Réseaux et communications informatiques

Objectifs :

- Être capable de caractériser un réseau informatique
- Être capable d'analyser une communication informatique

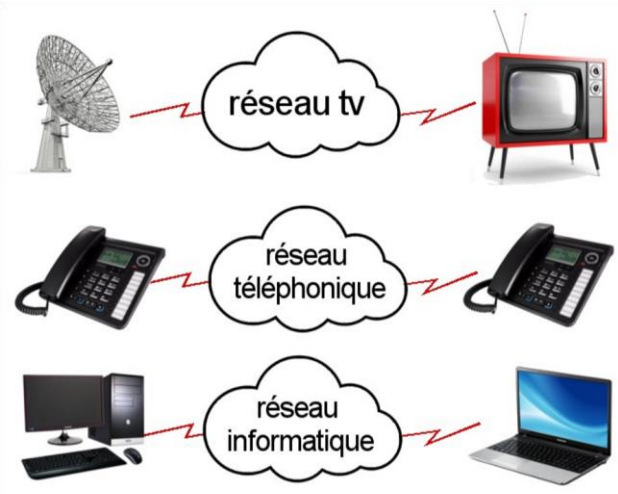
Prérequis :

- Connaissance du binaire, décimal, ….
- Connaissances de base sur les réseaux (voir les TP)

Plan de l'étude :

I. Introduction

De l'idée de faire communiquer des ordinateurs entre eux est née l'idée de réseau informatique. Au début il s'agissait de faire communiquer 2 ordinateurs puis plusieurs autres. Maintenant avec la généralisation des communications informatiques on constate que des moyens de communication autrefois séparés convergent en un réseau commun (et mondial). De même autrefois, chacun de ces services nécessitait une technologie différente pour acheminer son signal de communication particulier. Ainsi chaque service avait son propre ensemble de règles et de normes destiné à gérer les communications de ses services sur un support spécifique. Les progrès technologiques nous permettent aujourd'hui de réunir ces réseaux disparates sur un même réseau global.



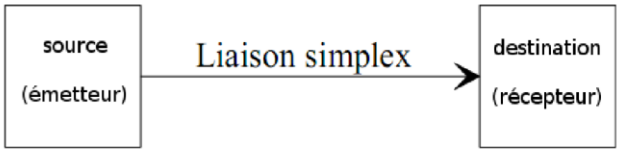
Autrefois les réseaux étaient séparés


Aujourd'hui on a des réseaux convergents (un réseau global)

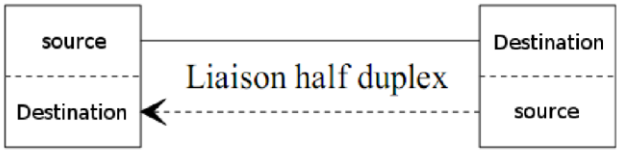
II. Réseaux informatiques

1 . Principes généraux

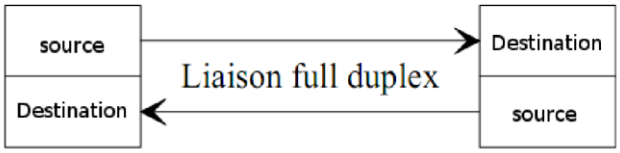
On peut considérer 3 cas de communications entre éléments :



Lorsque l'échange a lieu dans une seule direction, on parle de liaison **simplex**.



Si les éléments peuvent, alternativement, remplir les fonctions d'émetteur et de récepteur, la liaison est dite: **half duplex**.



Lorsque l'échange peut s'effectuer en même temps dans les deux sens la liaison est appelée bidirectionnelle intégrale ou **full duplex**.

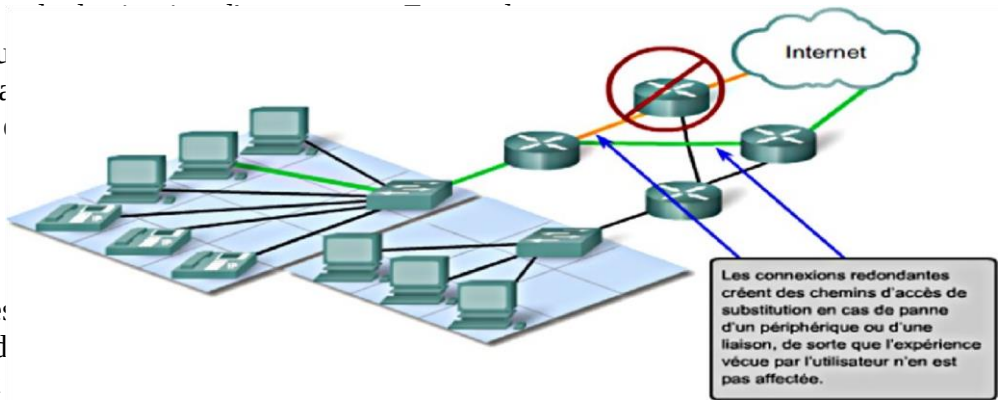
Quelques contraintes :

Les réseaux doivent d'une part prendre en charge une large gamme d'applications et de services et d'autre part fonctionner sur de nombreux types d'infrastructures physiques. Aujourd'hui, l'expression « architecture réseau » désigne aussi bien les technologies prenant en charge l'infrastructure (le hardware) que les services programmés et les protocoles qui déplacent les messages dans l'infrastructure (le software). Alors qu'Internet, et les réseaux en général, évoluent, nous découvrons que les architectures sous-jacentes doivent prendre en considération quatre caractéristiques de base si elles veulent répondre aux attentes des utilisateurs : tolérance aux pannes, évolutivité, qualité de service et sécurité.

Tolérance aux pannes (exemple avec le réseau Internet):

Comme des millions d'utilisateurs attendent d'Internet qu'il soit constamment disponible, il faut une architecture réseau conçue et élaborée pour tolérer les pannes. Un réseau tolérant aux pannes est un réseau qui limite l'impact des pannes du matériel et des logiciels et qui peut être rétabli rapidement

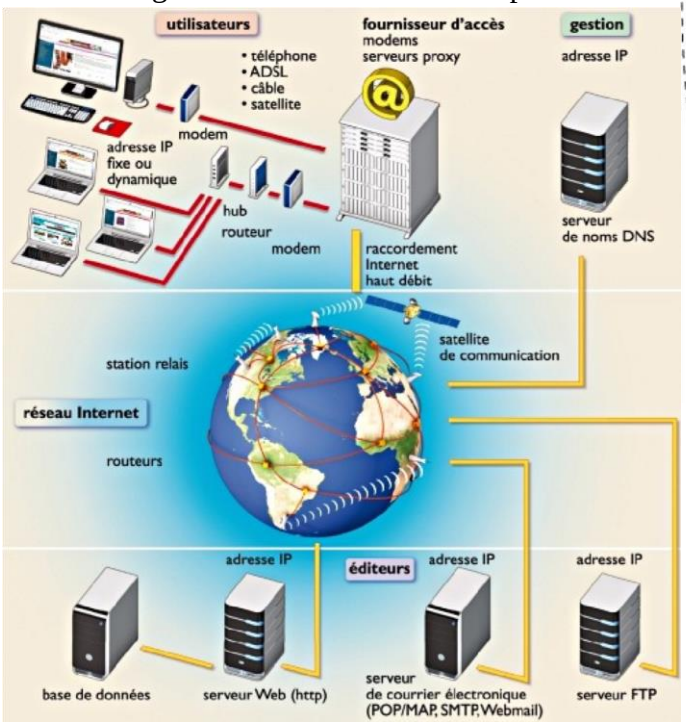
quand des pannes se produisent. De tels réseaux dépendent de liaisons, ou chemins, redondantes entre la source
défaillance d'une liaison (ou
les messages sont insta
routés sur une autre liaison
ceci de manière totalement transparente pour les utilisateurs aux deux extrémités. Aussi bien les infrastructures physique
les processus logiciels qui d
messages sur le réseau sont

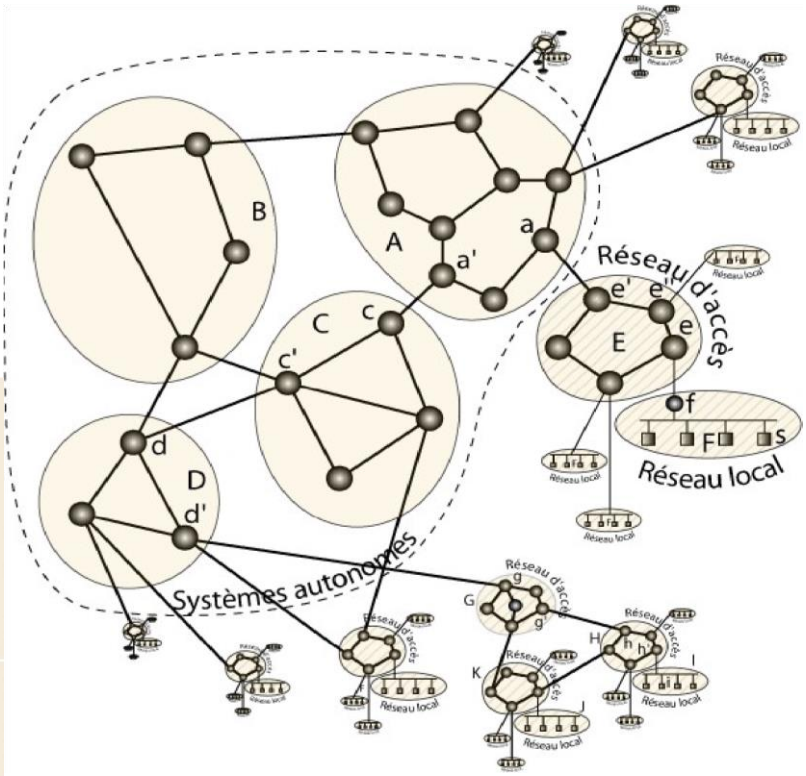


cette redondance. Il s'agit d'une caractéristique essentielle des réseaux actuels.

Ainsi le réseau internet ressemble à une immense pieuvre avec de multiples liaisons possibles entre 2 points. Donc, en cas de panne, l'information circule par un autre point (ou nœud) du réseau. Il existe malheureusement quelques points « critiques » où la redondance est faible. Il s'agit notamment des liaisons entre continents. Par exemple il y a une quantité très limité de fibres optiques qui relient l'Europe à l'Amérique. En cas de panne sur l'une d'elle, le trafic s'en trouve forcément impacté.

Dans les faits internet est constitué d'un maillage de réseaux publics et privés. Ainsi l'autorité administrative sur le réseau est partagée et distribuée entre tous les opérateurs parties prenantes; les décisions de ces derniers relèvent de contrats passés entre eux et de l'application de l'ensemble des normes et protocoles de transport et d'adressage dont la gestion est à la charge d'organisations internationales spécialisées.



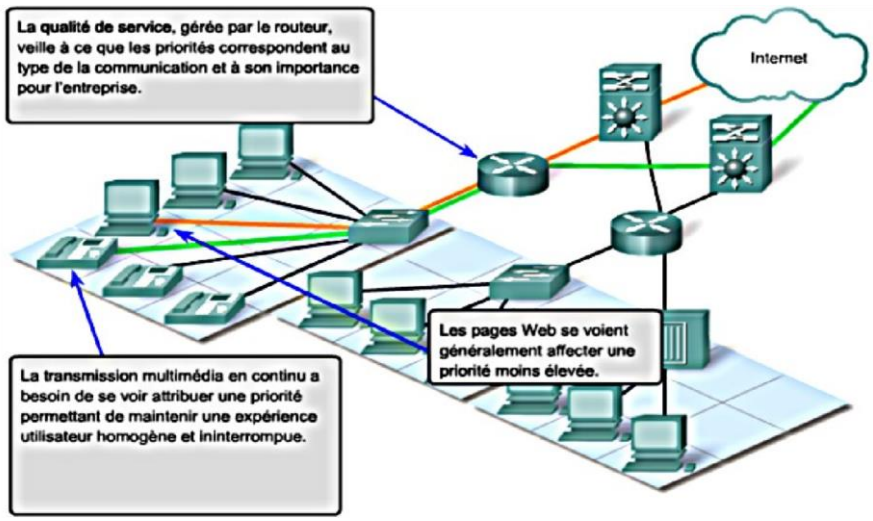


On notera que chaque ordinateur directement connecté à internet possède au moins une adresse IP propre.
Cependant, les utilisateurs ne veulent pas travailler avec des adresses numériques du genre 194.153.205.26 mais avec un nom de domaine ou des adresses plus explicites du type
[www.lamache.org].
Ainsi, il est possible d'associer des noms en langage courant aux adresses numériques grâce à un système appelé DNS (Domain Name System). On appelle résolution de noms de domaines (ou résolution d'adresses) la corrélation entre les adresses IP et le nom de domaine associé.

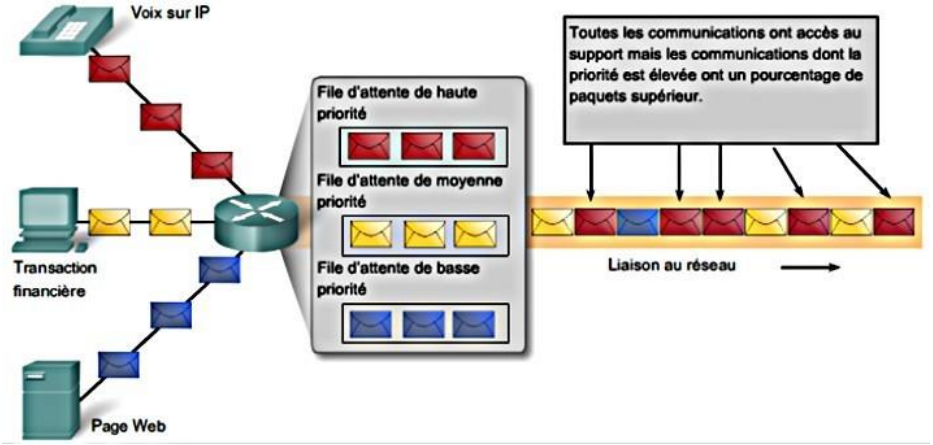
La société qui gère ces DNS est l'Internet Corporation for Assigned Names and Numbers (ICANN). Il s'agit d'une autorité de régulation de l'Internet. C'est une société de droit californien à but non lucratif ayant pour principales missions d'administrer les ressources numériques d'Internet, telles que l'adressage IP et les noms de domaines de premier niveau (.org, .com, .fr, …). Le reste de la gestion des DNS est réalisée par différents éléments du réseau.

Évolutivité :

Un réseau évolutif est en mesure de s'étendre rapidement afin de prendre en charge de nouveaux utilisateurs et applications sans que cela n'affecte les performances du service fourni aux utilisateurs existants.



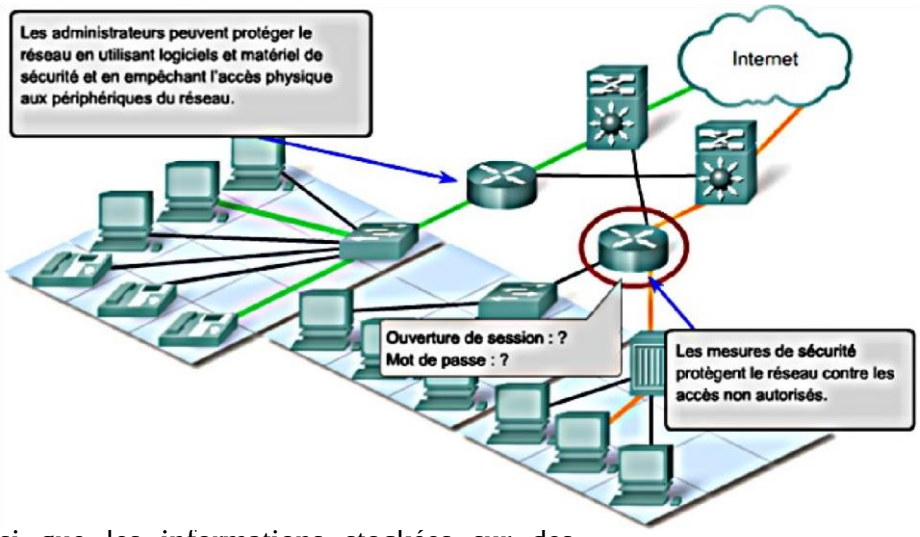
Qualité de services



Quand les réseaux ne servaient qu'à des échanges informatiques (données, courriers, …), un service comportant des interruptions était acceptable. Aujourd'hui avec le développement des transmissions audio et vidéo ce n'est plus possible. Ces transmissions exigent, en effet, un niveau de qualité constant (une grande bande passante) et un service ininterrompu.
C'est pour cela que les périphériques intermédiaires qui assurent la qualité de service gèrent des files d'attentes selon le niveau de priorité des messages. Ainsi, les messages d'un service de voix sur IP seront prioritaires devant ceux d'un service de transaction financière, eux-mêmes prioritaires devant ceux du service web.

Sécurité

L'infrastructure réseau, les services et les données contenues par un réseau relié à des ordinateurs sont des actifs personnels et professionnels essentiels. Toute compromission de l'intégrité de ces actifs pourrait avoir de graves conséquences professionnelles et financières.



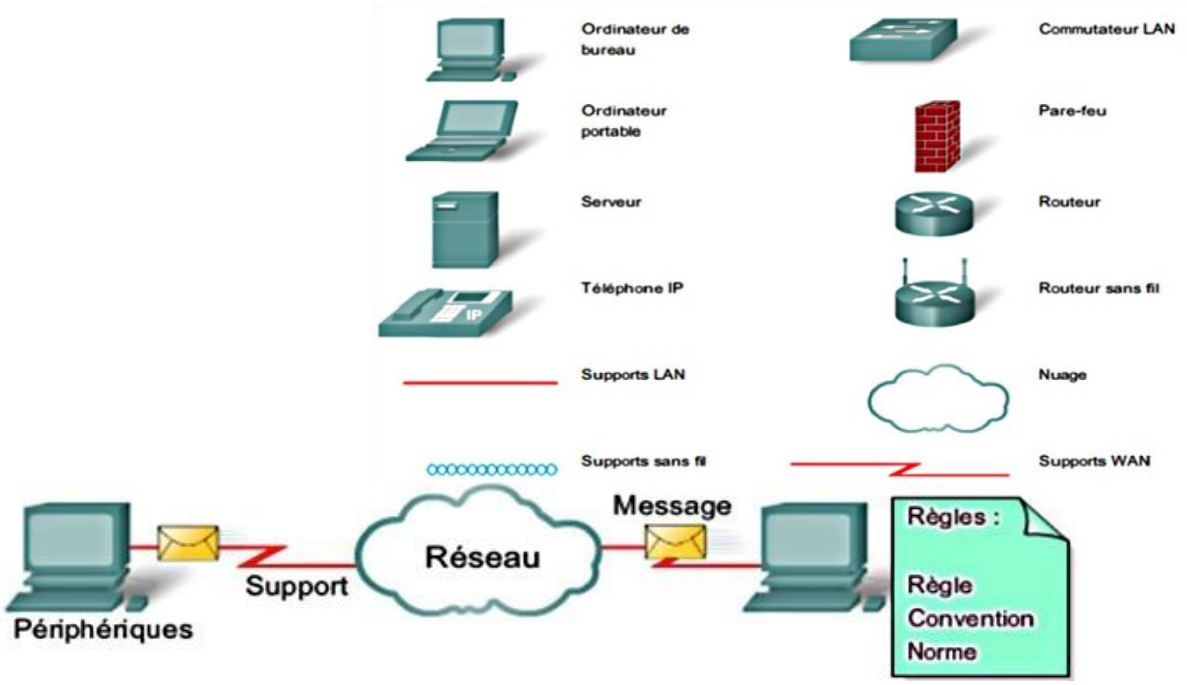
En matière de sécurité des réseaux, deux points doivent être pris en considération pour éviter des conséquences graves : la sécurité de l'infrastructure réseau et la sécurité du contenu.

Sécuriser l'infrastructure réseau implique de sécuriser matériellement les périphériques qui assurent connectivité du réseau et d'empêcher t non autorisé au logiciel de gestion qu'i

Sécuriser le contenu consiste à protége paquets transmis sur le réseau ainsi que les informations stockées sur des périphériques reliés au réseau par exemple en les cryptant.

2 . Éléments d'un réseau

Un réseau est constitué de périphériques, de supports et de services reliés par des règles et qui collaborent pour envoyer des messages. Le terme messages sert à désigner des pages Web, des courriels, des messages instantanés, des appels téléphoniques et toutes autres formes de communication prises en charge par le réseau.



Les éléments du réseau :

On distingue deux types de périphériques :

Les périphériques terminaux :

- Serveurs, Ordinateurs de bureau, Ordinateurs portables, Imprimantes, Téléphones IP, ….

Les périphériques intermédiaires :

- Commutateur (périphérique le plus couramment utilisé pour interconnecter des réseaux locaux),
- Pare-feu (assure la sécurité du réseau),
- Routeur (contribue à orienter les messages transitant sur un réseau),
- Routeur sans fil (type particulier de routeur souvent présent dans les réseaux familiaux),
- Nuage (sert à représenter un groupe de périphériques réseau)
- ….

Les connexions :

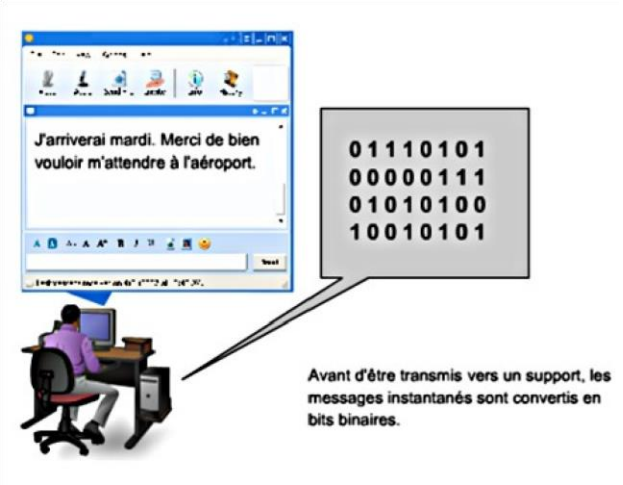
- Filaires (câble droit, croisé, téléphonique, série, bus, ...)
- Sans-fil - ondes électromagnétiques (WiFi, GSM, Bluetooth, ...)
- Optique (fibre monomode, multimode, ...)

Périphériques et supports de transmission

Pour envoyer et recevoir des messages divers et variés on utilise des applications informatiques qui ont besoin que le réseau leur fournisse certains services. Ces services sont régis par des règles, ou protocoles.

Aujourd'hui, la norme en matière de réseaux est un ensemble de protocoles appelé TCP/IP (Transmission Control Protocol/Internet Protocol). Le protocole TCP/IP est non seulement utilisé dans les réseaux privés et professionnels, mais il est aussi le principal protocole d'Internet. C'est en effet le protocole TCP/IP qui définit les règles de formatage, d'adressage et de routage utilisés pour veiller à ce que les messages soient livrés aux destinataires appropriés.

Les services de haut niveau tels que le World Wide Web, les messageries électroniques, les messageries instantanées et la téléphonie sur IP répondent à des protocoles normalisés.
Avant d'être envoyés vers leurs destinations, tous les types de messages doivent être convertis en bits, c'est-à-dire en signaux numériques codés en binaire. Ceci est obligatoire quel que soit le format d'origine du message : texte, vidéo, audio ou données informatiques, et quelque soit le service sollicité.



Avant d'être transmis vers un support, les messages instantanés sont convertis en bits binaires.

La carte réseau du PC génère des signaux électriques qui représentent les bits qu'elle place sur le support. Les bits arrivent sur le premier périphérique réseau.

3 . Adresses des éléments d'un réseau

3.1 L'adresse physique ou adresse MAC

Chaque appareil qui possède une possibilité de raccordement à un réseau informatique possède une adresse unique déterminé lors de sa fabrication.

Cet identifiant unique s'appelle l'adresse MAC (Media Access Control) et se présente sous la forme d'une suite de 6 octets (donc 48 bits) en général noté en hexadécimal.

Exemple : sous Windows, quand on fait « ipconfig /all » on obtient :

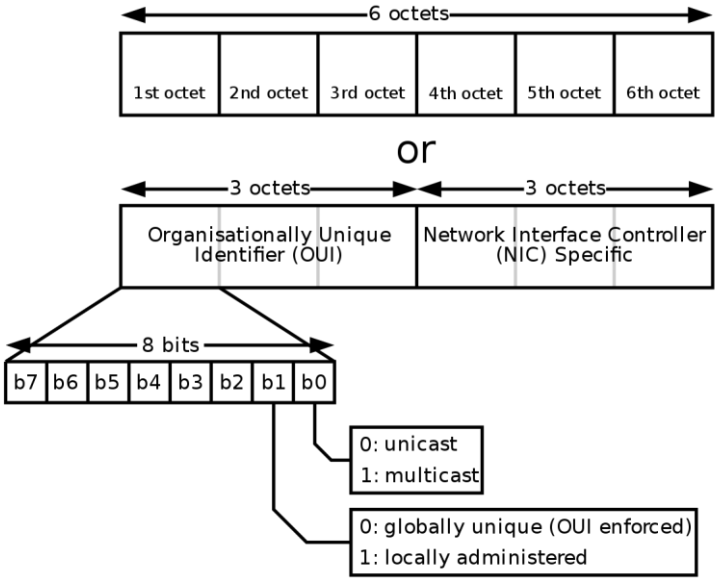
```
Invite de commandes
   Liste de recherche du suffixe DNS.: home

Carte Ethernet Ethernet :

   Suffixe DNS propre à la connexion. . . : home
   Description. . . . . . . . . . . . . . : Intel(R) Ethernet Connection (6) I219-LM
   Adresse physique . . . . . . . . . . . : 34-48-ED-01-14-D0
   DHCP activé. . . . . . . . . . . . . . : Oui
   Configuration automatique activée. . . : Oui
   Adresse IPv6. . . . . . . . . . . . . .: 2a01:cb14:85f:d100:10e4:efb2:f6aa:a2bf(préféré)
   Adresse IPv6 temporaire . . . . . . . .: 2a01:cb14:85f:d100:b48c:91fd:5895:47fa(préféré)
   Adresse IPv6 de liaison locale. . . . .: fe80::10e4:efb2:f6aa:a2bf%11(préféré)
   Adresse IPv4. . . . . . . . . . . . . .: 192.168.1.13(préféré)
   Masque de sous-réseau. . . . . . . . . : 255.255.255.0
   Bail obtenu. . . . . . . . . . . . . . : lundi 25 mai 2020 09:01:33
   Bail expirant. . . . . . . . . . . . . : mardi 26 mai 2020 09:01:29
   Passerelle par défaut. . . . . . . . . : fe80::7a81:2ff:fe2f:b2f2%11
                                    192.168.1.1
   Serveur DHCP . . . . . . . . . . . . . : 192.168.1.1
```

L'adresse MAC de notre matériel est donc : **34-48-ED-01-14-D0**

Structure d'une adresse MAC :



- Les 3 premiers octets sont l'OUI (Organizationally Unique Identifier) : il s'agit d'un nombre de 24 bits assigné par l'IEEE (Institute of Electrical and Electronics Engineers). Ce numéro identifie le fabricant.
- Les 3 octets de poids faible correspondent à un identifiant fixé par le fabricant afin que chaque appareil soit unique.

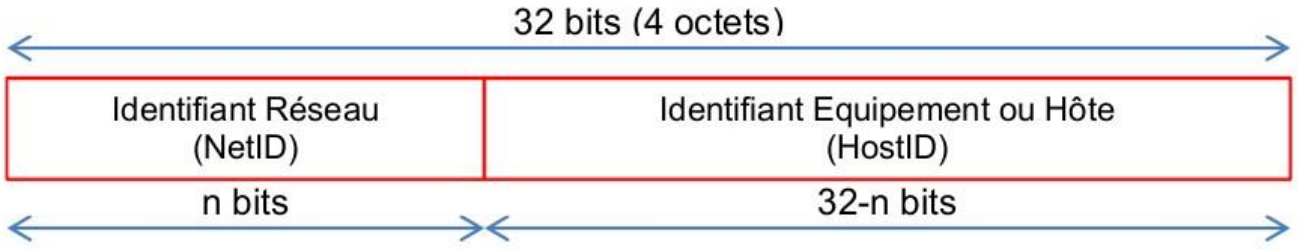
3.2 L'adresse IP

L'adresse IP (Internet Protocol) est une adresse « logique » affectée à une machine manuellement par l'administrateur réseau ou automatiquement par un serveur DHCP (Dynamic Host Configuration Protocol). Cette adresse est modifiable. Ce sera cette adresse IP qui servira pour tous les échanges au sein du réseau.

Le format IPV4

Une adresse IPV4 est constituée d'un nombre binaire de 32 bits. Pour faciliter la lecture et la manipulation de cette adresse on la représente plutôt en notation décimale, par groupe de 8 bits, séparés par un point. Exemple : 192.168.2.6 (en binaire : 11000000.10101000.00000010.00000110)

Un adresse IPV4 est composée d'un identifiant réseau (**NetID**) et d'un identifiant équipement (ou hôte) (**HostID**) :



Il existe au final cinq classes d'adresses IP. Chaque classe est identifiée par une lettre allant de A à E.

Ces différentes classes ont chacune leurs spécificités quant à la répartition du nombre d'octets servant à identifier le réseau ou les ordinateurs connectés à ce réseau :

- Une adresse IP de classe A dispose d'une partie **NetID** comportant uniquement un seul octet.
- Une adresse IP de classe B dispose d'une partie **NetID** comportant deux octets.
- Une adresse IP de classe C dispose d'une partie **NetID** comportant trois octets.
- Les adresses IP de classes D et E correspondent à des adresses IP particulières.

Cela donne :

Classe	**Début départ**	**Fin**	**Notation CIDR**	**Bits de Masque de sous-réseau par défaut**

Classe A	0	126.255.255.255 (127 0.0.0.0 est réservé)	/8	255.0.0.0
Classe B	10	128.0.0.0 191.255.255.255	/16	255.255.0.0
Classe C	110	192.0.0.0 223.255.255.255	/24	255.255.255.0
Classe D (multicast)	1110	224.0.0.0 239.255.255.255		255.255.255.255
Classe E (réservée)	1111	240.0.0.0 255.255.255.255		non défini

Masques de sous réseau :

Un sous-réseau est une subdivision logique d'un réseau de taille plus importante. Le masque de sousréseau permet de distinguer la partie de l'adresse commune à tous les appareils du sous-réseau et celle qui varie d'un appareil à l'autre.

Exemple : adresse 192.168.1.13 et masque 255.255.255.0

Le masque de sous réseau va nous permettre, à l'aide de la fonction logique ET, de récupérer l'adresse de notre matériel débarrassé de la partie commune :

	11000000.10101000.00000001.00001101		
ET	00000000.00000000.00000000.11111111		
on obtient :	00000000.00000000.00000000.00000000	0.0.0.13	(**HostID**)

ou l'inverse :

	11000000.10101000.00000001.00001101		
ET	11111111.11111111.11111111.00000000		
on obtient :	11000000.10101000.00000001.00000000	192.168.1.0	(**NetID)**

Notation CIDR :

Une forme plus courte est connue sous le nom de « notation CIDR » (Classless Inter-Domain Routing). Elle donne le numéro du réseau suivi par un slash et le nombre de bits à 1 dans la notation binaire du masque de sous-réseau. Le masque 255.255.255.0, équivalent en binaire à 11111111.11111111.11111111.00000000 , sera donc représenté par /24 (24 bits à la valeur 1, suivis de 8 bits 0).

La notation 192.168.1.13/24 désigne donc l'adresse IP 192.168.1.13 avec le masque 255.255.255.0, et signifie que les 24 premiers bits de l'adresse sont dédiés à l'adresse du sous-réseau (192.168.1) et le reste à l'adresse de l'ordinateur hôte à l'intérieur du sous-réseau (ici 13).

Résumé pour la classe C :

Bits de départ	Masque de sous réseau par défaut	Nombre de bits de NetID	Nombre de bits de HostID	Nombres d'adresses possibles sur le sous réseau	Nombre d'adresses de réseaux possibles	Plage d'adresses disponibles

110	255.255.255.0	21	8	254 (2^8-2)	2097152 (2^{21})	192.0.0.1 à 223.255.255.254

Explications :

- les trois premiers bits d'une adresse de classe C ont toujours les valeurs 110. En effectuant la conversion en décimal, on obtient pour la classe C un premier octet ayant une valeur comprise entre 192 et 223. (**110**00000 et **110**11111).
- Il y a toujours 2 adresses inutilisables sur un réseau, celle correspondant à la valeur 0 et la dernière dite « de diffusion » (réservée).

Le format IPV6

Le nombre d'adresses IP disponibles avec le protocole IPv4, environ 4 milliard, n'est plus suffisant pour répondre à la demande croissante notamment avec l'arrivée des objets connectés. C'est pourquoi un nouveau protocole internet a été créé: IPv6

L'adressage se fait sur 16 octets (16*8=128 bits), ce qui représente 2^{128} adresses possibles (contre 2^{32} pour l'IPv4).

La notation décimale employée pour les adresses IPv4 est abandonnée au profit d'une écriture hexadécimale, où les 8 groupes de 2 octets (soit 16 bits par groupe) sont séparés par un signe deuxpoints.

Exemple et règles d'écriture :

2001:0db8:0000:85a3:0000:0000:ac1f:8001

La notation complète ci-dessus comprend exactement 39 caractères (32 chiffres hexa et 7 deux-points).

Simplification d'écriture :
Il est permis d'omettre de 1 à 3 chiffres zéros non significatifs dans chaque groupe de 4 chiffres hexadécimaux. Ainsi, l'adresse IPv6 ci-dessus est équivalente à : 2001:db8:0:85a3:0:0:ac1f:8001

De plus, une unique suite de un ou plusieurs groupes consécutifs de 16 bits tous nuls peut être omise, en conservant toutefois les signes deux-points de chaque côté de la suite de chiffres omise, c'est-à-dire une paire de deux-points « :: ». Ainsi, l'adresse IPv6 ci-dessus peut être abrégée en : 2001:db8:0:85a3::ac1f:8001

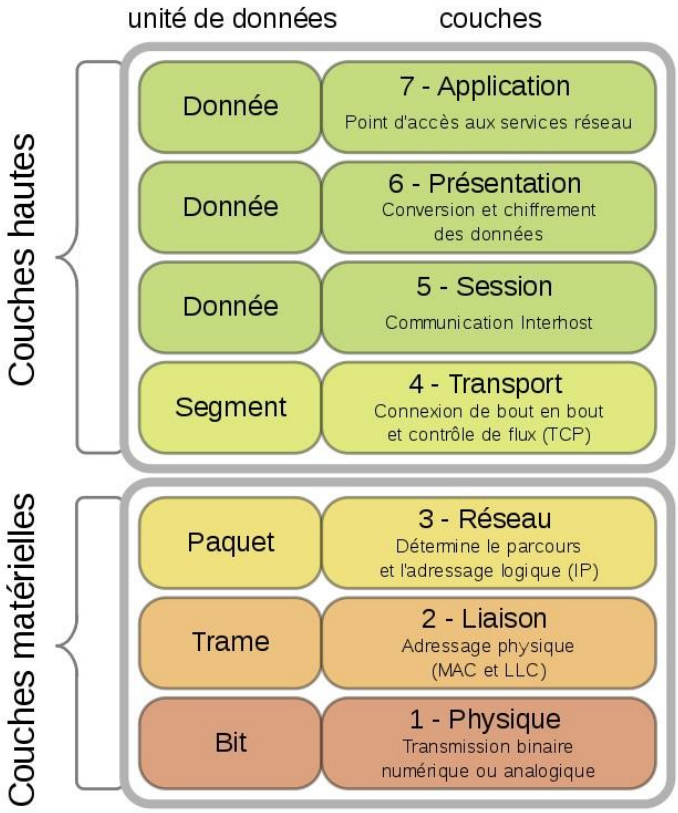
Plus d'information : https://fr.wikipedia.org/wiki/Adresse_IPv6

4 . Le modèle de référence OSI

Au début des années 70, chaque constructeur a développé sa propre solution réseau autour d'architecture et de protocoles privés et il s'est vite avéré qu'il serait impossible d'interconnecter ces différents réseaux «propriétaires» si une norme internationale n'était pas établie. Cette norme établie par l'International Standard Organization (ISO) est la norme Open System Interconnection (OSI, interconnexion de systèmes ouverts).

Le modèle de référence OSI est une représentation abstraite en couches servant de guide à la conception des protocoles réseau. Il divise le processus de réseau en sept couches logiques, chacune comportant des fonctionnalités uniques et se voyant attribuer des services et des protocoles spécifiques.

Chaque couche ne peux communiquer qu'avec celle du dessus et celle du dessous.



Description détaillée :

7- Application

Cette couche est le point de contact entre l'utilisateur et le réseau. C'est donc elle qui va apporter à l'utilisateur les services de base offerts par le réseau, comme par exemple le transfert de fichier, la messagerie...

6- Présentation

Cette couche s'intéresse à la syntaxe et à la sémantique des données transmises : c'est elle qui traite l'information de manière à la rendre compatible entre tâches communicantes. Elle va assurer l'indépendance entre l'utilisateur et le transport de l'information. Typiquement, cette couche peut convertir les données, les reformater, les crypter et les compresser.

5- Session

La couche session fournit des services à la couche présentation pour organiser son dialogue et gérer l'échange de données.

4- Transport

Cette couche est responsable du bon acheminement des messages complets au destinataire. Le rôle principal de la couche transport est de prendre les messages de la couche session, de les découper s'il le faut en unités plus petites et de les passer à la couche réseau, tout en s'assurant que les morceaux arrivent correctement de l'autre côté. Cette couche effectue donc aussi le réassemblage du message à la réception des morceaux.

3- Routage

La couche réseau fournit des services pour échanger les parties de données individuelles sur le réseau entre des périphériques terminaux identifiés.

2- Liaison

Les protocoles de la couche liaison de données décrivent des méthodes d'échanges de trames de données entre des périphériques sur un support commun.

1- Physique

Les protocoles de la couche physique décrivent les moyens mécaniques, électriques, fonctionnels et méthodologiques permettant d'activer, de gérer et de désactiver des connexions physiques pour la transmission de bits vers et depuis un périphérique réseau.

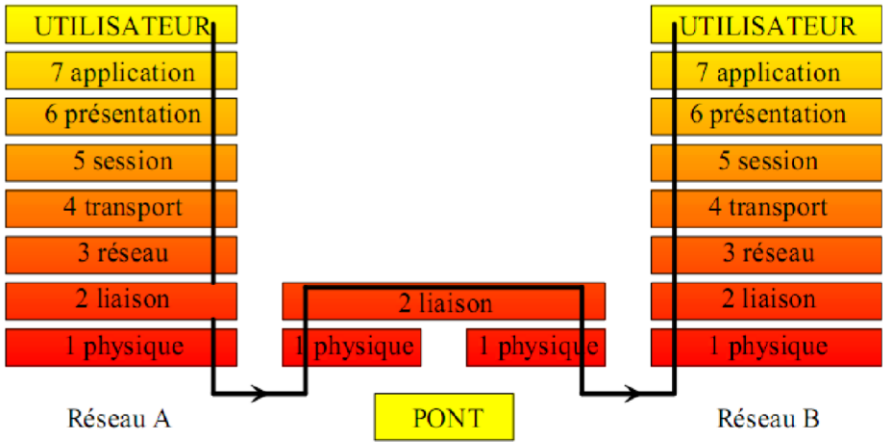
Dans les faits comment cela se passe-t-il ?

Trois types de dispositifs permettent de remplir la fonction d'interconnexion des réseaux:

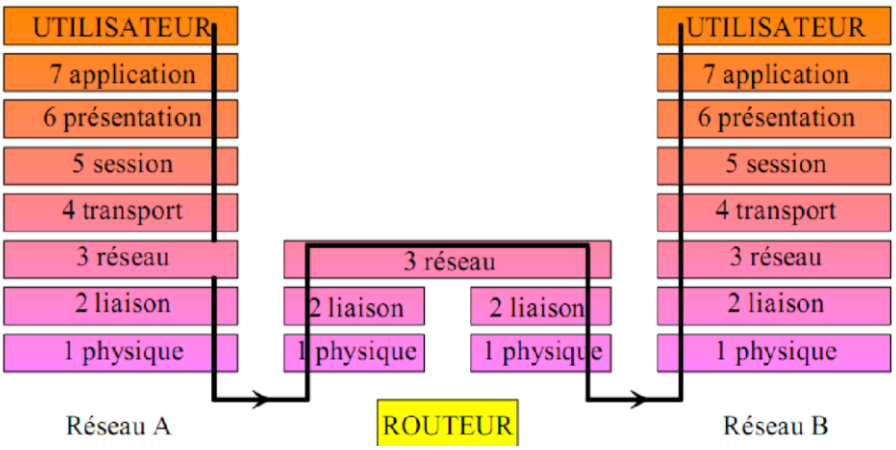
- les ponts
- les routeurs
- les passerelles.

Les ponts :

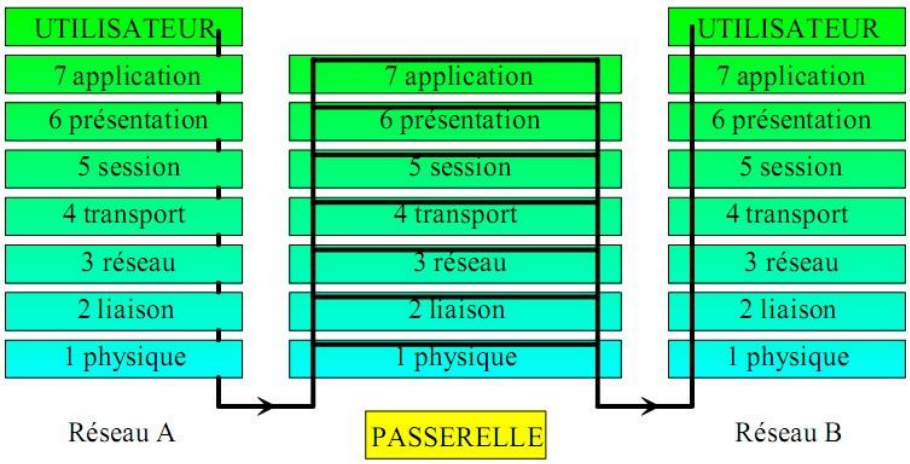
L'objectif du pont est d'interconnecter deux segments de réseaux distincts, soit de technologies différentes, soit de même technologie, mais physiquement séparés à la conception pour diverses raisons (géographique, extension de site etc.). Son usage le rapproche fortement de celui d'un commutateur (switch), à l'unique différence que le commutateur ne convertit pas les formats de transmissions de données.
Ils permettent ainsi d'interconnecter des réseaux ayant la couche 1 et 2 du modèle OSI (couche liaison) différentes, mais les couches supérieures à la 2 identiques.



Les routeurs :
Un routeur est un élément intermédiaire dans un réseau informatique assurant le routage des paquets. Son rôle est de faire transiter des paquets d'une interface réseau vers une autre.
Les routeurs opèrent au niveau de la couche 3 (couche réseau) du modèle OSI.

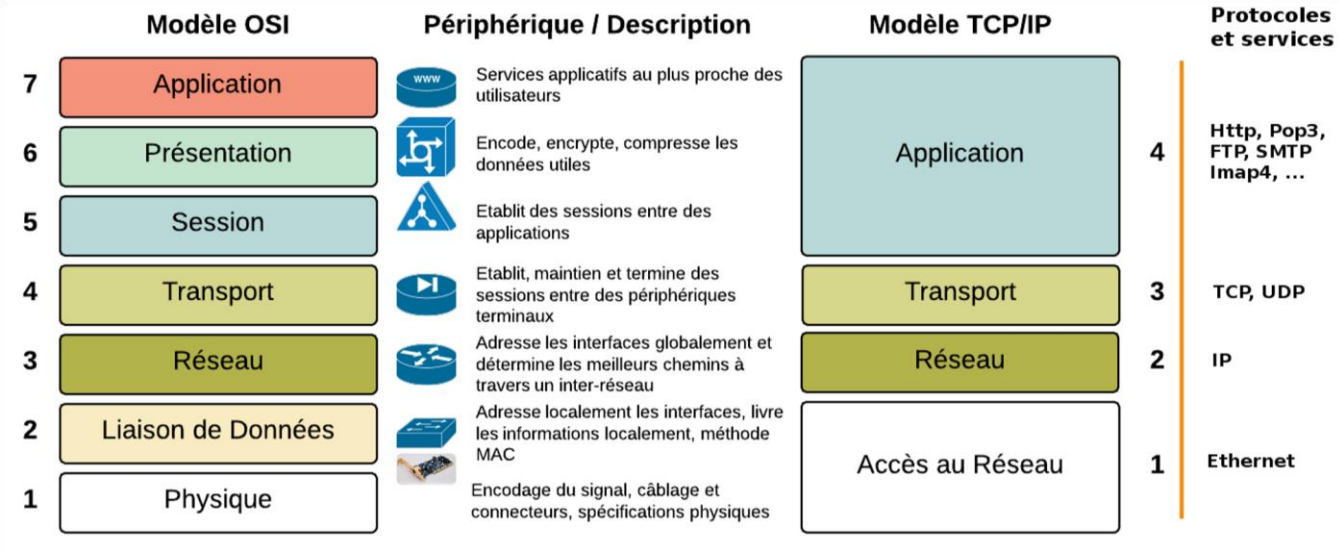


Les passerelles :
En informatique, une passerelle (en anglais, gateway) est le nom générique d'un dispositif permettant de relier deux réseaux informatiques de types différents, par exemple un réseau local et le réseau Internet.
Elles permettent l'interconnexion de réseau en adaptant l'ensemble des couches du modèle OSI afin de les rendre compatible avec l'autre réseau.



5 . Comparaison des modèles OSI et TCP/IP

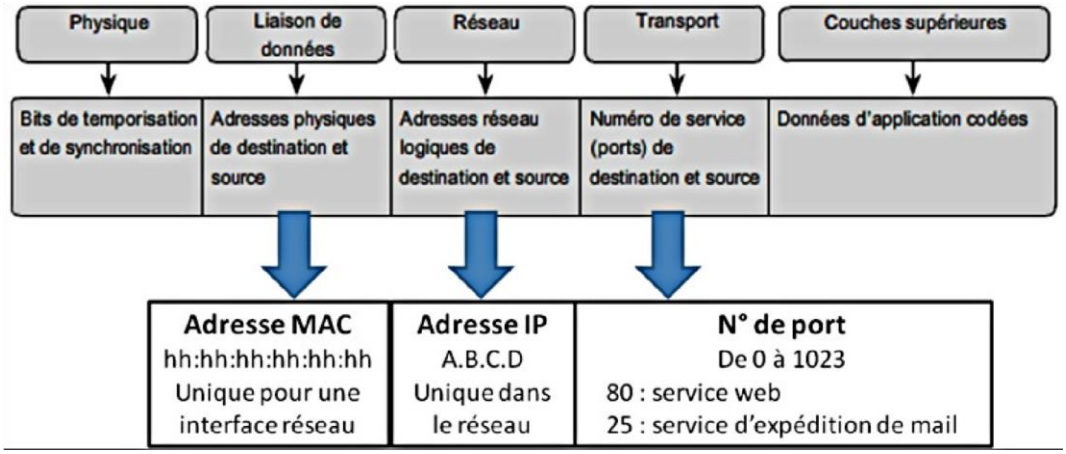
TCP/IP est une suite de protocoles utilisés pour internet. Le sigle TCP/IP signifie «Transmission Control Protocol/Internet Protocol. Ces protocoles qui constituent la suite de protocoles TCP/IP peuvent être décrits selon les termes du modèle de référence OSI :



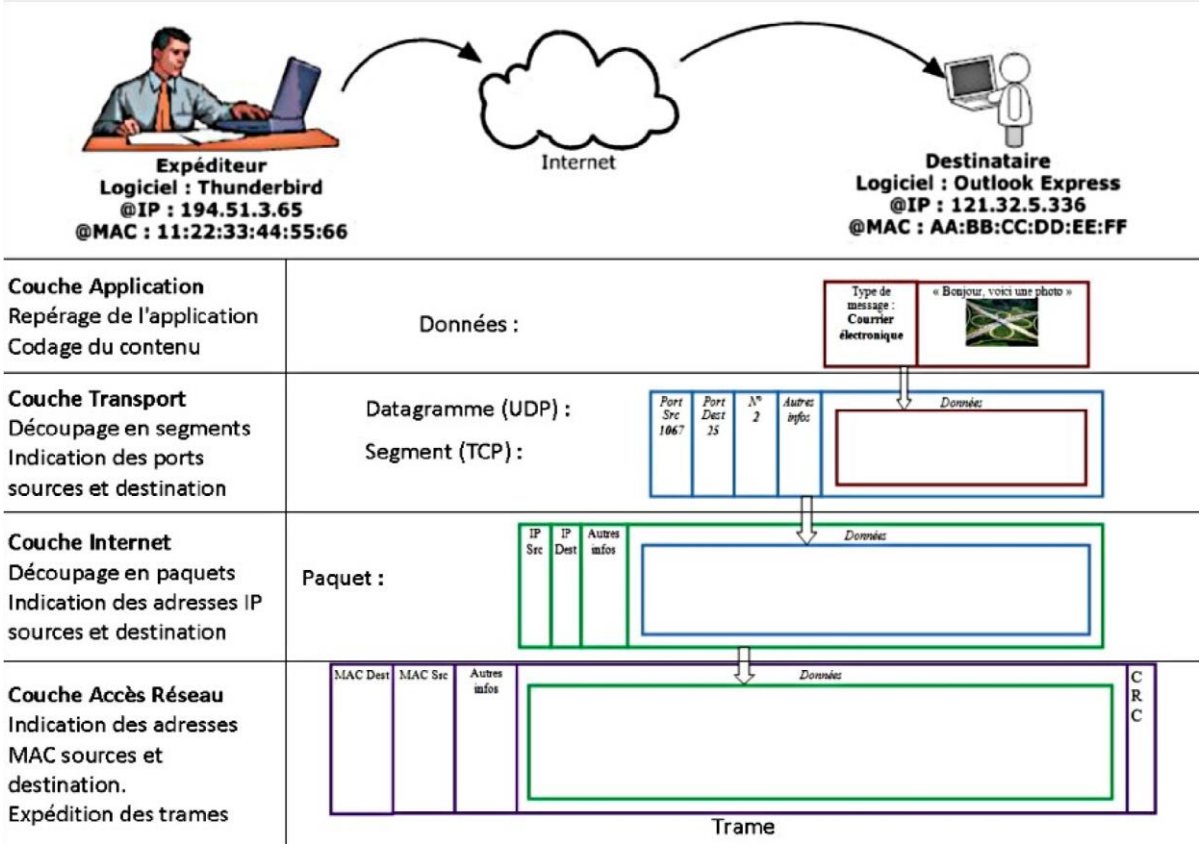
6 . Principe de l'adressage et de l'encapsulation

Le modèle OSI décrit des processus de codage, de mise en forme, de segmentation et d'encapsulation de données pour la transmission sur le réseau. Un flux de données envoyé depuis une source vers une destination peut être divisé en parties et entrelacé avec des messages transmis depuis d'autres hôtes vers d'autres destinations. À n'importe quel moment, des milliards de ces parties d'informations se déplacent sur un réseau. Il est essentiel que chaque donnée contienne les informations d'identification suffisantes afin d'arriver à bonne destination.

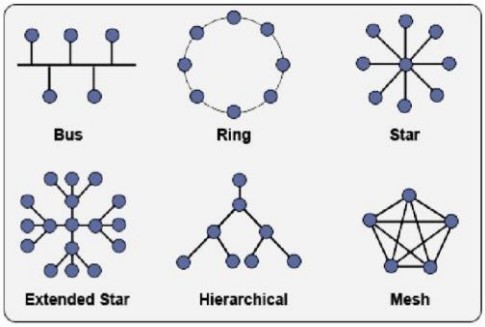
Il existe plusieurs types d'adresses qui doivent être incluses pour livrer correctement les données depuis une application source exécutée sur un hôte à l'application de destination correcte exécutée sur un autre.



Exemple : Un utilisateur veut envoyer un message (mail) conformément au schéma ci-dessous.



7 . Topologie des réseaux



La manière dont sont interconnectées les machines est appelée « topologie ». On distingue la topologie physique (la configuration spatiale, visible, du réseau) de la « topologie logique ». La topologie logique représente la manière dont les données transitent dans les câbles.

Les différents types de réseaux

On distingue différents types de réseaux selon leur taille (en terme de nombre de machines), leur vitesse de transfert des données ainsi que leur étendue. On fait généralement trois catégories de réseaux :

- **LAN** (Local Area Network) : réseau local
- **MAN** (Metropolitan Area Network) : réseau à l'échelle d'un ville ou d'un campus universitaire
- **WAN** (Wide Area Network) : il s'agit d'un réseau étendu c'est à dire un réseau informatique (ou de télécommunications) couvrant une grande zone géographique (pays, continent ou la planète entière pour le réseau Internet.

Il existe deux autres types de réseaux :

- TAN (Tiny Area Network) identique au LAN mais moins étendus (2 à 3 machines).
- CAN (Campus Area Network) identiques au MAN (avec une bande passante maximale entre tous les LAN du réseau).

Le réseau local LAN (Local Area Network) :

C'est un réseau informatique à une échelle géographique relativement restreinte, il est utilisé pour relier entre eux les ordinateurs : par exemple d'une habitation particulière, d'une entreprise, d'une salle informatique, d'un bâtiment. L'infrastructure est privée et est gérée localement. À l'intérieur, ou « sur » le réseau local il y a des ordinateurs fixes ou portables connectés par des câbles ou sans fil (Réseaux locaux sans fil : WLAN). Ces deux mondes communiquent par l'intermédiaire d'une box ou modem ADSL (selon le FAI).
La taille d'un réseau local peut atteindre jusqu'à 100 voire 1000 utilisateurs. En élargissant le contexte de la définition aux services qu'apportent le réseau local, il est possible de distinguer deux modes de fonctionnement :

- dans un environnement « paire à paire : P2P » (en anglais peer to peer), dans lequel il n'y a pas d'ordinateur central et chaque ordinateur a un rôle similaire.
- dans un environnement « client/serveur », dans lequel un ordinateur central fournit des services réseau aux utilisateurs.

Les MAN (Metropolitan Area Network) interconnectent plusieurs LAN géographiquement proches (au maximum quelques dizaines de km) à des débits importants.

Un **VLAN** (Virtual Local Area Network ou Virtual LAN, en français « Réseau Local Virtuel ») est un réseau local regroupant un ensemble de machines de façon logique et non physique.
Ainsi dans un réseau local la communication entre les différentes machines est normalement régie par l'architecture physique. Grâce aux réseaux virtuels (VLANs) il est possible de s'affranchir des limitations de l'architecture physique (contraintes géographiques, contraintes d'adressage, ...) en définissant une segmentation logique (logicielle) basée sur un regroupement de machines grâce à des critères (adresses MAC, numéros de port, protocole, etc.).
Technologies utilisées : Ethernet (sur câbles de paires torsadées), ou Wifi.

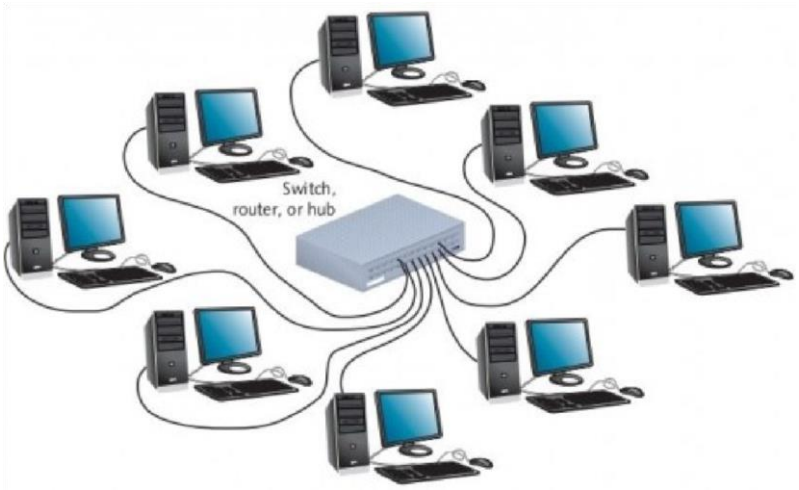
Le réseau MAN (Metropolitan Area Network) :
C'est un réseau métropolitain qui désigne un réseau composé d'ordinateurs habituellement utilisés dans les campus ou dans les villes. Ainsi, un MAN permet à deux nœuds (ordinateurs) distants de communiquer comme si ils faisaient partie d'un même réseau local. Un MAN est formé de commutateurs ou de routeurs interconnectés par des liens hauts débits qui utilisent généralement des fibres optiques.
Ces réseaux peuvent être placés sous une autorité publique ou privée comme le réseau intranet d'une entreprise ou d'une ville. Il permet donc pour une société, une ville, de contrôler elle-même son réseau. Ce contrôle comprend la possibilité de gérer, surveiller et effectuer des diagnostics à distance, à la différence de la connexion WAN, pour laquelle elle doit se fier à son fournisseur d'accès pour gérer et maintenir la liaison entre elle et son bureau distant.
Ce type de réseau, s'il est municipal par exemple, permet une infrastructure multiservice : il permet de véhiculer la téléphonie, la vidéo surveillance urbaine, la télégestion des feux tricolores, les installations de chauffage, les parkings, l'éclairage de l'Hôtel de Ville, ...

Technologies utilisées : Fibre optique, ondes radios (Wi-Fi).
Le réseau WAN (Wide Area Network) ou réseau étendu :

Le réseau Internet (WAN) est un réseau couvrant une grande zone géographique, à l'échelle d'un pays, d'un continent, voire de la planète entière. Il permet l'interconnexion de réseaux locaux et métropolitains vers l'internet mondial. L'infrastructure est en général publique.
Le plus grand réseau WAN est le réseau internet : à l'extérieur du réseau dit local, c'est à dire de l'autre côté de la « box » il existe un réseau que l'on nomme communément internet. Les fournisseurs d'accès à internet (ou FAI), moyennant finance, procurent un accès à ce réseau.

Technologies utilisées : Câble, fibre optique, satellite, technologie sans fil 3G et ondes hertziennes.

Réseau en étoile



Les équipements du réseau sont reliés à un système matériel central (le nœud). Celui-ci a pour rôle d'assurer la communication entre les différents équipements du réseau. Notamment utilisée par les réseaux Ethernet actuels en RJ45, elle concerne maintenant la majorité des réseaux. Lorsque toutes les stations sont connectées à un commutateur, on parle de topologie en étoile. Les nœuds du réseau sont tous reliés à un nœud central. Dans cette topologie tous les hôtes sont interconnectés grâce à un SWITCH (il y a encore quelques années c'était par un HUB = concentrateur) : sorte de multiprise pour les câbles réseaux placés au centre de l'étoile. Les stations émettent vers ce concentrateur qui renvoie les données vers tous les autres ports réseaux (hub) ou uniquement au destinataire (switch).
Le câble entre les différents nœuds est désigné sous le nom de « paires torsadées » car ce câble qui relie les machines au switch comporte en général 4 paires de fils torsadées et se termine par des connecteurs nommés RJ45.

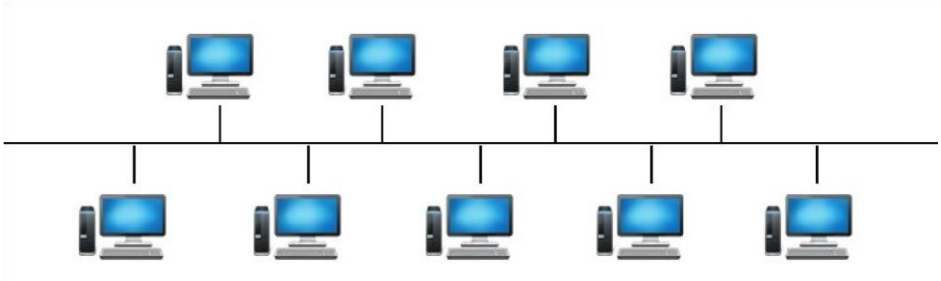
Les avantages :

- ajout facile de postes ;
- localisation facile des pannes ;
- le débranchement d'une connexion ne paralyse pas le reste du réseau ;
- simplicité éventuelle des équipements au niveau des nœuds : c'est le concentrateur qui est intelligent.
- évolution hiérarchisée du matériel possible. On peut facilement déplacer un appareil sur le réseau.

Les inconvénients :

- plus onéreux qu'un réseau à topologie en bus (achat du concentrateur et d'autant de câbles que de nœuds) ;
- si le concentrateur est défectueux, tout le réseau est en panne.
- utilisation de multiples routeur ou switch afin de pouvoir communiquer entre différents réseaux ou ordinateur

Réseau en bus



Un réseau en bus est une architecture de communication où la connexion des matériels est assurée par un bus partagé par tous les utilisateurs.
Les réseaux de bus permettent de relier simplement de multiples matériels, mais posent des problèmes quand deux machines veulent transmettre des données au même moment sur le bus. Les systèmes qui utilisent une topologie en bus ont normalement un arbitre qui gère l'accès au bus.
Cette topologie en bus a été très répandue car son coût d'installation est faible. Il est très facile de relier plusieurs postes d'une même salle, de relier chez soi deux ou trois ordinateurs. Aujourd'hui cette topologie n'est plus adaptée aux réseaux importants.

Avantages :

- Facile à mettre en œuvre et à étendre.
- Utilisable pour des réseaux temporaires (installation facile).
- Présente l'un des coûts de mise en réseau le plus bas.

Inconvénients

- Longueur du câble et nombre de stations limités.
- Un câble coupé peut interrompre le réseau.
- Les coûts de maintenance peuvent être importants à long terme.
- Les performances se dégradent avec l'ajout de stations.
- Faible sécurité des données transitant sur le réseau (toutes les stations connectées au bus peuvent lire toutes les données transmises sur le bus).

On remarquera que la technologie « bus » reste très utilisée dans l'industrie pour raccorder par exemple des capteurs à une unité centrale (automate, carte électronique, ordinateur, …). On parle alors de « bus de terrain » par opposition au bus informatique. En effet, le bus de terrain est en général beaucoup plus simple, du fait des faibles ressources numériques embarquées dans les capteurs et actionneurs industriels.Il est également plus robuste face aux perturbations externes. Exemples de bus de terrain : Bus CAN, MODBUS, protocole Dali, Profibus …..

Réseau en anneau

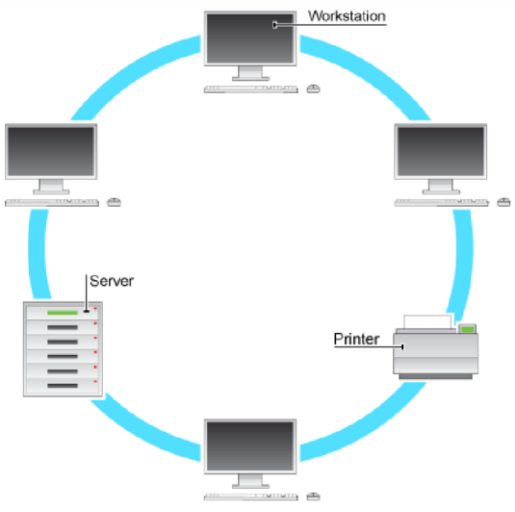
Toutes les machines sont reliées entre elles dans une boucle fermée. Les données circulent dans une direction unique, d'une entité à la suivante. Les ordinateurs communiquent chacun à leur tour. Cela ressemble à un bus mais qui serait refermé sur lui-même : le dernier nœud est relié au premier.
Souvent, dans une topologie en anneau, les ordinateurs ne sont pas reliés en boucle, mais sont reliés à un répartiteur (appelé MAU, Multistation Access Unit) qui va gérer la communication entre les ordinateurs qui lui sont reliés en répartissant à chacun d'entre-eux un temps de parole.
Elle utilise la méthode d'accès à "jeton" (Token ring). Les données transitent de stations en stations en suivant l'anneau qui chaque fois régénèrent le signal. Le jeton détermine quelle station peut émettre, il est transféré à tour de rôle vers la station suivante. Lorsque la station qui a envoyé les données les récupère, elle les élimine du réseau et passe le jeton au suivant, et ainsi de suite... La topologie en anneau est dite « topologie active » parce que le signal électrique est intercepté et régénéré par chaque machine.

Avantages :

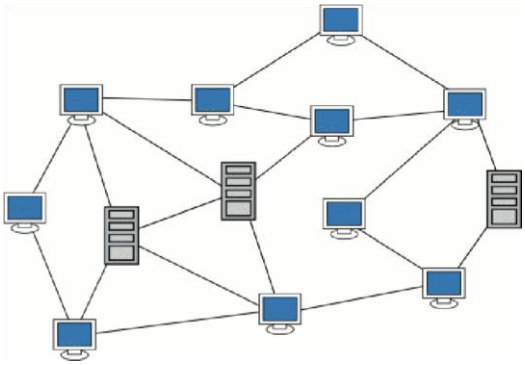
- La quantité de câble nécessaire est réduite
- Le protocole est simple, il évite la gestion des collisions
- Taux d'utilisation de la bande passante optimum (proche de 90%)
- Fonctionne mieux qu'une topologie de bus sous une lourde charge de réseau
- Il est assez facile à installer et à reconfigurer, car ajouter ou retirer un matériel nécessite de déplacer seulement deux connexions.

Inconvénients :

- Le retrait ou la panne d'une entité active paralyse le trafic du réseau.
- Le délai de communication est directement proportionnel au nombre de noeuds du réseau
- Le déplacement, l'ajout et la modification machines connectées peuvent affecter le réseau

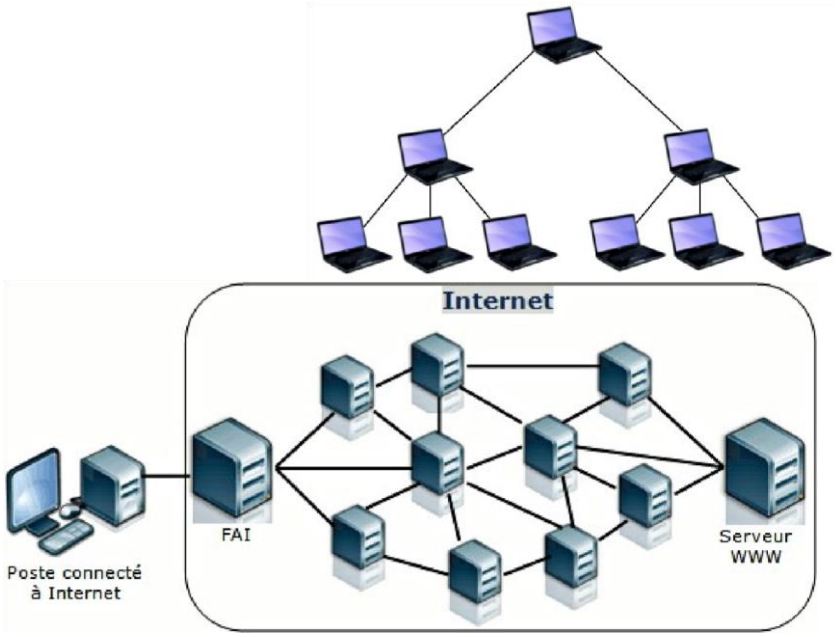


Réseau maillé



Le réseau maillé est une topologie de réseau qualifiant les réseaux (filaires ou non) dont tous les hôtes sont connectés pair à pair sans hiérarchie centrale, formant ainsi une structure en forme de filet. Par conséquent, chaque nœud doit recevoir, envoyer et relayer les données. Cela évite d'avoir des points sensibles, qui en cas de panne, isolent une partie du réseau. Si un hôte est hors service, ses voisins passeront par une autre route.
Les réseaux maillés utilisent plusieurs chemins de transferts entre les différents nœuds. Cette méthode garantit le transfert des données en cas de panne d'un nœud.

Le réseau Internet est basé sur une topologie maillée (sur le réseau étendu « WAN », elle garantit la stabilité en cas de panne d'un nœud).



Réseau en arbre (ou hiérarchique)

Une topologie en arbre ou topologie arborescente ou hiérarchique peut être considérée comme une collection de réseaux en étoile disposés en hiérarchie. Ce réseau est divisé en niveaux. Le sommet, de haut niveau, est connectée à plusieurs nœuds de niveau inférieur, dans la hiérarchie. Ces nœuds peuvent être eux-mêmes connectés à plusieurs nœuds de niveau inférieur.
Comme dans le réseau en étoile conventionnel, des nœuds individuels peuvent ainsi encore être isolés du réseau par une défaillance d'un seul point d'un trajet de transmission vers le nœud. Si un lien reliant une branche échoue, cette branche est isolée; Si une connexion à un nœud échoue, une section entière du réseau devient isolée du reste.

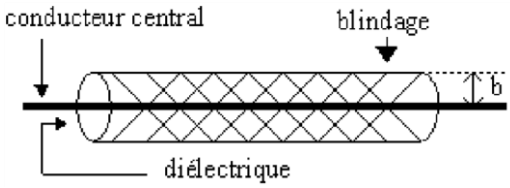
III. Communications informatiques

1 . Les supports de transmission

Le cuivre : câbles coaxiaux ou à paires torsadées

Le **câble coaxial** est un câble permettant entre autres le transport de données. Il est composé, au moins, de deux conducteurs.

L'âme centrale, qui peut être mono-brin ou multi-brins (en cuivre ou en cuivre argenté, voire en acier cuivré), est entourée d'un matériau diélectrique (isolant). L'isolant est entouré d'une tresse conductrice (ou feuille d'aluminium enroulée), puis d'une gaine isolante et protectrice.



Une **paire torsadée** est formée de deux fils conducteurs enroulés en hélice l'un autour de l'autre. Un câble peut contenir plusieurs paires torsadées.

Pour limiter les interférences, les paires torsadées sont souvent blindées. Comme le blindage est fait de métal, celui-ci constitue également un référentiel de masse. Le blindage peut être appliqué individuellement aux paires, ou à l'ensemble formé par celles-ci.

Tableau récapitulatif avec les dénominations officielles (norme ISO/IEC 11801) :

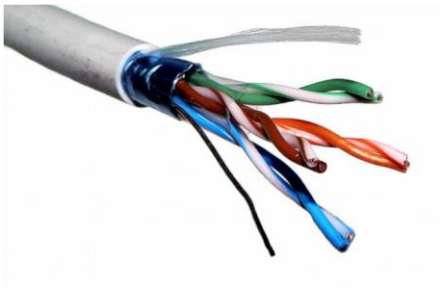
Dénomination courante	**Désignation**	**Dénomination officielle**	**Blindage de l'ensemble du câble**	**Blindage des paires individuelles**
UTP	*Unshielded twisted pair* : Paire torsadée non blindée	U/UTP	aucun	aucun
STP	*Shielded twisted pair*: Paire torsadée blindée	U/FTP	aucun	feuillard
FTP	*Foiled twisted pair* : Paire torsadée écrantée	F/UTP	feuillard	aucun
FFTP	*Foiled foiled twisted pair:* Paire torsadée doublement écrantée	F/FTP	feuillard	feuillard
SFTP	*Shielded foiled twisted pair:* Paire torsadée écrantée et blindée :	SF/UTP	feuillard, tresse	aucun
SSTP	*Shielded shielded twisted pair:* Paire torsadée doublement blindée	S/FTP	Tresse	feuillard

Légende :

TP = twisted pair ou paire torsadée
U = unshielded ou non blindé
F = foil shielding ou blindage par feuillard

Exemple d'un câble FTP :

S = braided shielding ou blindage par tresse
Les câble sont aussi caractérisées par leur catégorie :



Catégorie	Classe	Impédance	Fréquence max.	Application
3	C	100-120 Ω	16 MHz	Token Ring 4 Mbit/s, 10 Base T, Fast Ethernet, 100 VG Any, LAN 100 Base T4
4	D	100 Ω	20 MHz	Token Ring 16 Mbit/s
5	D	100 Ω	100 MHz	Câble UTP et FTP, 100 Base Tx, ATM 155 Mbit/s, 1000 Base T (Cat 5E)
6	E	100 Ω	250 MHz	Câble FTP et SFTP, 1000 Base Tx
6a	E	100 Ω	500 MHz	Câble FTP et SFTP, 1000 Base Tx, 10 G Base T
7	F	100 Ω	600 MHz	Câble SFTP

Divers organismes de normalisation contribuent à la définition des propriétés physiques, électriques et mécaniques des supports disponibles pour différentes communications de données. Ces spécifications garantissent que les câbles et connecteurs fonctionnent comme prévu avec différentes mises en œuvre.

Par exemple, des normes pour les supports en cuivre sont définies pour :

- Le type de câblage en cuivre utilisé
- La bande passante de la communication
- Le type de connecteurs utilisés
- Le brochage et les codes couleur des connexions avec le support
- La distance maximale du support

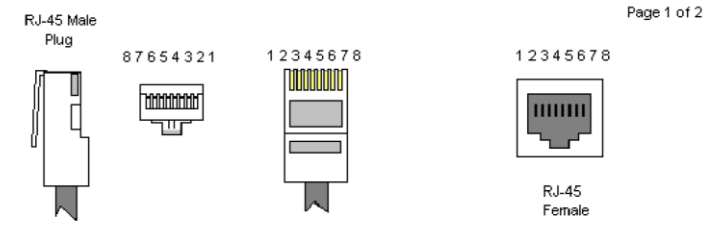
Un exemple de connecteur utilisé pour les liaisons Ethernet : RJ 45

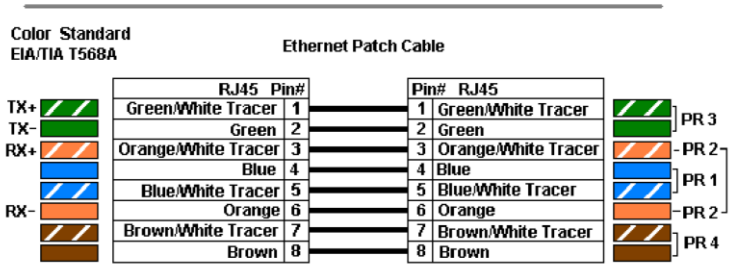
RJ45 est le nom usuel du connecteur 8P8C (8 positions et 8 contacts électriques) utilisé couramment pour les connexions Ethernet, et plus rarement pour les réseaux téléphoniques. La référence « RJ » vient de l'anglais Registered Jack (prise jack enregistrée).

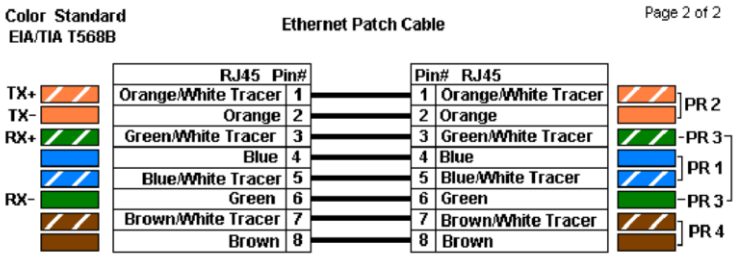
Câblage :
Lors d'un câblage informatique en 10/100 Mbit/s, seules les quatre broches 1-2 et 3-6 sont utilisées pour transmettre les informations. Lors d'un câblage informatique en 1 000 Mbit/s (1 Gbit/s), les 8 broches sont utilisées.

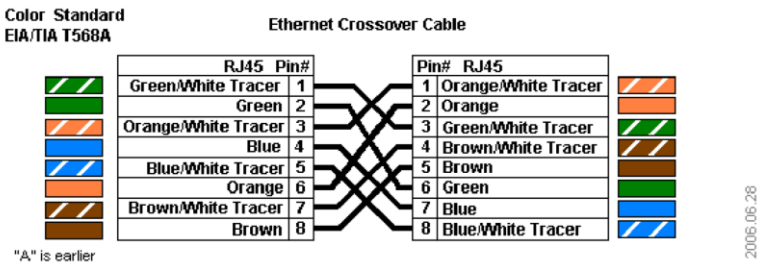
- Lorsqu'on branche un poste de travail dans un concentrateur (hub) ou un commutateur (switch), un câble droit doit être utilisé.
- Lorsqu'on doit brancher deux postes de travail ensemble, un câble croisé doit être utilisé. Dans le câble croisé, les paires utiles sont inversées, c'est-à-dire que la paire de transmission d'un côté est connectée aux broches de réception de l'autre côté.

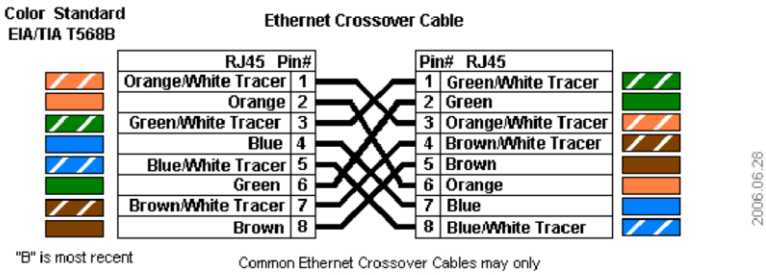
La règle générale est la suivante : pour deux périphériques travaillant au niveau de la couche 2 (MAC) du modèle OSI comme un Hub Ethernet ou un switch sans fonction de routage, ou deux périphériques de la couche 3 (IP) comme un PC ou un routeur, on utilise un câble croisé. Dès que l'on change de couche entre deux équipements, on peut alors utiliser un câble droit (PC à Switch, Routeur à Switch, Hub à PC, etc.).





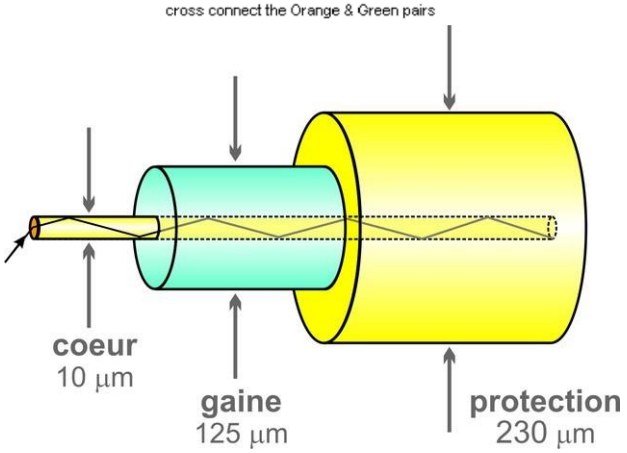






Il existe plusieurs normes (T568A et T568B) : même si ces deux normes sont déployées, la norme T568A est principalement utilisée dans le domaine du résidentiel (souvent avec du câblage simple non blindé de type UTP) alors que la norme T568B est plutôt employée dans le domaine professionnel.

Le verre : fibre optique



Le câblage en fibre optique utilise des fibres de verre ou de plastique pour guider des impulsions lumineuses de la source à la destination. Au final la fibre optique est un guide d'onde qui exploite les propriétés réfractrices de la lumière. Elle est habituellement constituée d'un cœur entouré d'une gaine.

Comme l'électronique est essentiellement basée sur l'électricité il faudra convertir les bits électriques (tension) en lumière pour la transmission et inversement pour la réception.

Les bits sont codés sur la fibre sous forme d'impulsions lumineuses. Les émetteurs utilisés sont de trois types :

- les diodes électroluminescentes (LED) qui fonctionnent dans le proche infrarouge (850 nm),
- les lasers, utilisés pour la fibre monomode, dont la longueur d'onde est 1 310 ou 1 550 nm,
- les diodes à infrarouge qui émettent dans l'infrarouge à 1 300 nm.

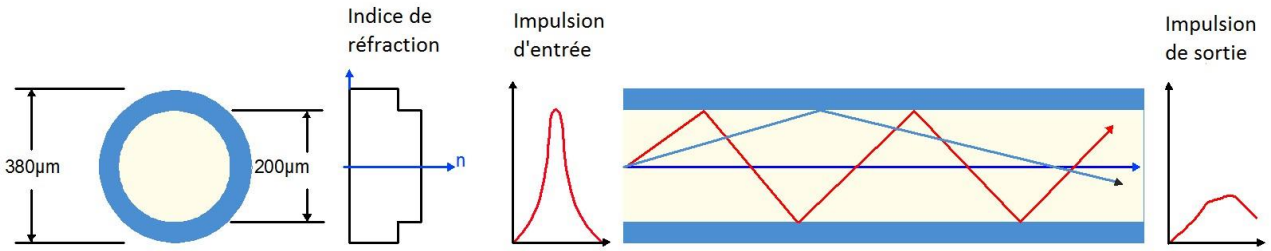
Le câblage en fibre optique prend en charge des débits de bande passante de données brutes très élevés.
Des dispositifs à semi-conducteur électronique appelés photodiodes détectent les impulsions lumineuses et les convertissent en tensions qui peuvent ensuite être reconstituées en trames de données.
Au cours de son parcours, le signal est atténué et déformé : des répéteurs et des amplificateurs placés à intervalles réguliers permettent de conserver l'authenticité du message.

Fibres multimodes

Les fibres multimodes (dites MMF, pour Multi Mode Fiber), ont été les premières sur le marché. Ce sont les plus courantes. Elles ont pour caractéristique de transporter plusieurs modes (trajets lumineux). Du fait de la dispersion modale, on constate un étalement temporel du signal proportionnel à la longueur de la fibre. En conséquence, elles sont utilisées uniquement pour des bas débits ou de courtes distances. Elles sont caractérisées par un diamètre de cœur de plusieurs dizaines à plusieurs centaines de micromètres (les cœurs en multimodes sont de 50 ou 62,5 µm pour le bas débit). Cependant les fibres les plus récentes, de type OM3, permettent d'atteindre le Gbit/s sur des distances de l'ordre du km.

Il existe plusieurs modes de propagation de la lumière au sein de son cœur de silice (verre).

Multimode à saut d'indice :



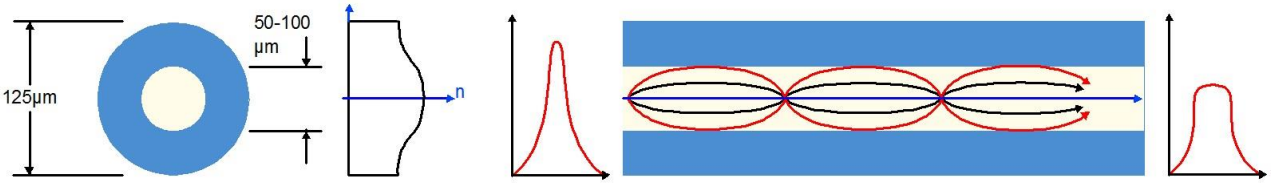
Fibre à saut d'indice

L'atténuation sur ce type de fibre est très importante comme on peut le voir sur la différence des impulsions d'entrée et de sortie.

- Débit: environ 100 Mbit/s
- Portée maximale: environ 2 Km

Multimode à gradient d'indice :

La fibre multimode à gradient d'indice est elle aussi utilisée dans les réseaux locaux. C'est une fibre multimode, donc plusieurs modes de propagation coexistent. A la différence de la fibre à saut d'indice, il n'y a pas de grande différence d'indice de réfraction entre cœur et gaine.
Cependant, le cœur des fibres à gradient d'indice est constitué de plusieurs couches de matière ayant un indice de réfraction de plus en plus élevé. Ces différentes couches de silice de densités multiples influent sur la direction des rayons lumineux, qui ont une forme elliptique.



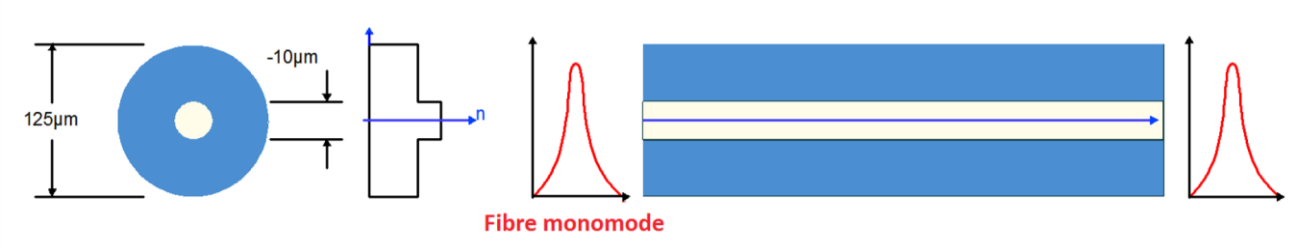
Fibre à gradient d'indice

La fibre à gradient d'indice possède un cœur de taille intermédiaire. L'atténuation sur ce type de fibre est moins importante que sur les fibres à saut d'indice.

- Débit: environ 1 Gbit/s
- Portée maximale: environ 2 Km

Fibres monomodes

Pour de plus longues distances et/ou de plus grands débits, on préfère utiliser des fibres monomodes (dites SMF, pour Single Mode Fiber), qui sont technologiquement plus avancées car plus fines (voire très fines). Ce sont les meilleures fibres optiques actuellement disponibles. Leur cœur très fin n'admet ainsi qu'un mode de propagation, le plus direct possible c'est-à-dire dans l'axe de la fibre. Les pertes sont donc minimes (moins de réflexion sur l'interface cœur/gaine) que cela soit pour de très haut débits ou de très longues distances. Les fibres monomodes sont de ce fait adaptées pour les lignes intercontinentales (câbles sous-marin).



- Débit: environ 100 Gbit/s
- Portée maximale: environ 100 Km

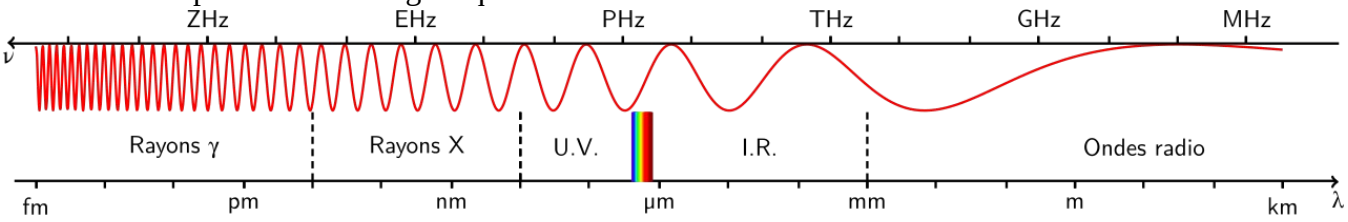
Ondes électromagnétiques : sans fil

Les supports sans fil transportent des signaux (sons, données, …) à l'aide d'ondes électromagnétiques.

Les technologies de communication de données sans fil fonctionnent bien dans les environnements ouverts. Cependant, certains matériaux de construction utilisés dans les bâtiments, ainsi que le terrain local (montagnes, collines, ...), limitent la couverture effective. De plus, la transmission sans fil est sensible aux interférences et peut être perturbée par des appareils aussi courants que les téléphones fixes sans fil, certains types d'éclairages fluorescents, les fours à micro-ondes et d'autres communications sans fil.

En outre, la couverture de communication sans fil n'exigeant aucun accès à un fil physique de support, des périphériques et utilisateurs non autorisés à accéder au réseau peuvent accéder à la transmission. La sécurité du réseau constitue par conséquent un composant essentiel de l'administration de réseau sans fil.

Domaines du spectre électromagnétique :



Nom	Longueur d'onde(m)	Fréquence(Hz)	Énergie du photon (eV)
Rayon gamma	< 10 pm	> 30 EHz	> 124 keV
Rayon X	10 pm – 10 nm	30 EHz – 30 PHz	124 keV – 124 eV

Ultraviolet	10 nm – 390 nm	30 PHz – 750 THz	124 eV – 3,2 eV
Visible	390 nm – 750 nm	770 THz – 400 THz	3 ,2 eV – 1,7 eV
Infrarouge	750 nm – 0,1 mm	400 THz – 3 THz	1 ,7 eV – 12,4 meV
Térahertz / submillimétrique	0,1 mm - 1 mm	3 THz - 300 GHz	12 ,4 meV - 1,24 meV
Micro-ondes	1 mm - 1 m	300 GHz - 300 MHz	1 ,24 meV - 1,24 µeVeV
Ondes radio	1 m – 100 000 km	300 MHz – 3 Hz	1 ,24 µeVeV – 12,4 feV

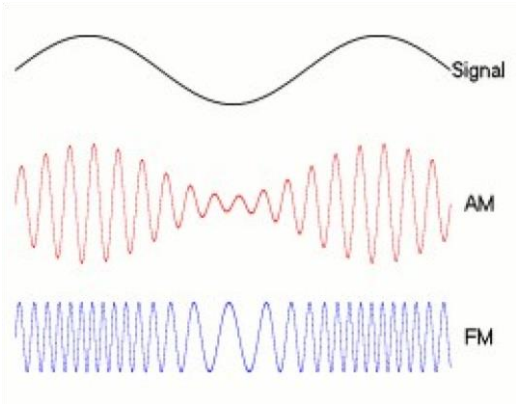
Les normes et technologies les plus courantes sont le GSM, le Wifi, le Bluetooth. Il en existe beaucoup d'autres.

Bande de fréquence	Service/Application
9 kHz-30 MHz	Radio grandes ondes, ondes moyennes et ondes courtes, détecteurs de victimes d'avalanches, systèmes RFID, applications médicales, plaques de cuisson à induction, CPL...
30 MHz-87,5 MHz	Télédiffusion (bande I), réseaux taxis, pompiers... radioamateurs, microphones sans fil, radars...
87,5 MHz - 108 MHz	Bande FM (modulation de fréquence)
108 MHz - 136 MHz	Trafic aéronautique
136 MHz - 400 MHz	Télédiffusion (bande II et III), réseaux professionnels (police, pompiers, SAMU...), vol libre (talkie-walkie), trafic amateur, trafic maritime, radiomessagerie...
400 MHz - 470 MHz	Balises ARGOS, réseaux professionnels (SNCF, EDF...), télécommandes, télémesure médicale, réseaux cellulaires
470 MHz - 860 MHz	Télédiffusion bande IV et V
704 MHz - 960 MHz	Téléphonie mobile bandes des 700, 800 et 900 MHz
960 MHz - 1 710 MHz	Radiodiffusion numérique, faisceaux hertziens
1 710 MHz - 1 880 MHz	Téléphonie mobile, bande 1 800 MHz
1 880 MHz - 1 900 MHz	Téléphonie DECT
1 900 MHz - 2 170 MHz	Téléphonie mobile UMTS
2 400 MHz - 2 500 MHz	Réseaux Wi-Fi, Bluetooth, four à micro-ondes
2 500 MHz - 2 690 MHz	Téléphonie mobile (LTE), bande des 2 600 MHz
3 400 MHz - 3 600 MHz	Boucle locale radio de type WiMAX

Exemple d'utilisation des ondes électromagnétiques pour transporter des informations

Au temps de l'analogique :

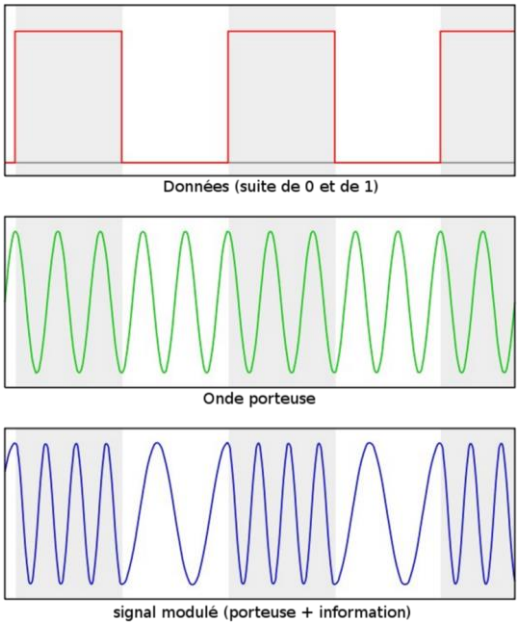
Ci-contre les 2 principales méthodes pour transmettre une information analogique (ici du son) à l'aide d'ondes électromagnétiques.
AM : modulation d'amplitude (l'amplitude du signal varie en fonction du signal à transporter)
FM : modulation de fréquence (la fréquence du signal varie en fonction du signal à transporter)



Maintenant en numérique.
On utilise aussi les 2 principes utilisés du temps de l'analogique (modulation d'amplitude et modulation de fréquence) parfois en les combinant.

Exemple :

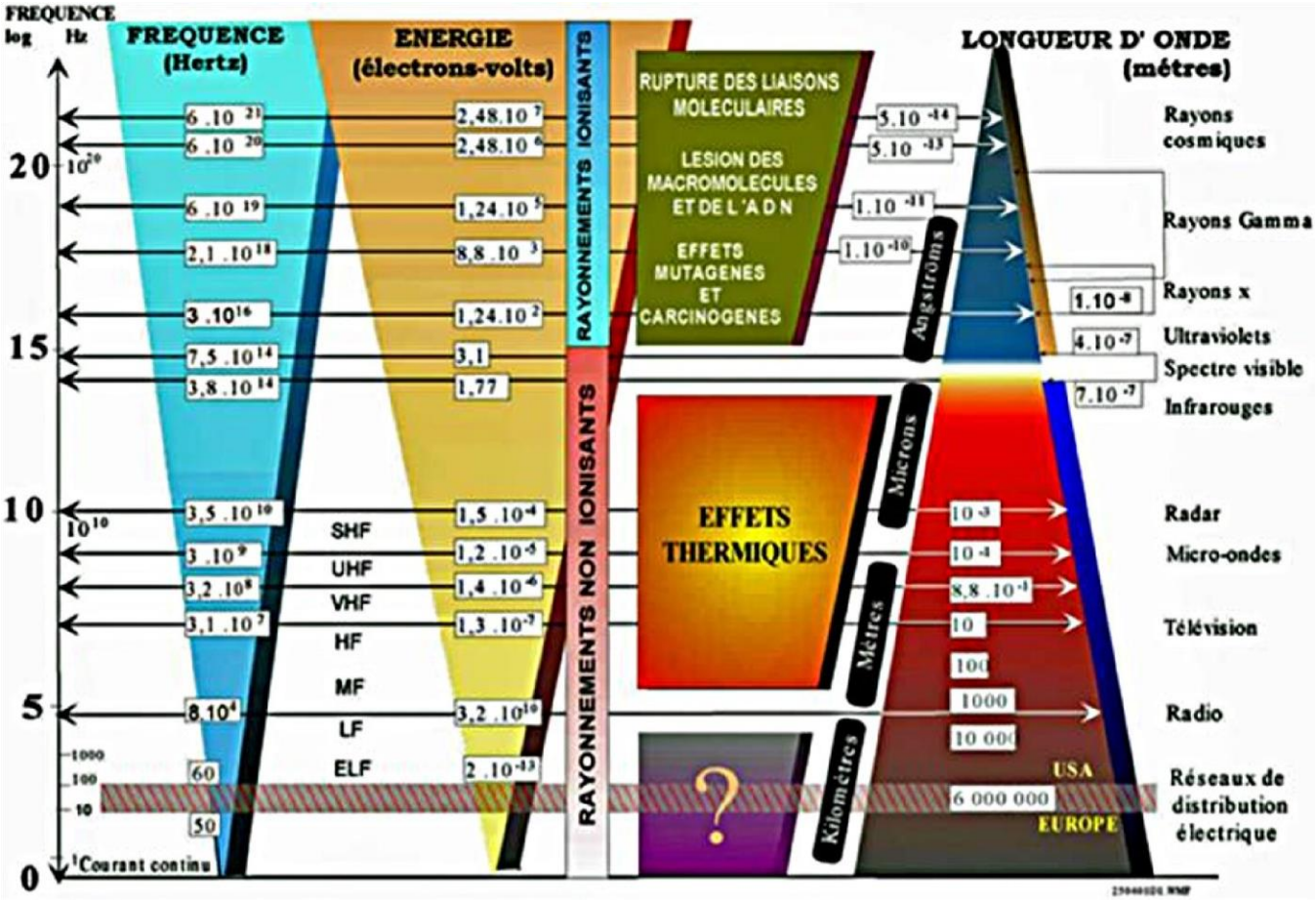
La modulation par déplacement de fréquence (MDF), plus connue sous sa dénomination anglophone de frequencyshift keying (FSK) est un mode de modulation de fréquence numérique dans lequel le signal modulé varie entre des fréquences prédéterminées.



Il y a bien sûr de nombreuses autres manières de transporter des données numériques mais elles n'entrent pas dans le cadre de ce cours.

Risques sanitaires des télécommunications

Les champs électromagnétiques créées par les télécommunications hertziennes (téléphone mobile, le téléphone domestique sans fil, le Wi-Fi, ou encore les antenne-relais de téléphonie mobile) sont perçus par certains comme une « pollution électromagnétique » dangereuse pour la santé, alors que les études scientifiques de ces dernières années ont donné des résultats contradictoires. Il semble quand même y avoir un risque que les études scientifiques n'ont pas encore permis de confirmer totalement ni d'évaluer (il faut dire que les études sont assez rares et celles qui existent sont souvent financées par les sociétés qui émettent ces ondes électromagnétiques donc leurs résultats ne sont pas toujours fiables).
Bref il s'agit d'un sujet à controverse et les impacts sur le très long terme de l'exposition au rayonnement électromagnétique issus des appareils modernes sont encore relativement méconnus.



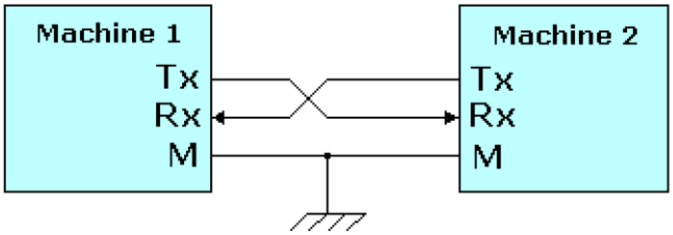
2. Exemple N°1 : la liaison série (RS232 et Arduino)

La liaison série va permettre de faire communiquer 2 appareils (ordinateurs, capteurs, …).

Des liaisons séries, il en existe beaucoup (RS-232, Universal Serial Bus (USB), Serial ATA, SPI, …). Nous allons nous intéresser à la RS-232, qui est très répandue ainsi qu'à la version présente sur les cartes micro-contrôleur Arduino.

Pour communiquer via la voie série, deux dispositifs doivent avoir 3 câbles minimum.

- le premier câble est la référence électrique, communément appelée masse électrique. Cela permet de prendre les mesures de tension en se fixant un même référentiel. Dans notre cas, on considérera que le 0V sera notre référentiel électrique commun.
- Les deux autres câbles permettent la transmission des données. L'un sert à l'envoi des données pour un émetteur, mais sert aussi pour la réception des données venant de l'autre émetteur. Idem pour l'autre câble. Il permet l'émission de l'un et la réception de l'autre.



Il s'agit du strict minimum. La norme n'interdit pas l'utilisation d'autres câbles qui servent à faire du contrôle de flux et de la gestion des erreurs.

La vitesse de transmission de l'émetteur doit être identique à la vitesse d'acquisition du récepteur. Ces vitesses sont exprimées en BAUDS (1 baud correspond à 1 bit par seconde). Il existe différentes vitesses normalisées: 9600, 4800, 2400, 1200... bauds
La communication peut se faire dans les deux sens (duplex), soit émission d'abord, puis réception ensuite (half-duplex), soit émission et réception simultanées (full-duplex)
La transmission étant du type asynchrone (pas d'horloge commune entre l'émetteur et le récepteur), des bits supplémentaires sont indispensables au fonctionnement: bit de début de mot (start), bit(s) de fin de mot (stop).

Le principal intérêt de la communication série est le nombre de fils réduits: la communication la plus simple peut être faite sur 3 fils (Tx, Rx et masse).

Le signal électrique et le protocole

Avant tout, il faut savoir que pour communiquer, deux dispositifs électronique ou informatique utilisent des données sous forme de bits. Ces bits sont des états logiques (vrai ou faux, 0 ou 1) qui peuvent être regroupés pour faire des ensembles de bits. Quand ces ensembles de bits sont constitués de 8 bits ils forment alors un octet. Jusqu'ici rien de nouveau !

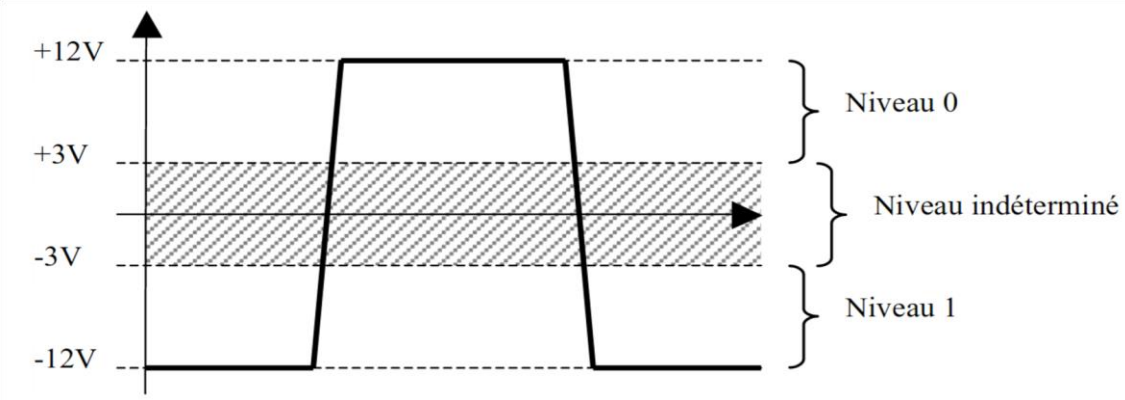
Les tensions utilisées

Ces bits sont en fait des niveaux de tension électrique. Et la norme RS-232 définit quelles tensions doivent être utilisées (ici norme V28 présente sur les ordinateurs) :

	Niveau logique 0	**Niveau logique 1**
Tension électrique minimale	+3V	-3 V
Tension électrique maximale	+25V	-25 V

Ce qui donne : -3v > 1 logique > -25v et +3v < 0 logique < +25v

En général on obtient :



On note que les tensions comprises entre +3V et -3V sont ignorées car c'est dans ces zones là que se trouvent la plupart des parasites. C'est un moyen permettant d'éviter un certain nombre d'erreurs de transmissions.
C'est aussi un moyen de contrôler que la liaison physique (les fils) est correcte : lorsqu'il n'y a pas de communication sur la voie série, il y a ce qu'on appelle un état de repos. C'est à dire un niveau logique toujours présent. Il s'agit du niveau logique 1. Soit une tension comprise entre -3V et -25V. Si cet état de repos n'est pas présent, c'est qu'il peut y avoir un problème de câblage (fil coupé, …).

Les données

Les données qui transitent par la voie série sont transmises sous une forme numérique (binaire). C'est à dire avec des niveaux logiques 0 et 1. Prenons une donnée que nous voudrions envoyer, par exemple la lettre « P » majuscule. Il faut savoir qu'une lettre du clavier est codé sur un nombre de 8 bits, donc un octet. Réellement c'est en fait sur 7 bits qu'elle est codée, mais en rajoutant un 0 devant le codage, cela conserve sa valeur et permet d'avoir un codage de la lettre sur 8 bits. Ces codes sont définis selon la table ASCII. Ainsi, pour chaque caractère du clavier, on retrouve un codage sur 8 bits.

ASCII TABLE

Decimal	Hex	Char	Decimal	Hex	Char	Decimal	Hex	Char	Decimal	Hex	Char
0	0	[NULL]	32	20	[SPACE]	64	40	@	96	60	`
1	1	[START OF HEADING]	33	21	!	65	41	A	97	61	a
2	2	[START OF TEXT]	34	22	"	66	42	B	98	62	b
3	3	[END OF TEXT]	35	23	#	67	43	C	99	63	c
4	4	[END OF TRANSMISSION]	36	24	$	68	44	D	100	64	d
5	5	[ENQUIRY]	37	25	%	69	45	E	101	65	e
6	6	[ACKNOWLEDGE]	38	26	&	70	46	F	102	66	f
7	7	[BELL]	39	27	'	71	47	G	103	67	g
8	8	[BACKSPACE]	40	28	(	72	48	H	104	68	h
9	9	[HORIZONTAL TAB]	41	29	)	73	49	I	105	69	i
10	A	[LINE FEED]	42	2A	*	74	4A	J	106	6A	j
11	B	[VERTICAL TAB]	43	2B	+	75	4B	K	107	6B	k
12	C	[FORM FEED]	44	2C	,	76	4C	L	108	6C	l
13	D	[CARRIAGE RETURN]	45	2D	-	77	4D	M	109	6D	m
14	E	[SHIFT OUT]	46	2E	.	78	4E	N	110	6E	n
15	F	[SHIFT IN]	47	2F	/	79	4F	O	111	6F	o
16	10	[DATA LINK ESCAPE]	48	30	0	80	50	P	112	70	p
17	11	[DEVICE CONTROL 1]	49	31	1	81	51	Q	113	71	q
18	12	[DEVICE CONTROL 2]	50	32	2	82	52	R	114	72	r
19	13	[DEVICE CONTROL 3]	51	33	3	83	53	S	115	73	s
20	14	[DEVICE CONTROL 4]	52	34	4	84	54	T	116	74	t
21	15	[NEGATIVE ACKNOWLEDGE]	53	35	5	85	55	U	117	75	u
22	16	[SYNCHRONOUS IDLE]	54	36	6	86	56	V	118	76	v
23	17	[ENG OF TRANS. BLOCK]	55	37	7	87	57	W	119	77	w
24	18	[CANCEL]	56	38	8	88	58	X	120	78	x
25	19	[END OF MEDIUM]	57	39	9	89	59	Y	121	79	y
26	1A	[SUBSTITUTE]	58	3A	:	90	5A	Z	122	7A	z
27	1B	[ESCAPE]	59	3B	;	91	5B	[	123	7B	{
28	1C	[FILE SEPARATOR]	60	3C	<	92	5C	\	124	7C	|
29	1D	[GROUP SEPARATOR]	61	3D	=	93	5D	]	125	7D	}
30	1E	[RECORD SEPARATOR]	62	3E	>	94	5E	^	126	7E	~
31	1F	[UNIT SEPARATOR]	63	3F	?	95	5F	_	127	7F	[DEL]

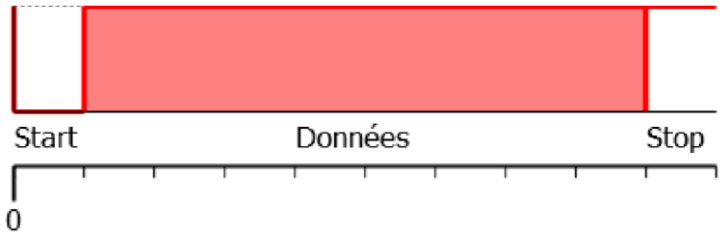
En observant la table, on tombe sur la lettre « P » majuscule et l'on voit que sa correspondance en décimal est 80 donc en binaire : 01010000.

L'ordre et les délimiteurs

On va à présent voir comment est transmit un octet sur la voie série en envoyant notre exemple, la lettre « P ».
Pour comprendre suivons l'analogie d'un appel téléphonique :

- Lorsque l'on passe un coup de fil, bien généralement on commence par dire « Bonjour » ou « Allo ». Ce début de message permet de faire l'ouverture de la conversation. En effet, si l'on reçoit un appel et que personne ne répond après avoir décroché, la conversation ne peut avoir lieu. Dans la norme RS-232, on va avoir une ouverture de la communication grâce à un bit de départ. C'est lui qui va engager la conversation avec son interlocuteur. Dans la norme RS-232, ce dernier est un état 0.
- Ensuite, vous allez commencer à parler et donner les informations que vous souhaitez transmettre. Ce sera les données. L'élément principal de la conversation (ici notre lettre 'P').

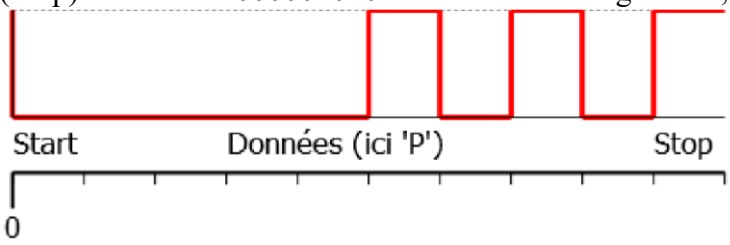
- Enfin, après avoir renseigné tout ce que vous aviez à dire, vous terminez la conversation par un « Au revoir ». Cela termine la conversation. Il y aura donc un bit de fin ou bit de stop qui fera de même sur la voie série. Dans la norme RS-232, c'est un état 1.



C'est de cette manière là que la communication série fonctionne. D'ailleurs, savez-vous pourquoi la voie série s'appelle ainsi ? En fait, c'est parce que les données à transmettre sont envoyées une par une, à la queue leu-leu. Exactement comme une conversation entre deux personnes : la personne qui parle ne peut pas dire plusieurs phrases en même temps, ni plusieurs mots ou sons. Chaque élément se suit selon un ordre logique. L'image précédente résume la communication que l'on vient d'avoir, il n'y a plus qu'à la compléter pour envoyer la lettre « P ».

Donc il y a le bit de start, notre lettre P et le bit de stop. D'après ce qu'on a dit, cela donnerait, dans l'ordre, ceci : 0 (Start) 01010000 (Données) et 1 (Stop).

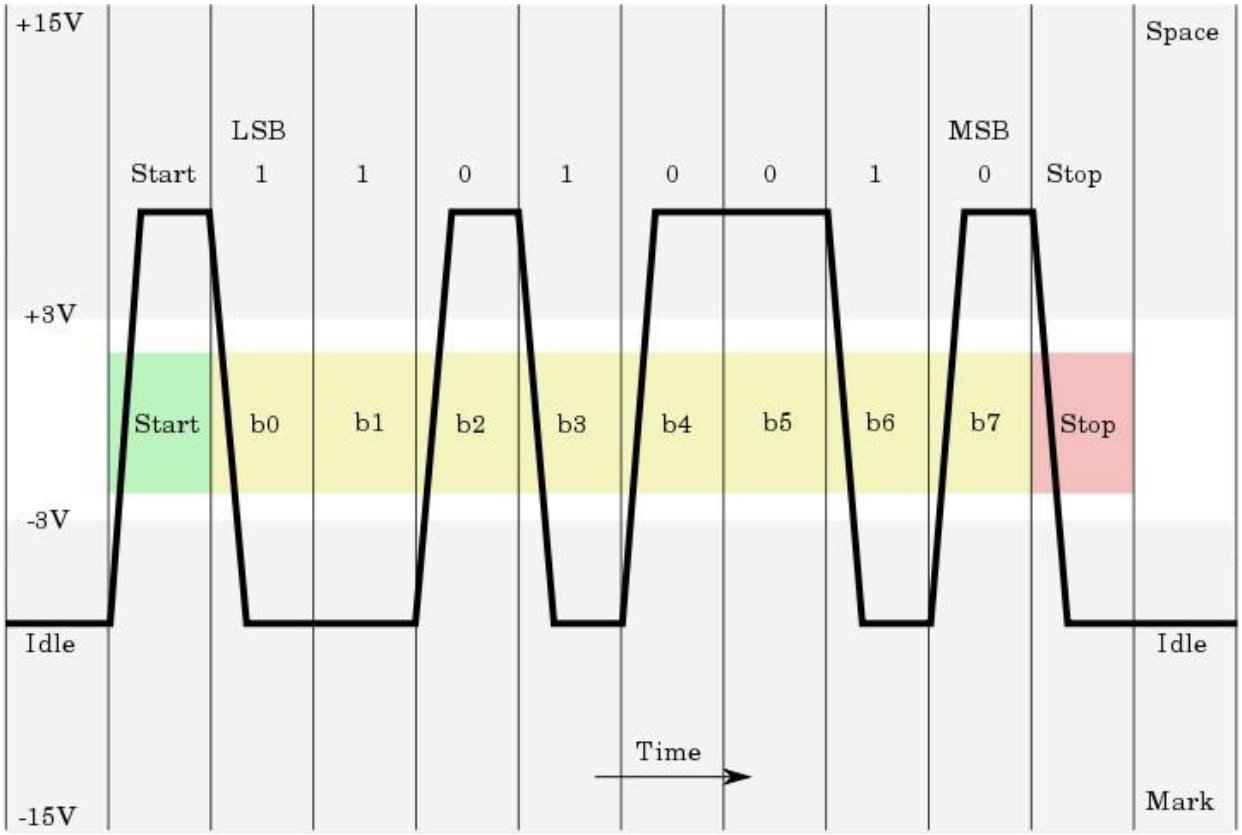
Eh bien… c'est presque ça. Sauf que les ingénieurs qui ont inventé ce protocole ont eu la bonne idée de transmettre les données à l'envers… Par conséquent, la bonne réponse était : 0(Start)00001010(données)1(Stop) c'est à dire 0000010101. Avec un chronogramme, on observerait ceci :



Un peu de vocabulaire

Les données sont donc envoyées à l'envers. Ce qu'il faut savoir c'est que le bit de donnée qui vient après le bit de start s'appelle le bit de poids faible ou LSB en anglais pour Less Significant Bit. C'est un peu comme un nombre qui a des unités (tout à droite), des dizaines, des centaines, des milliers (à gauche), etc. Par exemple le nombre 6395 possède 5 unités (à droite), 9 dizaines, 3 centaines et 6 milliers (à gauche). On peut faire référence au bit de poids faible en binaire qui est donc à droite. Plus on s'éloigne et plus on monte vers… le bit de poids fort ou MSB en anglais pour Most Significant Bit. Et comme les données sont envoyées à l'envers sur la liaisons série, on aura le bit de poids faible juste après le start, donc à gauche et le bit de poids fort à droite.
Il est donc essentiel de savoir où est le bit de poids faible pour pouvoir lire les données à l'endroit. Sinon on se retrouve avec une donnée erronée !

Pour regrouper un peu tout ce que l'on a vu sur le protocole de la norme RS-232, voici une image d'une trame :



Vous devrez être capable de trouver quel est le caractère envoyé sur cette trame… alors ? Indice : c'est une lettre… On lit les niveaux logiques de gauche à droite, soit 11010010 ; puis on les retourne soit 01001011 ; enfin on compare à la table ASCII et on trouve la lettre « K » majuscule. Attention aux tensions négatives qui correspondent à l'état logique 1 et les tensions positives à l'état logique 0.

La vitesse

La norme RS-232 définit la vitesse à laquelle sont envoyée les données. Elles sont exprimés en bit par seconde (bit/s). Elle préconise des vitesse inférieures à 20 000 bits/s. Sauf qu'en pratique, il est très courant d'utiliser des débits supérieurs pouvant atteindre les 115 200 bits/s. Quand on va utiliser la voie série, on va définir la vitesse à laquelle sont transférées les données. Cette vitesse dépend de plusieurs contraintes que sont : la longueur du câble utilisé reliant les deux interlocuteurs et la vitesse à laquelle les deux interlocuteurs peuvent se comprendre. Voilà ce que dit la norme RS-232 :

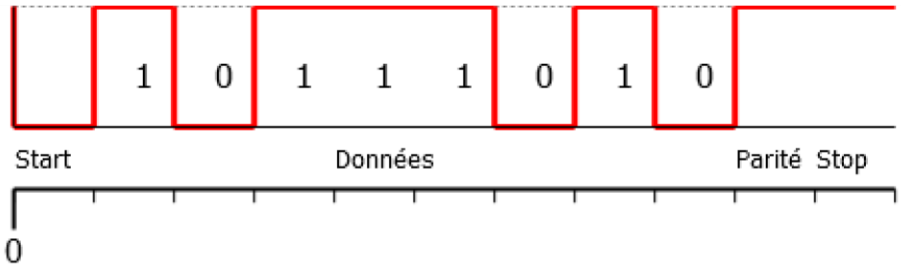
Débit (bit/s) - (bauds)	**Longueur (m)**
2 400	60
4 800	30
9 600	15
19 200	7 , 6
38 400	3 , 7
56 000	2 , 6

Plus le câble est court, plus le débit pourra être élevé car moins il y a d'affaiblissement des tensions et de risque de parasites.

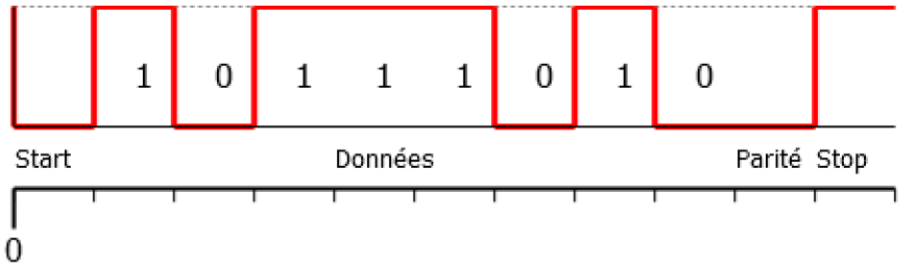
La gestion des erreurs

Malgré les tensions imposées par la norme, il arrive qu'il y ai d'autres parasites et que des erreurs de transmission surviennent. Pour limiter ce risque, il existe une solution. Elle consiste à ajouter un bit de contrôle appelé bit de parité. Juste avant le bit de stop, on va ajouter un bit qui sera pair ou impair. Donc, respectivement, soit un 0 soit un 1. Le paramétrage de la liaison va permettre de choisir une parité paire ou impaire.

Si l'on choisi une **parité paire**, alors le nombre de niveaux logiques 1 dans les données plus le bit de parité doit donner un nombre paire. Donc, dans le cas ci-dessous où il y a 5 niveaux logiques 1 sans le bit de parité, ce dernier devra prendre un niveau logique 1 pour que le nombre de 1 dans le signal soit paire. Soit 6 au total :



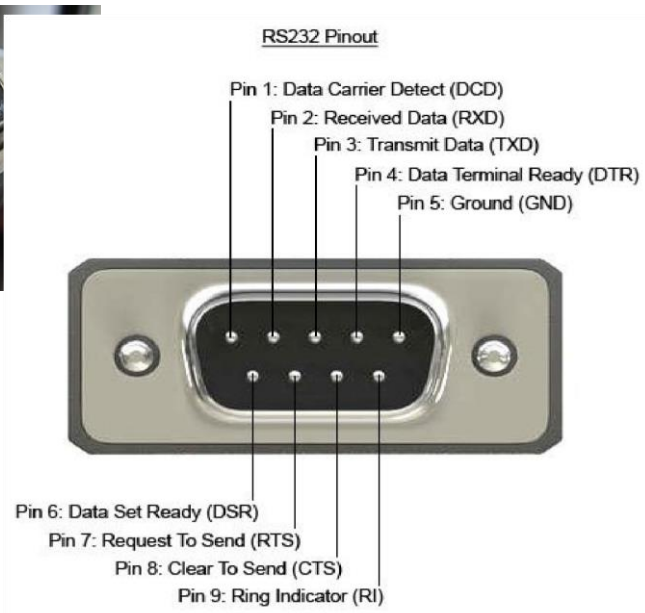
Dans le cas où l'on choisirait une **parité impaire**, alors dans le même signal où il y a 5 niveaux logiques 1 , eh bien le bit de parité devra prendre la valeur qui garde un nombre impaire de 1 dans le signal. Soit un bit de parité égal à 0 dans notre cas :



Après, c'est le récepteur qui va vérifier si le nombre de niveaux logiques 1 est bien égale à ce que indique le bit de parité. Dans le cas où une erreur de transmissions serait survenu, ce sera au récepteur de traiter le problème et de demander à son interlocuteur de répéter.

Le connecteur de la liaison série RS232

Le connecteur utilisé par la norme RS232 est du type DB9 :



On notera la présence des 3 fils obligatoires au minimum : RxD (receive Data), TxD et la masse GROUND mais aussi d'autres possibilités de fils permettant une gestion plus efficace de la liaison série (on ne traitera pas de leur utilisation dans ce cours).

La liaison série de la carte microcontrôleur Arduino.

Prenons l'exemple suivant : le but est de connecter deux microcontrôleurs Arduino ensemble pour qu'ils puissent s'échanger des données.

La tension des microcontrôleurs :

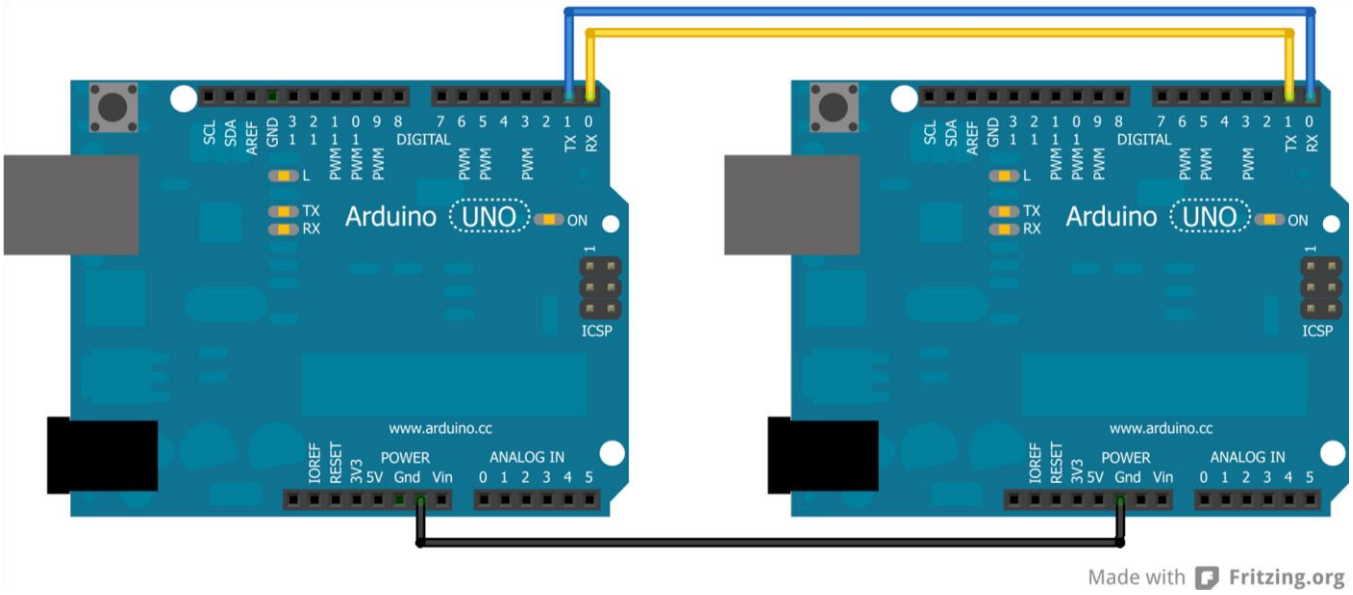
	Tension
Niveau Logique 0	0 V
Niveau Logique 1	+5 V

Contrairement à ce qu'impose la norme RS-232, les microcontrôleur ne peuvent pas utiliser des tensions négatives. Du coup, ils utilisent les seuls et uniques tensions qu'ils peuvent utiliser, à savoir le 0V et le +5 V. Il y a donc quelques petits changement au niveau de la transmission série. Un niveau logique 0 correspond à une tension de 0V et un niveau logique 1 correspond à une tension de +5V. Fort heureusement, comme les microcontrôleurs utilisent quasiment tous cette norme, il n'y a aucun problème à connecter deux microcontrôleurs entre-eux même s'ils ne sont pas de même marque. Cette norme s'appelle alors UART pour Universal Asynchronous Receiver Transmitter plutôt que RS232. Hormis les tensions électriques et le connecteur, c'est la même chose !

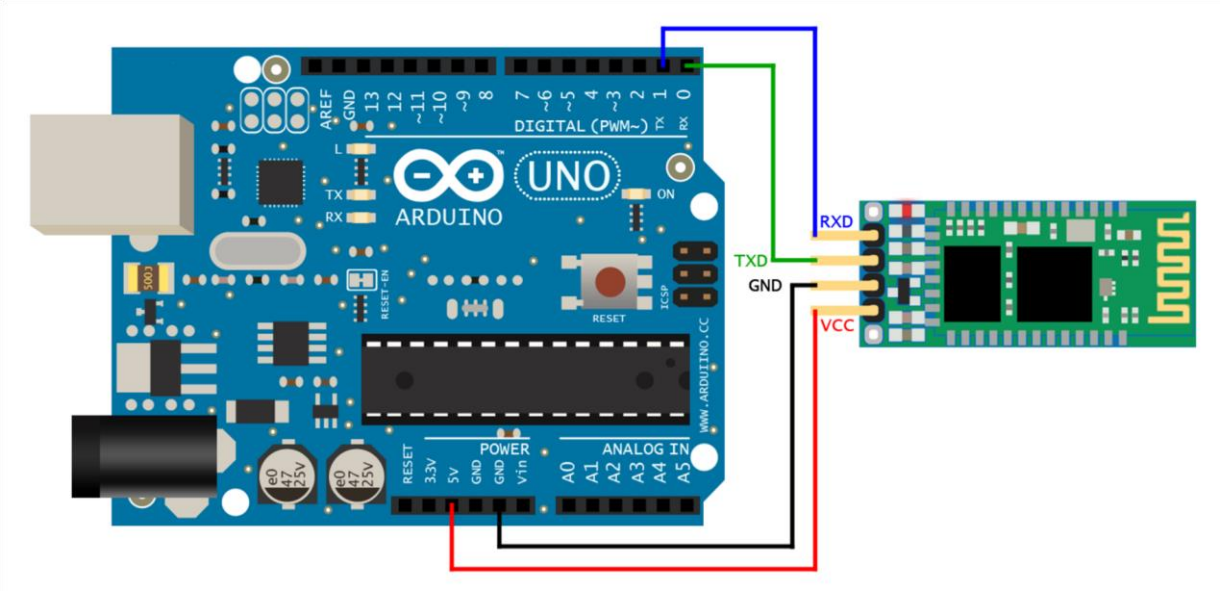
Croisement de données

Il va simplement falloir faire attention à bien croiser les fils. On connecte le Tx (broche de transmission) d'un microcontrôleur au Rx (broche de réception) de l'autre microcontrôleur. Et inversement, le Tx de l'autre au Rx du premier. Et bien sûr, la masse à la masse pour faire une référence commune.

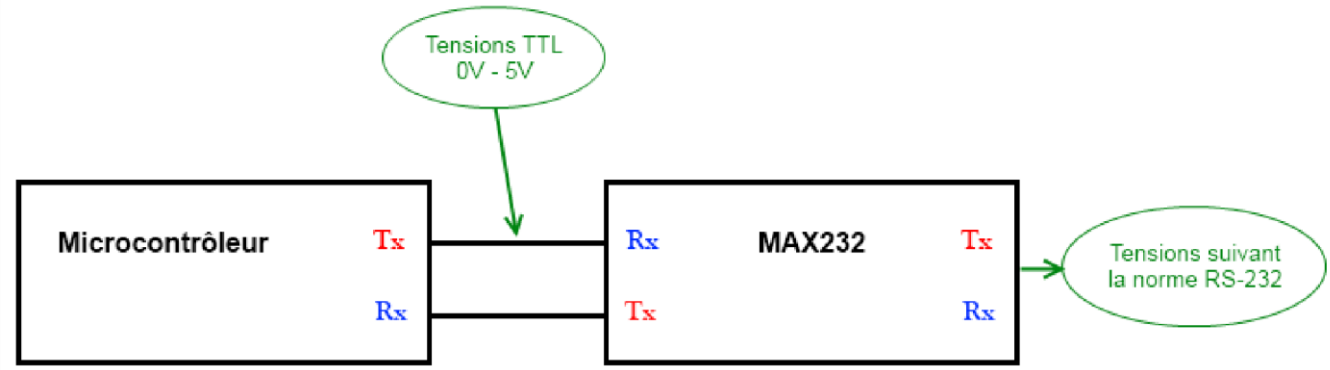
Exemple 1 : entre 2 cartes arduino



Exemple 2 : entre une carte Arduino et un capteur équipé d'une liaison série



Exemple 3 : entre une carte arduino et un ordinateur



Le circuit électronique MAX232 va adapter les tensions de la liaison série de l'arduino à la liaison série (RS232) de l'ordinateur.
Remarque : lorsque l'on utilise le moniteur série du logiciel Arduino, la carte et l'ordinateur dialoguent à l'aide de la liaison série. Ils utilisent alors le port USB.

Remarque N°2 : il existe différentes librairies Arduino permettant de gérer les liaisons série (celle qui est standard s'appelle « serial »).

Remarque N°3 : sur la carte Arduino Uno précédente, on a utilisé les broches 0 et 1 qui sont les broches standard de la liaison série. Si on a besoin de plusieurs liaisons série, certaines autres broches peuvent devenir des broches « série » (Tx et Rx). Il faut consulter la documentation pour vérifier lesquelles sont compatible. Attention, tout est différent avec la carte Arduino Mega.

3. Exemple N°2 : le bus I²C

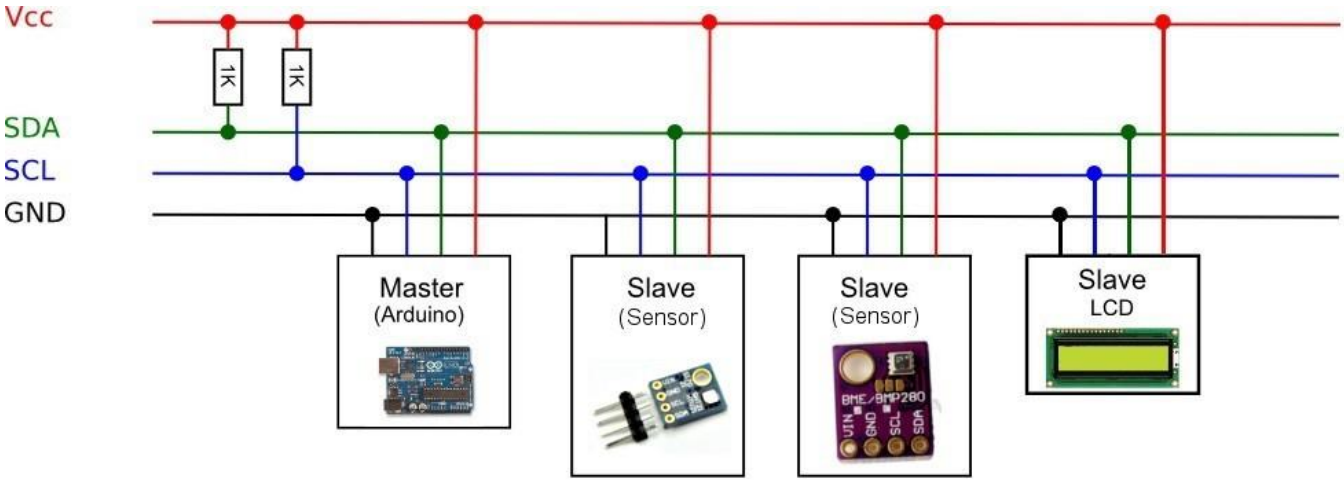
Le bus I²C (I²C signifie : Inter-Integrated Circuit) a été créé au début des années 80 par RTC Philips afin d'apporter une solution simple et peu coûteuse à la communication entre les circuits intégrés numériques à l'intérieur des appareils grand public (téléviseurs, magnétoscopes, jouets, ...). Le principal avantage du bus I²C est de limiter le nombre de liaisons entre circuits intégrés.

Le bus I²C est un bus de type série synchrone ne nécessitant que deux signaux.

- SDA (Serial Data Line), le signal de données bidirectionnelle.
- SCL (Serial Clock Line), le signal d'horloge bidirectionnel.

Ce bus permet la communication entre un circuit maître et un circuit esclave. Le montage peut comporter plusieurs maîtres et plusieurs esclaves. Le maître est le circuit qui émet le signal d'horloge de synchronisation, un seul maître peut envoyer ce signal. Les données peuvent circuler dans les deux sens sur le fil des données, de sorte que chaque circuit, qu'il soit maître ou esclave peut servir d'émetteur ou de récepteur (de données).

Les différents circuits sont placés en parallèle sur les lignes SDA et SCL comme sur le schéma suivant :



Remarques :

- Les 2 lignes SDA et SCL sont tirées au niveau de tension du Vcc (niveau haut) à travers des résistances de pull-up (ici 1KΩ).
- Cartes Arduino : I²C est disponible sur une carte Arduino Uno sur la broche analogique 5 pour SCL qui fournit un signal d'horloge, et la broche analogique 4 pour SDA, qui s'occupe du transfert des données (sur la Mega, il faut utiliser la broche 20 pour SDA et la broche 21 pour SCL). La bibliothèque utilisée est WIRE.
- Raspberry Pi : pour type B, il faut utiliser les broches GPIO2 et GPIO3 pour SDA et SCL repérées sur le « Pi Cobbler ».
- En général il n'y a qu'un seul « maître » mais il est toutefois possible d'en avoir plusieurs.

Nombre d'éléments connectables :

Le nombre maximal d'équipements est limité par le nombre d'adresses disponibles, 7 bits pour l'adresse et un bit pour définir si on écrit ou on lit, soit 128 périphériques, mais il dépend également de la caractéristique physique (capacité) du bus. Il faut savoir que des adresses sont réservées par les fabricants ce qui limite grandement le nombre d'équipements.

Protocole :

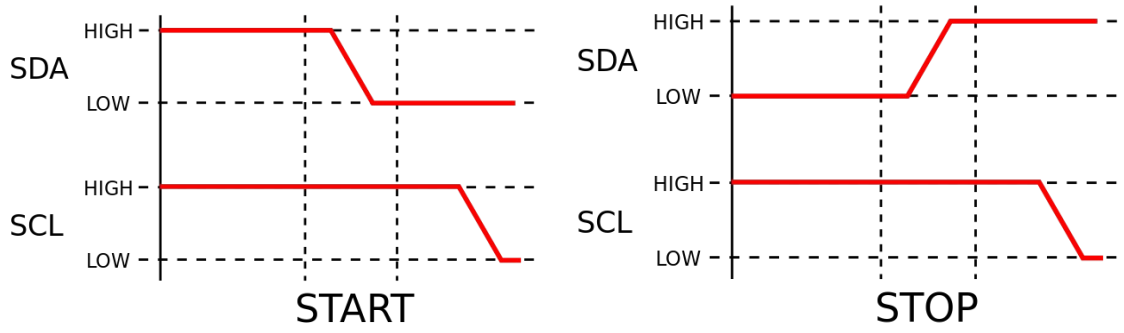
Au repos, c'est à dire lorsque aucun circuit n'émet, les signaux SDA et SCL sont au niveau logique haut. Pour éviter les conflits, un maître qui veut émettre doit attendre que le bus soit au repos.

Principe :

- Quand une ligne (SDA ou SCL) est au repos (niveau 1), on peut la forcer à 0.
- Quand une ligne (SDA ou SCL) est au niveau 0, on ne peut pas la forcer à 1.

Comme la transmission s'effectue sous forme série, une information de début et de fin doit être prévue. L'information de début se nomme START et l'information de fin STOP.

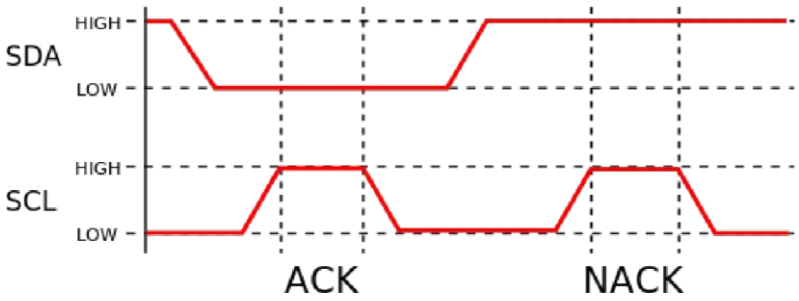
Un maître prend le contrôle du bus en effectuant un START : il met SDA à 0, SCL restant à 1. Au cours de la communication, l'horloge SCL est envoyée par le maître et SDA ne peut changer d'état que lorsque SCL est à 0 :



Les données sont envoyées par paquets de huit bits (ou octets). Le bit de poids fort est envoyé le premier, chaque octet est suivi par un bit d'acquittement (ACK) de la part du destinataire.

Le message peut être décomposé en deux parties :

1. Le maître est l'émetteur, l'esclave est le récepteur :
   - émission d'une condition de START par le maître (« S »),
   - émission de l'octet ou des octets d'adresse par le maître pour désigner un esclave, avec le bit $R/\overline{W}$ à 0
   - réponse de l'esclave par un bit d'acquittement ACK (ou de non-acquittement NACK),
   - après chaque acquittement, l'esclave peut demander une pause (« PA »).
   - émission d'un octet de commande par le maître pour l'esclave,
   - réponse de l'esclave par un bit d'acquittement ACK (ou de non-acquittement NACK),
   - émission d'une condition de RESTART par le maître (« RS »),
   - émission de l'octet ou des octets d'adresse par le maître pour désigner le même esclave, avec le bit R/W à 1.

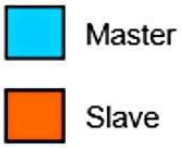


2. Le maître devient récepteur, l'esclave devient émetteur :
   - émission d'un octet de données par l'esclave pour le maître,
   - réponse du maître par un bit d'acquittement ACK (ou de non-acquittement NACK),
   - (émission d'autres octets de données par l'esclave avec acquittement du maître),
   - pour le dernier octet de données attendu par le maître, il répond par un NACK pour mettre fin au dialogue,
   - émission d'une condition de STOP par le maître (« P »).

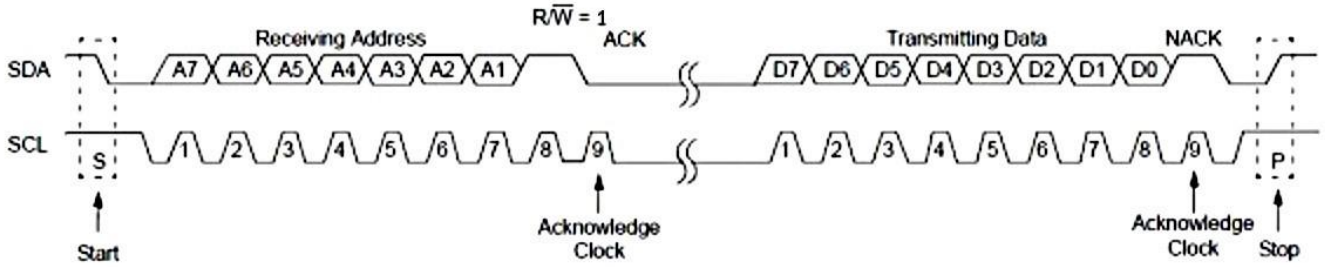
Des exemples de trame I^2C :

Cela donne dans le cas où le maître ne fait que lire ce que l'esclave envoi:

avec :

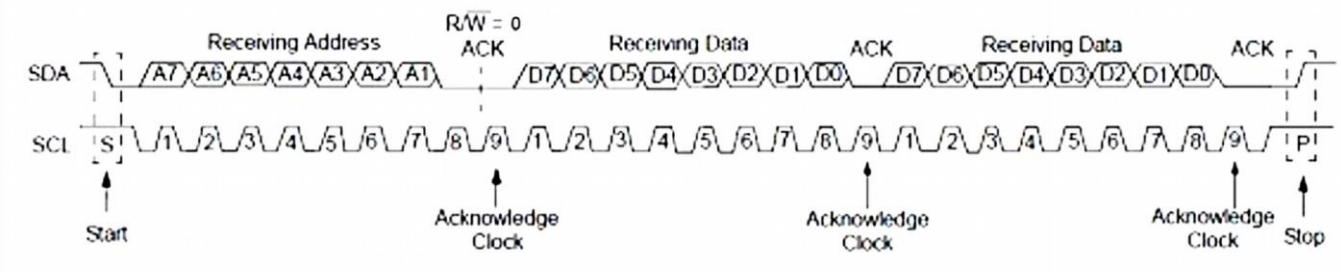


et en signal électrique :

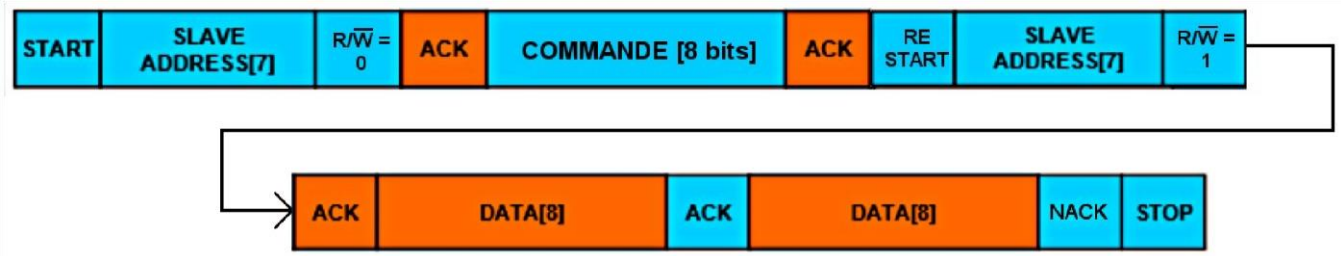


Cela donne dans le cas où le maître écrit à l'esclave envoi:

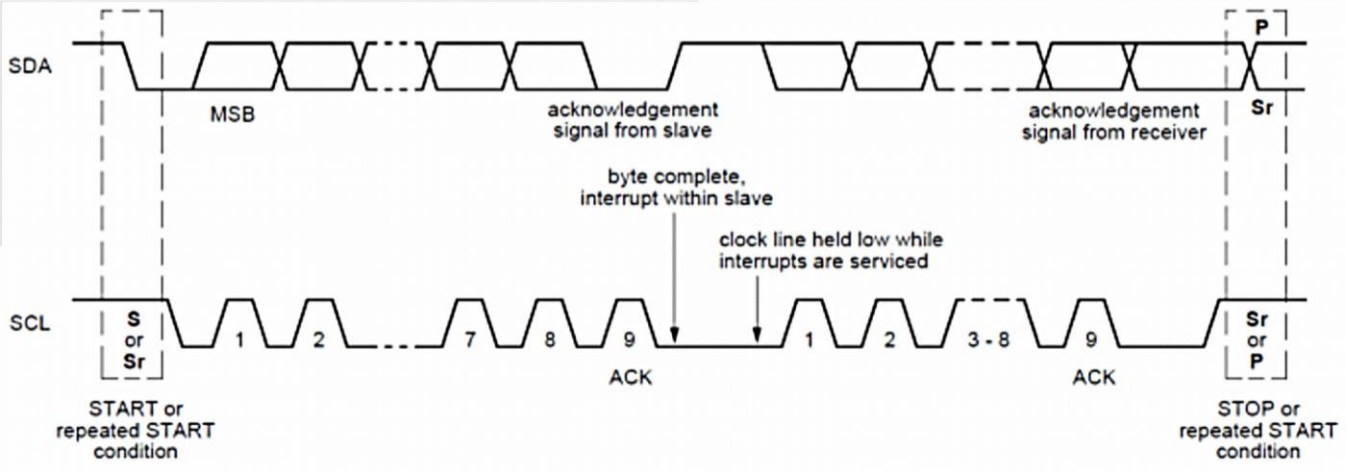
et en signal électrique :



Cela donne dans où le maître écrit (envoie une commande) puis lit ce que l'esclave envoi:

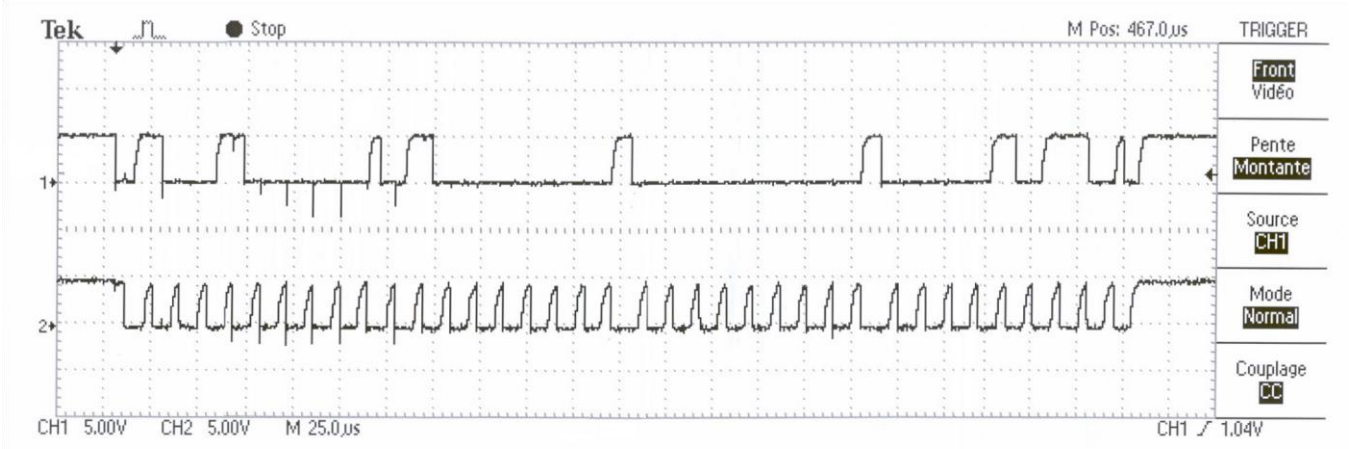


On remarque que pour que le maître envoie une commande il faut mettre le bit R/W à 0 et pour que le maître lise les données envoyées par un esclave il faut mettre le bit R/W à 1 et en signal électrique :



On remarque que SDA est "préparé" avant que SCL soit à l'état haut. Ainsi s'explique le décalage entre le changement d'état de SCL et celle de SDA pendant la transmission.

Exemple d'un relevé réel (oscilloscope) :



Calcul des résistances de Pull-up : R_P

Les temps et les niveaux de tension dépendent de la capacité du bus (CB) et de la valeur des résistances de pull-up (RP). Il est difficile de modifier la valeur de la capacité du bus, mais on peut choisir la valeur des résistances pull-up.

La valeur minimale des résistances de pull-up est limitée par le courant des sorties SDA et SCL (I_{OL}) lorsqu'elles sont à l'état LOW (V_{OL}) :

$$R_{Pmin} = \frac{V_{DD} - V_{OLmax}}{I_{OL}}$$

Mode	**V_{OLmax}**	**I_{OL}**	**R_{Pmin} pour V_{DD}=5 V**
Standard	0,4V	3mA	1534Ω
Fast	0,6V	6mA	733Ω

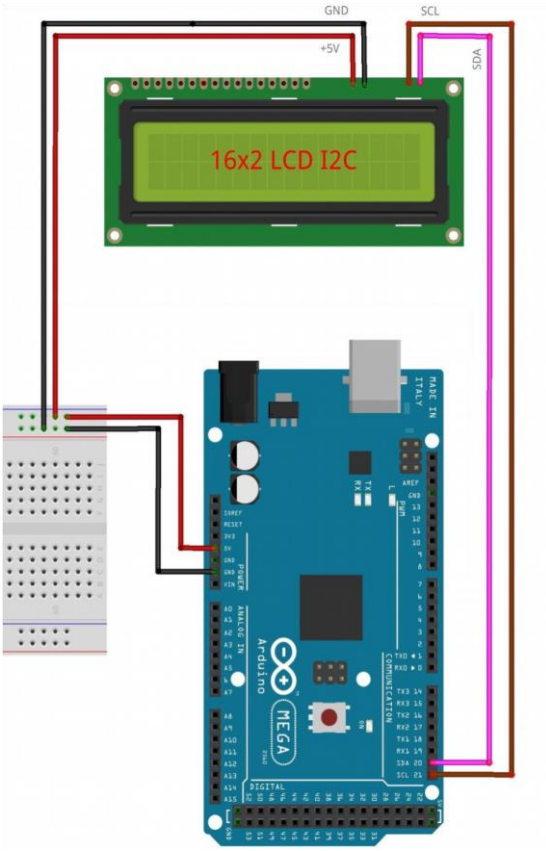
Fast plus 0,4V 20mA 230Ω

Les valeurs max (avec t_r, le temps de montée des signaux SDA et SCL):

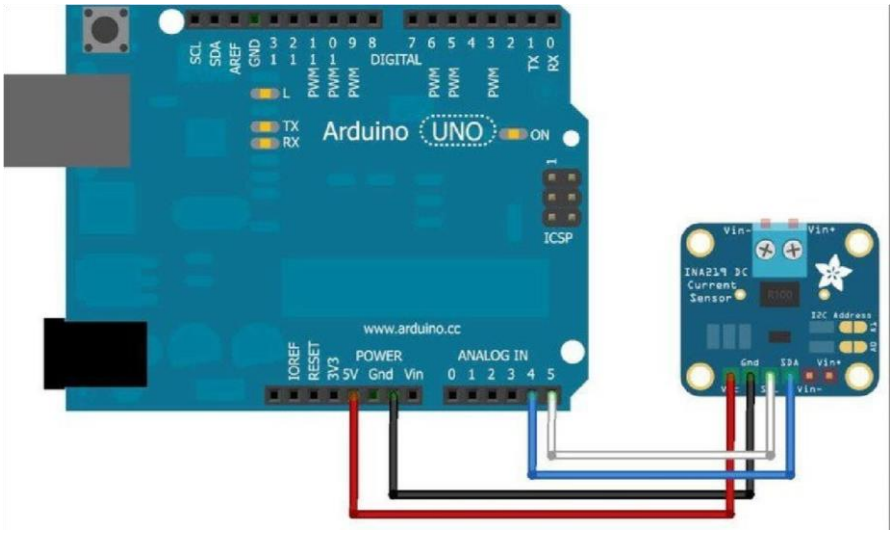
Mode	tr	CB	RPmax
Standard	1µeVs	400pF	2950Ω
Fast	300ns	400pF	885Ω
Fast plus	120ns	550pF	257Ω

Des exemples avec Arduino :

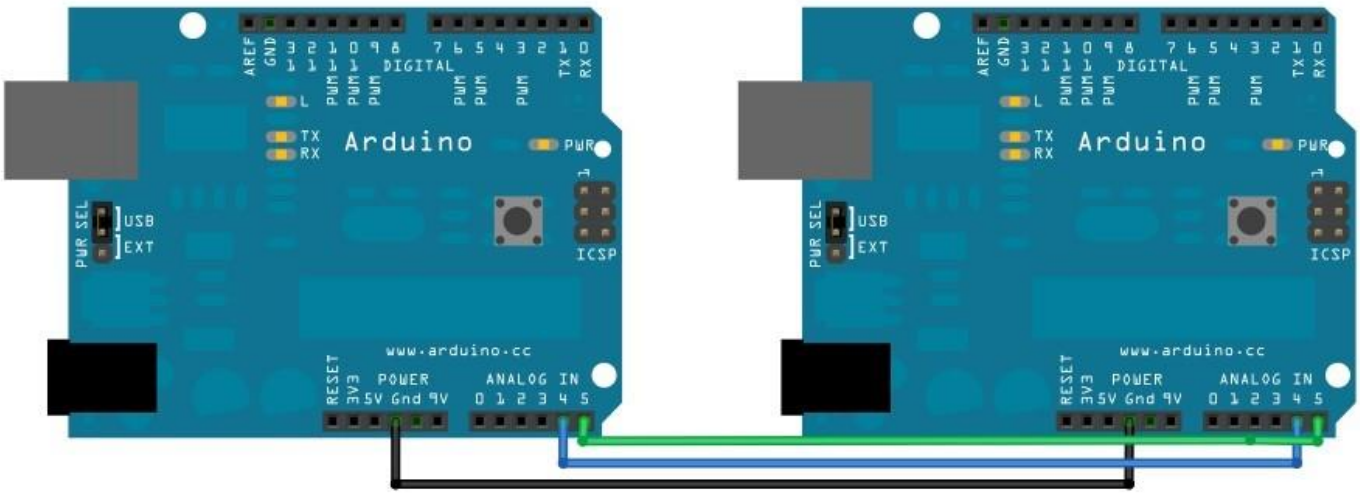
Arduino et un afficheur LCD I²C:



Arduino et un capteur de courant I²C:



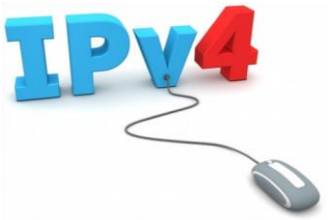
Deux Arduino (un maître, un esclave) :



IV. Exercices

Exercice 1 : adresses IPv 4

IPv4 (Internet Protocol version 4) est la première version d'Internet Protocol (IP) à avoir été largement utilisée aussi bien pour internet que pour les réseaux informatiques en général. Elle permet une définition commune (mondialement) de la manière d'écrire les adresses des machines (ordinateur, serveur, …) reliées à un réseau informatique.



Exemple 1 : le réseau d'un particulier

Le réseau des particuliers est en général le suivant :
192.168.1 .x où x est l'adresse des éléments connectés au réseau

1. ***'x' pouvant prendre comme valeur 0 à 255 (en décimal), sur combien de bits est-il codé en binaire ?***
2. ***L'adresse de mon ordinateur étant 192.168.1.2, écrivez cette adresse en binaire.***
3. ***Combien de matériels différents puis-je relier sur ce réseau ?***

Exemple 2 : le réseau d'une petite entreprise

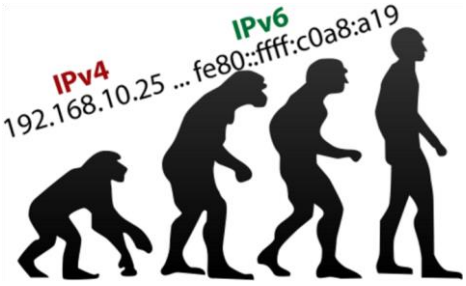
Le réseau de l'entreprise est : 192.168.x.y où x et y sont les octets codant l'adresse des éléments connectés au réseau

4. ***'x' et 'y' pouvant <u>chacun</u> aller de 0 à 255 (en décimal), sur combien de bits au total l'adresse des éléments est-elle codée ?***
5. ***Combien de matériels différents puis-je relier sur ce réseau ?***

Généralisation

6. ***Si tous les élément de l'adresse peuvent être choisi (w.x.y.z), chacun pouvant aller de 0 à 255 (en décimal), sur combien de bits au total l'adresse est-elle codée ?***
7. ***Combien de matériels différents puis-je relier sur le réseau internet avec cette norme IPv4?***

Exercice 2 : adresses IPv 6



IPv6 (Internet Protocol version 6) est le protocole réseau qui a été conçu pour succéder à l'IPv4.

La plage des adresses va de 0:0:0:0:0:0:0:0 à FFFF:FFFF:FFFF : …….. :FFFF (l'adresse est en 8 parties séparées par des « deux points », chaque nombre est donné en hexadécimal)

Exemple d'une adresse IPv6 :
2001:0db8:0000:85a3:0010:0a0b:8001:ec1 f

Préliminaires :

1. ***Convertissez le chiffre hexadécimal 'E' en décimal puis en binaire***
2. ***Combien faut-il de bits pour coder un 'chiffre' hexadécimal ?***

Étude d'un des 8 éléments composant une adresse IPv6 :
Cet élément peut avoir comme valeur 0000 à ffff. Prenons l'élément 'ec1f'

3. ***Convertissez ce nombre hexadécimal en décimal***
4. ***Convertissez ce nombre hexadécimal en binaire***
5. ***Sur combien de bits est-il codé ?***

Généralisation :

6. ***Sur combien de bits une adresse IPv6 complète est-elle codée ?***
7. ***Combien de matériels différents puis-je relier sur le réseau internet avec IPv6?***

Exercice 3 : généralités

Un téléphone portable possède-t-il une adresse MAC ?

Combien d'adresses MAC possède un routeur ?

Combien d'adresses IP possède un routeur ?

Un réseau a comme masque 255.255.255.224. Combien de machines peut- il y avoir sur un tel réseau ?

En utilisant l'adressage par classe, l'adresse 190.24.12.8/16 fait partie de quel réseau ?
1 : 190.0.0.0 2:190.255.255.255 3 : 190.24.0.0 4 : 190.24.12.0

On trouve comme adresse réseau : 74.125.100.80/8. Quel est le masque réseau ?

Combien peut-on mettre de machines sur un réseau du type 78.0.0.0/16 ?

Soit l'adresse suivante 77.45.234.56/17. Donnez le masque se sous réseau.

Quelle adresse réseau (NetID) possède la machine 192.168.5.17/24 (aidez vous de masque de sous réseau)?

Quels adresses réseau (NetID) et équipement (HostID) possède la machine 194.45.67.98/26 (aidez vous de masque de sous réseau)?

Notre réseau a comme adresse 172.16.0.0/12 ***1.***
Donnez son masque de sous réseau :

2 . Donnez son adresse de diffusion (broadcast) en vous aidant du masque de sous réseau.

Exercice 4 : IPV4 classe A et B

voici le résumé pour la classe C :

Bits de départ	Masque de sous réseau par défaut	Nombre de bits de NetID	Nombre de bits de HostID	Nombres d'adresses possibles sur le sous réseau	Nombre d'adresses de réseaux possibles	Plage d'adresses disponibles
110	255.255.255.0	21	8	254 (2^8-2)	2097152 (2^{21})	192.0.0.1 à 223.255.255.254

Complétez le résumé pour la classe A :

Bits de départ	Masque de sous réseau par défaut	Nombre de bits de NetID	Nombre de bits de HostID	Nombres d'adresses possibles sur le sous réseau	Nombre d'adresses de réseaux possibles	Plage d'adresses disponibles
					126 (2^7-2)	

Complétez le résumé pour la classe B :

Bits de départ	Masque de sous réseau par défaut	Nombre de bits de NetID	Nombre de bits de HostID	Nombres d'adresses possibles sur le sous réseau	Nombre d'adresses de réseaux possibles	Plage d'adresses disponibles
					16384 (2^{14}2)	

Exercice N°5 Topologie des réseaux

soit le réseau d'une petite entreprise:

Entourez, en les nommant, les 3 types de topologie de réseau présent sur le réseau.

Exercice N°6 Des question de bits, de débits, ….

Remarque : dans les questions suivantes on partira du principe qu'un Kb = 1000bits, qu'un Mbits=1000000, ….

Sur une liaison hertzienne urbaine à 1200 bits/s (débit max) on envoie des messages de 8 octets. La fréquence d'émission est de 12 messages par seconde.

1. ***Calculez le débit réel (en bits/s) de la ligne avec l'utilisation précédente.***
2. ***En déduire le taux d'utilisation de la ligne (en%)***

Différents réseaux Ethernet

3. ***Quel est le temps de transmission de 1Kb sur un réseau dont le débit est 10 Mb/s***
4. ***Quel est le temps de transmission de 1Kb sur un réseau dont le débit est 100 Mb/s***

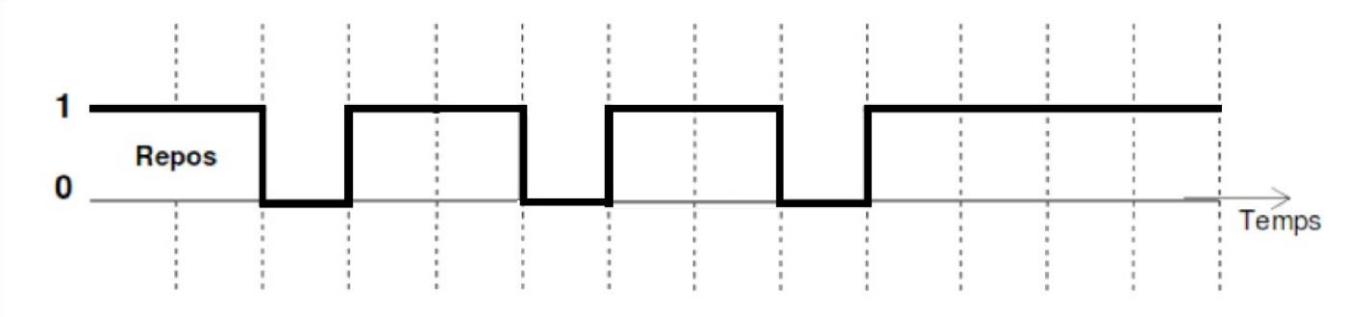
On considère maintenant un réseau dont le débit est de 10 Mbits/s. Les messages envoyés sur ce réseau ont une taille maximale de 1000 bits dont un champ de contrôle de 16 bits.

5. ***Quel est le nombre de messages nécessaires pour envoyer un fichier de 4 Mbits d'un ordinateur à l'autre?***

Exercice N°7 Analyse d'une trame RS232

La liaison série est paramétrée de la manière suivante :
- Donnée sur 7 bits
- Parité paire
- 2 bits de stop

On relève la trame suivante :

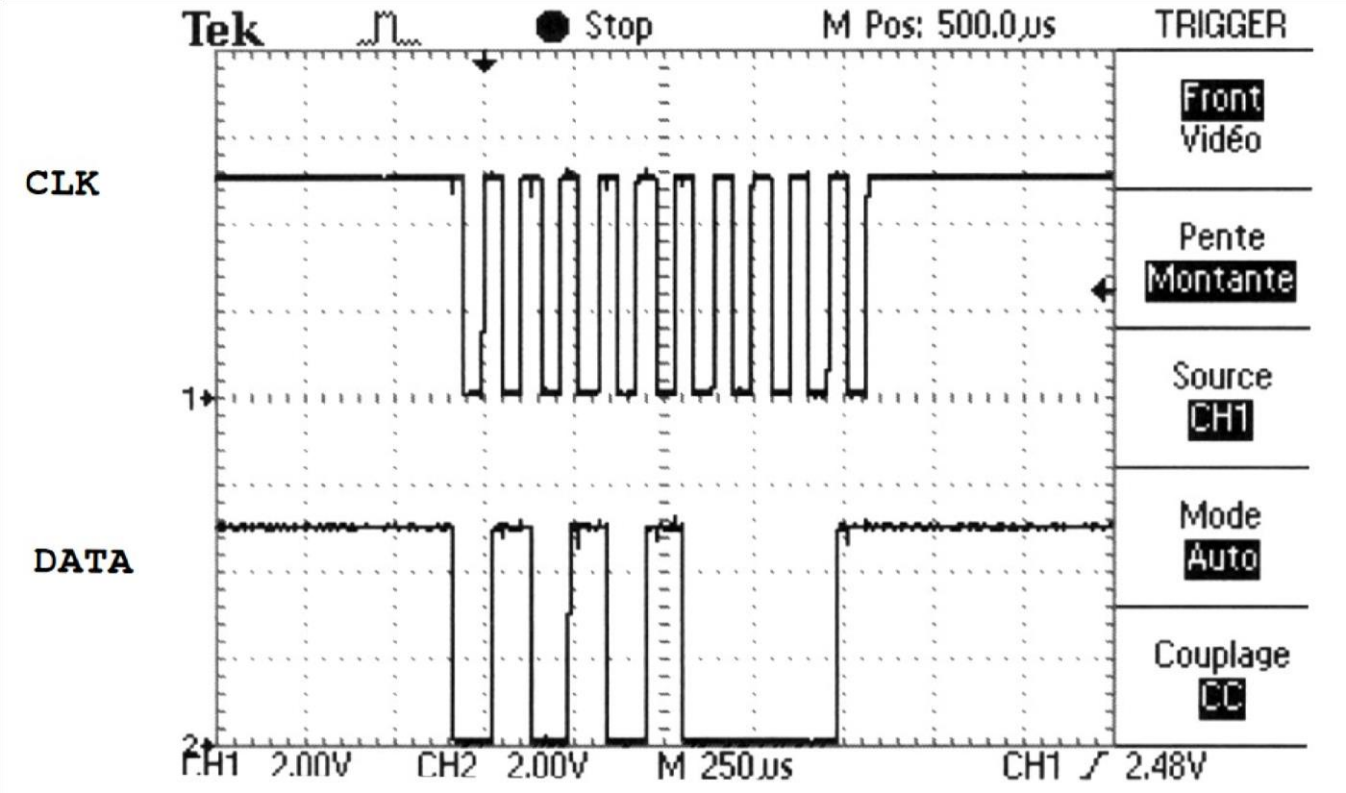


1. ***Repérez sur la trame précédente :***
   - ***le bit de start***
   - ***les bits de donnée***
   - ***le bit de poids faible (LSB)***
   - ***le bit de poids fort (MSB)***
   - ***les bits de stop***
   - ***le bit de parité***
2. ***La donnée transporté est un caractère. Quel est-il ?***
3. ***La parité est-elle bonne ? Justifiez votre réponse.***

Exercice N° 8 Analyse d'une trame RS232

Une liaison série entre un capteur de température et une carte Arduino est paramétrée de la manière suivante :
- Donnée sur 8 bits
- 1 bit de stop

On relève, à l'oscilloscope, la trame suivante (l'horloge semble être active sur le front descendant du signal CLK):



1. ***Repérez sur la trame précédente (entourer sur l'oscillogramme précédent) :***
   - ***le bit de start***
   - ***les bits de donnée***
   - ***le bit de poids faible (LSB)***
   - ***le bit de poids fort (MSB)***
   - ***le bits de stop***
   - ***le bit de parité***
2. ***Quelle est le type de parité utilisée? Justifiez votre réponse.***
3. ***La donnée transportée représente une température (nombre entier). Le bit de poids fort représente le signe de cette température. Quelle est la température mesurée?***

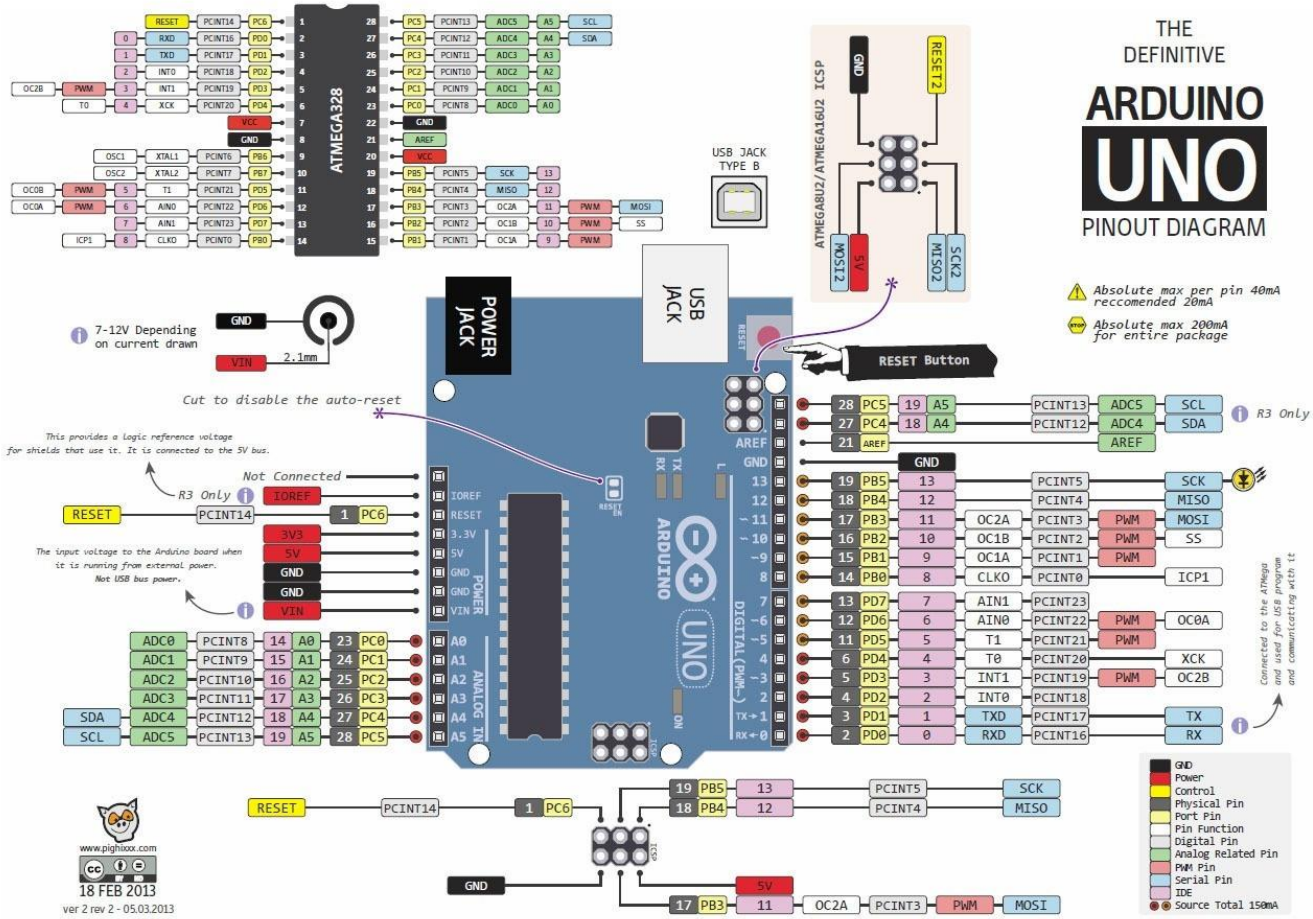
Exercice N°9 Écriture d'une trame RS232

La liaison série est paramétrée de la manière suivante :
- Donnée sur 7 bits
- Parité impaire
- 1 bits de stop

Dessinez la trame si la donnée transportée est le caractère "R"

Exercice N°10 Câblage sur carte Arduino UNO

Description des affectations possibles des broches (pin) d'une carte Arduino uno :



Description des capteurs du système :

TSL2561 Digital Luminosity/Lux/Light Sensor :

Specification :

- Approximates Human eye Response
- Precisely Measures Illuminance in Diverse Lighting Conditions
- Temperature range: -30 to 80 *C
- Dynamic range (Lux): 0.1 to 40,000 Lux
- Voltage range: 2.7-3.6V
- Interface: I2C
- This board/chip uses I2C 7-bit addresses 0x39, 0x29, 0x49, selectable with jumpers

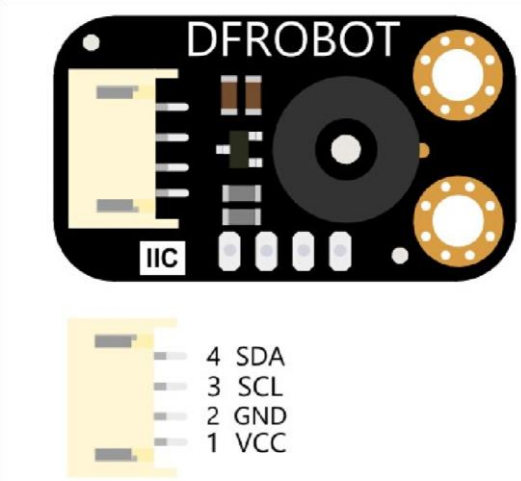
Connect the VCC pin to a 3.3V or 5v power source Connect
GND to the ground pin.
Connect the i2c SCL clock pin to your i2c clock pin.
Connect the i2c SDA data pin to your i2c data pin.
Don’t connect the INT pin

Accéléromètre 3 axes BMA220 SEN0168

This Triple Axis Accelerometer with Bosch BMA220 is an ultra small triaxial, low-g acceleration sensor breakboard with I2C interface, aiming for lowpower consumer market applications. It allows measurement of accelerations in 3 perpendicular axes and thus senses tilt, motion, shock and vibration in cell phones, handhelds, computer peripherals, man-machine interfaces, virtual reality features and game controllers. Specification :

- Power supply: 2.0-3.6V
- Interface: I2C
- Acceleration range:±2g/±4g/±8g/±16g
- LED power indication

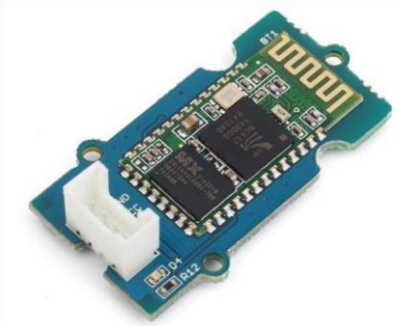
Capteur de température IR SEN0206



Specification

- Operating Voltage: 3.3V - 5V
- Operating Current: 1.2mA
- Temperature: -70.01℃ to +382.19℃, (0.01 ℃ to +382.19℃ to +382.19℃, (0.01 ℃, (0.01 ℃ to +382.19℃, (0.01 ℃ resolution)
- Interface Type: I2C
- Interface Line Sequence: VCC, GND, SCL, SDA

Module Bluetooth Grove 113020008



Grove - Serial Bluetooth is an easy to use module compatible with the existing Grove Base Shield, and designed for transparent wireless serial connection setup. The serial port Bluetooth module is fully qualified Bluetooth V2.0+EDR(Enhanced Data Rate) 2Mbps Modulation with complete 2.4GHz radio transceiver and baseband.

Specifications

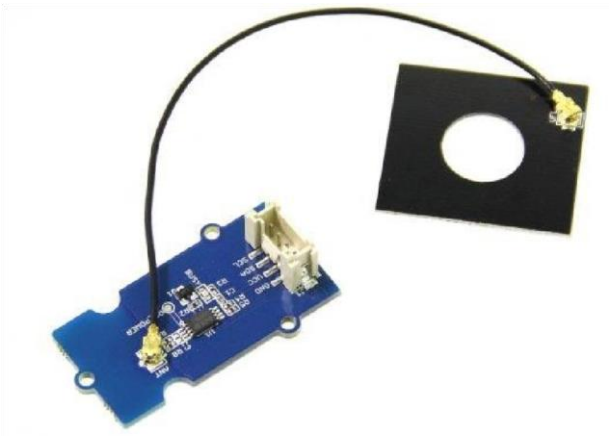
- Operating Voltage: 5.0VDC
- Data Rate: 2Mbps
- Fully Qualified Bluetooth V2.0+EDR 3Mbps Modulation
- Selectable baud rate
- Communication : serial port

Module NFC Tag 101020070

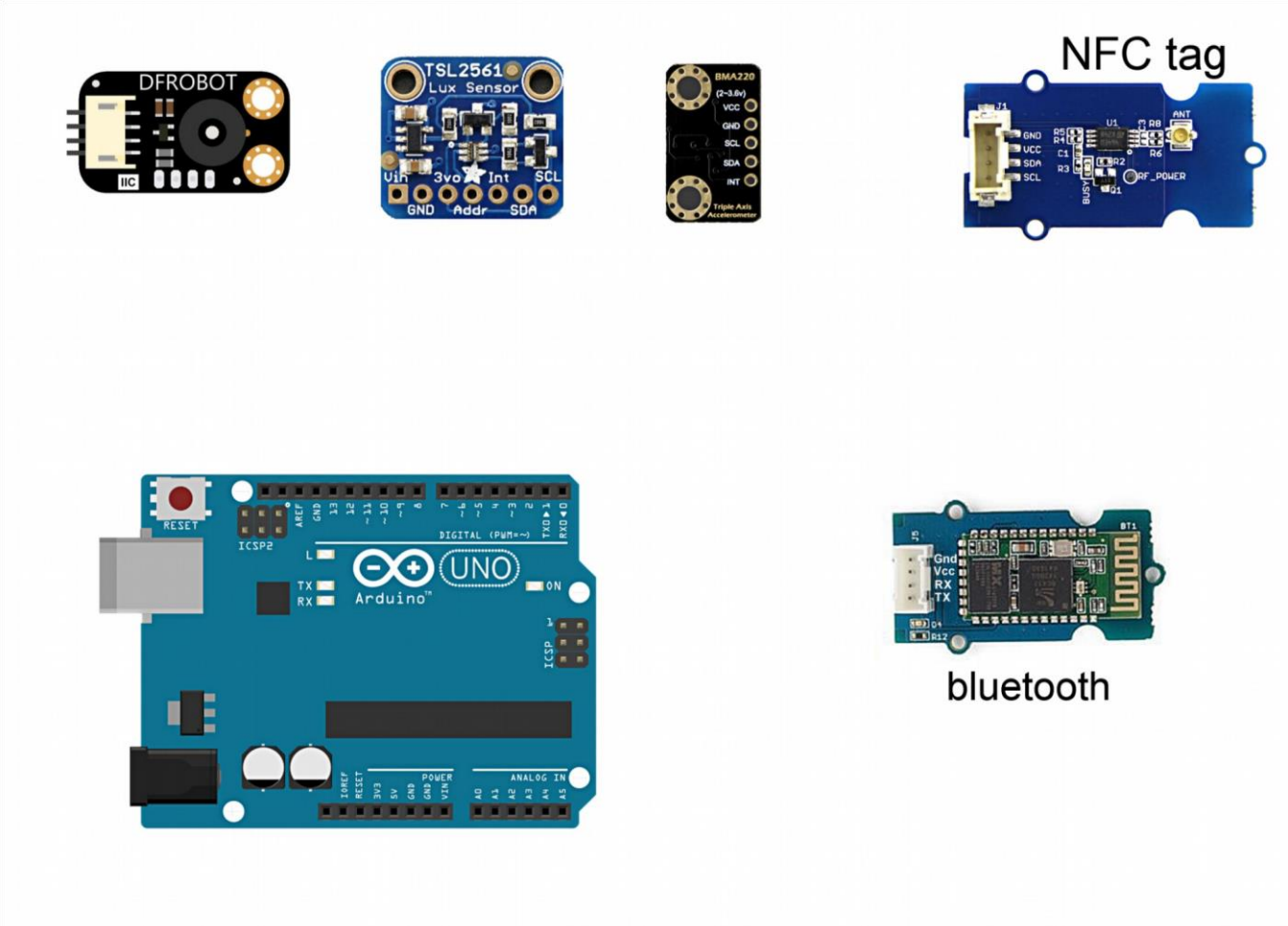
Grove - NFC Tag is a highly integrated Near Field Communication Tag module,this module is I2C interface,which base on M24LR64E-R,M24LR64E-R have a 64-bit unique identifier and 64 -Kbit EEPROM.Grove - NFC Tag attach an independent PCB antenna which can easily stretch out of any enclosure you use, leaving more room for you to design the exterior of your project.

Specifications

- Working Voltage:5V or 3,3V
- Effective range<2cm
- Serve for contactless communication at 13.56 MHz
- 64- bit unique identifier (UID)
- Read Block & Write (32-bit blocks)
- Grove I2C Interface



Faites le câblage des capteurs sur la carte Arduino (signaux et alimentations):



Exercice N°11 Trame bus I²C

Nous allons brancher sur une carte Arduino un capteur de température infrarouge avec communication par bus I²C
Caractéristiques du capteur:

- Le capteur fonctionne sur 12 bits
- plage de mesure : -40°C à 85°C
- la mesure est linéaire
- le capteur envoi d'abord les bits de poids faible (B7 à B0) puis ceux de poids plus forts (B11 à B8)

La liaison I²C est classique donc les adresses sont sur 7 bits On

relève la trame I2C suivante :

1. ***Décodage de la trame :***
   - ***Entourez sur la trame le bit de START***
   - ***Relevez l'adresse du capteur. La mettre en hexadécimal***
   - ***Entourez sur la trame le bit de R/W***
   - ***Quel est son état logique et que cela signifie-t-il ?***

- ***Entourez sur la trame les bits d'acquittement (ACK)***
- ***Entourez sur la trame les bits de données transmis par le capteur***
- ***Entourez sur la trame le bits de non-acquittement (NACK)***
- ***Entourez sur la trame le bit de STOP***

2. ***Analyse des données :***
   - ***Calculez la résolution du capteur***
   - ***Donnez la valeur des 12 bits de mesure que le capteur a envoyé (lus sur la trame)***
   - ***En déduire la température mesurée par le capteur***