INF1311 : Introduction aux Réseaux Informatiques

R. DOMGA

I. Présentation générale

1. Origines et évolution des réseaux informatiques

Les réseaux informatiques sont aujourd'hui répandus partout, et font partie intégrante de la vie quotidienne des Hommes. Cette généralisation de l'utilisation des réseaux a bouleversé les habitudes et la façon dont nous communiquons, achetons, travaillons, étudions, nous amusons, etc. La naissance et le développement des réseaux informatiques dates du début des années 70 avec les nombreux projets du DoD, dont l'objectif était de connecter les ordinateurs devenu autonomes. Les informations (sous formes numériques) sont transportées d'un point à l'autre (équipements finaux/terminal) du système d'information à l'aide de supports (média) de toutes sortes et suivant des règles bien établies (protocoles). A ses débuts, les plateformes matérielles et les méthodes de transmission différaient d'un constructeur à l'autre (incompatibilité). Il a fallu développer des règles (protocoles) et standards (normes) pour permettre à des équipements quelconques (constructeurs) d'échanger à travers l'infrastructure réseau.

2. Organisation des réseaux

Les réseaux informatiques se différencient selon le type et la topologie. Le type fait principalement référence à l'étendu du réseau, ainsi on distingue les réseaux locaux dont l'étendue est réduite à un environnement géographique restreint (salle, un bâtiment). On appelle encore ce type de réseau LAN (*Local Area Network*).

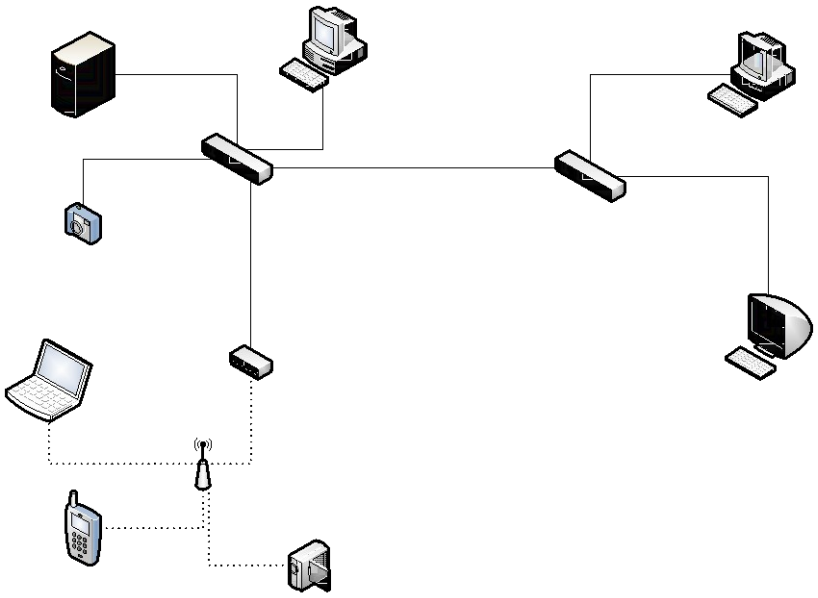


Illustration 1: Réseau Local

Lorsqu'il s'agit de transporter les informations et signaux à de grandes distances on a des réseaux grandes distances ou WAN (*Wide Area Network*). Dans un réseau local la brique de base est constituée des stations de travail (machine, serveur, imprimantes) tandis que dans un réseau grande distance elle est constituée de réseaux locaux.

NB : A l'intermédiaire (entre réseau local et réseau grande distance) on a généralement des réseaux métropolitains qui s'étendent à l'échelle d'une ville (quelques centaines de km). Ils sont encore appelés MAN (*Metropolitan Area Network*).

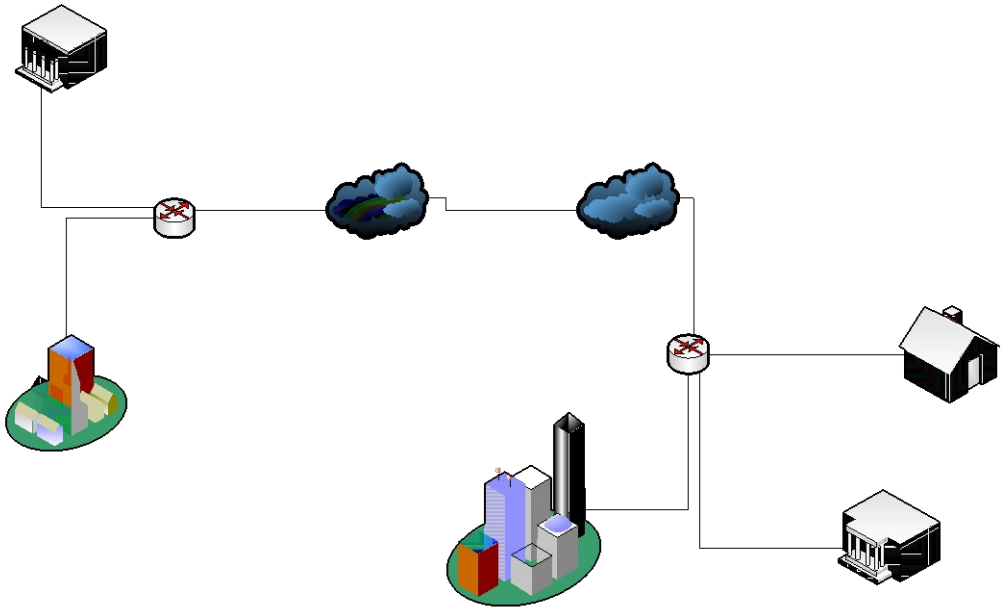


Illustration 2: Réseau grande distance

La topologie d'un réseau fait référence à l'organisation des composants du réseau. Ainsi on distingue les topologies en bus, en étoile (et étoile étendue), en anneau, en maille, etc.

a. **Topologie en bus :** tous les équipements sont connectés le long d'une tige principale, qui sert de conducteur de l'information. Cette topologie a été utilisé pour l'architecture des premiers réseaux faisant usage du câble coaxial comme média de transmission : 10 base 5 (câble coaxial épais ou thicknet) et 10 base 2 (câble coaxial fin ou thinnet). Le débit maximal de transmission dans ces réseaux était de 10Mbits/s et la distance maximale entre deux extrémités de câble est de 500m (thicknet), 185m (thinnet).

b. **Topologie en étoile :** les équipements sont organisés autour d'un nœud central qui est un

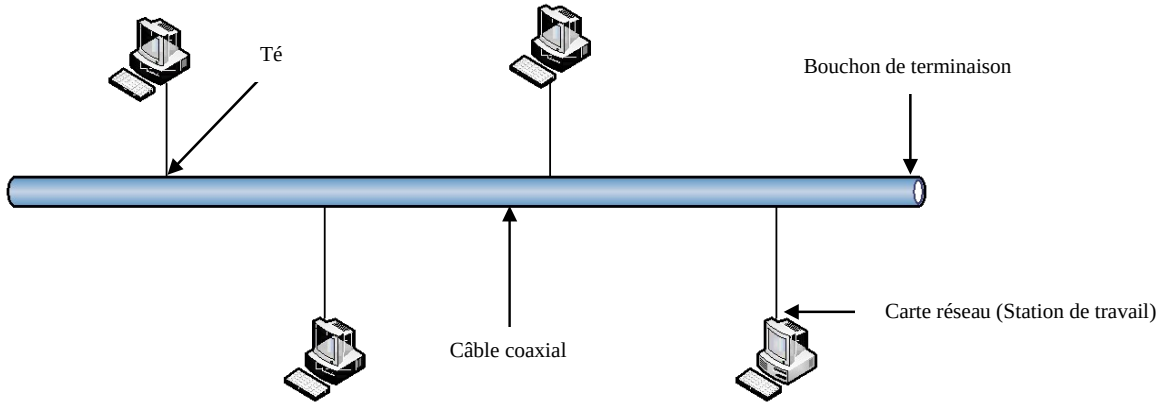


Illustration 3: Topologie en Bus

équipement spécialisé. C'est la topologie la plus utilisé de nos jours dans les réseaux locaux. L'équipement spécialisé est un commutateur (switch) ou un concentrateur (hub). L'étoile étendue est une variante de cette topologie où l'on cascade des commutateurs ou des concentrateurs entre eux.

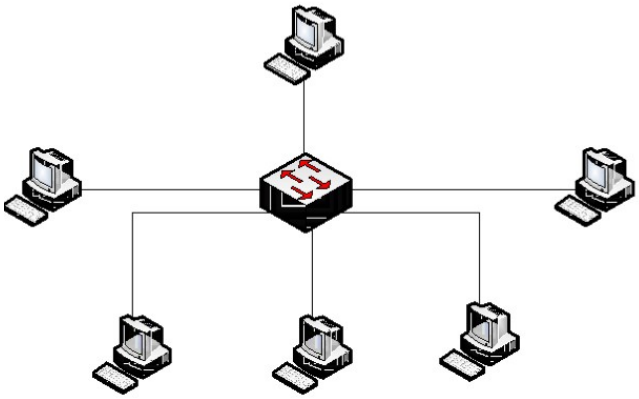


Illustration 4: Réseau en étoile simple

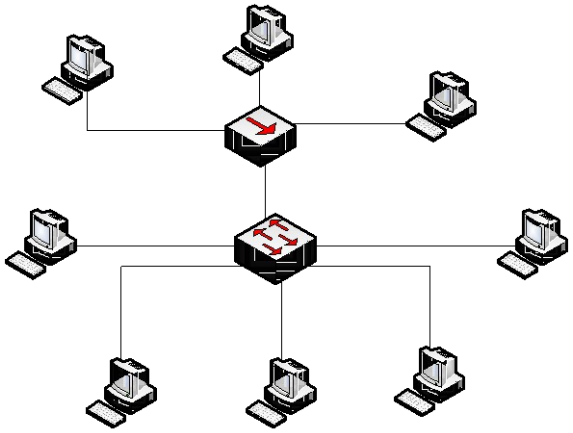


Illustration 5: Réseau en étoile étendue

c. **Topologie en anneau :** les équipements sont organisés autour d'un anneau physique. L'information circule dans un sens bien déterminé (d'un nœud à l'autre), tout nœud ne transmettant l'information que lorsqu'il s'agit de son tour. Le réseau Token Ring utilise cette topologie. Une variante de celleci est le double anneau : le réseau FDDI en est un exemple.

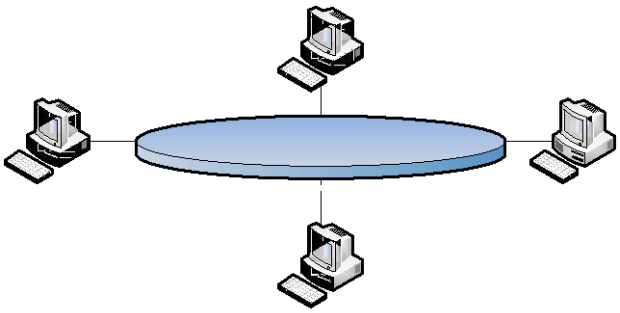


Illustration 6: Topologie en Anneau

d. **Topologie maillée :** Dans cette topologie, les nœuds sont connectés les uns aux autres dans une structure évoquant une toile d'araignée. La maille peut être partielle ou complète. Les réseaux WAN (en particulier Internet) sont construits suivant cette topologie.

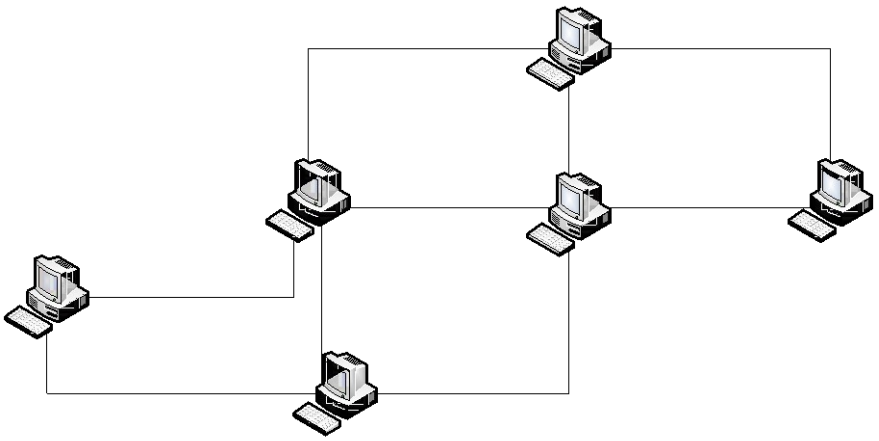


Illustration 7: Réseau maillé

NB : Toutes ces topologies sont des topologies physiques et concerne la façon dont les nœuds sont connectés physiquement. Il existe un autre type de topologie qui concerne la façon dont l'information est échangée (topologie logique). **Cf.** : Partage de jeton ou accès aléatoire (contention). La première utilise des algorithmes déterministe tandis que dans la seconde l'accès au médium est non déterministe.

3. Quelques caractéristiques des architectures réseaux :

L'un des principaux objectifs lors de la mise en œuvre d'une infrastructure réseau est d'assurer la transmission des informations à tout moment, et n'importe où. De plus, il doit offrir une large gamme d'applications et services variées (navigation, messagerie instantanée, transfert de fichier de toute sorte, vidéo à la demande, voix sur IP (*VoIP)*, outils de collaboration, réseau sociaux, etc.). Pour garantir une plateforme fonctionnelle offrant toutes ces possibilités et répondre aux attentes des utilisateurs finaux, quatre principales caractéristiques doivent être prise en compte lors de la conception/planification du réseau : tolérance aux pannes, évolutivité (*scalability*), qualité de service (QoS) et sécurité.

3.a) Tolérance aux pannes

Un réseau est tolérant aux pannes s'il limite l'impact des pannes (matérielles ou logicielles) et peut être rétabli rapidement lorsque celle-ci surviennent. Des exemples de mécanismes mis en œuvre dans les réseaux pour assurer cette propriété et la redondance (équipement et services) et l'utilisation de chemins multiples. Exemple de réseau tolérant aux pannes : réseau téléphonique, réseau Internet.

3.b) Evolutivité

Un réseau évolutif (qui passe à l'échelle) est un réseau extensible, c'est-à-dire qu'il peut prendre en compte de nouveaux utilisateurs et services sans que ceci n'affecte *gravement* les performances du réseau. Pour offrir cette possibilité, la conception des architectures réseaux sont généralement basée sur une organisation hiérarchique. Exemple de réseau évolutif : Internet. Chaque jour de milliers de nouveaux utilisateurs et fournisseurs de service se connecte à ce réseau sans que ceci n'impacte les performances des services et des utilisateurs existants.

3.c) Qualité de service

Même si le réseau est tolérant aux pannes et passe à l'échelle, la prise en compte d'application exigeant des performances et niveau de services différents peut être compromise par l'ajout de nouvelles applications. Celles ci rajoutent des délais supplémentaires dans le traitement des demandes des utilisateurs ou des services. Des exemples de services ou d'applications exigeant en qualité de service sont les transmissions audio (*VoIP*) et vidéo (streaming) qui nécessite un débit constant, et qui lorsque cette constante n'est pas assurée, dégrade la qualité de la transmission. Pour garantir cette propriété, les réseaux doivent fournir des services prévisibles, mesurables et parfois garantis. Une architecture réseau capable de transporter à la fois des données, du son et de la vidéo est appelée ***réseau convergeant***. Dans ce type de réseau la QoS est mise en œuvre par des techniques de gestion de trafic avancées telles que la classification et la « *prioritisation* » (attribution des priorités) du trafic.

3.d) Sécurité

Les réseaux étant aujourd'hui ouvert et accessible par tous, la nécessité de protéger les informations confidentielles contre toute forme d'intrusion ou d'utilisation illicite. Des techniques de chiffrement (cryptographie) permettent d'assurer la confidentialité de l'information, tandis que les techniques d'authentification assurent l'accès sécurisé aux ressources. L'intégrité de l'information est quand à elle mise en œuvre par des techniques et fonction de hachage.

II. Modèle OSI (Aproche Top Down)

4. Introduction

Il s'agit du modèle dit « de référence », il a été proposé par l'organise de normalisation ISO (International Standard Organization) dans le but de permettre la conception des protocoles pour les systèmes ouverts. Il n'est pas destiné à une implémentation spécifique mais plutôt de permettre une compréhension claire des fonctions et processus impliqués dans le réseau. Ce modèle est constitué de 7 couches comme illustré par la figure ci-contre :

Illustration 8: Modèle OSI

Pour la conception et l'implémentation d'Internet, le protocole TCP/IP à été préféré à OSI. TCP/IP reste également ouvert et n'est contrôlé par aucun organisme. Les normes sont pour la plupart publié par l'IETF (Internet Engineering Task Force) sous forme de document RFC (Request For Comments). Ces documents décrivent les protocoles et spécification formelle et technique pour leur fonctionnement. Il existe une certaine correspondance (illustrée par la figure) entre les couches du modèle TCP/IP et celles du modèle OSI.

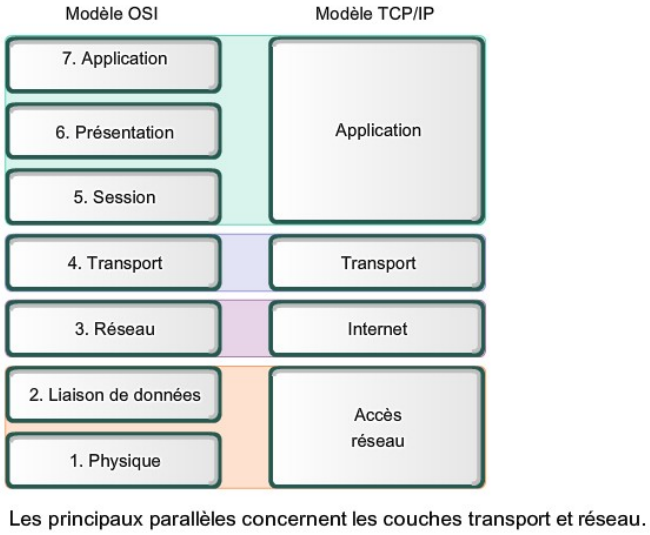


Illustration 9: Modèle TCP/IP

Chaque couche est caractérisée par un certain nombre de paramètres :

- ✓ Les protocoles utilisés à cette couche,
- ✓ Les équipements mettant en œuvre ces protocoles,
- ✓ L'unité de données (en anglais PDU : Protocol Data Unit) utilisée au niveau de cette couche,
- ✓ L'adressage utilisé au niveau de cette couche.

Ainsi en considérant le modèle TCP/IP ont rencontre au fur et à mesure que l'on descend dans les couches :

- Couche 7 : le PDU = Donnée
- Couche 4 : le PDU = Segment (informations d'adressage numéro de port)
- Couche 3 : le PDU = Paquet (informations d'adressage adresse IP ou adressage logique)
- Couche 2 : le PDU = Trame (informations d'adressage : l'adresse physique [@MAC dans le cas d'Ethernet])
- Couche 1 : le PDU = suite de bits.

NB :

a. Le processus qui consiste à ajouter les informations dans un PDU avant de le transmettre à la couche inférieure s'appelle **encapsulation.** Le processus inverse se déroule au niveau du périphérique cible (**décapsulation**).
b. Le processus de communication entre un équipement source et une cible se réalise toujours entre couches homologues.

Illustration : Echange de donnée entre un serveur et un client Web.

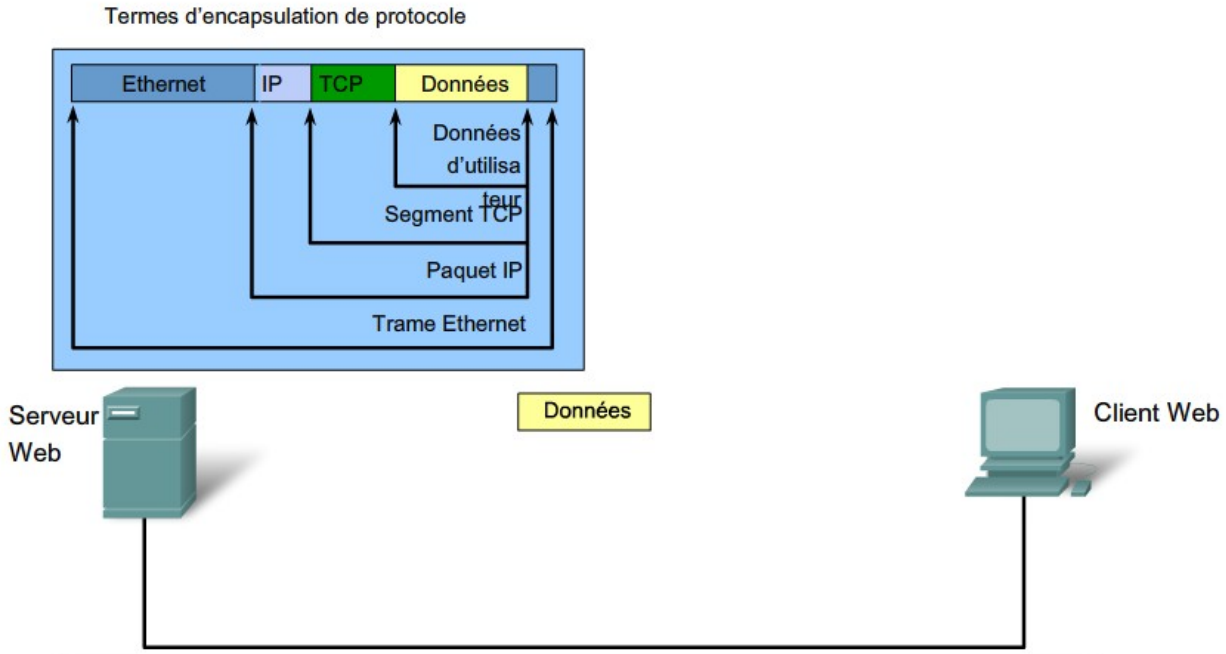


Illustration 10: Encapsulation

5. Couche applicative

Dans cette section il s'agit de la couche application tel que décrit dans le modèle TCP/IP et intègre donc les trois couches supérieures du modèle OSI (session, présentation et application).

La couche session fournit des services à la couche présentation et gère les dialogues, l'ouverture et la fermeture des sessions entres les services et utilisateurs. Une session est une connexion logiques entre deux entités nécessitant une synchronisation et regroupe un ensemble d'activités ou transactions. Les outils utilisés à ce niveau peuvent intégrer RPC, CORBA, SQL, etc.

La couche présentation assure la cohérence de représentation de l'information entre les différentes architectures matérielles du réseau (hétérogènes). Elle va donc gérer les services de codage, de cryptage et de compression de données. La convention/langage de représentation de donnée indépendante de toute architecture matérielle généralement utilisé est le codage ASN.1 (Abstract Syntax Notation One).

La couche application intègre les services et programmes utilisateurs : ces services sont mis en œuvre par des protocoles tels que : HTTP (service www) ; FTP, TFTP (transfert de fichier) ; SMTP, POP3 (messagerie électronique) ; DHCP ; DNS ; Telnet, ssh (terminal distant) ; etc. Ces services constituent

l’interface entre le réseau et l’utilisateur humain et sont généralement intuitifs c'est-à-dire que nous les utilisons très souvent sans savoir comment ils fonctionnent, cependant un professionnel de réseau doit en connaître les mécanismes sous-jacent. La plupart de ces protocoles fonctionnent en mode client/serveur. La connexion est dans ce cas toujours initiée par le client, toutefois le serveur est toujours en écoute en attentes des demandes d’éventuels clients. Ces protocoles définissent le type de message échangés entre les parties, leurs formats, la syntaxe des commandes et les erreurs qui surviennent.

6. Couche Transport

Elle se place entre les couches basses (1 à 3) et les couche hautes (5 à 7) du modèle OSI. Elle est chargée de fournir les services de livraison d'informations aux couches supérieures, en donnant la possibilité à plusieurs processus clients s'exécutant sur la même machine de communiqué en même temps avec un ou plusieurs serveurs. Pour ce faire elle s'appuie sur deux protocoles TCP et UDP. En fonction du niveau de fiabilité requis cette livraison peut être orienté connexion (TCP) ou non orienté connexion (UDP). D'autres mécanismes mis en œuvre dans cette couche sont la segmentation, l'adressage et la négociation du flux d'information.

6.a) Fonction de la couche transport :

- **Segmentation des données :** Elle est chargée de découper les données provenant des couches applicatives pour maximiser l'utilisation du canal de communication. Cette fonction est couplée avec le multiplexage des flux de communication. Elle utilise pour ce faire un champ dans l'en-tête du PDU de cette couche : le numéro de séquence (d'ordre) qui l'aide dans la reconstitution du message originel au niveau de l'équipement de réception.

- **Identification des applications :** Le flux d'information reçu dans cette couche peut provenir de diverses application de la couche 7, pour différencier ces application, la couche transport utilise un autre champ d'en-tête : le numéro de port. Ainsi chaque application répertorié se voit attribué un numéro d'identification unique. Ce numéro fonctionne en doublon : un qui identifie l'application sur la machine émettrice (port source) l'autre sur la machine destinatrice (port de destination). L'IANA (Internet Assigned Numbers Authority) est chargé de contrôler l'attribution de ces identifiants. On distingue trois blocs d'identifiant :

    - Numéro de port réservé : 0 à 1023. Utilisé par les services bien connus, généralement côté serveur de la communication.
      Ex : HTTP (80), FTP (20 et 21), SMTP (25), Telnet (23) DNS (53), HTTPS (443), TFTP (69), SNMP (161), DHCP (49) etc.
    - Numéro de port inscrit : 1024 à 49 151. Utilisé par les processus clients et sont pour la plupart octroyé par le SE ou généré dynamiquement par les applications clientes.
    - Numéro de port privés ou dynamique : 49152 à 65535. Utilisé par certaines applications particulière comme le service peer-to-peer et sont négocié dynamiquement par les parties.

  NB : La commande ***netstat [-n]*** permet d'afficher les connexions actives sur un hôte.
- **Fiabilisation des communications :** Cette couche fournit deux protocoles en fonction du niveau de fiabilité requis.

6.b) Le protocole TCP

Il dispose d'une structure de message plus complexe qu'UDP et définit également des mécanismes plus complexes. La taille du champ d'en-tête est de 20 octets et illustré par la figure ci-dessous :

En-têtes TCP et UDP

Segment TCP

Bit (0)	Bit (15) Bit (16)	Bit (31)
Port source (16)	Port de destination (16)	
Numéro d'ordre (32)		
Numéro de reçu (32)		
Longueur de l'en-tête (4) Réservé (6) Bits de code (6)	Fenêtre (16)	
Somme de contrôle (16)	Urgent (16)	
Options (0 ou 32 le cas échéant)		
DONNÉES DE LA COUCHE APPLICATION (Taille variable)		

20 octets

Datagramme UDP

Bit (0)	Bit (15) Bit (16)	Bit (31)
Port source (16)	Port de destination (16)	
Longueur (16)	Somme de contrôle (16)	
DONNÉES DE LA COUCHE APPLICATION (Taille variable)		

8 octets

Les propriétés de TCP sont :

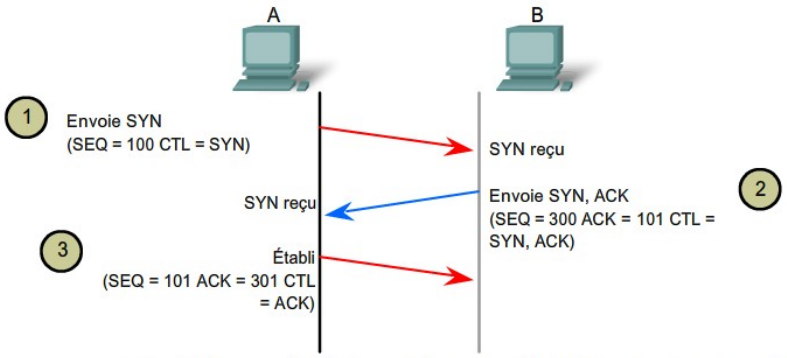
(1) L'orienté connexion : Etablissement de la connexion avant tout processus d'échange de message.

(2) L'acheminement fiable des segments : Utilise des numéros d'accusé de réception (ACK) pour acquitter les messages reçus.

(3) Livraison ordonnée des messages : Numéro de séquence

(4) Contrôle de flux : Pour contrôler l'utilisation des ressources (taille des tampons, bande passante) au niveau du serveur et gérer la vitesse de connexion. Champ d'en-tête : Taille de la Fenêtre. Ce mécanisme anticipe la perte des messages et évite de surcharger le serveur par les requêtes des clients. Les pairs peuvent négocier la taille de la fenêtre on parle de ***fenêtre glissante.***

Processus de connexion TCP en trois étapes



CTL = Indique quels bits de contrôle de l'en-tête TCP sont configurés sur 1.

6.c) Le protocole UDP

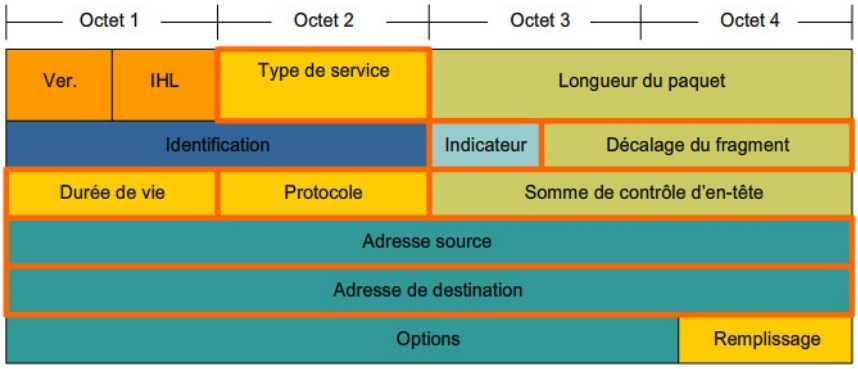
UDP est un protocole beaucoup plus simple que TCP qui ne se souci pas d'établir la connexion avant l'envoie des informations, n'envoie pas d'ACK, ne gère pas l'ordre de livraison ni le contrôle de flux. Si une application souhaite utiliser ces fonctions elle doit s'appuyer sur TCP ou (dans le cas où UDP est utilisé) les mettre en œuvre elle-même. Malgré sa pauvreté UDP est utilisé dans de contextes particuliers (VoIP : SIP port 5060 ; VoD et VoIP : RTP port 5004 ; TFTP, SNMP) est plus rapide que TCP et n'engendre qu'une faible surcharge sur réseau (8 octets d'en-tête).

7. Couche réseau

Elle définit les mécanismes devant transporter les données des utilisateurs d'un point à l'autre de l'inter réseau. Le protocole IP (autres IPX, AppleTalk) est le protocole le plus répandu pour ce transport des informations de la couche réseau : c'est un protocole routé. Il décrit la technique d'adressage utilisé pour identifier les hôtes dans le réseau ainsi que l'organisation hiérarchique du réseau. D'autres processus impliqués dans cette couche : les protocoles de routage, qui définissent les mécanismes d'échange d'information entre les routeurs.

7.a) Protocole IP

Le protocole assure un transport des informations d'un point à l'autre de manière non fiable, il doit s'appuyer sur les couches supérieures s'il a besoin de fiabilité : il est dit protocole d'acheminement au mieux et reste indépendant vis-à-vis du média de transmission. Il existe en fonction du format de message et du système d'adressage en deux versions (IPv4 et IPv6). Les champs d'en-tête pour IPv4 sont nombreux (voir figure ci contre) :



7.b) Adressage de base

Les réseaux et les hôtes au niveau de cette couche sont repérés par des adresses logiques ou adresse IP. L'objectif d'une subdivision en réseau peut être justifié par un besoin de performance, de sécurité et localité/gestion. Le système d'adressage proposé est un système hiérarchique car une partie permet de localiser le réseau (bits de poids fort) l'autre identifie l'hôte (bits de poids faible).

Format d'une adresse IP : suite de 32 bits sous forme de 4 groupes d'octets représenté en décimale pointée. En fonction de la façon dont on affecte les groupes d'octet pour représenter le réseau et/ou la partie hôte on distingue trois classes d'adresse principalement utilisé pour les réseaux de donnée.

- ✓ Classe A : Bit de poids fort à 0 0.0.0.0 à 127.255.255.255
- ✓ Classe B : 2 Bits de poids forts à 10 128.0.0.0 à 191.255.255.255
- ✓ Classe C : 3 bits de poids forts 110 192.0.0.0 à 223.255.255.255

NB : il existe la classe D (multicast) et E (expérimental) dont les adresses ne sont pas destinées à être attribuées à des hôtes spécifiques du réseau.

Adresses particulières :

- **Adresse hôte :** Identifie un équipement terminal dans le réseau.
- **Adresse réseau :** Fait référence au réseau, obtenu en remplaçant l'écriture binaire de la partie hôte par des 0.
- **Adresse de diffusion :** Permet d'envoyer une information à tous les hôtes d'un réseau particulier (ou du réseau). Deux types : diffusion généralisée (255.255.255.255) ou diffusion dirigée (spécifique à un réseau), obtenu en remplaçant l'écriture binaire de la partie hôte par des 1.

Adresses spéciales :

Certaines des adresses de ces plages (Classe A, B et C) sont réservées à une utilisation spéciale :

- **Adresse réseau et diffusion**
- **Adresse de boucle locale :** 127.0.0.1 Désigne la machine hôte elle-même.
- **Route par défaut :** 0.0.0.0
- **Adresse de lien local :** attribué à l'hôte par le SE lorsqu'aucun paramètres IP n'est explicitement défini : 169.254.0.0 à 169.254.255.255

7.c) Paramètres IP :

Toute machine pour communiquer dans le réseau a besoin d'être configuré. Celle-ci se fait en définissant les paramètres IP de ce dernier :

- **Adresse IP hôte :** Identifie un hôte de façon unique dans son réseau.
- **Masque de sous-réseau :** Permet à un hôte de calculer son propre réseau. Il peut encore être exprimé sous forme de préfixe, dans ce cas il correspond au nombre de bits qui représente la partie réseau de l'adresse IP.
- **Adresse IP de la passerelle :** sert d'équipement de sortie vers les autres réseaux.
- **Optionnel : les serveurs DNS.**

Pour consulter les paramètres IP d'un poste on utilise la commande **ipconfig [/all]** (sous Windows) ou **ifconfig** (sous Linux).

8. Couche Liaison de données

Dans les sections précédentes nous avons vu que : pour que deux hôtes échangent dans le réseau :

- la couche application génère le flux de données et présente une interface aux utilisateurs finaux ;
- Données qui seront transportées après une fragmentation et numérotation de la couche transport ;
- La couche réseau assure le voyage des informations entre les différents réseaux rencontrés (séparant l'hôte source et l'hôte destination) ;

Le rôle de la couche liaison de donnés est de préparer les données qui seront transportées sur le support physique. Etant donné la différence des supports et technologies rencontrés, l'adaptation réalisée dépendra de ceux-ci. Cette couche assure ainsi l'indépendance du protocole de couche réseau (tel qu'IP) vis-à-vis du support utilisé. Parmi les fonctions offertes par cette couche nous pouvons citer : le contrôle d'accès au support et le verrouillage de trame.

8.a) Contrôle d'accès au support

La méthode de contrôle d'accès au support (**MAC** : Medium Access Control) définit comment les trames sont placées et retirées sur un support physique. Etant donné les différentes caractéristiques des supports rencontrés, la façon dont ce dernier est partagée et la topologie physique du réseau, on distingue deux principales techniques de contrôle d'accès au support : accès contrôlé et accès basé sur le conflit.

8.a.i. Accès contrôlé

Dans cette méthode les nœuds accèdent au support tour à tour, un mécanisme est mis en œuvre pour contrôler cet accès dit déterministe (car prévisible). Bien qu'offrant l'avantage d'être organisé et prévisible, cette méthode est très souvent inefficace car offrant des débits peux élevés (chaque périphérique devant attendre son tour avant de transmettre même si aucun nœud n'est entrain de le faire).
Exemple de technologie : Token Ring, FDDI.

8.a.ii. Accès basé sur le conflit

Dans cette méthode, chaque nœud qui a des données à transmettre essaye d'accéder au support, s'il est libre la transmission est possible sinon il faut attendre. Cette méthode est dite non déterministe et très souvent des conflits surviennent entraînant des **collisions**. Pour gérer/limiter ceux-ci, des techniques sont proposées comme le CSMA (Carrier Sense Multiple Access). Exemple de technologie : Ethernet (CSMA/CD) et IEEE 802.11 (CSMA/CA).

Les méthodes d'accès basé sur le conflit offrent en général des performances meilleurs que leur semblables (méthodes contrôlés), mais celles-ci s'écroulent lorsque le réseau est surchargé.

NB : Lorsque seuls deux équipements sont connectés en point à point sur le même support la couche liaison de donnée définit le modèle de communication à mettre en œuvre : half duplex (bidirectionnel non simultané) ou full duplex (bidirectionnel simultané).

- **Half duplex :** chaque nœud impliqué sur le support peut recevoir et transmettre, mais pas simultanément.
- **Full duplex :** chacun des nœuds peut transmettre et recevoir à tout moment, éventuellement simultanément.

8.b) Verrouillage de trame

Les données sont envoyées sur le support comme un train de bit incompréhensible entant que tel, le verrouillage de trame permet de diviser ce flux en groupe de bits déchiffrable. Pour ce faire on a

besoin d'un adaptateur au niveau du nœud qui accède au réseau qui se traduit très souvent en **carte réseau.** Parmi les champs rencontrés en dehors des données provenant des couches supérieures la plupart sont des champs de contrôle indiquant :

- Quand ce produit la communication ? **Préambule ou SOF**
- Quels nœuds doivent communiquer ? **Adresses physique ou @MAC**
- Quelles erreurs sont survenues pendant la communication ? **FCS**

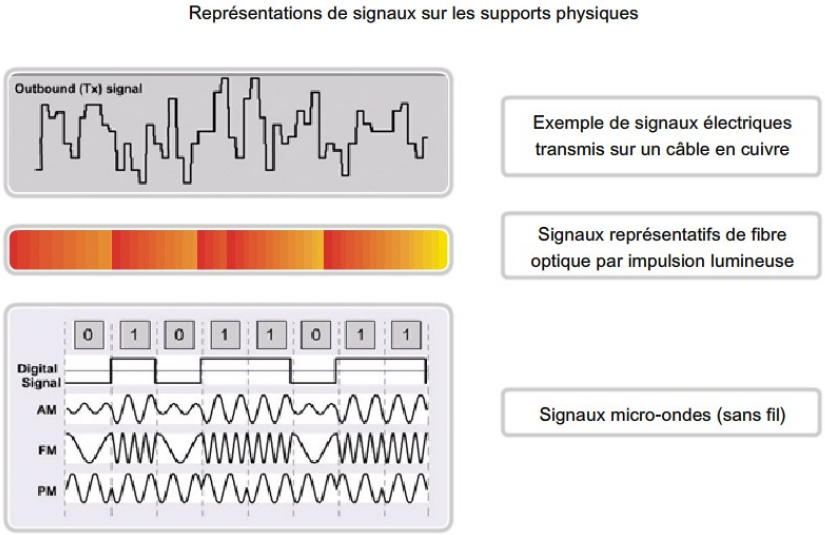
Ces champs sont organisés en en-tête et queue de bande. La structure de la trame varie avec le support physique rencontré, mais les champs génériques rencontrés sont illustrés par la figure ci-dessous.

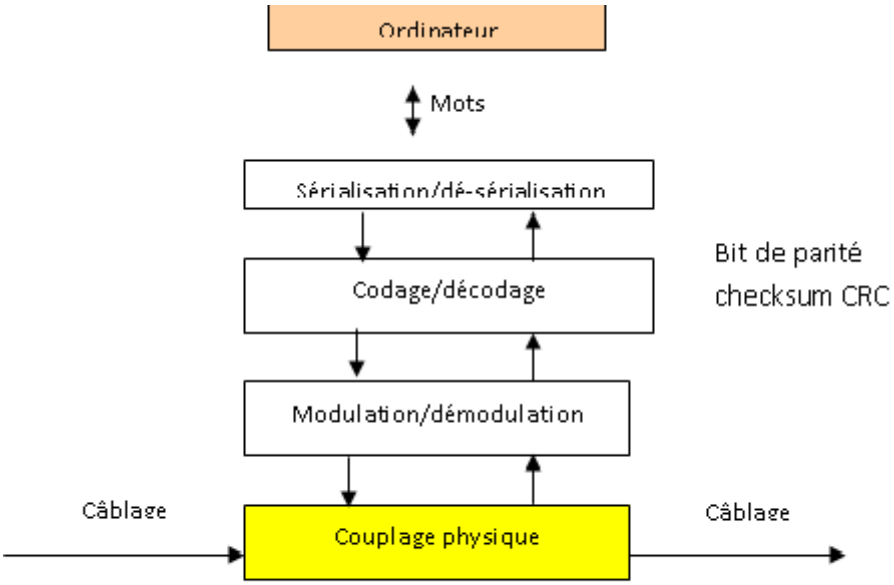
8.c) Technologies et protocoles de couche 2

Dépendant du média, les protocoles et technologies implémentés au niveau de la couche liaison de donnée qui définissent chacun sont format de trame sont : Ethernet (IEEE 802.3), HDLC, PPP, Frame relay, IEEE 802.11, RNIS, et ATM.

9. Couche physique

Elle est responsable de transmettre le flux de données provenant de la couche supérieure (liaison de données) comme un train de bits codé en un signal qui dépend du média utilisé (impulsion électrique, lumineuse ou ondes électromagnétiques). C'est également cette couche qui est responsable de ramasser ces signaux sur le support au niveau de l'équipement récepteur et les transmettre. Cette transmission met en jeu un certain nombre de concepts :





Processus mis en œuvre par la couche physique

9.a) Signalisation et Codage

9.a.i. Signalisation

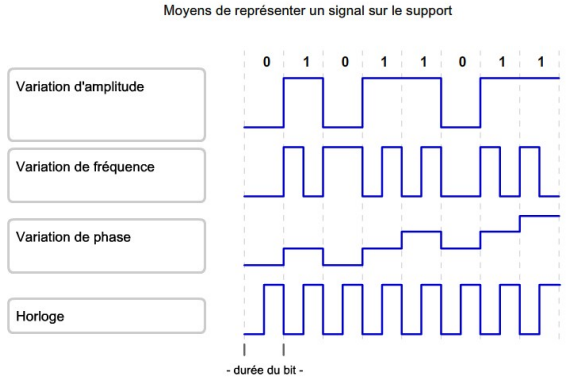
L'information est transmise de façon discrète (1 et 0), la signalisation et le codage sont deux techniques utilisées pour transporter ce dernier sur le support. La signalisation permet à la couche physique de faire correspondre aux états logiques (1 et 0) deux états physiques. Cette correspondance peut se faire au moins de deux façons :

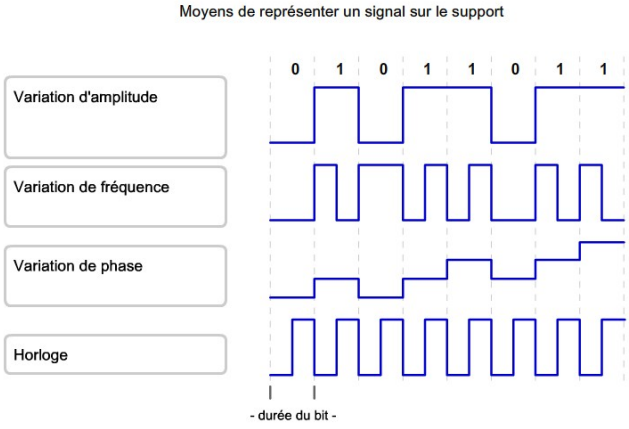
- A chaque état logique, l'on fait correspondre un état physique,
- A chaque état logique, l'on fait correspondre une transition entre états physiques.

Exemple : pour la norme RS 232 on a : 0 ≈ 3 ± 0,5 v et 1 = 6± 0,5 **v**

Pour le placement du signal sur le support, les méthodes de signalisation qui définissent les différents états physiques peuvent être :

- La modulation d'amplitude,
- La modulation de phase,
- La modulation de fréquence.



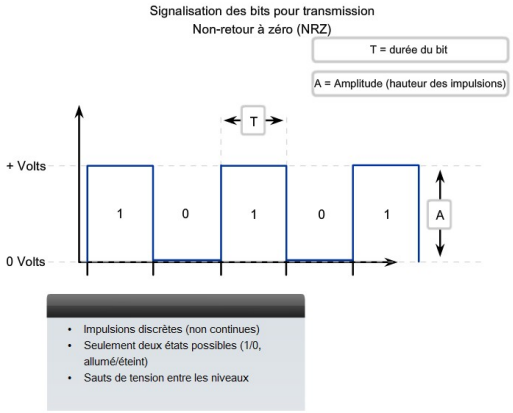


Chaque signal (binaire) envoyé sur le support met un temps spécifique d'occupation du support appelé **temps bit** ou **durée du bit.**

Quelques exemples de signalisations concrètes :

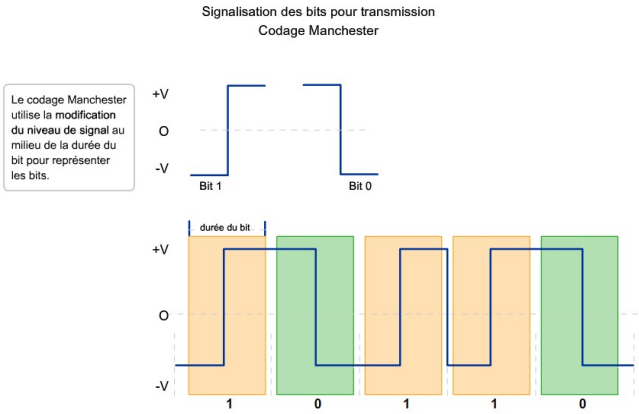
- ✓ **Le NRZ (Non Retour à Zéro) :**

  Dans cette signalisation, une valeur de tension faible représente un 0 logique, une valeur de tension élevée représente un 1 logique. Cette signalisation n'est adaptée qu'à des communications bas débits.



✓ **Le code Manchester :**

Au lieu de représenter les bits comme impulsions de valeurs de tension simples, le système de codage Manchester représente les valeurs binaires comme transitions de tension. 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



Le codage Manchester n'est pas assez efficace pour être utilisé à des vitesses de transmission supérieures, mais il est meilleur que le NRZ. C'est la méthode de signalisation employée par Ethernet 10BaseT (Ethernet s'exécutant à 10 mégabits par seconde).

9.a.ii. Codage

Lorsqu'on veut transmettre à des débits très élevés, l'utilisation d'une étape de codage avant de placer les signaux sur le support améliore l'efficacité lors de transmissions de données à plus haut débit. Le codage est une méthode de conversion d'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. Par exemple, les bits de code 10101 peuvent représenter les bits de données 0011. Bien que l'utilisation de groupes de codes introduise une surcharge sous la forme de bits supplémentaires à transmettre, ils améliorent la robustesse d'une liaison de communication.

Les avantages de l'utilisation de groupes de codes comprennent :

- Réduction des erreurs au niveau du bit
- Limitation de l'énergie effective transmise sur le support
- Meilleure distinction entre les bits de données et les bits de contrôle
- Meilleure détection d'erreur sur le support

Exemple de codage : 4B/5B

Cette technique, 4 bits de données sont transformés en symboles de code à 5 bits pour transmission sur le système de support. Ces symboles représentent les données à transmettre ainsi qu'une série de codes facilitant le contrôle de la transmission sur le support. La plupart des codes utilisés dans le système 4B/5B équilibrent le nombre de 1 et de 0 utilisés dans chaque symbole.
Cette technique, 4 bits de données sont transformés en symboles de code à 5 bits pour transmission sur le système de support. Ces symboles représentent les données à transmettre ainsi qu'une série de codes facilitant le contrôle de la transmission sur le support. La plupart des codes utilisés dans le système 4B/5B équilibrent le nombre de 1 et de 0 utilisés dans chaque symbole.

Symboles de code 4B/5B

Codes de données

Code 4B	Symbole 5B
0000	11110
0001	01001
0010	10100
0011	10101
0100	01010
0101	01011
0110	01110
0111	01111
1000	10010
1001	10011
1010	10110
1011	10111
1100	11010
1101	11011
1110	11100
1111	11101

Codes de contrôle et non valides

Code 4B	Symbole 5B
inactif	11111
début de flux	11000
début de flux	10001
fin de flux	01101
fin de flux	00111
erreur de transmission	00111
non valide	00000
non valide	00001
non valide	00010
non valide	00011
non valide	00100
non valide	00101
non valide	00110
non valide	01000
non valide	10000
non valide	11001

Comme l'illustre la figure, 16 des 32 combinaisons possibles de groupes de codes sont allouées aux bits de données, et les groupes de codes restants sont utilisés pour les symboles de contrôle et symboles non valides. Six des symboles sont utilisés pour des fonctions spéciales identifiant la transition de l'inactivité aux données de trame et le délimiteur de fin de flux. Les 10 symboles restants indiquent des codes non valides.

10. Supports de transmission

On distingue deux types de supports pour la transmission d'information dans un réseau : les supports matériels et les supports immatériels. Les normes pour les supports spécifient :

- 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.

10.a) Supports matériels

Dans cette catégorie on rencontre : les supports à base de cuivre et la fibre optique.

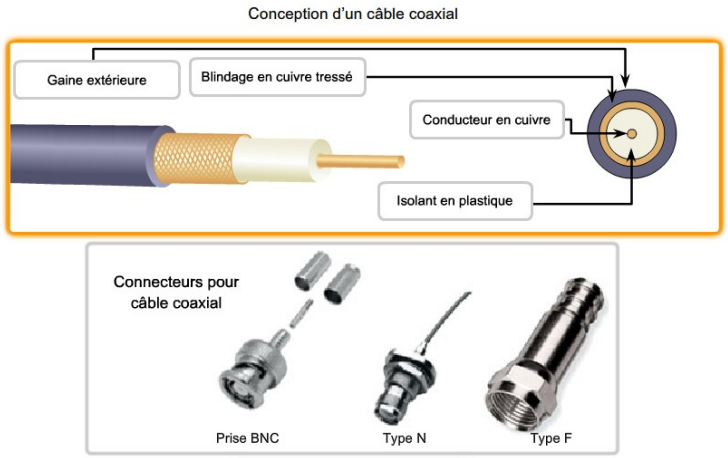
10.a.i. Support en cuivre

C'est le type de support le plus utilisé pour les transmissions dans le réseau. Il utilise des fils en cuivre. On rencontre deux types de support en cuivre : Le câble coaxial et la paire torsadée.

Câble coaxial

Il s'agit d'un conducteur principal en cuivre, recouvert d'une gaine isolante et d'un blindage tressé. Ce type de support était utilisé pour les premiers réseaux informatiques (Ethernet à au plus 10Mbits/s) avec des connecteurs de type BNC au niveau de la station de travail. Aujourd'hui il est

plus utilisé dans les réseaux étendus pour la connexion d'un client à l'équipement du fournisseur de service ou de l'opérateur télécom. **Exemple :** Communication large bande comme CATV.



Paire torsadée

Le câble à paire torsadée existe en deux variantes : une blindée (UTP : Unshielded twisted-pair), l'autre non blindée (STP : Shielded Twisted-Pair).

Le câble UTP est utilisé pour les réseaux locaux à basé de la technologie Ethernet. Il est constitué de 8 fils regroupé en 4 paires torsadées, chacun fils protégé dans une gaine en plastique souple. La torsion a pour but d'annuler les signaux indésirables dus à l'interférence générée par le passage du signal électrique dans chaque fils : **diaphonie.**

Ce type de câbles existe en plusieurs catégories en fonction de la version d'Ethernet supportée :

Catégorie 3 et 4 □ Ethernet à 10Mbits/s (10Base-T ou Ethernet)

Catégorie 5 □ Ethernet à 100Mbits/s (100Base-TX ou FastEthernet)

Catégorie 5^{e} et 6 □ Ethernet à 1000Mbits/s (1000Base-T ou GigabitEthernet)

La longueur maximale de câble sans amplification de signal est de 100m. Le connecteur utilisé est un connecteur de type RJ-45.

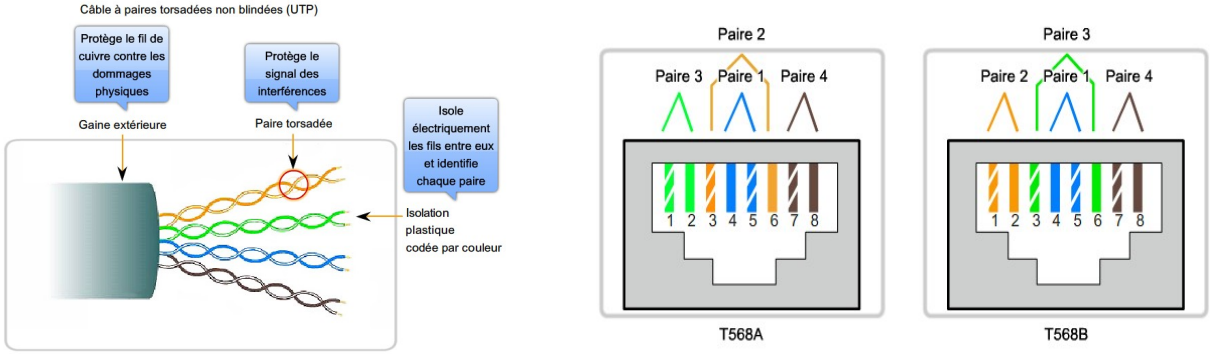
Les différentes paires de câble sont codé par des couleurs : Orange/Orange-Blanc ; Vert/Vert-Blanc ; Bleu/Bleu-Blanc et Marron/Marron-Blanc qui définissent le type de câble (croisé ou droit) à utiliser. Il existe deux normes pour la fabrication des câbles UTP : Norme T568A et Norme T568B.

Classement des fils pour la norme T568A : Vert-Blanc ; Vert ; Orange-Blanc ; Bleu ; Bleu-Blanc ; Orange ; Marron-Blanc et Marron.

Classement des fils pour la norme T568B : Orange-Blanc ; Orange; Vert-Blanc; Bleu ; Bleu-Blanc ; Vert ; Marron-Blanc et Marron.

Fabrication de câble droit : Utiliser la même norme aux deux extrémités.

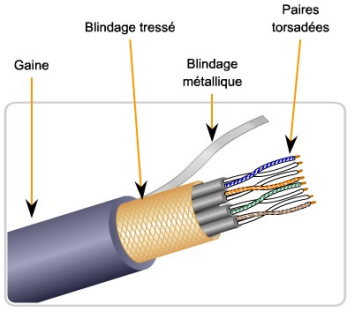
Fabrication de câble croisé : Utiliser des normes différentes aux deux extrémités.



La version blindé (STP) est utilise pour la conception des réseaux Token Ring. Le câble est mieux protégé que UTP et les coûts d'acquisition et d'installation sont plus élevés.

Câble à paires torsadées blindées (STP)

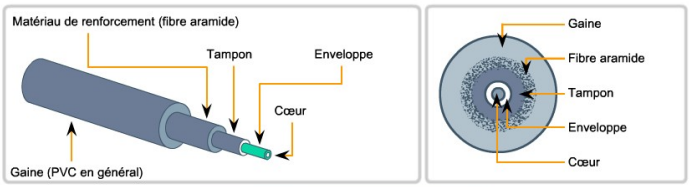
Fiches UTP RJ-45



10.a.ii. Fibre optique

La fibre optique est constituée d'un conducteur central en verre ou plastique, protégé par plusieurs couches de gaine qui empêche la lumière de s'échapper du conduit central. Ce support existe en deux variantes : la fibre optique monomodale (débits plus élevé et distances plus importantes jusqu'à 100km) et la fibre optique multimodale.

Conception d'un câble de support en fibre optique



Connecteurs pour fibre optique

La fibre optique les caractéristiques suivantes :

- Coûts d'acquisition élevés,
- Très longues distances sans régénération du signal,
- Nécessite des compétentes élevé pour la préparation des terminaisons de câble,
- Des débits de données très élevés.
- Absence d'interférence ou bruits.

Les câbles en fibre optique fonctionnent en paire pour le transport bidirectionnel du signal (câble TX et RX). Le principal problème que l'on rencontre dans le support à fibre optique est appelé **distorsion modale**, qui limite la longueur des segments de fibre multimode.

10.b) Supports immatériels

Il est essentiellement caractérisé par l'utilisation des ondes électromagnétiques et micro-ondes pour le transport du signal dans l'air. Etant donné la nature versatile du médium radio et la nature ouverte de l'infrastructure, des mécanismes de contrôle et de sécurité robuste doivent être mis en œuvre pour exploiter pleinement ces technologies. Les principales technologies existantes pour le transport des informations sont :

- IEEE 802.15.1 : Spécification Bluetooth
- IEEE 802.11 (a, b, g, n): Spécification WIFI
- IEEE 802.16 : Technologie WiMax
- GPRS, GSM, CDMA, UMTS, etc. : Réseaux Télécoms et cellulaires.
- Etc.

Des réglementations (nationales et internationales) rigoureuses sont mises en place pour le contrôle d'utilisation de ces ondes radios.