est un annuaire pour ordinateur.
- Lorsque vous voulez accéder à un ordinateur dans le réseau, votre ordinateur va interroger le serveur DNS pour récupérer l'adresse de l'ordinateur que vous voulez joindre.
- Une fois, que l'ordinateur ait récupéré l'adresse du destinataire, il pourra le joindre directement avec son adresse IP.

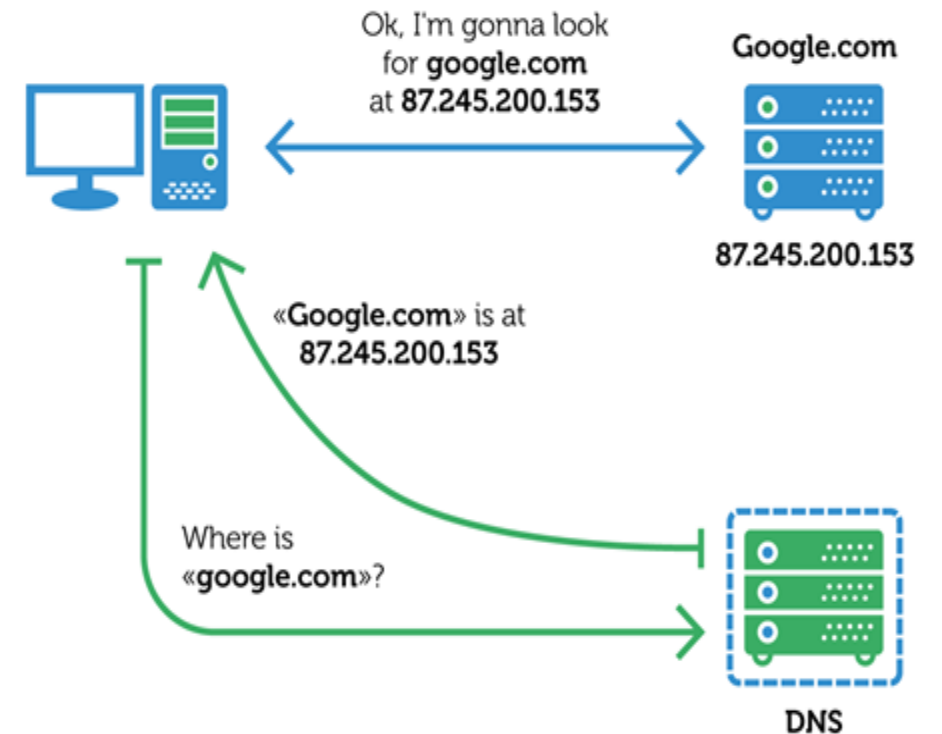
Le DNS

- Toutes les machines (ordinateurs, serveurs, routeurs, etc.) connectées à Internet possèdent, elles aussi, une adresse IP.
- Cette adresse IP permet aux machines de communiquer entre elles.
- Cependant, cela va nous poser un petit problème. Nous avons beau être des êtres humains avec une bonne mémoire, notre cerveau n'est pas fait pour retenir des séries de chiffres comme 193.194.69.93. On aimerait mieux avoir à retenir des noms comme www.univ-guelma.dz.
- Il ne s'agit donc pas d'un problème technique, Internet fonctionne très bien avec des adresses IP, mais d'un problème de nommage pour permettre un accès simplifié à Internet pour nous tous. Ce système de nommage est tout simplement le Domain Name System (DNS).

Le DNS

- Exemple

Vous avez lancé votre navigateur Internet et vous avez utilisé “www.google.com” comme moteur de recherche par défaut. Donc la page Google s’est affichée. Voici le mécanisme complet et regardez à quel endroit le serveur DNS est appelé.

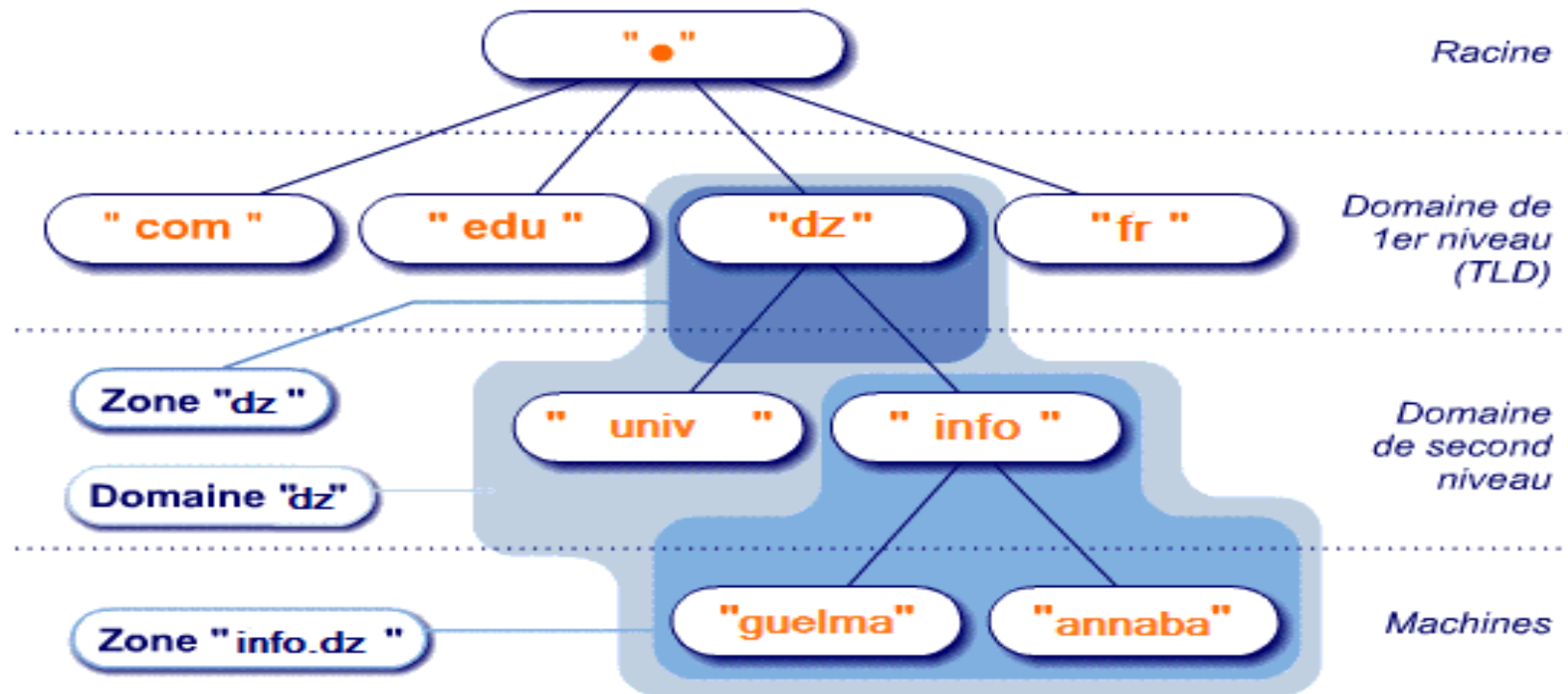


Le DNS

- Dans l'exemple ci-dessus, on voit que la requête "quelle est l'adresse de `www.google.com`" a répondu `87.245.200.153`. Cette requête s'appelle une résolution de nom de domaine.
- Si l'on poursuit, on peut constater que le serveur DNS n'est utilisé que sur la partie 1-Question et 2-Réponse. Une fois que l'ordinateur a récupéré l'adresse du serveur à joindre, il n'a plus besoin du serveur DNS.
- Cette adresse IP n'est pas une adresse au hasard. Elle correspond bien à un des serveurs de Google. (Il y en a évidemment un grand nombre).
- Donc, si dans votre dans la barre d'adresse de votre navigateur, vous tapez : `http:// 87.245.200.153`, la page de recherche de Google doit s'afficher.

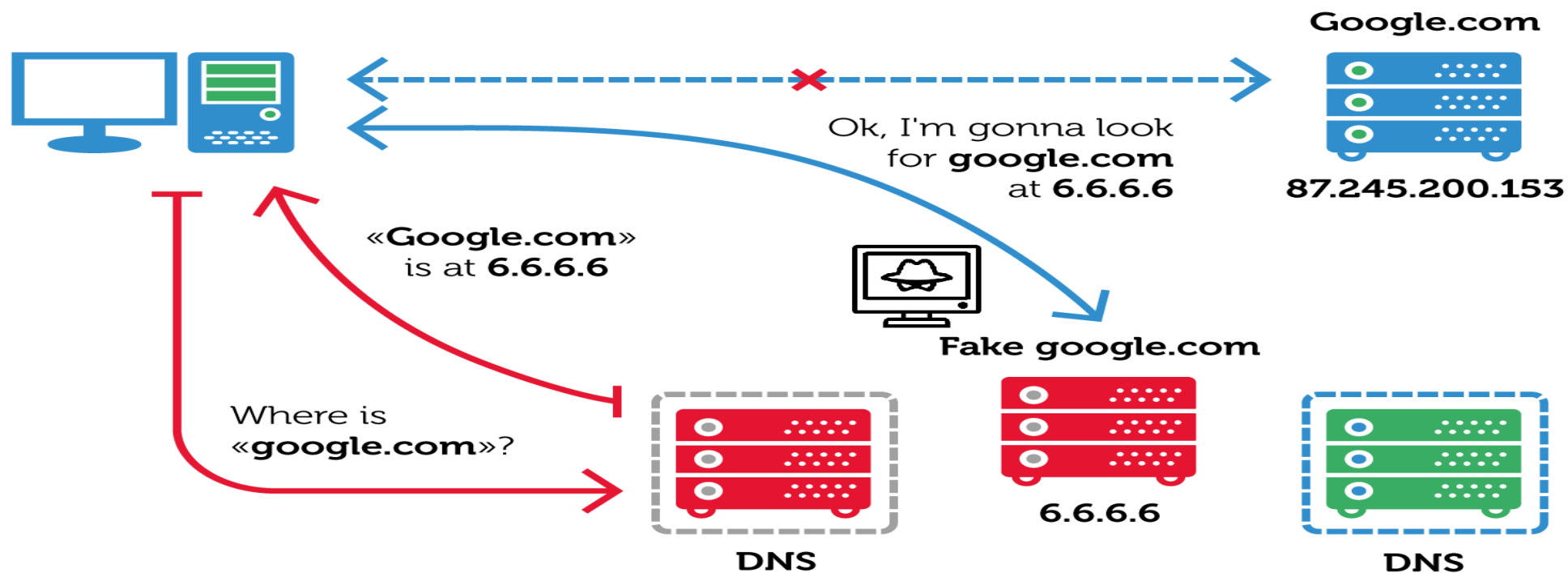
Le DNS

- Les serveurs DNS fonctionnent en cascade. Pour expliquer cela, on pourrait dire que lorsqu'un serveur ne connaît pas la réponse, il va demander à son "parent".



Le DNS

Il existe des virus qui modifient vos paramètres réseaux ou votre fichier "hosts" pour faire pointer les requêtes DNS vers des serveurs pirates. Vous verrez que les navigateurs peuvent afficher des messages lorsque cela se produit.



Serveurs DNS primaire et auxiliaire

Sous Windows, au niveau des propriétés d'une connexion au réseau local, il y a les adresses Serveur DNS préféré et auxiliaire, on peut se poser la question, où se trouvent ses serveurs et sont-ils physiques ou logiciels ? et c'est quoi la différence entre eux ?

- Il y a deux possibilités :
 - Si vous êtes un particulier, vous utilisez les DNS de votre fournisseur d'accès à Internet, car votre box envoie ces paramètres à votre ordinateur.
 - Si votre ordinateur est connecté à un réseau d'entreprise, les DNS sont généralement des serveurs situés au sein de l'entreprise. Ces serveurs peuvent être des serveurs physiques ou des serveurs virtuels.

Serveurs DNS primaire et auxiliaire

- Tout réseau n'étant pas à l'abri d'une panne, il est fortement recommandé d'avoir deux serveurs DNS dans un réseau : le Principal étant celui qui répond aux requêtes en temps normal, le secondaire prenant le relais si le principal ne répond pas ou met trop de temps à répondre.
- Ces informations sont bien souvent renseignées automatiquement par le DHCP.

Le DHCP

- Un serveur DHCP (ou service DHCP : Dynamic Host Configuration Protocol) est un serveur (ou service) qui délivre des adresses IP aux équipements qui se connectent sur le réseau.
- La plupart du temps, les cartes réseaux de ces équipements sont en attente d'une adresse IP leur permettant de communiquer sur le réseau.
- En même temps qu'il envoie l'adresse, le service DHCP envoie quelques informations complémentaires concernant le réseau sur lequel est branché l'hôte qui reçoit cette adresse.

Le DHCP

- Les cartes réseaux des ordinateurs (ou plus généralement de tous les équipements qui sont branchés sur un réseau : ordinateur, smartphone, objets connectés, etc.) doivent être paramétrées pour recevoir automatiquement des adresses lorsque l'ordinateur démarre ou que l'on le connecte au réseau.
- Par défaut c'est le cas, car c'est la méthode la plus simple pour obtenir une adresse IP.
- Exemple si vous n'avez pas attribué d'adresse IP à votre ordinateur, votre box internet remplit ce rôle de serveur DHCP sans que vous le sachiez !

Le DHCP

- On rappelle que l'adresse IP doit être unique sur un réseau donc le serveur DHCP va gérer les adresses et n'attribuer que des adresses non utilisées à tout nouvel hôte qui en fait la demande.
- Le serveur DHCP va délivrer un bail DHCP à l'ordinateur qui en fait la demande. (Et uniquement à ceux qui en font la demande, et non pas à tous les ordinateurs qui se connectent sur le réseau).
- Un bail, contient 3 choses qui nous intéressent :
 - Une durée de vie (durée du bail)
 - Une adresse IP.
 - Les paramètres du réseau.

NetBIOS

- NetBIOS (NETwork Basic Input Output System) est une architecture réseau codéveloppée par IBM et Sytek (en) au début des années 1980.
- NetBIOS est utilisé principalement par Microsoft.
- Ce n'est pas un protocole réseau, mais un système de nommage et une interface logicielle qui permet d'établir des sessions entre différents ordinateurs d'un réseau.
- NetBIOS a connu plusieurs implémentations :
 - NBF (NetBIOS Frames Protocol, connu à tort sous le nom NetBEUI)
 - NBX (NetBIOS over IPX/SPX)
 - NBT (NetBIOS over TCP/IP)
- Les deux premières ont disparu de nos jours.
- Les noms NetBIOS sont appelés à disparaître en faveur des noms DNS. De plus, le partage de fichiers avec le protocole SMB peut à présent se passer de NetBIOS et fonctionner directement par-dessus TCP/IP.

WINS

- Windows Internet Name Service (WINS) est un serveur de noms et services pour les ordinateurs utilisant NetBIOS.
- Depuis Windows 2000, Microsoft conseille à ses clients d'utiliser Active Directory (et le DNS Dynamique) plutôt que WINS.
- En pratique, WINS est aux noms Netbios, ce que le DNS est au FQDN - un dépôt central d'informations (base de données), auquel un client voulant contacter un ordinateur sur le réseau peut envoyer des requêtes pour trouver l'adresse IP à joindre, plutôt que d'envoyer une requête globale (à tout le monde - broadcast -) pour demander l'adresse à contacter.
- L'objectif est de réduire le trafic global sur le réseau.

Adresse IP

- Format d'une adresse IP: w.x.y.z (4 octets) avec w,x,y,z compris entre 1 et 254 (0 réservé pour le réseau, 255 pour le broadcast).
- Une adresse w.x.y.z peut se lire comme suit:
 - Machine d'adresse w.x.y.z,
 - Machine d'adresse z du réseau w.x.y.0,
 - Machine d'adresse y.z du réseau w.x.0.0,
 - Machine d'adresse x.y.z du réseau w.0.0.0 .

Classes de réseau IP

Classe	Valeur de w	adresse réseau	Nb de réseaux	Nb max de machines
A	0 – 127	1 octet	127	16777216
B	128 – 191	2 octets	16384	65536
C	192 – 223	3 octets	2097152	256
D	224 – 239			
E	240 – 255			

➤ Plages d'adresses réservées pour les réseaux locaux :

- 10.0.0.1 à 10.255.255.254,
- 172.16.0.1 à 172.31.255.254,
- 192.168.0.1 à 192.168.255.254

Sous-réseaux

Pourquoi utiliser les sous réseaux ?

- Utilisation hétérogène de moyens de couche 1,
- Réduction de l'encombrement,
- Economise les temps de calculs,
- Isolation d'un réseau,
- Renforcement de la sécurité,
- Optimisation de l'espace réservé à une adresse IP.

Sous-réseaux

Nombre de sous réseaux :

RFC 1860 : $2^n - 2$, n étant le nombre de bits à 1

RFC 1878 : 2^n

=> Adresse des sous réseaux

Adresse de diffusion :

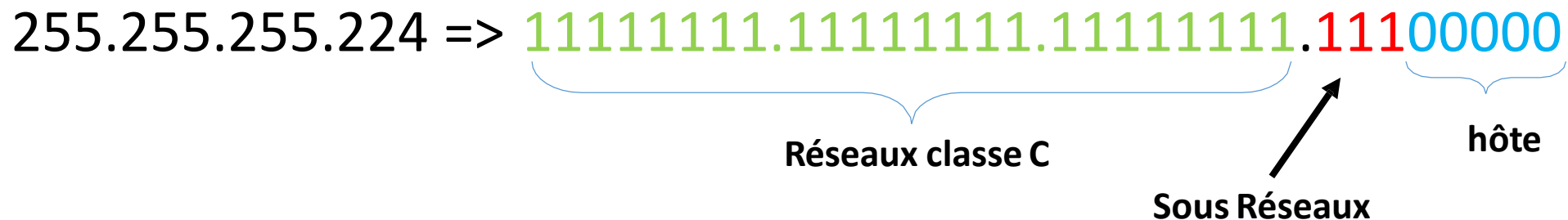
Mettre tous les bits de la partie hôte à 1

Nombre de machines du sous réseau :

$2^m - 2$, m étant le nombre de bits de la partie hôte

Masques de sous-réseaux

Ils permettent de segmenter un réseau en plusieurs sous-réseaux.
Exemple de masque :



Détermination du sous-réseau d'une machine :

200.100.40.33 => 11001000.01100100.00101000.00100001

On effectue et ET logique avec le masque de sous-réseau :

200.100.40.32 =>

11001000.01100100.00101000.00100000

Notation CIDR

- CIDR : Classless Inter Domain Routing
- RFC 1518 et RFC 1519
- Convention qui spécifie le nombre de bits utilisé pour la partie réseau
- Exemples :

142.12.42.145/24 $\Leftrightarrow$ 142.12.42.145 masque 255.255.255.0

153.121.219.14/20 $\Leftrightarrow$ 153.121.219.14 masque 255.255.240.0

- Facilite l'écriture des tables de routage.