

# Télécommunications et Réseaux

## Chapitre 3 : accès réseau

Cours de M. Petein Thomas

Email : thomas.petein@heh.be

## Accès réseau

### Introduction

Au niveau du modèle OSI, chaque couche fonctionne avec les couches supérieures et inférieures afin de transmettre des données.

Cependant, deux couches sont étroitement liées ce qui fait que dans le modèle TCP/IP, elle n'en forme plus qu'une.

Il s'agit de la couche liaison de données et de la couche physique qui forment ensemble la couche accès réseau !

Ce chapitre décrit d'abord les fonctions générales de la couche physique et les normes et protocoles qui gèrent la transmission de données sur le support local.

Il présente également les fonctions de la couche liaison de données et des protocoles qui lui sont associés.



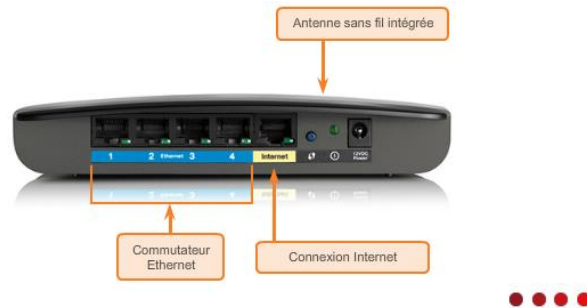
## Accès réseau

### Protocoles de la couche physique

Que vous vous connectiez à une imprimante locale chez vous ou à un site Web dans un autre pays, avant que toute communication réseau puisse se produire, vous devez vous connecter physiquement à votre réseau local.

Par connexion physique j'entend une connexion filaire par câble ou une connexion sans fil utilisant les ondes radio.

Le type de connexion physique utilisé dépend entièrement de la configuration du réseau.



## Accès réseau

### Comment se connecter au réseau ?

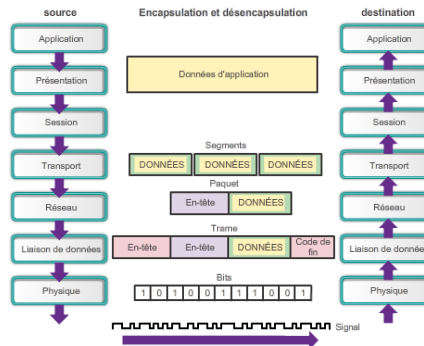
Les cartes réseau (NIC en anglais) connectent un périphérique au réseau. Les cartes réseau Ethernet sont utilisées dans les connexions filaires, tandis que les cartes réseau WLAN (réseau local sans fil) sont utilisées dans les connexions sans fil.

Bien entendu, pour pouvoir se connecter au réseau, un périphérique utilisateur doit comporter l'un de ces deux types de carte réseau (certains périphériques possèdent également les deux).

Le choix du type de connexions influencera certains paramètres comme les performances mais nous en discuterons plus tard.

## Accès réseau

Au niveau du cheminement subi par les données, du nœud source au nœud de destination, je rappelle qu'il se passe comme ceci :



## Accès réseau

Il existe trois formes élémentaires de support réseau sous lesquelles les données sont représentées :

- Câble de cuivre
- Fibre optique
- Sans fil

Quant à la représentation des bits (c'est-à-dire le type de signal véhiculé), cela dépend du type de support réseau qui est utilisé.

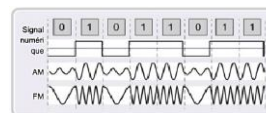
Pour un support à câble de cuivre, les signaux sont des variations d'impulsions électriques.



Pour la fibre optique, les signaux sont des variations lumineuses.



Pour les supports sans fil, les signaux sont des variations de transmissions radio.



### Principes fondamentaux de la couche physique

Les normes de la couche physique couvrent 3 parties :

#### 1. Les composants physiques

Il s'agit des périphériques électroniques, des supports et des connecteurs qui transportent et transmettent les signaux pour représenter les bits.

Les composants matériels, tel que les cartes réseau, les interfaces, les connecteurs, les matériaux et les types de câble, sont tous répertoriés dans les normes associées à la couche physique.

#### 2. Le codage

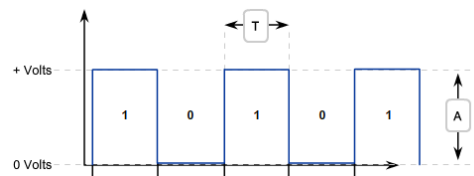
Le codage de données est une méthode permettant de convertir un flux de bits de données en code prédéfini.

Les codes sont des groupements de bits utilisés pour fournir un modèle prévisible pouvant être reconnu à la fois par l'expéditeur et le récepteur.

L'utilisation de modèles prévisibles aide à distinguer les bits de données des bits de contrôle et à offrir une meilleure détection des erreurs de support.

### Codage NRZ

Le codage NRZ (pour « Non Return to Zero ») est une méthode de signalisation simple dans laquelle le flux de bits est transmis en tant que série de valeurs de tension.



**T** = durée du bit  
**A** = Amplitude (hauteur des impulsions)

Une valeur de tension faible représente un 0 logique et une valeur de tension élevée un 1 logique. La plage de tensions dépend de la norme de couche physique utilisée.

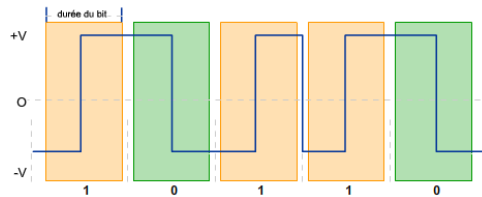
Cette méthode simple de signalisation convient uniquement aux liaisons de données à bas débit.

La signalisation NRZ n'utilise pas la bande passante de manière efficace et est sensible aux interférences électromagnétiques.

### Codage Manchester

Le système de codage Manchester représente les valeurs binaires comme transitions de tension :

La transition de tension doit se produire au milieu de chaque durée de bit.



Une transition d'une tension faible à une tension élevée représente la valeur binaire 1.

Une transition d'une tension élevée à une tension faible représente la valeur binaire 0.

La transition au milieu de la durée du bit est la direction haut ou bas pour chaque unité de temps dans laquelle un bit est transmis.

Il s'agit de la méthode de signalisation employée par Ethernet 10BaseT.

Il existe des codages plus complexe, par exemple de type 4B/5B ou de type 8B/10B, mais ces méthodes sortent du cadre de ce cours.

### 3. La signalisation

La couche physique doit générer les signaux électriques, optiques ou sans fil qui représentent le 1 et le 0 sur le support.

La méthode de représentation des bits est appelée méthode de signalisation.

Les normes de couche physique doivent définir le type de signal représentant un 1 et un 0.

Il peut s'agir simplement d'un changement de niveau du signal électrique ou de l'impulsion optique, ou encore d'une méthode de signalisation plus complexe.

Au niveau de la transmission des signaux, il existe deux types de transmission différentes :

- **Asynchrone** : L'intervalle de temps entre les caractères ou les blocs de données peut être défini arbitrairement, ce qui signifie qu'il n'est pas normalisé. → les trames doivent comporter des indicateurs de début et de fin.

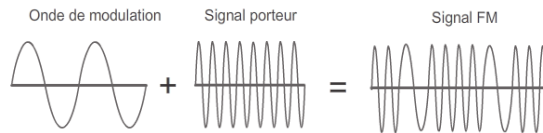
- **Synchrone** : les signaux de données sont envoyés synchronisés (c-à-d qu'ils se produisent à des intervalles réguliers appelés temps bits). Cette synchronisation se fait à l'aide d'un signal d'horloge échangé entre les deux périphériques qui doivent communiquer.

En plus de ces deux types de transmission, il existe plusieurs manières de transmettre des signaux. L'utilisation de techniques de modulation pour envoyer des données est courante.

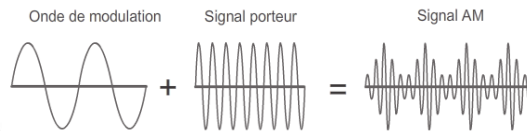
La **modulation** est le processus par lequel la caractéristique d'une onde (signal) modifie une autre onde (porteuse).

On peut donc retrouver 3 types de modulations :

• **Modulation de fréquence (FM)** : méthode de communication dans laquelle la fréquence porteuse varie selon le signal.



• **Modulation d'amplitude (AM)** : technique de transmission dans laquelle l'amplitude de la porteuse varie selon le signal.



• **Modulation par impulsions et codage (PCM)** : technique dans laquelle un signal analogique, tel que la voix est converti en un signal numérique en échantillonnant l'amplitude du signal et en exprimant les différentes amplitudes sous forme binaire. La fréquence d'échantillonnage doit être au moins deux fois supérieure à la plus haute fréquence du signal.

En résumé :

Support	Composants physiques	Technique de codage de trame	Méthode de signalisation
Câble de cuivre	<ul style="list-style-type: none"> <li>• UTP</li> <li>• Coaxial</li> <li>• Connecteurs</li> <li>• Cartes réseau (NIC)</li> <li>• Ports</li> <li>• Interfaces</li> </ul>	<ul style="list-style-type: none"> <li>• Codage Manchester</li> <li>• Techniques NRZ (non-return to zero)</li> <li>• Les codes 4B/5B sont utilisés dans le cadre d'une signalisation MLT de niveau 3 (MLT-3)</li> <li>• 8B/10B</li> <li>• PAM5</li> </ul>	<ul style="list-style-type: none"> <li>• Modifications du champ électromagnétique</li> <li>• Intensité du champ électromagnétique</li> <li>• Phase de l'onde électromagnétique</li> </ul>

Différents supports physiques prennent en charge le transfert de bits à différents débits. Ce transfert des données est généralement décrit par la bande passante.

La **bande passante** est la capacité d'un support à transporter des données.

La bande passante numérique mesure la quantité de données pouvant circuler d'un emplacement à un autre pendant une période donnée.

Elle est généralement exprimée en kilobits par seconde (kbit/s) ou en mégabits par seconde (Mbit/s).

Il faut garder à l'esprit que la bande passante pratique d'un réseau est déterminée par une combinaison de facteurs :

- les propriétés des supports physiques
- les technologies choisies pour signaler et détecter les signaux réseau

*Les propriétés du support physique, les technologies courantes et les lois de la physique jouent toutes un rôle dans la détermination de la bande passante disponible.*

Unité de bande passante	Abréviation	Équivalence
Bits par seconde	bits/s	1 bit/s = unité fondamentale de bande passante
Kilobits par seconde	Kbits/s	1 Kbits/s = 1 000 bits/s = $10^3$ bits/s
Mégabits par seconde	Mbits/s	1 Mbits/s = 1 000 000 bits/s = $10^6$ bits/s
Gigabits par seconde	Gbits/s	1 Gbits/s = 1 000 000 000 bits/s = $10^9$ bits/s
Térabits par seconde	Tbits/s	1 Tbits/s = 1 000 000 000 000 bits/s = $10^{12}$ bits/s

Les termes utilisés pour mesurer la qualité de la bande passante comprennent :

- La latence
- Le débit
- Le débit applicatif

La **latence** désigne le temps nécessaire (délais inclus) aux données pour voyager d'un point A à un point B.

Dans un inter-réseau ou un réseau à segments multiples, le débit ne peut pas être plus rapide que la liaison la plus lente du chemin menant de la source à la destination.

## Accès réseau

Le **débit** est la mesure du transfert de bits sur le support pendant une période donnée.

En raison d'un certain nombre de facteurs, le débit ne correspond généralement pas à la bande passante spécifiée dans les mises en œuvre au niveau de la couche physique.

Le débit est généralement inférieur à la bande passante et cela s'explique par trois facteurs qui ont une influence sur celui-ci :

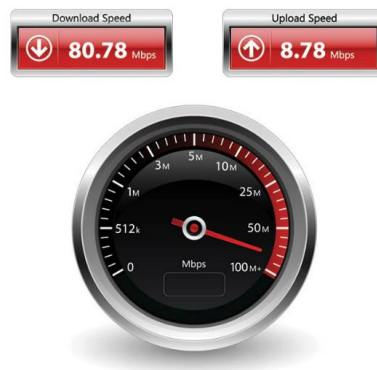
- La quantité de trafic
- Le type de trafic
- La latence créée par le nombre de périphériques réseau rencontrés entre la source et la destination

Quant au **débit applicatif**, il mesure les données utilisables transférées sur une période donnée.

Le débit applicatif correspond donc au débit moins la surcharge de trafic pour l'établissement de sessions, les accusés de réception, l'encapsulation et les bits retransmis (et il est forcément toujours inférieur à la valeur du débit).

## Accès réseau

Le débit est d'ailleurs ce que vous mesurez lorsque vous testez la vitesse de votre connexion internet notamment via le site <http://www.speedtest.net/fr/>

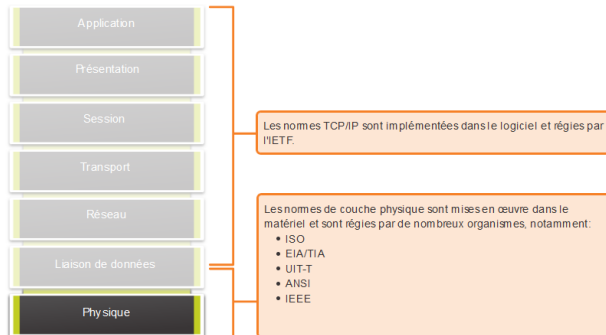




## Types de supports physiques

La couche physique produit la représentation et les groupements de bits sous forme de tensions, de radiofréquences ou d'impulsions lumineuses.

Divers organismes de normalisation ont contribué à la définition des propriétés physiques, électriques et mécaniques des supports disponibles pour différentes communications de données.



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

### A. Supports de cuivre

Le support le plus souvent utilisé pour les communications de données est un câblage qui utilise des fils de cuivre pour la transmission de bits de données et de contrôle entre les périphériques réseau.

Le câblage employé pour les communications de données se compose généralement d'une série de fils de cuivre individuels formant des circuits dédiés à des fins de signalisation spécifiques.

Les supports en cuivre sont utilisés sur certains réseaux, car ils sont bon marché, faciles à installer et qu'ils présentent une faible résistance au courant électrique. Cependant, les supports en cuivre sont limités par la distance et les interférences du signal.

Pour rappel, les données sont transmises sur les câbles en cuivre sous forme d'impulsions électriques. Un détecteur dans l'interface réseau d'un périphérique de destination doit recevoir un signal pouvant être décodé correctement pour correspondre au signal envoyé.

Toutefois, plus la distance de transmission du signal est longue, plus il se détériore selon un phénomène dit d'atténuation du signal.

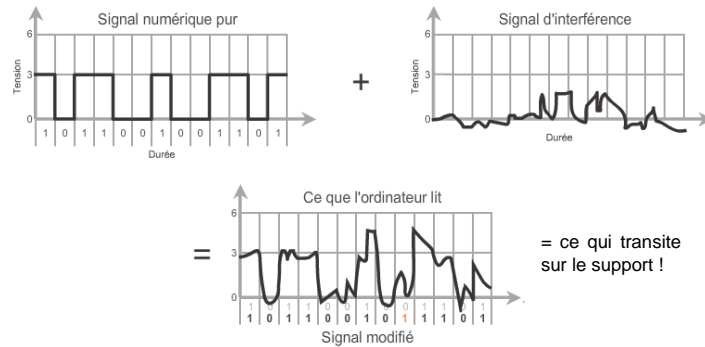
Pour cette raison, tous les supports en cuivre sont soumis à des restrictions de distance strictes spécifiées par les normes en la matière.

La durée et la tension des impulsions électriques sont également susceptibles de subir des interférences de deux sources :

- **Interférences électromagnétiques (EMI) ou interférences radioélectriques (RFI)** : les signaux électromagnétiques et radioélectriques peuvent déformer et détériorer les signaux de données transportés par les supports en cuivre. Les sources potentielles d'interférences EMI et RFI sont notamment les ondes radio et les appareils électromagnétiques (éclairage fluorescents, les moteurs électriques,...)

- **Diaphonie** : la diaphonie est une perturbation causée par les champs électriques ou magnétiques d'un signal dans un câble au signal traversant le câble adjacent. Plus précisément, lorsque le courant électrique circule dans un câble, il crée un petit champ magnétique circulaire autour du câble qui peut être capté par le fil adjacent.

Explications des perturbations électromagnétiques :



**Mais ce qu'interprète l'ordinateur qui reçoit le signal est différent du signal envoyé !!!**

Bien entendu, il existe des moyens pour contrer ou pour limiter les effets négatifs que produisent ces interférences !

Pour limiter la sensibilité des câbles en cuivre aux parasites électroniques on peut tout simplement choisir un câble adapté à l'environnement réseau spécifique dans lequel on se trouve ou encore concevoir une infrastructure de câblage afin d'éviter de faire passer les câbles trop près des sources connues d'interférences.

Par exemple, pour contrer les effets négatifs des perturbations électromagnétiques et radioélectriques, certains types de câbles en cuivre sont entourés d'un blindage métallique et nécessitent des connexions de mise à la terre appropriées.

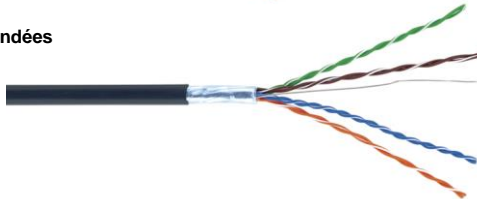
Pour contrer les effets négatifs de la diaphonie, certains types de câbles en cuivre utilisent des paires de fils opposés torsadés qui annulent la perturbation.

Il existe 3 types principaux de supports en cuivre utilisés dans les réseaux :

➤ **les câbles à paires torsadées non blindées**



➤ **les câbles à paires torsadées blindées**



➤ **les câbles coaxiaux**



➤ **les câbles à paires torsadées non blindées (UTP)**

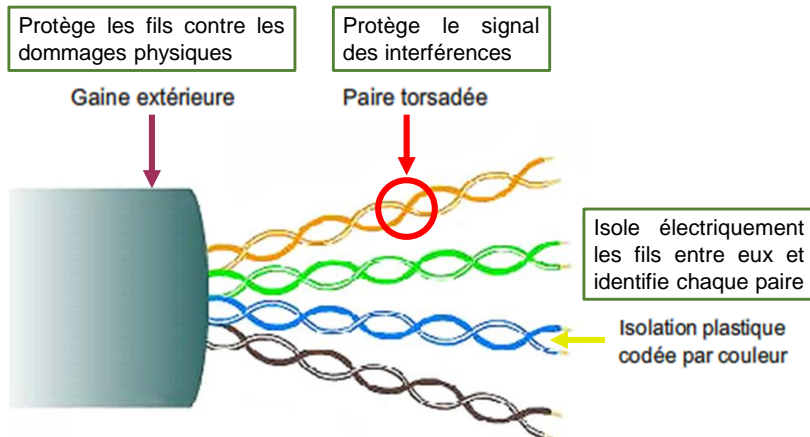
Le câblage à paires torsadées non blindées, appelé également câblage UTP (« Unshielded Twisted Pair »), utilisé dans les réseaux locaux Ethernet, se compose de quatre paires de fils à code de couleur qui ont été torsadés puis logés dans une gaine en plastique souple.

Des codes de couleur identifient les paires individuelles et les fils des paires afin de faciliter le raccordement des câbles.

Les fils sont torsadés afin d'éviter le phénomène de diaphonie dont on a parlé juste avant. En effet, lorsque du courant électrique circule dans un fil, il crée un champ magnétique circulaire autour de celui-ci.

Le courant circulant dans des directions opposées dans les deux fils d'une paire, les champs magnétiques, en tant que forces opposées égales, ont un effet d'annulation réciproque.

De plus, les différentes paires de fils torsadés dans le câble utilisent un nombre différent de torsades par mètre pour mieux protéger le câble contre la diaphonie entre les paires.



Le câblage UTP est bien évidemment soumis à une série de normes concernant divers éléments tels que :

- Les types de câbles
- Les longueurs de câbles
- Les connecteurs
- Le raccordement des câbles
- Les méthodes de test des câbles
- Les caractéristiques électriques

Ces normes (établies conjointement par la TIA et l'EIA) concernant le câblage utilisé permettent de différencier ainsi plusieurs catégories de câbles :

- **Catégorie 5** : La catégorie 5 permet une bande passante de 100 MHz. Ce standard permet l'utilisation du 100BASE-TX et du 1000BASE-T, ainsi que diverses applications de téléphonie ou de réseaux (« Token Ring »).
- **Catégorie 5e** : cette catégorie de câble est une adaptation de la catégorie 5. Elle permet une vitesse allant jusqu'à 1000 Mbits/s pour une bande passante max de 100 MHz. Ce type de câblage peut être utilisé sur une distance max de 100m.
- **Catégorie 6** : ce type de câble permet une bande passante max de 250 MHz et un débit maximum de 10Gbit/s. Sa distance maximum d'utilisation est de 55m.
- **Catégorie 6a** : ce type de câble permet toujours un débit maximum de 10Gbit/s mais va permettre une bande passante plus haute (500MHz) et une distance maximum plus grande (100m).
- **Catégorie 7** : cette catégorie de câblage permet l'utilisation d'une bande passante de 600 MHz sur une distance courte (max 15m) et permet un débit allant jusqu'à 100 Gbit/s.
- **Catégorie 7a** : cette version permet l'utilisation d'une bande passante de 1GHz sur une distance max de 100m avec un débit max pouvant toujours atteindre les 100 Gbit/s.
- **Catégorie 8** : cette catégorie permet d'atteindre les 40Gbit/s sur une distance max de 30m avec une bande passante de 2GHz.

Il existe également différents type de câblage :

De manière générale, le câblage UTP, terminé par des connecteurs RJ-45, est un support en cuivre courant pour l'interconnexion de périphériques réseau, tels que des ordinateurs, avec des périphériques intermédiaires, tels que des routeurs et commutateurs réseau.

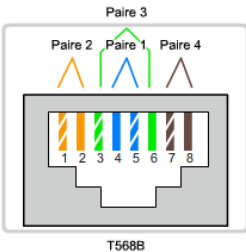
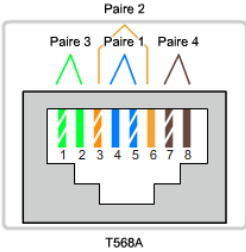
Mais certains scénarios peuvent exiger des câbles UTP répondant à différentes conventions de câblage.

→ Ceci signifie que les fils individuels du câble doivent être connectés dans des ordres différents à diverses séries de broches des connecteurs RJ-45.

Les principaux types de câbles obtenus en utilisant des conventions de câblage spécifiques sont les suivants :

- Ethernet droit
- Ethernet croisé
- Renversement, aussi appelé câble console (exclusivement pour Cisco)

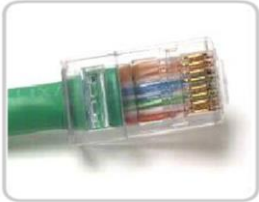
Type de câble	Standard	Application
Ethernet droit	Les deux extrémités T568A ou T568B	Connexion d'un hôte réseau à un périphérique réseau tel qu'un commutateur ou un concentrateur.
Ethernet croisé	Une extrémité T568A, l'autre T568B	Connexion de deux hôtes réseau. Connexion de deux périphériques intermédiaires réseau (un commutateur à un commutateur, ou un routeur à un routeur).
Renversement	Exclusif à Cisco	Connexion d'un port série de station de travail à un port console de routeur, à l'aide d'un adaptateur.



Remarque :

Chaque fois qu'un câblage en cuivre est raccordé, cela implique le risque de perte de signal et l'introduction de parasites dans le circuit de communication.

Il est donc impératif que le raccordement soit correctement réalisé afin d'éviter tout impact sur les performances de transmission.



Connecteur correct : les fils sont détorsadés sur la longueur nécessaire au raccordement du connecteur.



Connecteur incorrect : les fils sont détorsadés sur une trop grande longueur.

### ➤ les câbles à paires torsadées blindées

Le câble à paires torsadées blindées est un autre type de câblage utilisé dans les réseaux.

Les câbles blindés offrent une meilleure protection parasitaire que le câblage non blindé.

Toutefois, par rapport aux UTP, les câbles blindés sont bien plus onéreux.

Les câbles à paires torsadées blindées allient la technique de blindage pour contrer les interférences électromagnétiques et radioélectriques, et les torsades pour éviter la diaphonie.

Pour tirer entièrement parti des avantages du blindage, les câbles blindés sont terminés par des connecteurs de données (RJ-45) blindés spécifiques. Si le câble n'est pas correctement mis à la terre, le blindage peut agir comme une antenne et capter des signaux parasites.



Au niveau des câbles blindés, il existe pas mal de catégories différentes...

Et afin que vous puissiez distinguer les différentes câbles, je vous invite à lire le texte « STP, UTP, FTP Cable » qui est mis à votre disposition sur l'E-campus.

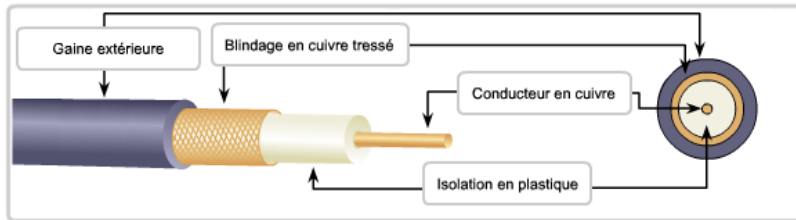


### ➤ les câbles coaxiaux

Un câble coaxial se compose d'un conducteur de cuivre entouré d'une couche de matériau isolant flexible.

Sur ce matériau isolant, une torsade de cuivre ou un film métallique constitue le second fil du circuit et fait office de protection pour le conducteur intérieur.

Cette seconde couche, ou blindage, réduit également les interférences électromagnétiques externes. La gaine du câble enveloppe le blindage.

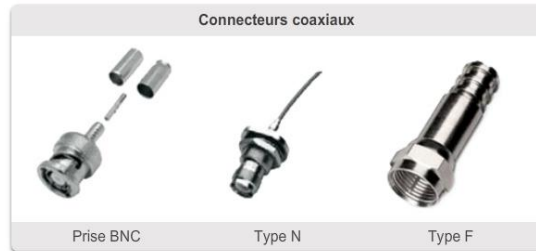


Les câbles coaxiaux étaient traditionnellement utilisés pour la télévision par câble et permettaient la transmission dans une seule direction (télédistribution). Ils ont également été largement utilisés dans les premières installations Ethernet.

Bien que les câbles UTP aient remplacé les câbles coaxiaux dans les installations Ethernet modernes, la conception du câble coaxial a été adaptée aux fins suivantes :

- **Installations sans fil** : les câbles coaxiaux relient les antennes aux périphériques sans fil. Le câble coaxial transporte de l'énergie en radiofréquence (RF) entre les antennes et le matériel radio.
- **Installations Internet par le câble** : les fournisseurs d'accès câblé convertissent actuellement leurs systèmes unidirectionnels en systèmes bidirectionnels afin de fournir une connectivité Internet à leurs clients. Afin de fournir ces services, des portions du câble coaxial et des éléments d'amplification associés sont remplacés par du câble à fibre optique. Cependant, la connexion finale avec le site du client et le câblage à l'intérieur de ses locaux restent coaxiaux. Cette utilisation mixte de fibre et de coaxial est appelée réseau hybride fibre et coaxial (HFC).

Il existe différents connecteurs pour les câbles coaxiaux :



Les prises BNC sont les connecteurs les plus répandus.

Au niveau de la sécurité des câblages de cuivre d'une manière générale, les trois types de supports en cuivre présentent des risques d'incendie et des risques électriques.

L'isolation et les gaines du câble peuvent être inflammables ou dégager des émanations toxiques lorsqu'elles sont chauffées ou brûlées, d'où le risque d'incendie.

Des risques électriques peuvent également exister puisque les fils de cuivre peuvent conduire l'électricité dans des directions non souhaitables.

Personnel et matériel peuvent alors être exposés à une série de risques électriques.

Pour finir, le câblage en cuivre peut conduire des tensions causées par la foudre vers des périphériques réseau.

## B. Fibre optique

La fibre optique est un fil en verre très pur (silice) transparent, à la fois flexible et très fin.

Le câble à fibre optique sert de guide d'ondes ou « tuyau lumineux » qui transmet la lumière entre les deux extrémités avec un minimum de perte de signal.

Son diamètre n'est pas beaucoup plus grand que celui d'un cheveu humain.

Celle-ci est de plus en plus utilisée pour interconnecter des périphériques réseau d'infrastructure.

Contrairement aux fils de cuivre, la fibre optique peut transmettre des signaux qui subissent moins d'atténuation et est entièrement insensible aux perturbations électromagnétiques et radioélectriques.

Elles peuvent fonctionner à des longueurs bien supérieures aux supports en cuivre, sans nécessiter de régénération des signaux.

Bien entendu tout n'est pas parfait et il y a des désavantages liés à la mise en œuvre de supports en fibre optique :

- Un coût plus élevé que les supports en cuivre pour la même distance (mais pour une capacité supérieure)
- Des compétences et matériel différents pour raccorder l'infrastructure réseau
- Une manipulation plus délicate que les supports en cuivre

Actuellement, les câbles à fibre optique sont utilisés dans quatre domaines d'application :

• **Les réseaux d'entreprise** : la fibre est utilisée pour les applications de câblage du réseau fédérateur et pour relier les périphériques d'infrastructure.

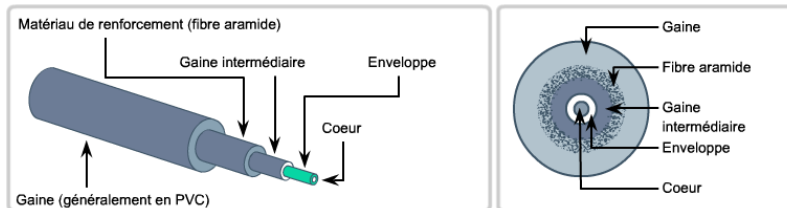
• **Les réseaux FTTH et d'accès** : la technologie FTTH (« Fiber To The Home » ou fibre optique jusqu'au domicile) est utilisée pour fournir des services haut débit disponibles en permanence aux particuliers et aux petites entreprises. Les réseaux FTTH permettent un accès Internet haut débit abordable, le télétravail, la télémédecine et la vidéo à la demande.

• **Les réseaux longue distance** : les fournisseurs d'accès utilisent des réseaux terrestres longue distance à fibre optique pour connecter les pays et les villes. Ces réseaux vont généralement de quelques dizaines à quelques milliers de kilomètres et utilisent des systèmes proposant jusqu'à 10 Gbit/s.

• **Les réseaux sous-marins** : des câbles à fibre spéciaux sont utilisés pour fournir des solutions haut débit et haute capacité fiables, à l'épreuve des environnements sous-marins sur des distances à l'échelle d'un océan.

### Mais à quoi ressemble une fibre optique ?

Bien que la fibre optique soit très fine, elle se compose de différentes couches qui sont les suivantes :



*La lumière pouvant uniquement voyager dans une direction par la fibre optique, deux fibres sont requises pour prendre en charge le fonctionnement bidirectionnel simultané.*



### Fonctionnement de la fibre optique

Au niveau des sources lumineuses utilisées dans la fibre optique, nous en retrouvons deux différents : des lasers ou des diodes électroluminescentes.

Les lasers (DL) ou les diodes électroluminescentes (DEL) génèrent les impulsions lumineuses utilisées pour représenter les données transmises sous forme de bits sur le support.

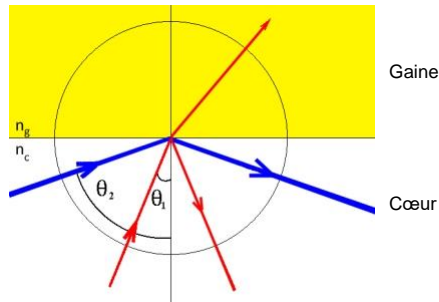
Des dispositifs à semi-conducteur électronique appelés photodiodes détectent les impulsions lumineuses et les convertissent en tensions qui peuvent ensuite être reconstituées en trames de données.

→ *La fibre optique est donc un guide d'onde qui exploite les propriétés réfractrices de la lumière.*

Sa particularité est que son cœur a un indice de réfraction (noté «  $n_c$  ») légèrement plus élevé que l'indice de réfraction de la gaine (noté «  $n_g$  ») qui l'entoure. C'est en utilisant cette particularité que l'on va pouvoir permettre la propagation de la lumière sans pertes.

En effet, en fonction de l'angle avec lequel la lumière sera insérée dans la fibre, et grâce au phénomène de réflexion interne totale, on va pouvoir confiner la lumière afin de la faire voyager d'un bout à l'autre de la fibre sans aucune perte.

Concrètement, on a deux milieux ayant un indice de réfraction différent, tel que  $n_c > n_g$



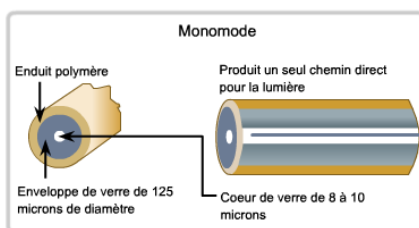
Selon la loi de Snell-Descartes, on a la formule  $n_c \sin \theta_c = n_g \sin \theta_g$

De cette formule, on peut déduire l'angle critique au dessus duquel le faisceau qui frappe les parois de la fibre est totalement réfléchi.  $\rightarrow \theta_{\text{critique}} = \arcsin(n_g/n_c)$

Il existe également deux types de fibre optique :

➤ La **fibre optique monomode (SMF)** transporte un seul rayon lumineux, généralement émis par un laser (DL).

La lumière laser étant unidirectionnelle et voyageant au centre de la fibre, ce type de fibre peut transmettre des impulsions optiques sur de très longues distances.



#### Caractéristiques :

- Cœur de petit diamètre
- Moins de dispersion
- Adapté aux applications longue distance (jusqu'à 100 km)
- Utilise des lasers comme source lumineuse

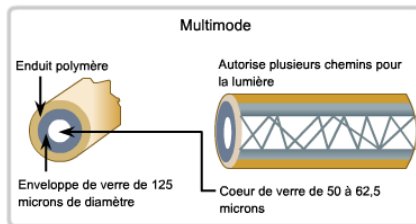
## Accès réseau

➤ La **fibres optique multimode (MMF)** utilise en principe des émetteurs à DEL qui ne créent pas une seule onde lumineuse cohérente.

La lumière d'une DEL entre au contraire dans la fibre multimode selon différents angles.

La traversée de la fibre prenant ainsi plus ou moins de temps, des longueurs de fibre importantes peuvent générer des impulsions troubles à l'arrivée à l'extrémité réceptrice.

Cet effet, appelé distorsion modale, limite la longueur des segments de fibre multimode.



### Caractéristiques :

- Cœur d'un diamètre plus large que le câble monomode (50  $\mu$ m ou plus)
- Dispersion → affaiblissement du signal
- Adapté aux longues distances, jusqu'à 2 km environ
- Utilise des DEL comme source lumineuse

## Accès réseau

À niveau de la connectique, il existe beaucoup de connecteurs différents :

Un connecteur à fibre optique termine l'extrémité d'un câble à fibre optique.

Un connecteur optique est constitué d'un raccord et de deux fiches.

Les fiches optiques contiennent des fêrues (de 1,25 ou 2,5 mm) assurant le raccordement et le positionnement des deux extrémités de fibre avec précision. Ces fiches optiques sont raccordées via un raccord qui assure l'alignement.

Le montage d'un connecteur sur une extrémité de fibre optique engendre une perte du signal optique, appelée la perte d'insertion (IL).

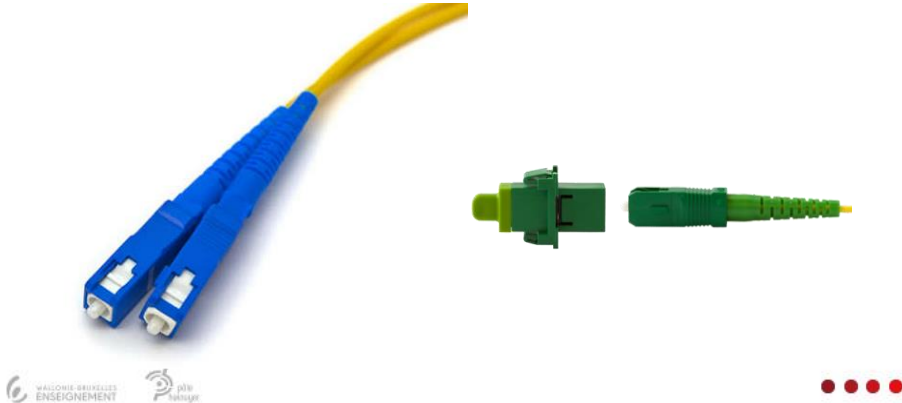
Une petite partie du signal transmis est également réfléchi par le connecteur directement vers la source lumineuse d'émission, ce qui engendre aussi des pertes (ORL).



## Accès réseau

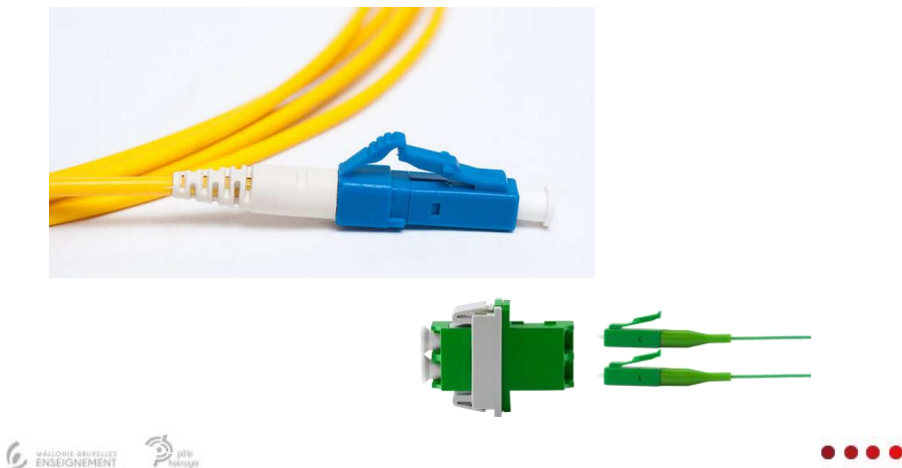
Cependant tous ne sont pas utilisés fréquemment. Les plus courants sont au nombre de 3 :

- Le **connecteur SC** (« **S**uscriber **C**onnector ») est un connecteur carré fonctionnant par encliquetage (couplage push-pull), ce qui garantit l'insertion dans le bon sens. Il est largement utilisé avec de la fibre optique monomode ou multimode. Son faible coût et sa facilité d'utilisation en font un connecteur très réputé sur le marché.



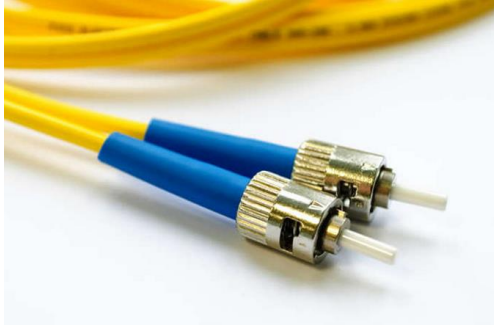
## Accès réseau

- Le **connecteur LC** (« **L**ucent **C**onnector ») est un petit connecteur SC. Ainsi, avec les mêmes propriétés, on peut le placer dans des endroits plus difficile d'accès.



## Accès réseau

- Le **connecteur ST** (« **Straight Tip** ») est l'un des premiers types de connecteur utilisés. Ce connecteur offre un verrouillage sécurisé grâce à un mécanisme à baïonnette (de type "Twist-on/twist-off"). C'est un connecteur très largement utilisé avec de la fibre optique multimode.



## Accès réseau

Bien entendu, pour simplifier encore un peu les choses, il existe une multitude de manières dont peuvent être agencés ces connecteurs pour former une fibre optique :



Câble de brassage multimode SC-SC



Câble de brassage multimode ST-LC



Câble de brassage monomode LC-LC



Câble de brassage monomode SC-ST



Alors, je vous ai dit, la fibre optique est beaucoup plus complexe à mettre en place que le câblage de cuivre. Le raccordement incorrect de supports en fibre optique diminue les distances de signalisation ou entraîne l'échec complet de la transmission.

Il faut donc une formation spécialisée et un matériel adapté pour effectuer le raccordement et l'épissage des câbles en fibre optique.

Pour tester les câbles à fibre optique, on peut notamment utiliser un réflectomètre optique (noté OTDR en anglais). Ce dispositif permet de tester chaque segment de câble à fibre optique en injectant une impulsion test de lumière dans le câble et mesurant la rétrodiffusion et la réflexion de lumière détectées en fonction du temps. Cela permet notamment de calculer la distance approximative à laquelle des défauts sont détectés le long du câble.

Au niveau du raccordement de la FO, 3 types d'erreurs sont assez courantes :

- **Mauvais alignement** : les supports en fibre optique ne sont pas alignés précisément lors de la jonction.
- **Écart à l'extrémité** : les supports ne se touchent pas complètement à l'épissure ou à la connexion.
- **Finition de l'extrémité** : les extrémités des supports ne sont pas bien polies ou de la poussière est présente au niveau du raccordement.

### Comparatif : FO vs câblage en cuivre

Problèmes de mise en œuvre	Câblage à paires torsadées non blindées (UTP)	Câblage à fibre optique
Bande passante	10 Mbit/s - 10 Gbit/s	10 Mbit/s - 100 Gbit/s
Distance	Relativement courte (1 à 100 m)	Relativement longue (1 à 100 000 m)
Résistance aux perturbations électromagnétiques et radioélectriques	Faible	Haute (résistance totale)
Résistance aux risques électriques	Faible	Haute (résistance totale)
Coûts des supports et des connecteurs	Moins élevé	Plus élevé
Compétences requises pour l'installation	Moins élevé	Plus élevé
Précautions à prendre concernant la sécurité	Moins élevé	Plus élevé

### Normes et dénominations

Voici un tableau reprenant le nom commercial, la vitesse théorique, la dénomination physique, le standard IEEE et des caractéristiques physiques sommaires des technologies Ethernet les plus courantes.

Nom commercial	Vitesse	Dénomination physique	Standard	Support, longueur
Ethernet	10 Mbps	10BASE-T	IEEE 802.3	Cuivre, 100 m
Fast Ethernet	100 Mbps	100BASE-TX	IEEE 802.3u	Cuivre, <100 m
Gigabit Ethernet	1 Gbps	1000BASE-SX, 1000BASE-LX	IEEE 802.3z	Fibre, 550 m, <5 Km
Gigabit Ethernet	1 Gbps	1000BASE-T	IEEE 802.3ab	Cuivre, <100 m
10Gigabit Ethernet	10 Gbps	10GBASE-SR, 10GBASE-LR	IEEE 802.3ae	Fibre, 300 m, <25 Km
10Gigabit Ethernet	10 Gbps	10GBASE-T	IEEE 802.3an	Cuivre, <100 m
40Gigabit Ethernet	40 Gbps	40GBASE-SR, 40GBASE-LR	IEEE 802.3ba	Fibre, 125 m, <10 Km
100Gigabit Ethernet	100 Gbps	100GBASE-SR, 100GBASE-LR	IEEE 802.3ba	Fibre, 125 m, <10 Km

T = *Twisted Pair*  
F = *Fiber*

SR = *Short range* (longueur d'ondes courte)  
LR = *Long range* (longueur d'ondes grande)

### La fibre optique sous-marine

Si l'on demande à quelqu'un par quel moyen transite la majorité des communications internationales : il y a de fortes chances qu'il réponde, après avoir réfléchi quelques instants, « via les satellites » !

Hé bien non... *"Pour les communications internationales, plus de 99% du trafic passe par les câbles sous-marins"*, a expliqué Alan Mauldin, directeur de la recherche de la société d'études TeleGeography.

Et la raison de ce choix est simple : les câbles peuvent transporter beaucoup plus d'informations, pour un coût minime.

Une autre raison est également évidente : *"Dans un monde où chaque milliseconde compte, l'aller-retour vers les satellites représente une perte de temps inutile"*, a indiqué Benjamin Bayart, spécialiste des télécommunications et porte-parole du fournisseur d'accès à Internet associatif FDN.

Si l'on demande à quelqu'un par quel moyen transite la majorité des communications internationales : il y a de fortes chances qu'il réponde, après avoir réfléchi quelques instants, « via les satellites » !

En 2021, on comptait déjà 464 câbles construits et mis en service afin de permettre à nos réseaux de communication de fonctionner.

<http://www.submarinecablemap.com>  
<https://submarine-cable-map-2021.telegeography.com/>

*Comment se passe la pose de câbles sous-marin et à quoi ressemblent-ils ?*

La pose d'un câble sous-marin est une opération complexe qui se prépare longtemps à l'avance. Outre les montages financiers et les partenariats entre opérateurs de télécommunication, la première étape consiste à faire une opération de reconnaissance des fonds (« survey » en anglais).

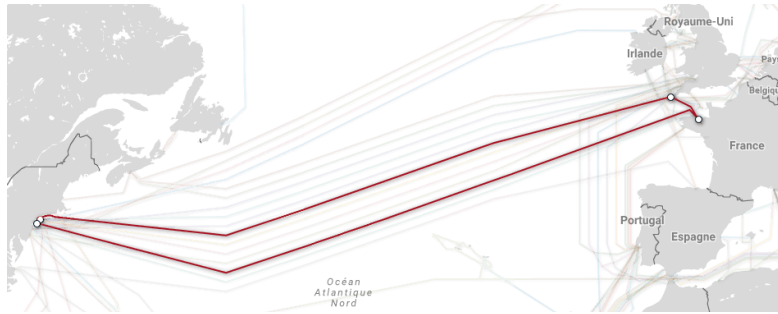
Cela comprend notamment l'étude du tracé pour positionner le câble et les répéteurs, l'étude de la profondeur d'immersion, l'analyse des sols marins,...

Ensuite un câble peut être :

- Soit déroulé sur le fond des océans. Selon la topographie sous-marine, il sera éventuellement "ancré" sur certains points du tracé.
- Soit enfoui dans une tranchée sous-marine à l'aide d'une charrue d'ensouillage, ce qui protégera un peu plus le câble mais qui par contre demande un équipement et un savoir-faire supplémentaire.

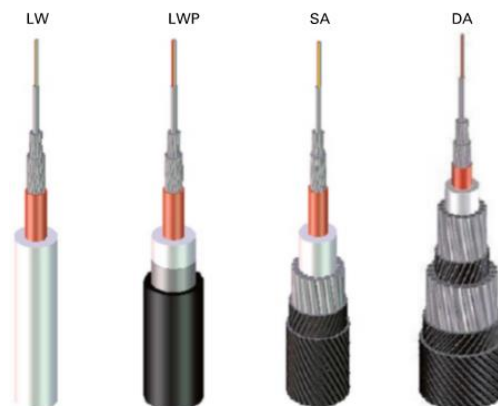
## Accès réseau

Pour vous donner une idée, un câble transatlantique tel que le FLAG Atlantic (FA-1) fait 14500km de long et a ainsi besoin de 70 répéteurs pour que le signal partant de Plérin (Côtes d'armor) parvienne jusqu'à Island Park (New York).



## Accès réseau

Bien évidemment, en fonction du risque d'exposition aux agressions externes (ancres et chaluts de bateaux, sols rocheux,...), il existe différents types de câbles sous-marin :



➤ **LW (Leight Weight)**

Ce câble est uniquement utilisé dans les zones d'eau profonde (> 1 500 m) à l'abri des agressions externes. Son diamètre externe est de 17 mm.

➤ **LWP (Leight Weight Protected)**

Ce câble est constitué d'un câble LW enrobé d'une couche d'acier et d'une gaine de polyéthylène à haute densité. Son diamètre externe est de 23 mm.

➤ **SA (Single Armured)**

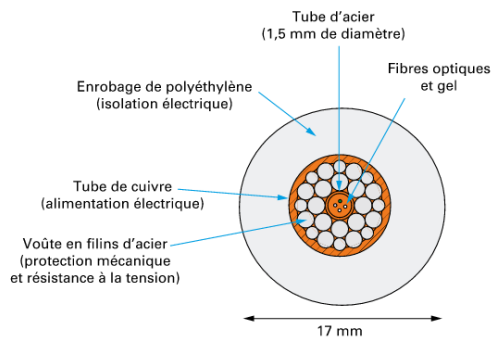
Câble LW autour duquel des fils d'aciers sont placés afin de constitué ce qui est appelé une couche d'armure : ces fils d'acier ont un diamètre de 3 mm et sont maintenus ensemble par un flux de goudron mélangé à des fibres de polypropylène. Son diamètre externe est de 30 mm.

➤ **DA (Double Armured)**

Câble SA autour duquel une seconde couche de fils d'acier est ajoutée. Son diamètre externe est de 40 mm.

Les câbles SA et DA sont déployés en zone d'eaux peu profondes (< 1 500 m) où les agressions externes sont fréquentes.

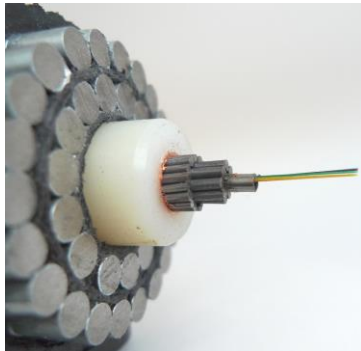
Le câble LW constitue la base commune à tous les types de câble, comporte les éléments suivants :



*vue en coupe d'un câble LW*

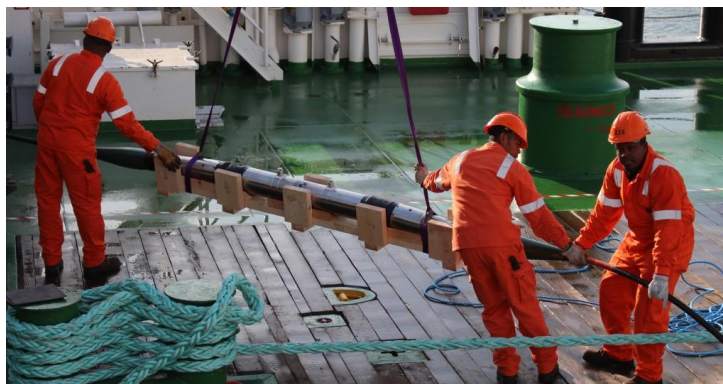
## Accès réseau

Un câble sous-marin Double Armured :



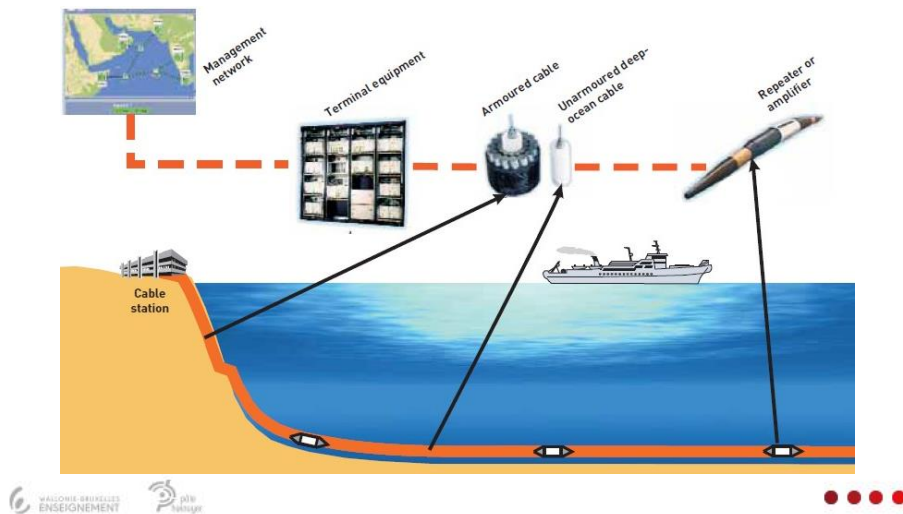
## Accès réseau

Bien entendu, des répéteurs doivent être installés au bout d'un certains nombres de km (en fct d'un tas de facteurs tel que la longueur d'onde utilisée, le type de modulation,...) afin de régénérer les signaux lumineux.



## Accès réseau

Déploiement d'un câble sous-marin :

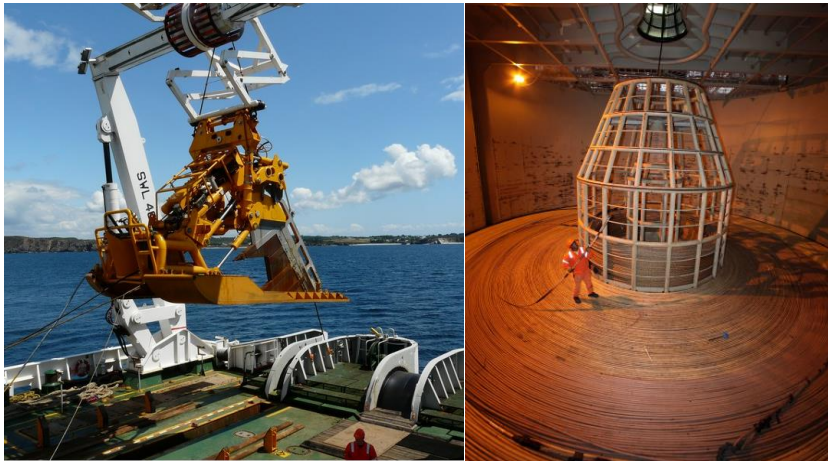


## Accès réseau

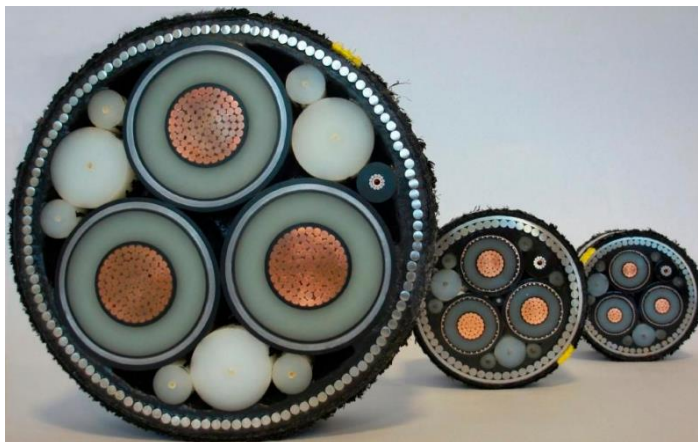
Voici quelques images d'un navire poseur de fibre ainsi que du robot utilisé pour poser le câble au fond de l'eau :







Parfois les câbles sous-marin peuvent combiner différentes technologies, comme ce câble hybride électrique et optique :





**DWDM**

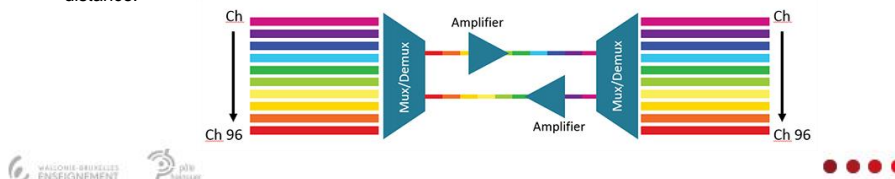
**DWDM** (« *Dense Wavelength-Division Multiplexing* ») ou **multiplexage en longueur d'onde** en français, est une technique utilisée en communication optique qui permet d'augmenter le débit sur une fibre optique en faisant circuler plusieurs signaux de longueurs d'onde différentes sur une seule fibre.

Il s'agit pour simplifier de faire passer plusieurs longueurs d'onde simultanément dans une fibre – ou le plus souvent une paire de fibres (émission/réception). Ces longueurs d'onde sont visibles séparément à chaque extrémité, mais circulent de concert sur le médium.

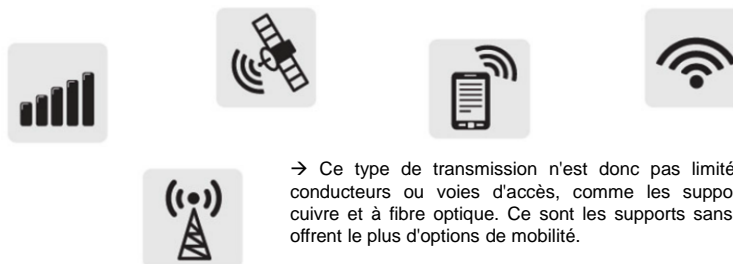
Chaque longueur d'onde constitue alors un lien réseau séparé et indépendant du point de vue des équipements qui l'utilisent.

DWDM permet des communications bidirectionnelles sur un même brin. Il est capable de multiplexer jusqu'à 80 canaux de 10 Gbps sur une seule fibre.

Les circuits DWDM sont utilisés dans tous les câbles sous-marins de communication et longue distance.

**c. Les supports sans fils**

Les supports sans fil transportent les signaux électromagnétiques qui représentent les bits des communications de données via des fréquences radio ou micro-ondes.



→ Ce type de transmission n'est donc pas limitée aux conducteurs ou voies d'accès, comme les supports en cuivre et à fibre optique. Ce sont les supports sans fil qui offrent le plus d'options de mobilité.

De plus, le nombre de périphériques sans fil augmente sans cesse. De ce fait, la technologie sans fil est devenue le support de choix pour les réseaux domestiques.



Toutefois, le sans fil présente également quelques contraintes :

- **Zone de couverture** : les technologies de communication de données sans fil fonctionnent bien dans les environnements ouverts. Cependant, certains matériaux de construction utilisés dans les bâtiments et structures, ainsi que le terrain local, limitent la couverture effective.
- **Interférences** : 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.
- **Sécurité** : la connexion à un réseau sans fil ne nécessite aucun accès physique à un support. Par conséquent, les périphériques et les utilisateurs non autorisés à accéder au réseau peuvent tout de même se connecter. La sécurité du réseau constitue donc un composant essentiel de l'administration des réseaux sans fil.

L'IEEE et les normes de l'industrie des télécommunications en matière de communication de données sans fil couvrent à la fois les couches liaison de données et physique.

Parmi ces normes, on retrouve 3 normes courantes :

- **Norme IEEE 802.11** : la technologie LAN sans fil (WLAN), plus communément appelée Wi-Fi, utilise un système avec gestion des conflits ou non déterministe et un processus d'accès au support CSMA/CA (*Carrier Sense Multiple Access/Collision Avoidance*).




### Normes IEEE 802.11

- Il existe différentes variantes :
  - 802.11a : 54 Mbit/s, 5 GHz
  - 802.11b : 11 Mbit/s, 2,4 GHz
  - 802.11g : 54 Mbit/s, 2,4 GHz
  - 802.11n : 600 Mbit/s, 2,4 et 5 GHz
  - 802.11ac : 1 Gbit/s, 5 GHz
  - 802.11ad : 7 Gbit/s, 2,4 GHz, 5 GHz et 60 GHz

## Accès réseau


- **Norme IEEE 802.15** : la norme relative au réseau personnel sans fil (WPAN), couramment appelée Bluetooth, utilise un processus de jumelage de périphériques pour communiquer sur des distances de 1 à 100 mètres.



Norme IEEE 802.15

- Prise en charge de débits jusqu'à 3 Mbit/s
- Propose le jumelage de périphériques sur des distances de 1 à 100 mètres

- **Norme IEEE 802.16** : la technologie d'accès couramment appelée WiMax (*Worldwide Interoperability for Microwave Access*) utilise une topologie point-à-multipoint pour fournir un accès à large bande sans fil.



Norme IEEE 802.16

- Propose des débits jusqu'à 1 Gbit/s
- Utilise une topologie point-à-multipoint pour fournir un accès à large bande sans fil

## Accès réseau

Une mise en œuvre courante de réseau de données sans fil est la possibilité pour des périphériques de se connecter sans fil via un réseau local.

Un réseau local sans fil exige généralement les périphériques réseau suivants :

- **Point d'accès sans fil** : il concentre les signaux sans fil des utilisateurs et se connecte, en général via un câble en cuivre, à une infrastructure réseau en cuivre existante telle qu'Ethernet. Les routeurs sans fil pour particuliers et petites entreprises intègrent à la fois les fonctions d'un routeur, d'un commutateur et d'un point d'accès.
- **Adaptateurs de carte réseau sans fil** : ils fournissent à chaque hôte du réseau la possibilité de communiquer sans fil.

Afin de fonctionner correctement, plusieurs normes Ethernet WLAN ont émergé au cours du temps. Celles-ci sont reprises dans le tableau ci-dessous :

802.11	Bande de fréquence	Débit théorique maximal	Portée	Congestion	Largeur canal	MIMO
WiFi 1 (a)	5 GHz	54 Mbps	Faible	Faible	20 MHz	Non
WiFi 2 (b)	2,4 GHz	11 Mbps	Correcte	Elevée	20 MHz	Non
WiFi 3 (g)	2,4 GHz	54 Mbps	Correcte	Elevée	20 MHz	Non
WiFi 4 (n)	2,4 GHz	288 Mbps	Bonne	Elevée	20 MHz	Non
WiFi 4 (n)	5 GHz	600 Mbps	Correcte	Faible	20 ou 40 MHz	Oui
WiFi 5 (ac)	5 GHz	5 300 Mbps	Correcte	Faible	20, 40, 80 ou 160 MHz	Oui
WiFi 6 (ax)	2,4 et 5GHz	10 530 Mbps	Correcte	Très faible	20, 40, 80 ou 160 MHz	Oui (+MU-MIMO)
ad	60 GHz	6 757 Mbps	Très faible	Faible	2 160 MHz	Oui (+MU-MIMO)

### Le WiMax

Le WiMax est une abréviation pour *Worldwide Interoperability for Microwave Access*. Le nom même de Wimax a été créé par les sociétés Intel et Alvarion en 2002 et est désormais un label commercial délivré par le WiMAX Forum.

Le WiMax est une technologie principalement utilisée pour les MAN (Métropolitain Area Network). Il permet, notamment, aux zones rurales de se doter d'une connexion internet haut débit. La technologie WiMax utilise la bande de fréquence des 3,5GHz.



L'objectif du WiMax est de fournir une connexion internet à haut débit sur une zone de couverture de plusieurs kilomètres de rayon (70 Mbit/s en débit théorique mais environ 20Mbit/s en pratique).

Le Wimax fonctionne en mode point-multipoint, c'est-à-dire le mode infrastructure que l'on connaît sur le Wifi ou encore le même fonctionnement que les technologies 2G, 3G de téléphonie mobile.

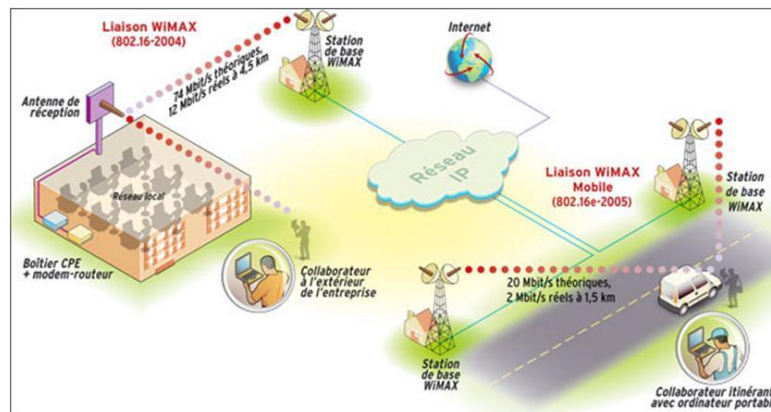
Une station de base nommée BTS (Base Transceiver Station) ou BS (Base Station) émet vers les clients et réceptionne leurs requêtes puis les transmet vers le réseau du fournisseur d'accès.

## Accès réseau

Il existe deux types d'application au Wimax :

- une version fixe (comparable au Wifi) sans « hand over », c-à-d que lorsque le client se déplace et change de BS, il se voit déconnecté et il doit se reconnecter à une autre BS.
- une version mobile, permettant la mobilité du client en assurant un hand over horizontal. En fait la carte du client reçoit des signaux des BS l'entourant et va choisir le meilleur signal parmi les signaux reçus. Cette vérification est faite constamment si le signal vient à s'affaiblir la carte choisira de nouveau le meilleur signal effectuant ainsi un soft hand over.

## Accès réseau



### c. Les supports à venir ?

Comme vous venez de le voir, nous avons déjà un vaste choix de supports de transmission, avec des propriétés et des caractéristiques différentes. Mais est-ce suffisant pour répondre à toutes les attentes ? Sommes nous toujours à la recherche de nouvelles technologies ?

Et bien la réponse est **oui** !

Récemment, une nouvelle technologie a fait son apparition sur le marché, il s'agit du **Li-Fi**

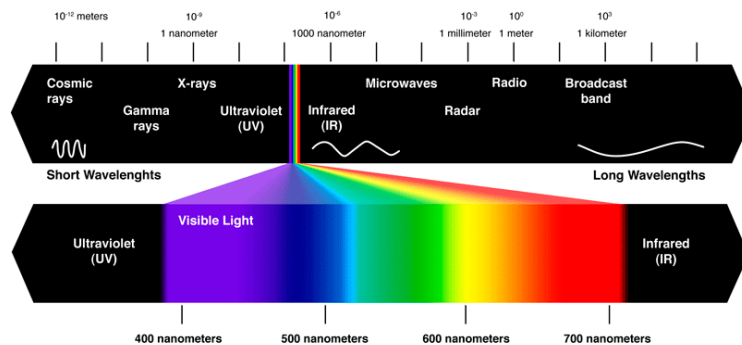


Va utiliser le spectre électromagnétique



Va utiliser le spectre optique

Le Li-Fi est une technologie de communication sans fil basée sur l'utilisation de la lumière visible.



La lumière visible couvre une bande d'environ 300 THz.

**Son spectre est 10 000 fois plus large que celui des ondes radio.**

Le Li-Fi est fait pour fonctionner jusqu'à une dizaine de mètres, ce qui est légèrement plus que la norme Bluetooth actuelle.

Cette technologie suit un protocole de communication spécifique établi par le comité IEEE 802, afin de développer des solutions compatibles à l'échelle mondiale.

Bien entendu, cette nouvelle technologie n'est pas faite pour remplacer entièrement les réseaux actuels, mais pour les compléter !

Au niveau des débits, et à l'heure actuelle (septembre 2016), cette norme peut atteindre les 45 Mbit/s.

#### Fonctionnement :

Grâce à des lumières LED, on va pouvoir transmettre à distance différents contenus multimédias (vidéo, son, géolocalisation, ...) à une tablette, un smartphone, une TV,...

#### Comment ?

En allumant et en éteignant plusieurs de milliers de fois par seconde une lumière à LED, on peut transmettre des informations en créant une fréquence.

Si une LED est allumée, elle transmet un bit 1, si elle est éteinte, un bit 0.

Ces changements de fréquence étant extrêmement rapides, ils ne sont bien entendu pas perceptible par l'oeil humain.

#### Domaines d'applications

À l'heure où les chercheurs et les institutions réfléchissent aux infrastructures nécessaires pour permettre aux voitures autonomes de prendre la route, le Li-Fi pourrait donc être une solution.

Il permettrait la communication de véhicule à véhicule, mais également avec l'équipement urbain (les feux, les barrières) et les piétons.

L'éclairage public pourrait également permettre aux touristes et aux résidents d'obtenir des informations contextuelles selon l'endroit où ils se trouvent.

## Accès réseau

Dans les avions et les hôpitaux, le Li-Fi pourrait permettre d'utiliser son matériel sans risque d'interférence électromagnétique. Plusieurs compagnies aériennes sont par exemple intéressées pour utiliser la liseuse au-dessus des sièges pour transmettre des données ou diffuser des films.

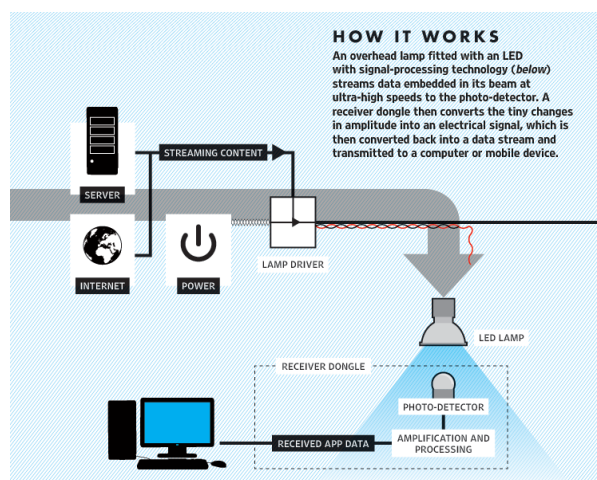
D'autres expérimentations prennent place dans des musées pour permettre aux visiteurs d'obtenir des informations en face d'une œuvre précise.

Mais la technologie permet également de localiser au centimètre un utilisateur. Ainsi, Philips et Carrefour se sont associés pour proposer au client de l'hypermarché Euralille une expérience d'achat innovante.

Grâce à une application et à des lumières Li-Fi réparties sur le magasin, les clients peuvent savoir exactement où ils se trouvent et obtenir la position de n'importe quel article.

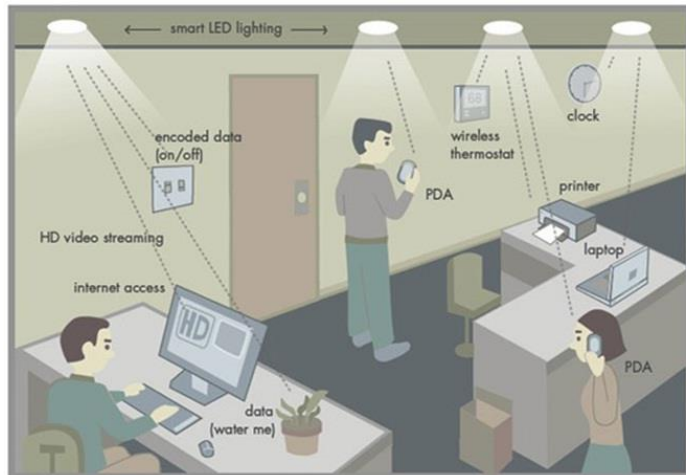


## Accès réseau





## Accès réseau



## Accès réseau

### Avantages/inconvénients :

Cette technologie présente plusieurs avantages :

- ✓ Le débit peut être important.
- ✓ Une source lumineuse est simple à mettre en place.
- ✓ Contrairement aux ondes électro-magnétiques, les ondes lumineuses ne traversent pas le corps humain, et donc ne sont pas susceptibles de poser des problèmes de santé.
- ✓ C'est directionnel, donc les informations ne peuvent être captées que sur le trajet de l'onde lumineuse, on peut donc penser que cela peut être plus sécurisé que du wifi. (ne traverse pas les murs)
- ✓ Cela permet d'éviter à terme la saturation des réseaux WiFi en proposant un nouveau canal de distribution de l'information numérique.

Par contre, il y a néanmoins des inconvénients :

Puisque l'information ne traverse ni le corps ni les murs, cela rend impossible un réseau LiFi constitué d'un seul émetteur, même dans une maison. Il faudra un émetteur et un récepteur (mais pour le récepteur c'est valable aussi pour le wifi) pour chaque source ayant besoin de recevoir de la donnée.

Pour l'instant, cette technologie est très chère.

### Protocoles de la couche liaison de données

Pour rappel, la couche liaison de données est la couche 2 du modèle OSI et ses rôles sont d'assurer deux services de base :

- Elle accepte les paquets de couche 3 et les encapsule dans des unités de données appelées des trames.
- Elle contrôle l'accès au support et détecte les erreurs.

La couche liaison de données se divise en fait en deux sous-couches :

• **Contrôle de liaison logique (LLC)** : cette sous-couche supérieure définit les processus logiciels qui fournissent des services aux protocoles de couche réseau. Elle place les informations dans la trame qui indique le protocole de couche réseau utilisé pour la trame. Ces informations permettent à plusieurs protocoles de couche 3 (par exemple, IPv4 et IPv6) d'utiliser la même interface réseau et les mêmes supports.

• **Contrôle d'accès au support (MAC)** : cette sous-couche inférieure définit les processus d'accès au support exécutés par le matériel. Elle assure l'adressage de couche liaison de données et la délimitation des données en fonction des exigences de signalisation physique du support et du type de protocole de couche liaison de données utilisé.

Diviser la couche liaison de données en sous-couches permet à un type de trame défini par la couche supérieure d'accéder à différents types de supports définis par la couche inférieure. Il en est ainsi avec de nombreuses technologies de réseau local, y compris Ethernet.

Réseau	Protocole de couche réseau		
Liaison de données	Sous-couche LLC	Sous-couche LLC - IEEE 802.2	
	Sous-couche MAC	Ethernet IEEE 802.3	Réseau local sans fil IEEE 802.11
		Différentes normes Ethernet pour Fast Ethernet, Gigabit Ethernet, etc.	Différentes normes WLAN pour différents types de communications sans fil
Physique			WPAN IEEE 802.15 Différentes normes WPAN pour Bluetooth, RFID, etc.

Remarque : Au niveau de la couche liaison de données, les périphériques réseau connectés à un support commun sont appelés des nœuds.

Au niveau des normes de la couche liaison de données, les protocoles de couche liaison de données ne sont généralement pas définis par des documents RFC (Request For Comments).

Bien que le groupe IETF maintienne les protocoles et les services fonctionnels de la suite de protocoles TCP/IP dans les couches supérieures, il ne définit pas les fonctions ni le fonctionnement de la couche d'accès réseau de ce modèle.

Les protocoles et services fonctionnels de la couche liaison de données sont décrits par :

- Les organismes d'ingénierie qui définissent les normes et protocoles publics et ouverts.
- Les sociétés du secteur des communications qui définissent et utilisent des protocoles propriétaires pour tirer parti de nouvelles avancées technologiques ou d'opportunités commerciales.

Au niveau de la structure de la couche liaison de données, celle-ci prépare un paquet (provenant de la couche 3) pour le transport à travers les supports locaux en l'encapsulant avec un en-tête et un code de fin pour créer une trame.

La description d'une trame est un élément clé de chaque protocole de couche liaison de données. Il doit permettre de répondre à des questions tels que :

Quels nœuds sont en communication ?

Quelles erreurs se sont produites lorsque les nœuds communiquaient ?

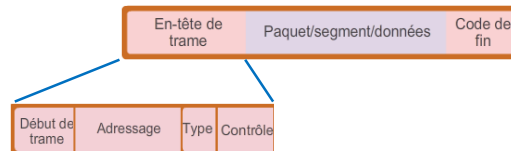
Quand commence ou se termine une communication ?

Pour ce faire, en plus des données (qui comprennent des informations telles que l'en-tête IP, l'en-tête de la couche transport et les données d'application) la trame de couche liaison de données nécessite les éléments suivants :

- **Un en-tête** : il contient des informations de contrôle telles que l'adressage et est situé au début de l'unité de données de protocole.
- **Une fin de trame** : elle contient des informations de contrôle pour la détection d'erreurs, ajoutées à la fin de l'unité.

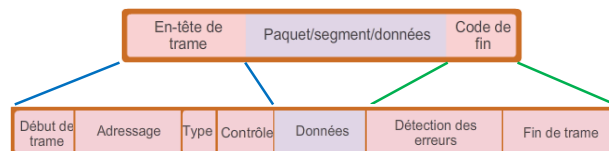


Mais que contiennent vraiment cet en-tête et cette fin de trame ?



Au niveau de l'en-tête, on retrouve les éléments suivants :

- **Indicateur de début de trame** : séquence de bits prédéfinies utilisé par la sous-couche MAC pour identifier le début d'une trame.
- **Adressage** : utilisé par la sous-couche MAC pour identifier les nœuds source et de destination.
- **Type** : ce champ permet à la sous-couche LLC d'identifier le protocole de couche 3.
- **Contrôle** : ce champ permet d'identifier les services de contrôle de flux spécifiques.



Ensuite viennent les données à transmettre bien entendu !

Au niveau de la fin de trame, on retrouve les éléments suivants :

- **Détection d'erreur** : inclus après les données pour constituer la fin de trame, ces champs de trame sont utilisés pour la détection des erreurs.
- **Indicateur de fin de trame** : séquence de bits prédéfinies utilisé par la sous-couche MAC pour identifier la fin d'une trame.

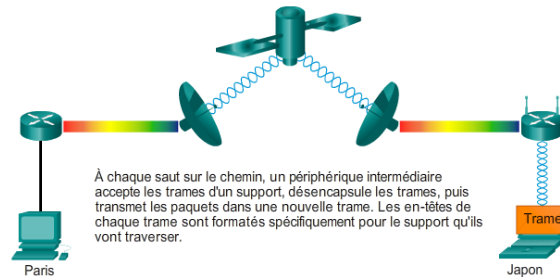
Remarque : la représentation ci-dessus est la représentation des champs d'en-tête et de fin de trame Ethernet.

## Accès réseau

Les protocoles de couche 2 spécifient l'encapsulation d'un paquet dans une trame et les techniques permettant de placer le paquet encapsulé sur chaque support et de le récupérer.

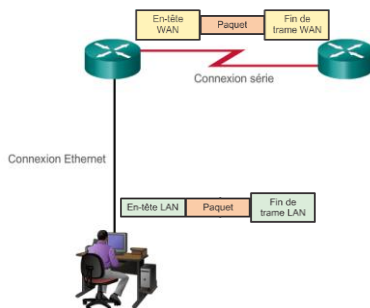
La technique utilisée pour placer la trame sur les supports et la récupérer à partir des supports est dite **méthode de contrôle d'accès au support**.

Lorsque les paquets voyagent de l'hôte source à l'hôte de destination, ils traversent généralement différents réseaux physiques.



## Accès réseau

On a donc différentes méthodes de contrôle d'accès au support qui peuvent être requises au cours d'une même communication.



Dans l'exemple ci contre, nous avons un routeur qui comporte une interface Ethernet pour se connecter au réseau local et une interface série pour se connecter au réseau étendu.

Pour traiter les trames, le routeur utilise des services de couche liaison de données afin de recevoir la trame d'un support, de décapsuler cette trame dans l'unité de données de protocole de la couche 3, de réencapsuler l'unité de données de protocole dans une nouvelle trame et de placer la trame sur le support de la liaison suivante du réseau.

Le contrôle d'accès au support est très important puisque c'est lui qui régit le placement des trames de données sur les supports.

Il existe différentes manières de réguler le placement des trames sur les supports, qui seront définies par les protocoles opérant au niveau de la couche liaison de données.

Certaines méthodes de contrôle d'accès au support utilisent des processus hautement contrôlés pour s'assurer que les trames sont placées sur le support en toute sécurité. Ces méthodes sont définies par des protocoles sophistiqués, qui nécessitent des mécanismes à l'origine d'une surcharge sur le réseau.

La méthode de contrôle d'accès au support utilisée dépend des critères suivants :

- **Topologie** : comment la connexion établie entre les nœuds apparaît à la couche liaison de données.
- **Partage de support** : comment les nœuds partagent les supports. Le partage de supports peut être de type point à point comme dans les réseaux étendus, ou partagé comme dans les réseaux locaux.

Pour rappel, il faut distinguer la topologie physique, qui désigne les connexions physiques et identifie la façon dont les périphériques finaux et les périphériques d'infrastructure sont interconnectés, et la topologie logique, qui désigne la manière dont un réseau transfère des trames d'un nœud à l'autre.

La couche liaison de données « voit » la topologie logique d'un réseau lorsqu'elle contrôle l'accès des données aux supports. C'est la topologie logique qui influence le type de trame réseau et de contrôle d'accès au support utilisé.

Les méthodes d'accès fournissent les procédures permettant de gérer l'accès au réseau de sorte que toutes les stations de travail puissent accéder au réseau. Lorsque plusieurs entités partagent le même support, un mécanisme doit être mis en place pour contrôler l'accès à ce support.

Certaines topologies réseau partagent un support commun avec plusieurs nœuds. À tout moment, des périphériques peuvent tenter d'envoyer et de recevoir des données à l'aide des supports réseau.

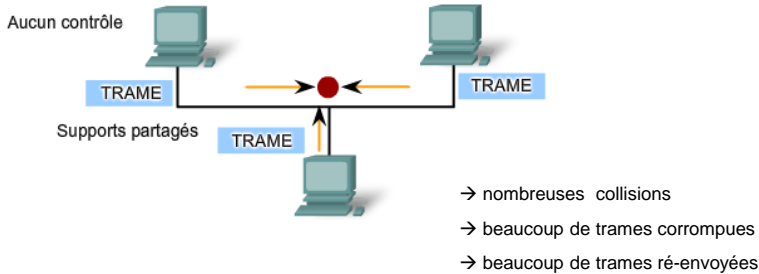
→ Il faut des règles qui régissent la manière dont ces périphériques partagent les supports.

## Accès réseau

Pour les supports partagés, deux méthodes élémentaires de contrôle d'accès au support sont utilisées :

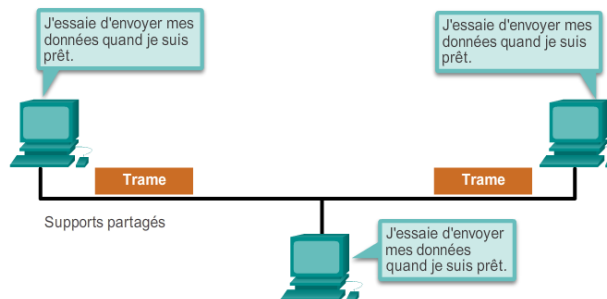
- Le plus simple c'est de ne définir aucun contrôle. C'est ce qu'on appelle une méthode d'**accès basé sur le conflit** ou **accès non déterministe** !

Dans ce cas précis, tous les nœuds sont en concurrence pour utiliser le support, mais savent comment réagir en cas de conflit.



## Accès réseau

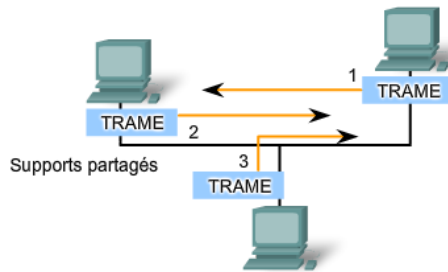
### Accès avec gestion des conflits



Caractéristiques	Contention-Based Technologies
<ul style="list-style-type: none"> <li>• Les postes peuvent transmettre des données à n'importe quel moment.</li> <li>• Des collisions existent.</li> <li>• Il existe des mécanismes permettant de résoudre les conflits pour les supports.</li> </ul>	<ul style="list-style-type: none"> <li>• CSMA/CD pour les réseaux Ethernet 802.3</li> <li>• CSMA/CA pour réseaux sans fil 802.11</li> </ul>

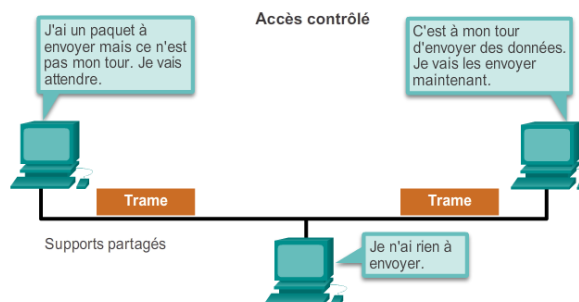
## Accès réseau

- Le seconde possibilité est d'utiliser des méthodes qui assurent un niveau de contrôle élevé, ce qui empêche les collisions mais qui provoque également une forte surcharge. C'est ce qu'on appelle une méthode d'**accès contrôlé** ou **accès déterministe** ! Dans ce cas, chaque nœud peut uniquement utiliser le support que lorsque c'est à son tour.



- pas de collisions
- débit prévisible

## Accès réseau



Caractéristiques	Technologies d'accès contrôlé
<ul style="list-style-type: none"> <li>Une seule station transmet des données à la fois.</li> <li>Les périphériques ayant des données à transmettre doivent attendre leur tour.</li> <li>Sans collision</li> <li>Utilisation possible d'une méthode de passage de jeton</li> </ul>	<ul style="list-style-type: none"> <li>Token Ring (IEEE 802.5)</li> <li>Interface de données distribuées sur fibre (FDDI)</li> </ul>



## Accès réseau

Revenons au cas des méthodes d'accès basées sur le conflit. Lorsqu'une méthode de ce type est utilisée, un périphérique réseau peut tenter d'accéder au support chaque fois qu'il doit envoyer des données.

Pour éviter que le chaos total ne règne sur les supports, ces méthodes utilisent un processus d'accès multiple avec écoute de porteuse (notée **CSMA** pour « Carrier Sense Multiple Access ») pour d'abord détecter si le support véhicule un signal.

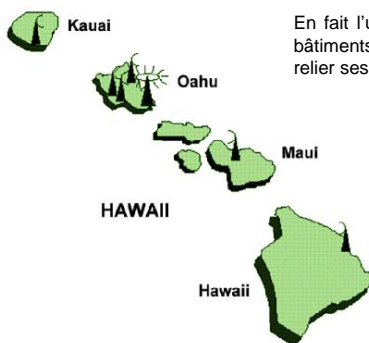
Afin d'expliquer ces méthodes de CSMA, reprenons depuis le début et voyons comment on en est arrivé là.

### La méthode Aloha

Cette technique a été développée à Aloha dans les années 70.



## Accès réseau



En fait l'université d'Hawaï, qui était composé de plusieurs bâtiments sur des îles, imagine un réseau hertzien pour relier ses entités :

- 1 station centrale (SC) + des stations secondaires (SS)
- 2 fréquences radio :
  - une pour la diffusion SC → SS
  - et l'autre pour l'accès multiples SS → SC

## Accès réseau

### Principe de l'Aloha

Dans cette méthode, lorsqu'une des SS veut transmettre une information, elle l'envoie, sans se préoccuper de vérifier la disponibilité du support.

Elle attend un ACK (« *Acknowledge* »), qui est un signal logique indiquant que l'opération demandée a été prise en compte.

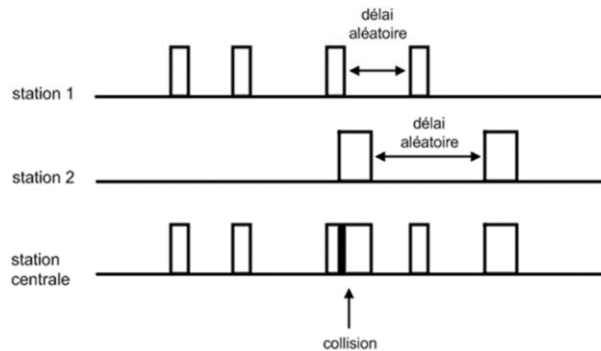
S'il y a collision, c'est-à-dire superposition des signaux de deux ou plusieurs utilisateurs, les signaux deviennent indéchiffrables et sont perdus (donc les stations ne reçoivent pas d'ACK).

Les stations réémettent l'information après un délai d'attente aléatoire.

→ **Système performant si peu de stations et faible charge !**

## Accès réseau

### Principe de l'Aloha



Cette technique est à l'origine de toutes les méthodes d'accès aléatoire.

Le CSMA

La méthode d'accès **CSMA** (« Carrier Sense Multiple Access ») est une amélioration de l'Aloha pour les réseaux câblés.

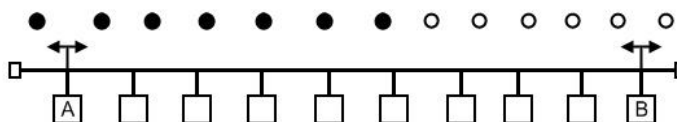
Au niveau de son fonctionnement, en l'absence d'information à transmettre, la station écoute (ou reçoit) les paquets qui circulent sur le média dans un sens ou dans l'autre.

Quand la station a besoin d'émettre un ou plusieurs paquets, elle vérifie qu'aucune trame n'est émise sur le média.

- Si c'est le cas elle commence à émettre son paquet.

- Si ce n'est pas le cas elle attend la fin de la transmission en cours avant de commencer à transmettre.

Chaque machine ayant à tout instant la possibilité de débiter une transmission de manière autonome, la méthode d'accès est distribuée : elle est dite à accès multiple (« *Multiple Access* » : MA). La machine observe le média en cherchant à détecter une porteuse (« *Carrier Sense* » : CS). Si aucune trame n'est transmise, elle ne trouve pas de porteuse.



Prenons l'exemple ci-dessus. Si le périphérique A veut envoyer des données au périphérique B. Si aucune transmission n'est détectée sur le support, commence à émettre et attend un accusé de réception (ACK) de la part de la machine B lui confirmant la bonne réception de la transmission.

Cette méthode ne supprime donc pas complètement les collisions car le temps de propagation sur le câble n'étant pas nul, la durée de vulnérabilité du paquet = temps de propagation sur la longueur du câble.

Si jamais une collision se produit, aucun ACK n'est reçu et il y a une réémission du paquet après un intervalle aléatoire.

Le CSMA/CD

La méthode du **CSMA/CD** est une amélioration du CSMA grâce à l'ajout de la CD (« *Collision Detection* ») : à l'écoute préalable du réseau s'ajoute l'écoute pendant la transmission.

Fonctionnement :

Une station prête à émettre (ayant détecté le canal libre) transmet et continue à écouter le canal.

S'il se produit une collision, elle interrompt dès que possible sa transmission et envoie des signaux spéciaux, appelés bits de bourrage (« *jam signal* »), afin que toutes les stations présentes sur le réseau soient prévenues de la collision.

Elle retentera une émission ultérieurement (après un temps d'attente aléatoire) suivant un algorithme que nous présenterons ci-après.

Cette technique engendre un gain d'efficacité par rapport aux autres techniques d'accès aléatoire car il y a détection immédiate des collisions et interruption de la transmission en cours. Les stations émettrices reconnaissent une collision en comparant le signal émis avec celui qui passe sur la ligne. Les collisions ne sont donc plus reconnues par absence d'ACK mais par détection d'interférences !

Temps d'attente aléatoire :

1 slot-time = 512 bit-time à 10Mbps et 100Mbps et 4096 bit-time à 1 Gbps  
 1 bit-time = temps d'émission d'1 bit (en fonction du débit bien entendu)

Après	1 <sup>ère</sup> collision :	attente entre 0 et 1	slot-time
	2 <sup>ème</sup> collision :	attente entre 0 et 2 <sup>2</sup> -1	slot-time
	3 <sup>ème</sup> collision :	attente entre 0 et 2 <sup>3</sup> -1	slot-time
	...		
	10 <sup>ème</sup> collision :	attente entre 0 et 1023	slot-time
de la 10 <sup>ème</sup> à la 15 <sup>ème</sup> collision :		0 et 1023	slot-time

après la 16<sup>ème</sup> tentative, la carte réseau renonce et en informe sa couche supérieure !

### Le CSMA/CA

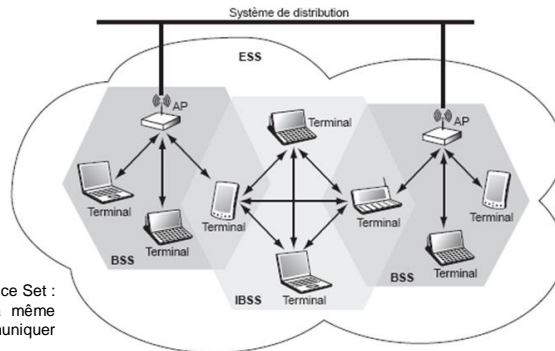
La méthode **CSMA/CA** (« Carrier Sense Multiple Access with Collision Avoidance ») est la méthode de contrôle d'accès au support utilisée par les périphériques sans fils. Le but de cette méthode est différente du CSMA/CD puis qu'ici les périphériques vont, par des mécanismes particuliers, essayer d'éviter les collisions en prévenant les autres stations qu'elles vont émettre des données .

ESS = Extended Service Set :  
ensemble de plusieurs BSS.

BSS = Basic Service Set :  
il s'agit d'un groupe de stations utilisant la même fréquence.

AP = Access Point :  
station intégrée au WLAN et au système de distribution.

IBSS = Independant Basic Service Set :  
groupe de stations utilisant la même fréquence mais pouvant communiquer directement entre eux.



Le **CSMA/CA** utilise une technique appelée **DCF** (« *Distributed Coordination Function* »). Cette contrôle le temps d'attente d'une station avant d'initier une transmission sur un support (médium) libre.

DCF attribue aussi certaines durées du slot aux participants du réseau pour d'autres actions créant ainsi une structure temporelle contraignante.

Cette procédure est l'axe central de la prévention des collisions !

DCF prend en compte divers intervalles, lors de la création de la structure temporelle :

- **Distributed Interframe Space (DIFS)** : dans un premier temps, les participants doivent surveiller le réseau pendant la durée d'un DIFS afin de déterminer si le réseau est bien libre. Pour le CSMA/CA, cela signifie qu'aucune station n'émet à portée au moment de la transmission. Le DIFS, compris entre 28 et 50  $\mu$ s, résulte du SIFS + 2 fois la durée d'un slot (*slot time*).
- **Short Interframe Space (SIFS)** : c'est le temps qu'il faut pour traiter un paquet de données. La durée dépend de la norme IEEE 802.11 utilisée et se situe entre 10  $\mu$ s et 16  $\mu$ s. Après l'envoi du paquet de données, le nœud destinataire envoie une notification si la procédure RTS/CTS est aussi utilisée. Cependant cette station attend également une période de temps fixe avant de transmettre.

- **Contention Window** : si les participants déterminent que le canal est libre, ils attendent une période de temps aléatoire avant de commencer à transmettre. Cette durée correspond à la fenêtre de contention. Cette fenêtre temporelle double à chaque collision et correspond au BEB (*Binary Exponential Backoff*), comme dans le CSMA/CD.

Une **durée de slot** (*slot time*) est le temps qu'il faut pour que les données passent à travers la longueur maximale du réseau. Pour les réseaux sans fil, cela dépend de la norme utilisée et se situe entre 9  $\mu$ s et 20  $\mu$ s.

En plus de cette technique, le CSMA/CA peut utiliser des trames spéciales appelées RTS et CTS :

Si un participant détermine que le support de transmission est libre, l'émetteur envoie alors d'abord une trame **RTS** (« *Request To Send* ») au destinataire des données. Cette trame sert à indiquer clairement, à l'ensemble des périphériques présents sur le support, qu'il veut démarrer une transmission et occupera le support de transmission pendant un certain temps.

De même, le destinataire envoie à son tour une trame **CTS** (« *Clear To Send* ») à l'expéditeur. Comme pour la trame RTS, tous les autres participants sont informés que le support de transmission est actuellement occupé. Ce n'est qu'une fois ces trames échangées que l'émetteur commence à transmettre les données (« *Data* »).

Contrairement au CSMA/CD, il n'est pas possible pour les participants à un réseau sans fil de détecter les collisions ou bien d'autres interférences pendant la transmission. Pour ces raisons, il est nécessaire que la station de réception envoie un **accusé de réception** (ACK) lorsque le paquet de données est correctement arrivé.

Si la trame ACK n'apparaît pas, l'expéditeur des données suppose qu'une complication s'est produite et renvoie le paquet de données. La station a un droit prioritaire à utiliser le média, elle n'a pas besoin d'attendre jusqu'à ce que le canal soit libre.

La trame RTS envoyée à tous les autres participants permet également de signifier (dans le champ *Duration* de la trame RTS) combien de temps le réseau sera occupé par la transmission. C'est ce qu'on appelle le **NAV** (« *Network Allocation Vector* »).

Tout autre appareil sur le support saisit cette information dans son NAV personnel. Celle-ci est traitée en interne et spécifie le moment à partir duquel une nouvelle tentative de transmission est possible.

Un NAV détermine la durée maximale pendant laquelle un expéditeur peut bloquer le support (max 33 ms). Les appareils du réseau sont inactifs jusqu'à l'expiration du NAV (ce qui permet d'économiser de l'énergie). Ce n'est que lorsque le compteur arrive à 0 que l'abonné redevient actif et vérifie si le réseau est libre.

Le NAV n'est pas seulement ajustée par le RTS, mais elle est aussi influencée par le CTS et ACK.

## Accès réseau

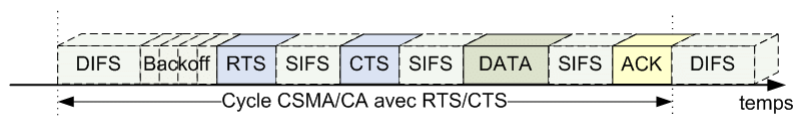
### Principe de fonctionnement du CSMA/CA

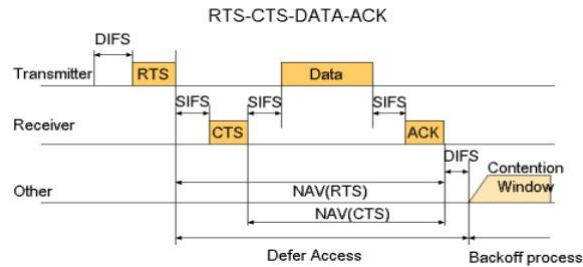
- Une station qui veut émettre va d'abord écouter le support pour voir si il est libre.
- S'il s'avère que le support de transmission est actuellement occupé, un **backoff aléatoire** est déclenché : la station attend une période de temps aléatoire jusqu'à ce qu'un nouveau contrôle commence. Toutes les autres stations, qui ne sont pas occupées à transmettre ou recevoir, font de même. (cela ne se produit que si la station n'est pas déjà consciente que le média est occupé en raison du NAV.)
- Si le réseau est libre, la station initie le **DCF** : tout d'abord, le canal est vérifié pendant toute la durée du DIFS. S'il reste libre pendant cette période, un backoff aléatoire démarre et **l'échange RTS/CTS** peut commencer. Si la trame RTS est parvenue au destinataire et qu'il n'y a donc pas eu de collision, l'expéditeur reçoit de la trame CTS la permission d'occuper le support d'émission.

## Accès réseau

### Principe de fonctionnement du CSMA/CA (suite)

- En même temps, tous les autres participants sont informés que le réseau est alors actuellement occupé. Cela les amène à augmenter à nouveau leur NAV et à attendre jusqu'à ce qu'ils vérifient une nouvelle fois si le canal est libre. Maintenant, **la station démarre la transmission**. Lorsque cela est terminé, le destinataire attend la durée d'un SIFS et répond ensuite avec une trame ACK pour confirmer la réception complète à l'expéditeur et régler le NAV à 0, le réseau est libre pour une nouvelle transmission.





DIFS: Distributed IFS  
 RTS: Request To Send  
 SIFS: Short IFS  
 CTS: Clear To Send  
 ACK: Acknowledgement  
 NAV: Network Allocation Vector  
 DCF: Distributed Coordination Function

### Trame liaison de données

Peu importe le protocole de liaison de données utilisés pour transmettre les données, dans tout les cas, chaque trame comprend 3 parties :

- un en-tête
- des données
- un code de fin

En fait, la structure de la trame et les champs contenus dans l'en-tête et le code de fin varient selon le protocole.

Il n'existe aucune structure de trame répondant aux besoins de tout le transport de données sur tous les types de supports. En fonction de l'environnement, la quantité d'informations de contrôle requises dans la trame varie selon les exigences du contrôle d'accès au support et de la topologie logique.

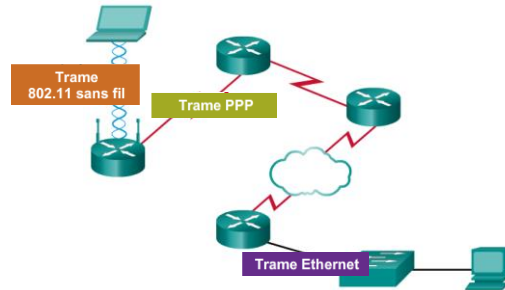
Par exemple, dans un environnement fragile, plus de contrôle sont nécessaire pour assurer la transmission. → les champs d'en-tête et de fin sont plus grands.

A contrario, dans un environnement protégé, on est sûr que la trame arrivera à destination. → les champs d'en-tête et de fin sont réduits.



Les protocoles courants de couche liaison de données sont :

- Ethernet
- PPP (Point-to-Point Protocol)
- IEEE 802.11 (sans fil)



### La trame Ethernet

Ethernet est la technologie de réseau local prédominante (définies par les normes IEEE 802.2 et 802.3).

Les normes Ethernet définissent à la fois les protocoles de la couche 2 et les technologies de la couche 1.

Ethernet est la technologie de réseau local la plus utilisée et prend en charge des bandes passantes de données de 10 Mbit/s, 100 Mbit/s, 1 Gbit/s (1 000 Mbit/s) ou 10 Gbit/s (10 000 Mbit/s).

Ethernet fournit un service non orienté connexion sans accusé de réception sur un support partagé en utilisant les méthodes CSMA/CD comme méthodes d'accès au support.

Le support partagé nécessite que l'en-tête de trame Ethernet utilise une adresse de couche liaison de données, nommée adresse MAC, pour identifier les nœuds source et de destination. Une adresse MAC Ethernet comporte 48 bits et est généralement représentée dans un format hexadécimal.

Exemple : F4-6D-04-97-96-73

Trame					
Nom du champ	Préambule	Destination	Source	Type	Séquence de contrôle de trame
Taille	8 octets	6 octets	6 octets	2 octets	46 à 1 500 octets

- Préambule : champ utilisé pour la synchronisation.
- Adresse de destination : contient l'adresse MAC du destinataire.
- Adresse source : contient l'adresse MAC source de l'émetteur.
- Type : valeur indiquant le protocole de couche supérieure qui recevra les données après la fin du processus Ethernet.
- Données : généralement un paquet IPv4 qui doit être transporté à travers le support.
- Séquence de contrôle de trame (FCS) : valeur utilisée pour vérifier l'absence d'erreurs dans la trame.

Remarque : Au niveau de la couche liaison de données, la structure de trame est presque la même pour tous les débits Ethernet.

### La trame PPP

Le protocole **PPP** (défini par la RFC 1661) est utilisé pour acheminer des trames entre deux nœuds.

Le protocole PPP a été développé en tant que protocole de réseau étendu et demeure le protocole de choix pour mettre en œuvre de nombreux réseaux étendus série.

Il peut aussi bien être utilisé sur les câbles à paires torsadées, la fibre optique ou la transmission par satellite.

Pour prendre en compte les différents types de supports, le protocole PPP établit des connexions logiques, nommées sessions, entre deux nœuds.

Le protocole PPP permet également aux deux nœuds de négocier des options au sein de la session PPP.

Cela inclut des mécanismes d'authentification, comme PAP (« *Password Authentication Protocol* ») ou CHAP (« *Challenge Handshake Authentication Protocol* »).

Il permet de faire de la compression de données.

Il offre également la possibilité d'utiliser des liaisons multiples (agrégation de liens).

## Accès réseau

Trame						
Nom du champ	Indicateur	Adresse	Contrôle	Protocole	Données	FCS
Taille	1 octet	1 octet	1 octet	2 octets	variable	2 ou 4 octets

- Indicateur : champ qui indique le début d'une trame
- Adresse : contient l'adresse de diffusion PPP standard (puisque PPP n'attribue pas d'adresses de stations individuelles).
- Contrôle : champ qui appelle la transmission des données utilisateur dans une trame non séquencée.
- Protocole : identifie le protocole encapsulé dans le champs de données de la trame.
- Données : contient le datagramme du protocole précisé dans le champ de protocole.
- Séquence de contrôle de trame (FCS) : en général 16 bits qui permettent de vérifier l'absence d'erreurs dans la trame mais peut être augmenté à 32 bits pour une détection améliorée des erreurs.

## Accès réseau

### La trame 802.11

La norme IEEE 802.11 utilise la même sous-couche LLC 802.2 et le même schéma d'adressage à 48 bits que les autres réseaux locaux 802. Cependant, il existe de nombreuses différences au niveau de la sous-couche MAC et de la couche physique.

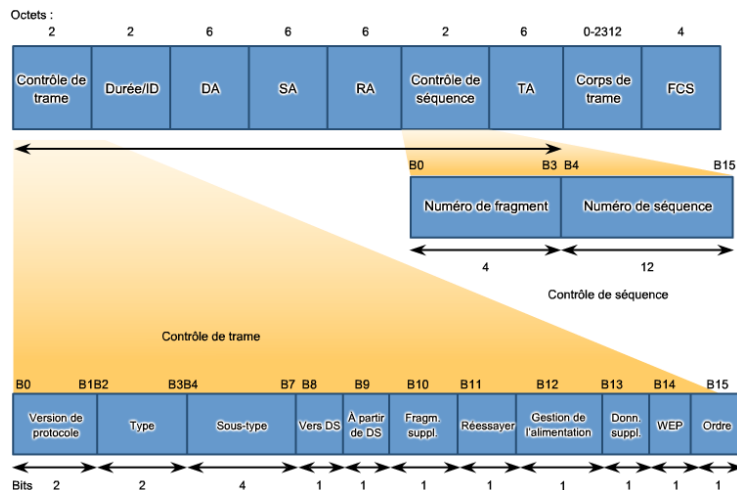
Ces différences sont dues au fait qu'il n'existe aucune connectivité physique définissable.

→ les facteurs externes peuvent interférer avec le transfert des données et le contrôle de l'accès est difficile.

Comme vu précédemment, la norme IEEE 802.11 (communément appelée Wi-Fi) utilise une méthode d'accès au support de type CSMA/CA.

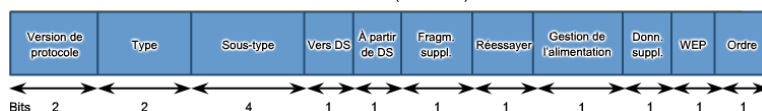
D' autres services pris en charge par les réseaux 802.11 sont l'authentification, l'association (connectivité à un périphérique sans fil) et la confidentialité (chiffrement).

## Accès réseau



## Accès réseau

Penchons nous d'abord sur le contrôle de trame (2 octets) :



- *Version de protocole* : indique la version de la trame 802.11 utilisée.
- *Type* : identifie une des trois fonctions (contrôle, données et gestion)
- *Sous-type* : indique de quel type de trame il s'agit (parmi 25 sous catégories)
- *Vers DS* : indique les trames destinées au système de distribution.
- *À partir de DS* : indique les trames quittant le système de distribution.
- *Fragments supplémentaires* : indique les trames comportant un autre fragment.
- *Réessayer* : indique si la trame est une retransmission d'une trame antérieure.
- *Gestion de l'alimentation* : indique si un nœud sera mis en mode économie d'énergie.
- *Données supplémentaires* : indique à un nœud étant en mode économie d'énergie que plus de trames sont mises en mémoire tampon pour ce nœud.
- *WEP* : indique si la trame contient des informations chiffrées WEP à des fins de sécurité.
- *Ordre* : indique que la trame utilise une classe de services strictement ordonnée (pas de réorganisation nécessaire).

Au niveau de la trame 802.11, après le contrôle de trame, on retrouve :

Octets : 2	2	6	6	6	2	6	0-2312	4
Contrôle de trame	Durée/ID	DA	SA	RA	Contrôle de séquence	TA	Corps de trame	FCS

- **Durée/ID** : selon le type de trame, indique le temps, en microsecondes, nécessaire pour transmettre la trame ou une identité d'association (AID, Association Identity) pour la station de travail ayant transmis la trame.
- **DA** : adresse MAC du nœud de destination final sur le réseau.
- **SA** : adresse MAC du nœud ayant établi la trame.
- **RA** : adresse MAC du destinataire immédiat de la trame.
- **Contrôle de séquence** : subdivisé en 2 parties
  - Numéro de séquence (4 bits) : indique le numéro de séquence attribué à la trame.
  - Numéro de fragment (12 bits) : indique le numéro de chaque fragment d'une trame.
- **TA** : adresse MAC qui identifie le périphérique sans fil ayant transmis la trame.
- **Corps de Trame** : contient les informations transportées.
- **FCS** : contient un contrôle par redondance cyclique (CRC) 32 bits de la trame.

A titre d'informations, voici les différentes possibilités de valeurs concernant les types/sous-types de l'en-tête d'une trame 802.11 :

Type	Description du type	Sous-type	Description du sous-type
00	Management (gestion)	0000	Association request (requête d'association)
00	Management (gestion)	0001	Association response (réponse d'association)
00	Management (gestion)	0010	Reassociation request (requête ré-association)
00	Management (gestion)	0011	Reassociation response (réponse de ré-association)
00	Management (gestion)	0100	Probe request (requête d'enquête)
00	Management (gestion)	0101	Probe response (réponse d'enquête)
00	Management (gestion)	0110-0111	Reserved (réservé)
00	Management (gestion)	1000	Beacon (balise)
00	Management (gestion)	1001	Announcement traffic indication message (ATIM)
00	Management (gestion)	1010	Disassociation (désassociation)
00	Management (gestion)	1011	Authentication (authentification)
00	Management (gestion)	1100	Deauthentication (désauthentification)
00	Management (gestion)	1101-1111	Reserved (réservé)
01	Control (contrôle)	0000-1001	Reserved (réservé)
01	Control (contrôle)	1010	Power Save (PS)-Poll (économie d'énergie)
01	Control (contrôle)	1011	Request To Send (RTS)
01	Control (contrôle)	1100	Clear To Send (CTS)
01	Control (contrôle)	1101	ACK
01	Control (contrôle)	1110	Contention Free (CF)-end
01	Control (contrôle)	1111	CF-end + CF-ACK
10	Data (données)	0000	Data (données)
10	Data (données)	0001	Data (données) + CF-Ack
10	Data (données)	0010	Data (données) + CF-Poll
10	Data (données)	0011	Data (données) + CF-Ack+CF-Poll
10	Data (données)	0100	Null function (no Data (données))
10	Data (données)	0101	CF-Ack
10	Data (données)	0110	CF-Poll
10	Data (données)	0111	CF-Ack + CF-Poll
10	Data (données)	1000-1111	Reserved (réservé)
11	Data (données)	0000-1111	Reserved (réservé)

Concernant les normes 802.11, pour les particuliers, on retrouve 5 normes différentes, ayant chacune leurs spécificités :

802.11	Bande de fréquence	Débit théorique maximal	Portée	Congestion	Largeur canal	MIMO
a	5 GHz	54 Mbps	Faible	Faible	20 MHz	Non
b	2,4 GHz	11 Mbps	Correcte	Elevée	20 MHz	Non
g	2,4 GHz	54 Mbps	Correcte	Elevée	20 MHz	Non
n	2,4 GHz et 5 GHz	De 72 à 450 Mbps	Bonne	Elevée et faible	20 ou 40 MHz	Oui
ac	5 GHz	De 433 à 1300 Mbps	Bonne	Faible	40 ou 80 MHz	Oui

**Attention, il faut noter que le débit relevé en pratique est largement inférieur au débit théorique maximal.** Comme vous le savez, le débit est fortement dépendant de la distance entre les appareils mais également des obstacles (comme les murs) qui se dressent sur le passage. **Dans le meilleur des cas, il faut compter sur un débit pratique environ deux fois inférieur au débit théorique.**

Les normes **802.11a/b/g** sont celles qui posent le moins de problèmes puisque leur fonctionnement est simple.

La première fonctionne dans la bande des 5 GHz, et c'est ce qui lui permet d'avoir un débit élevé pour l'époque, à 54 Mbps. Cependant, sa portée est faible puisque plus une fréquence est élevée et plus sa portée diminue. En revanche, **l'avantage de la bande des 5 GHz est sa faible congestion (= moins d'interférences) qui permet, dans les faits, d'atteindre des débits plus élevés et une meilleure stabilité de la connexion.**

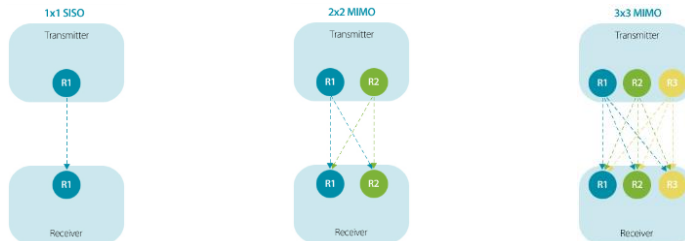
Pour information, la bande des 2,4 GHz est congestionnée puisque de nombreux appareils l'utilisent également : les micro-ondes, les téléphones DECT ou encore les appareils Bluetooth.

Concernant les normes 802.11b et 802.11g, elles sont très proches l'une de l'autre puisque la deuxième est une légère évolution de la première qui permet tout de même de rehausser fortement les débits avec un fonctionnement différent : de 11 Mbps, on passe à 54 Mbps, soit le même débit que la version 802.11a, avec une meilleure portée.

## Accès réseau

La norme **802.11n** a introduit deux éléments importants à prendre en compte pour le calcul du débit théorique maximal : le MIMO et la largeur de canal. **MIMO est l'acronyme de Multiple Input Multiple Output.**

L'utilisation du **MIMO** permet à un appareil de disposer de plusieurs antennes pour envoyer et recevoir les informations.



De base, un appareil dispose d'une seule antenne (on parle aussi de stream ou de canal spatial) pour télécharger les informations (download) et pour les émettre (upload).

Ensuite sont apparus les appareils MIMO 2x2 (2 antennes en réception et 2 en émission) voire du MIMO 3x3. Passer à 2 antennes (MIMO 2x2) permet de doubler le débit par rapport à une seule antenne.

## Accès réseau

Concernant **la largeur de canal**, plus celui-ci est large, plus il permet de faire transiter **des données dans un même cycle d'horloge.**

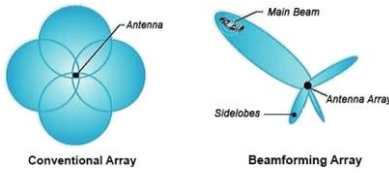
Donc pour un nombre d'antennes équivalent, un appareil utilisant un canal de 20 MHz de large sera donc moins rapide qu'un appareil faisant appel à un canal de 40 MHz de large. La largeur des canaux a commencé à évoluer depuis la norme 802.11n.

A l'heure actuelle on utilise des largeurs de bande allant jusque 160MHz !

# Accès réseau

En plus du MIMO, 2 autres technologies intéressantes sont arrivées avec le 802.11n : le *beamforming* et le *band steering*.

Pour faire simple, le *beamforming* ou focalisation a pour but d'adapter le signal émis par le routeur afin de cibler plus précisément un appareil, augmentant ainsi les débits sur celui-ci.



De son côté, le *band steering* est une technologie qui permet au routeur et au terminal mobile d'échanger des informations et de se connecter sur la bande de fréquence la plus adaptée (dans le cas où le réseau 2,4 GHz et 5 GHz portent le même SSID).



# Accès réseau

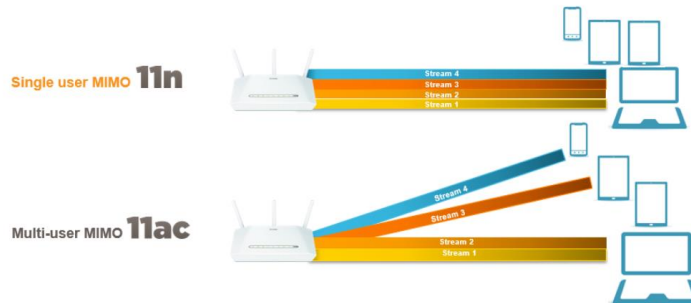
En 2017, la dernière version de la norme **802.11ac** permet d'utiliser des blocs de fréquences de 160 MHz (permettant encore de doubler la bande passante théorique par rapport à la norme de 2013) et grimpe jusqu'à quatre flux simultanés (4x4 MIMO).

	802.11n	802.11n	802.11ac Wave 1	802.11ac Wave 2	802.11ac
	IEEE Specification		Today	WFA Certification Process Continues	IEEE Specification
Band	2.4 GHz & 5 GHz	2.4 GHz & 5 GHz	5 GHz	5 GHz	5 GHz
MIMO	Single User (SU)	Single User (SU)	Single User (SU)	Multi User (MU)	Multi User (MU)
PHY Rate	450 Mbps	600 Mbps	1.3 Gbps	2.34 Gbps - 3.47 Gbps	6.9 Gbps
Channel Width	20 or 40 MHz	20 or 40 MHz	20, 40, 80 MHz	20, 40, 80, 80+80, 160 MHz	20, 40, 80, 80+80, 160 MHz
Modulation	64 QAM	64 QAM	256 QAM	256 QAM	256 QAM
Spatial Streams	3	4	3	3-4	8
MAC Throughput*	293 Mbps	390 Mbps	845 Mbps	1.52 Gbps - 2.26 Gbps	4.49 Gbps

\* Assuming a 65% MAC efficiency with highest MCS



## Accès réseau



Le 802.11ac Wave 2 ajoute également une autre nouveauté : le MU-MIMO (Multiple Users MIMO). Pour faire simple, cela permet au routeur de communiquer avec plusieurs appareils simultanément en MIMO, plutôt que chacun leur tour.

## Accès réseau

Et la compatibilité dans tout ça ?



Dans le meilleur des mondes, toutes ces normes seraient compatibles entre elles. Malheureusement, nous sommes dans le monde de l'informatique, et l'interopérabilité entre toutes les normes est parfois délicate.

Tout d'abord, **si le routeur est configuré sur la bande des 5 GHz, il ne sera pas visible par les appareils de la bande des 2,4 GHz et vice versa**. Pour outrepasser cette limitation, la plupart des **routeurs sont dual-band** pour que l'utilisateur puisse configurer deux réseaux Wi-Fi différents : un sur la bande des 2,4 GHz et un autre sur celle des 5 GHz.


### Attention aux constructeurs et à la machine marketing...







Parfois, des constructeurs annoncent des débits supérieurs à ce que la norme autorise. Par exemple, un routeur à 2,167 Gb/s sur la bande des 5 GHz... Or le maximum théorique devrait être de 1,7 Gb/s (4x 433 Mb/s) dans cette configuration. En fait ils utilisent d'un tour de passe-passe avec un QAM 1024 au lieu de 256, permettant d'augmenter les débits de 25 % environ...

Avec la norme IEEE 802.11ac, certains constructeurs parlent parfois de « triple band » pour leurs produits. Il s'agit en fait d'utiliser une bande en 2,4 GHz et deux bandes différentes sur les 5 GHz, généralement avec l'une des deux qui offre de meilleures performances. Vous pourrez donc voir jusqu'à trois réseaux en simultané.

Quand on vous annonce plus de 5 Gb/s en 802.11ac, cela ne veut en aucun cas dire que vous pourrez atteindre une telle vitesse entre un portable et un routeur : c'est l'addition des débits des bandes de 2,4 et 5 GHz!!!

Souvent les fabricants détaillent les débits qu'il est possible de tenir sur chaque bande de fréquence dans les caractéristiques techniques des produits mais par contre sur le packaging c'est généralement la vitesse maximum cumulée qui est largement mise en avant.



2.4 GHz			1000 Mbps
5 GHz-1			2167 Mbps
5 GHz-2			2167 Mbps