

Première partie

Chapitre 1 : Introduction et généralités

1 Généralités fondamentales

1.1 Information

L'unité de base de l'information en informatique est le **bit** (b) qui peut prendre les valeurs 1 ou 0. Un groupe de 8 bits forme un octet (o) ou byte (B). Un octet peut prendre 256 valeurs différentes.

- 1 Ko = 1000 octets
- 1 Mo = 1000 Ko
- 1 Go = 1000 Mo
- 1 To = 1000 Go

1.2 Image et vidéo

Un **pixel** (px) est l'unité minimale adressable par le contrôleur vidéo.

La **définition** d'un écran est le nombre de pixels que peut afficher une carte graphique sur un écran. Définition = nombre de pixels verticaux * nombre de pixels horizontaux.

Les **frames per second** (fps) sont le nombre d'images affichées par le moniteur chaque seconde.

1.3 Débits

L'unité du débit est le **bits par seconde** (bit/s ou bps).

2 Rôles de l'administrateur

- La gestion des besoins, du budget et des priorités.
- La gestion des ordinateurs et des périphériques.
- La gestion des performances des systèmes.
- La gestion des utilisateurs.
- La gestion des fichiers et des disques.
- La gestion des services.
- La gestion des problèmes.
- La gestion des sauvegardes et du stockage des données.
- La gestion du réseau.
- La gestion de la sécurité.

2.1 La gestion des besoins, du budget et des priorités

L'administrateur réseau doit s'adapter aux besoins de l'entreprise et fournir une infrastructure correspondant aux besoins du client mais qui soit aussi évolutif.

L'administrateur réseau doit établir un cahier des charges reprennant les besoins matériels et logiciels de l'entreprise tout en établissant un ordre de priorités. L'administrateur réseau doit ensuite comparer les ordres et choisir la solution la plus sécurisée, évolutive, tolérante aux pannes et dans le budget de l'entreprise.

2.2 La gestion des ordinateurs et des périphériques

L'administrateur réseau doit pouvoir gérer le matériel (Machines, composants, périphériques) :

- Installer les OS, paramétrer le démarrage et l'arrêt.
- Gérer les disques (initialisation, partitionnement, remplacement...).
- Ajouter ou enlever un périphérique.
- Planifier le vieillissement de matériel et prévoir son remplacement.
- Ajouter (ou supprimer) un pilote de périphérique.

2.3 La gestion des performances des systèmes

L'administrateur réseau doit savoir :

- Paramétrer et réparer les ressources pour obtenir un système parfaitement fonctionnel.
- Surveiller les ressources afin de régir avant un éventuel manque de ressources.

2.4 La gestion des utilisateurs

L'administrateur réseau doit savoir :

- Créer, modifier et supprimer les comptes utilisateurs sur les systèmes dont il est en charge.
- Modifier l'environnement de travail des utilisateurs, changer leur mot de passe, gérer les droits d'accès...
- Eduquer les utilisateurs pour qu'ils utilisent correctement les outils informatiques mis à leur disposition.

2.5 La gestion des fichiers et des disques

L'administrateur réseau doit savoir gérer les fichiers et les systèmes de fichiers présents sur les disques :

- Mettre en place et gérer les systèmes de fichiers (création, configuration des permissions, cyptage...)
- Veiller à l'intégrité des systèmes de fichiers et donc des données.
- Gérer l'arborescence des fichiers (organisation et accès).
- Surveiller l'espace disque : contrôler le taux d'occupation des disques, mettre en place des quotas...

2.6 La gestion des services

L'administrateur réseau doit savoir configurer et utiliser les services qui répondent aux besoins du client. Par exemple les services fournis par un système Linux (gestion des tâches, service d'impression...)

2.7 La gestion des problèmes

L'administrateur doit connaître ses machines et leur configuration ainsi que son réseau pour pouvoir intervenir rapidement et efficacement en cas de problème. Il doit mettre en place des outils de diagnostics permettant de l'alerter en cas de panne. Il peut être utile de préparer des fiches permettant aux utilisateurs de faire part de leur problème au service informatique.

2.8 La gestion des sauvegardes et du stockage des données

La gestion des sauvegardes est un point très important pour un administrateur réseau. Il doit être capable de récupérer rapidement n'importe quelle donnée perdue.

2.9 La gestion du réseau

L'administrateur réseau doit mettre en place des outils de surveillance du réseau pour suivre les performances et les mettre en relation avec un changement. L'administrateur réseau doit savoir mettre en place et modifier l'architecture du réseau ; il doit donc pouvoir :

- Choisir la topologie du réseau.
- Choisir les protocoles réseau.
- Mettre en place de la redondance.
- Organiser le routage et le filtrage.

L'administrateur réseau doit savoir gérer les différents éléments du réseau :

- Choisir, installer et paramétrer les éléments.
- Paramétrer le démarrage et l'arrêt de tous les systèmes
- Automatiser le processus de démarrage des nouveaux services et produits sur les machines clientes et serveurs.

2.10 La gestion de la sécurité

L'administrateur réseau doit veiller à la sécurité en prenant compte des trois axes :

- **Assurer la confidentialité** : Limiter l'accès aux destinataires autorisés
- **Garentir l'intégrité des données** : Veiller à ce que les données transmises restent intactes
- **Assurer la disponibilité** : Faire en sorte que les utilisateurs puissent accéder en temps voulu aux données

Les menaces de sécurité peuvent être :

- **Virus, vers et chevaux de Troie** : Logiciels malveillants s'exécutant sur un périphérique utilisateur.
- **Logiciels espions et publicitaires** : Logiciels qui collectent secrètement les données sur un périphérique utilisateur.
- **Attaques zero-day** : Attaques se produisant peu de temps après qu'une vulnérabilité ait été détectée.
- **Attaques de pirates** : Attaques lancées sur un périphérique utilisateur ou une ressource réseau par une personne ayant de solides connaissances en informatique.

- **Attaques par dénis de service** : Attaques concuens pour ralentir voir bloquer les applications et processus d'un périphérique réseau.
- **Interceptions et vols de données** : Attaques visant à acquérir des informations confidentielle à partir du réseau d'une entreprise.
- **Usurpations d'identité** : Attaques visant à recueillir les identifiant de connexion d'un utilisateur affin d'accéder à des données confidentielles.

Les risques pour un entreprise liés à un manque de sécurités sont :

- Des pannes réseau empêchant les transfers de données, entrainant une perte d'activité et d'argent.
- Le vol de propriété intellectuelle.
- La divulgation ou la compromission de données privées.
- La perte de données importantes très difficiles à remplacer.
- Une perte de fonds.

Pour éviter celà il faut sécuriser l'infrastructure réseau et les données :

- **Sécuriser l'infrastructure réseau** : Sécuriser matériellement les périphériques et empêcher l'accès non autorisé aux logiciels qu'ils hébergent.
 - Contrôler l'accès aux salles contenant du matériel informatique.
 - Mettre en place un pare-feu.
 - Fermer à clé toute armoire contenant du matériel informatique.
 - Mettre en place de un système de vidéosurveillance.
 - Mettre en place des bannières et utiliser des VPN pour l'accès à distance.
 - Utiliser des mots de passes cryptés.
 - Mettre en place des logs.
 - Sensibiliser les utilisateur.
- **Sécuriser les données** : Protéger les informations stockées ainsi que celles qui sont transmissent sur le réseau.
 - Mettre en place des backup de manière. Leur régularité et leur automatisation dépend de la sensibilité des données. Ils peuvent être stockés en interne, en interne dans un salle séparé, en externe ou une combinaison de ces méthodes.
 - Mettre en place des logiciel antivirus et anti-espion.
 - Mettre en place de la redondance pour éviter les pertes de données en transit sur le réseau.

3 Méthodologie de l'administrateur

3.1 La documentation

La documentation est très importante pour un administrateur, elle permet de facilement trouver la cause d'un problème et de communiquer avec ses collègues.

Le journal de bord est un document daté dans lequel sont consignées toutes les informations relatives aux opérations importantes dur le réseau.

L'administrateur doit veiller à ce qu'une copie de la documentation relative au materiel soit à proximité de ce matériel.

Il doit effectuer un repérage sur les appareils.

Il doit bien commenter son code et ses configs.

3.2 Sauvegarder

L'administrateur doit choisir le bon type, le bon logiciel, la bonne fréquence, le bon support, le bon personnel pour ses sauvgardes. Il met en place un plan de sauvegarde et un plan de recouvrement après sinistre. Une sauvgarde non testée n'a pas de valeur.

3.3 automatiser

L'automatisation d'une procédure à utiliser plusieurs fois permet de gagner du temps et réduit le risque d'erreurs.

3.4 Agir de manière réversible

Chaque action de l'administrateur réseau peut créer des problèmes, il faut donc que ces actions soient réversible rapidement. D'où l'importance du journal et des sauvegardes.

3.5 Etre proactif

L'administrateur réseau doit anticiper tout les problèmes qui peuvent survenir.

3.6 Autres qualités requise de l'administrateur

3.6.1 Savoir communiquer

L'informatitien travail rarement seul.

3.6.2 Avoir une bonne connaissance du marché

Être aux courants des changment sur le marché qui peuvent avoir une influence sur les choix de gestion du parc informatique.

3.6.3 Connaitre ses limites

L'administrateur réseau doit savoir quand il a besoin d'aide pour ne pas se retrouver surchargé.

4 Les bases

4.1 Les différentes bases

- **La base 2**, ou base binaire peut prendre les valeurs 0 ou 1.
- **La base 8**, ou base octale peut prendre les valeurs de 0 à 7.
- **La base 10**, ou base décimale peut prendre les valeurs de 0 à 9.
- **La base 16**, ou base hexadécimale peut prendre les valeurs de 0 à 9 et de A à F.

4.2 Les conversions de bases

4.2.1 Conversion base 10 en base 2

Méthode de la soustraction

1. Trouver la plus grande puissance de 2 plus petite (ou égale) que le chiffre.
2. Le soustraire au chiffre de bases.
3. Noter 1 dans la colone correspondante à l'exposant de 2 utilisé.
4. Recommencer à l'étape 1 jusqu'à avoir 0.

Exemple : 580_{10}

1. $2^9 \leq 512 < 580$
2. $580 - 512 = 68$
3. 0
4. $2^6 = 64 \leq 68$
5. $68 - 64 = 4$
6. 01001
7. $2^2 4 \leq 4$
8. $4 - 4 = 0$
9. 01001000100₂

Méthode de la division

1. Si le nombre est impair, noter 1 dans la colonne correspondante et soustraire 1.
2. Diviser par 2 et passer à la colonne suivante.
3. recommencer jusqu'à obtenir 0.

Exemple : 580_{10}

1. 580 est pair donc 0₂
2. $580/2 = 290$
3. 290 est pair donc 00₂
4. $290/2 = 145$
5. 145 est impair donc 100₂
6. $145 - 1 = 144$
7. $144/2 = 72$
8. 72 est pair donc 0100₂
9. $72/2 = 36$
10. 36 est pair donc 00100₂
11. $36/2 = 18$
12. 18 est pair donc 000100₂
13. $18/2 = 9$
14. 9 est impair donc 1000100₂
15. $9 - 1 = 8$

16. $8/2 = 4$
17. 4 est pair donc 01000100_b
18. $4/2 = 2$
19. 2 est pair donc 001000100_b
20. $2/2 = 1$
21. 1 est impaire donc 1001000100_b
22. $1 - 1 = 0$
23. On a fini : 01001000100_b

4.2.2 Conversion base 2 en base 10

On additionne chaque multiple de 2 multiplié par le chiffre lui correspondant dans l'écriture binaire Exemple 01001000100_b :

$$0 * 2^0 + 0 * 2^1 + 1 * 2^2 + 0 * 2^3 + 0 * 2^4 + 0 * 2^5 + 1 * 2^6 + 0 * 2^7 + 0 * 2^8 + 1 * 2^9 + 0 * 2^{10} \\ = 4 + 64 + 512 = 580_d$$

4.2.3 Conversion base 2 en base 8

Il suffit de faire des groupe de 3 bits en partant de la gauche et de les transformer un par un en base 8.

Exemple $001\ 001\ 000\ 100_b$:

1. $100_b = 1 * 2^2 = 4$
2. $000_b = 0$
3. $001_b = 1 * 2^0 = 1$
4. $001_b = 1 * 2^0 = 1$
5. Donc on obtient 1104_o

4.3 Conversion base 2 en base 16

On procède comme pour la conversion de la base 2 en base 8 mais en faisant des groupement de 4 bits.

Exemple $0010\ 0100\ 0100_b$:

1. $0100_b = 1 * 2^2 = 4$
2. $0100_b = 1 * 2^2 = 4$
3. $0010_b = 1 * 2^1 = 2$
4. Donc on obtient 442_h

4.3.1 Conversion base 8 en base 2

On transforme chaque chiffre en base 2 suivant une des deux techniques permettant de passer de la base 10 à la base 2 (en l'adaptant si besoin).

Exemple 1104_o :

1. $4 = 1 * 2^2 = 100_b$
2. $0 = 000_b$
3. $1 = 1 * 2^0 = 001_b$
4. $1 = 1 * 2^0 = 001_b$
5. Donc on obtient $001\ 001\ 000\ 100_b$

4.3.2 Conversion base 16 en base 2

On procède comme pour la conversion de la base 8 en base 2 sauf qu'on obtient des groupement de 4 bits.

Exemple 442_{16} :

1. $4 = 1 * 2^2 = 0100_b$
2. $4 = 1 * 2^2 = 0100_b$
3. $2 = 1 * 2^1 = 0010_b$
4. Donc on obtient $0010\ 0100\ 0100_b$

4.3.3 Autres conversions

Pour les autres connexion il suffit de passer par la base 2 puisqu'on sait tout transformer en base 2 et qu'on sait transformer la base 2 en tout.

5 La communication et les réseaux d'aujourd'hui

L'homme a toujours eu besoin de communiquer, il a donc inventé des moyens de communication ayant une portée de plus en plus grande. Aujourd'hui on a une interconnexion de réseaux fiables et rapides.

Internet a modifié notre quotidien. Avant nos principales sources de savoir étaient les livres et les personnes, aujourd'hui internet nous donne accès à plus de savoir. Internet a aussi changé notre façon de communiquer, que ce soit de façon privée ou publique.

Internet et les réseaux ont aussi modifié le monde de l'entreprise, d'abord par les réseaux interne permettant le partage de données privées simples, puis par de nouveaux moyens de communication permettant même la formation d'employés. Cette transformation a permis un gain financier pour les entreprises. Enfin internet a changé la façon dont nous nous divertissons.

5.1 Les classifications de réseaux

Il existe 2 critères permettant de classer un réseau :

- L'étendue du réseau
- La technologie de transmission

5.1.1 L'étendue du réseau

Selon l'étendue du réseau on peut avoir :

- **PAN** (*Personal Area Network*)
- **LAN** (*Local Area Network*)
- **MAN** (*Metropolitan Area Network*)
- **WAN** (*Wide Area Network*)

Réseau PAN

Taille : 1m à 10m

Etendue : Equipement proche

Technologie associées : Bluetooth

Exemple : Réseau entre gsm, kit main libre

Réseau LAN

Taille : 10 à 1km

Etendue : Batiment ou campus

Technologie associées : Ethernet, Token Ring, FDDI

Exemple : Réseau de l'ISIMs

Réseau MAN

Taille : 1km à 100km

Etendue : Villes

Technologie associées : FDDI, DQDB, MPLS

Exemple : Réseau FedMAN

Réseau WAN

Taille : + de 100km

Etendue : Pays ou continent

Technologie associées : ATM, Frame Relay, Ethernet

Exemple : Réseau BELNET



FIGURE 1 – Les différents types de réseaux

5.1.2 La technologie de transmission

On distingue deux sous types :

- La diffusion
- Le point-à-point

La **topologie physique** d'un réseau est la structure physique de celui-ci, la façon dont il est arrangé dans l'espace.

La **topologie logique** d'un réseau est la façon dont les appareils se partagent le réseau et elle dépend de la méthode d'accès au réseau.

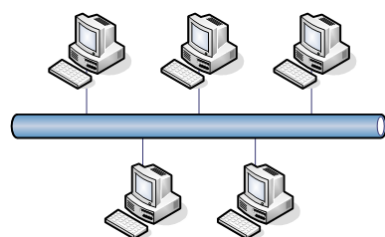
En générale quand on parle de topologie, on parle de topologie physique. C'est un schéma, une architecture ou encore un plan de ce réseau.

La topologie d'un réseau est très importante par rapport à l'évolution, l'administration et les compétences du personnel amené à s'occuper de ce réseau.

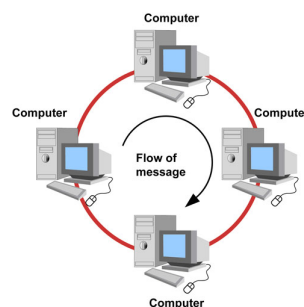
Les réseaux à diffusion

Un réseau à diffusion est composé d'un seul support de transmission partagé par tout les appareils.

Chaque message est envoyé à tous les équipement mais seul le (s) destinataire (s) le traite (nt). Ceci est appelé une transission à diffusion générale (envoi **broadcast**).



(a) Topologie en bus



(b) Topologie en anneau

Ethernet

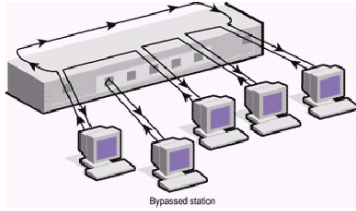
Ethernet est très utilisé, surtout en local. C'est une topologie en bus donc tout les appareils sont relié à un même support de transmission (appelé bus). Ethernet utilise les protocoles CSMA/CD (*Carrier Sense Multiple Acces with Collision Detection*) pour gérer la façon dont les données sont transmises.

Token Ring

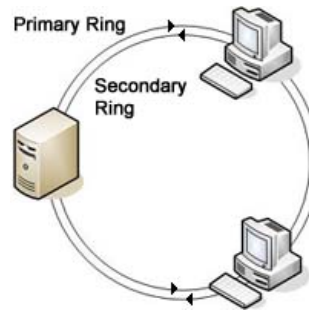
Le token ring utilise une topologie en anneau et la méthode d'accès par jeton. Seul l'appareil ayant le jeton à le droit de transmettre sur le réseau. Chaque noeud est relié à un MAUi (*Media Access Unit* ou *Multistation Access Unit*).

FDDI

Le FDDI (*Fiber Distributed Data Interface*) est prévu pour la fibre optique. Il est constitué de deux anneau (Un anneau primaire et un secondaire qui sert é détecter et corriger les erreurs). Il utilise également également le système de jeton et est capable de fonctionner même s un MAU tombe en panne.



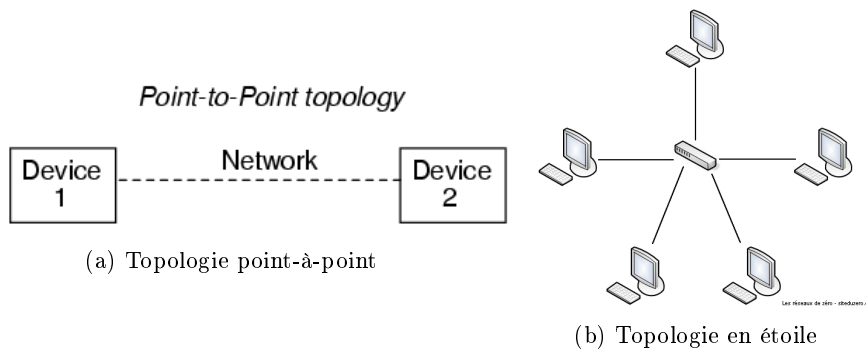
(a) Représentation d'un Token Ring



(b) Représentation d'un FDDI

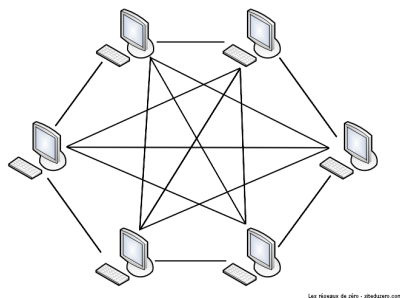
5.1.3 Les réseaux point-à-point

Un réseau point-à-point est composé d'un ou de plusieurs supports qui relient une paire d'appareil seulement. Si deux appareils ne sont pas connectés ensemble, le message va passer par d'autres appareils. Ceci est appelé une transmission à diffusion individuelle (envoi **unicast**).



(a) Topologie point-à-point

(b) Topologie en étoile



(c) Topologie maillée

5.2 Mode de fonctionnement des réseaux

5.2.1 Modèle client-serveur

Un appareil qui communique sur le réseau est appelé hôte. Un hôte peut être soit serveur, soit client soit les deux en fonction des logiciels installés.

Un **serveur** est un hôte capable de fournir des données. Il est passif, il est

constamment prêt à répondre à une requête d'un client grâce à un démon.
 Un **client** est une hôte capable de d'aller chercher des données sur un serveur.
 Il effectue une requête auprès d'un serveur pour obtenir des données ensuite il attend une réponse.

5.2.2 Modèle Peer to Peer

Les hôtes fonctionnent en tant que client ou en tant que serveurs aux autres simultanément.

Avantages du P2P

- Facile à configurer
- Moins complexe
- Coûts plus faible
- Pratique pour les tâches simples et les réseaux de petite envergure

Inconvénients du P2P

- Pas d'administration centralisée
- Peu sécurisé
- Non évolutif
- Risques du ralentissement (chaque hôte est serveur et client)

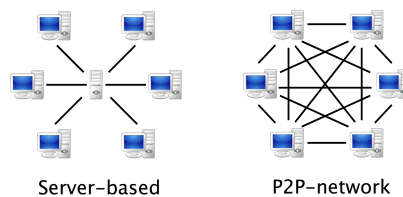


FIGURE 5 – P2P vs client-serveur

5.3 Les composants des réseaux

Peu importe son infrastructure, un réseau sera toujours composé des 3 catégories de composants suivants :

5.3.1 Les périphériques

- **Les périphériques finaux** ou hôtes. Ils servent d'interface entre le réseau et les utilisateurs.
- **Les périphériques intermédiaires** qui connectent les périphériques finaux et s'occupent de la transmission des données.

5.3.2 Les supports de transmissions

- Il peut être de plusieurs types :
- Cable en cuivre

- Fibre optique
- Transmission sans fil

En fonction du support le codage des données sera différent (impulsion électrique, impulsion lumineuse, onde électromagnétique. . .)

5.3.3 Les services et les processus

Ce sont les programmes exécutés sur les périphériques.

Un service fournit des informations suite à une requête.

Un processus fournit les fonctionnalités qui dirigent et déplacent les messages à travers le réseau.

5.4 Les symboles

Les schémas sont pratiques pour représenter un réseau. On a donc inventé des symboles reconnaissables par tous pour représenter les différents composants vu au point précédent :

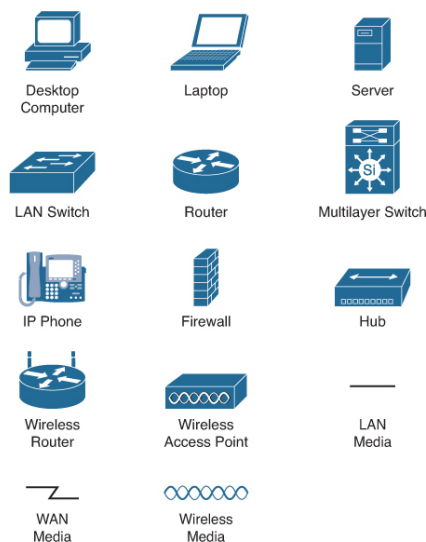


FIGURE 6 – Les différents icônes représentant les composants d'un réseau

Une **carte réseau** (NIC) Fournit la connexion physique à un périphérique.

Un **port physique** est un connecteur sur un périphérique par lequel celui-ci est connecté au réseau.

Une **interface** est un port spécifique d'un périphérique interréseau qui se connectent à des réseaux individuels.

Sur un **diagramme de topologie physique** on indique la configuration physique des périphériques, des ports, des câbles. . .

Sur un **diagramme de topologie logique** on indique les périphériques, les ports et le schéma d'adressage IP.

5.5 Internet, le seul vrai

Internet est un ensemble mondial de réseaux interconnectés qui coopèrent pour échanger des informations en utilisant des normes cohérentes et communément reconnues.

Il a donc fallu créer des normes et une structures et ce sont des organisations comme l'IETF, l'ICANN ou l'IAB qui s'en sont chargées.

Un **intranet** est un LAN privé grâce auquel une entreprise communique des information en interne.

Un **extranet** permet à une entreprise de communiquer des données privées avec d'autres entreprises.

Pour être connecté à internet, un particulier doit passer par un FAI qui peut lui permettre d'accéder à internet par différentes manières :

Par câble

En utilisant les câbles coaxiaux utilisés pour la télédistribution, on fournit un accès internet haut débit via un modem spécialisé qui sépare les différents signaux.

Par xDSL (*Digital Subscriber Line*)

En utilisant les câbles téléphoniques, le xDSL fournit un accès à internet par la séparation de trois canaux : Le premier pour les appels ; Le second plus rapide pour le download ; Le troisième un peu moins rapide pour l'upload. Sa vitesse dépend de la qualité du câble et de la distance avec la centrale téléphonique.

- L'**ADSL** (*Asymmetric DSL*) utilise une bande de fréquence en dessous de celle des appels pour connecter l'utilisateur en même temps qu'un éventuel appel téléphonique.
- Le **VDSL** (*Very-high-bit-rate DSL*) permet d'atteindre 13 à 55 Mb/s en download et 1,5 à 8 Mb/s en upload, ou 34 Mb/s en connexion symétrique
- Le **VDSL** permet d'atteindre 100Mb/s en full-duplex.

Par fibre (*FTTx pour Fiber to the x*)

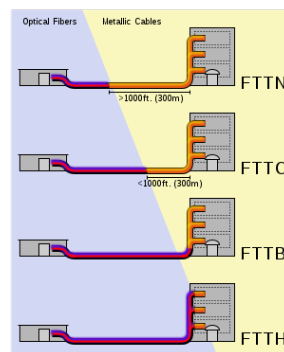


FIGURE 7 – Fiber To The x

La fibre optique permet des débits bien plus importants que les câbles et ses performances ne dépendent pas de la distance à parcourir. Il s'agit donc de l'amener au plus près du client.

- **FTTN** : *Fiber To The Neighbourhood*
- **FTTC** : *Fiber To The Curb*
- **FTTB** : *Fiber To The Building*
- **FTTH** : *Fiber To The Home*

Par satellite

Internet par satellite est accessible même pour les habitations isolées à condition qu'aucun obstacle ne se trouve entre l'antenne et le satellite. Il est très coûteux à installer mais fournit des débits importants et son déploiement est immédiat.

Par cellulaire

En utilisant les réseaux de téléphonies mobiles on fournit un accès à internet partout où le réseau cellulaire est disponible. C'est très pratique pour les personnes en déplacement ou qui n'ont pas d'autre solution. Son débit dépend du téléphone, de l'antenne et de la distance les séparants.

Par 3GPP (*3rd Generation Partnership Project*)

Grâce à la coopération d'organismes de standardisations tels que l'UIT, l'ETSI, l'ARIB/TTC, le CCSA, l'ATIS et le TTA des spécifications techniques pour les réseaux 3G et 4G ont été mises en place. Ces organisations veillent aussi à la maintenance et au développement des normes GSM (GPRS, EDGE, UMTS et LTE).

Par ligne commutée

Cette technologie est l'ancêtre de l'ADSL. Comme l'ADSL, elle requiert une ligne téléphonique et un modem. La connexion se fait par un appel au numéro de téléphone du FAI. Les débits sont donc faibles et le téléphone est inaccessible pendant ce temps.

Par WiMax (*Worldwide Interoperability for Microwave Access*)

En utilisant les ondes radio on peut fournir un accès à internet haut débit sur plusieurs kilomètres autour d'une antenne. Pour augmenter la distance entre le point de collecte et l'utilisateur on met en place des liaisons point-multipoint. Le débit maximum du WiMax varie entre 70 et 240 Mb/s partagé entre les utilisateurs raccordés à une même station, mais sont sensibles à de nombreux facteurs, comme par exemple les obstacles qui influencent grandement le débit. Ce standard, créé par Intel et Alvarion est ratifié par l'IEEE (*Institute of Electrical and Electronics Engineers*) sous le nom IEEE-802.16. Le WiMax est adapté pour les zones rurales car il permet de s'affranchir des limitations de l'ADSL, ne nécessite pas de travaux importants et permet de fournir un accès à internet nomade grâce à des bornes WiFi.

Pour être connecté à internet, une grosse entreprise utilise des moyens plus adaptés, tels que :

Par xDSL

Grâce au SDSL (*Symmetric DSL*) on peut fournir les mêmes débit en download et en upload.

Par ligne louée spécialisée

En reliant des bureaux distinct on permet l'échange plus rapide de données interne à l'entreprise. Cette solution est plus honoreuse. On trouve les lignes de E0 (64kb/s) à E4 (140Mb/s) en Europe et les lignes T1 (1,544Mb/s) à T4 (275Mb/s) aux USA.

Par fibre

Le service Ethernet sur fibre est très rapide et peu coûteux par rapport à ses performances, mais il n'est pas disponible pour tous.

Par ligne commutée

Le service par satellite n'est à privilégier que si aucun autre service par câbles n'est disponible car il est plus lent, plus coûteux et moins fiables que les solutions câblées.

5.6 Les réseaux d'hier et d'aujourd'hui

On parvient aujourd'hui à faire converger des réseaux qui étaient hermétiques entre eux par le passé. Avec ce réseau convergent on peut faire transiter n'importe quel type de donnée par le même canal. De nouvelles normes ont été mises en place. Pour pouvoir faire transiter plusieurs communications en même temps sur un réseau, on utilise pour la segmentation et le multiplexage.

La **segmentation** est le fait de découper une donnée en parties permettant d'entremêler les données. Le fait d'entremêler ces paquets s'appelle le **multiplexage** et permet de faire passer plusieurs communications en même temps sur le réseau et d'augmenter la fiabilité car les paquets ne passent pas forcément par le même chemin et les erreurs sont plus faciles à corriger. Par contre ces techniques sont plus complexes à manipuler.

Dans le contexte actuel l'architecture réseau désigne l'infrastructure, les services et les normes utilisées pour faire transiter des données sur le réseau. On essaie de concevoir les architectures selon la règle des 5 neufs (99,999% de disponibilité). Les architectures sous-jacentes doivent donc faire attention à :

5.6.1 La tolérance aux pannes

L'utilisateur veut être constamment connecté, il faut que le réseau limite l'impact des pannes. On utilise donc la **redondance**.

5.6.2 L'évolutivité

Il faut que les performances du réseau ne diminuent pas quand on ajoute des utilisateurs. Pour régler ce problème on utilise un **modèle hiérarchisé à plusieurs couches**.

5.6.3 La qualité de service

L'utilisateur veut une qualité de réseaux stable et ininterrompue. On utilise pour ça des **niveaux de priorités** qui classe les types de communications selon leur importance.

5.6.4 La sécurité

Les exigences en matière de sécurité ont évolué, il faut donc mettre en place ou adapter des **moyens de sécurisation adéquats**.

5.7 Les réseaux et les nouvelles tendances

De nouvelles tendances technologiques apparaissent, obligeant les réseaux à s'adapter.

5.7.1 Le BYOD

BYOD signifie *Bring Your Own Devices* est une tendance qui commence à se répandre et qui consiste à apporter son propre matériel informatique au travail.

5.8 La virtualisation

La **virtualisation** consiste à faire fonctionner différentes applications ou OS sur un même serveur physique.

Ses avantages sont :

5.8.1 Avantages et inconvénients

- Consolidation et rationalisation d'un parc de serveur car il est possible de réunir plusieurs applications sur un même serveur.
- Rationalisation des coûts en matériel et donc aussi en électricité.
- Portabilité des serveurs car une machine virtuelle peut être déplacée sans avoir à déplacer le serveur.
- Administration simplifiée.
- accélération des déploiements de systèmes et d'applications.

Mais ses désavantages sont :

- Coût du matériel important car pour une virtualisation efficace il faut un serveur multi-cœurs avec beaucoup de RAM.
- Panne de plusieurs services si un serveur tombe en panne.
- Compromission de toutes les VM présentes sur le serveur si un hacker a accès à celui-ci.

5.8.2 Les différents types d'hyperviseur

L'**hyperviseur de type 1** se place entre les VM's et le matériel physique. Il possède son propre noyau sur lesquels tournent les applications et il s'administre depuis une interface.

Exemple : VMWare vSphere

L'**hyperviseur de Type 2** ou architecture hébergée fonctionne comme une application sur un OS, les performances sont donc réduites mais l'étanchéité

entre les OS installés sont parfaits.

Exemple : VMWare Workstation

5.9 Le Cloud Computing

Le **Cloud Computing** consiste à utiliser des ressources informatiques situées sur un serveur distant moyennant paiement. Cela permet de soulager les ordinateurs locaux qui communiquent avec le Cloud grâce à un navigateur internet, ce qui permet d'utiliser le Cloud sur n'importe quel périphérique. On s'en sert aussi pour stocker des informations.

5.9.1 Les différents types de Cloud

Le **Cloud personnalisé** fournit des applications et des services répondant aux besoins d'un secteur spécifique.

Le **Cloud public** fournit des applications et des services accessibles par tous, il utilise Internet pour fournir ses services qui peuvent être gratuits.

Exemple : Dropbox

Le **Cloud privé** fournit des applications et des services réservés à une entité. Il est accessible via le réseau interne de l'entité ou grâce à une entreprise tiers suivant un protocole de sécurité très stricte.

Exemple : Amazon Web Service

Le **Cloud hybride** est composé d'un minimum de deux types de clouds différents mais indépendants donc les droits d'utilisations dépendent des droits de l'utilisateur.

5.9.2 Les avantages du Cloud computing

- La flexibilité car les utilisateurs peuvent accéder aux services à tout moment et partout.
- La réactivité et la rapidité de déploiement car le seul matériel nécessaire est celui pour accéder au Cloud.
- Des coûts d'infrastructures réduits car le matériel n'est plus à gérer sur le site.
- La création de nouveaux business models car ces ressources facilement accessibles permettent aux entreprises de réagir rapidement aux besoins de leurs clients et de développer des stratégies pour pénétrer de nouveaux marchés.

5.10 Le CPL

Le **CPL** (*Courant Porteur en Ligne*) permet de connecter un bâtiment via son réseau électrique un peu comme la technologie DSL. Cela permet de réduire les coûts en électricité et en matériel. Les utilisateurs peuvent se connecter en LAN depuis n'importe quelle prise courant, même si ce câblage n'est pas prévu pour ça, c'est une bonne alternative lorsque le réseau sans fil n'est pas une option.

5.11 Le Big Data

Le **Big Data** est né du besoin des chercheurs à analyser le monde grâce à un nouvel ordre de grandeur permettant l'utilisation des données. En effet nous produisons $2.5 \cdot 10_{18}$ octets de données par jours et le big data est une solution pour pouvoir exploiter ces données. Le Big Data répond à la règle des 3V :

- Le **Volume** important de données à traiter.
- La **Variété** des données à traiter.
- La **Vélocité** à laquelle les données doivent être traitées.

Le Big Data est utilisé dans de nombreux domaines comme la surveillance ou la statistique qui permettent aux entreprises de mieux se rendre compte des envies des clients.

Deuxième partie

Chapitre 2 : Communication et protocoles réseaux

6 Généralités sur les réseaux

6.1 Règles de communication

Pour que plusieurs périphériques soient en réseau il faut les connecter physiquement, mais cette connexion physique n'est pas suffisante pour qu'ils puissent communiquer, il leur faut une convention de langage. Peu importe le mode de communication, ils ont en commun trois éléments :

- L'**émetteur** qui envoie un message à un autre périphérique.
- Le **récepteur** qui reçoit le message de l'émetteur.
- Le **support de transmission** qui est le chemin que le message utilise pour aller de l'émetteur au récepteur.

Les protocoles doivent être respectés pour que l'échange d'information puisse se produire. Un protocole doit respecter certaines conditions :

6.1.1 Le codage du message

Le **codage** consiste à transformer des informations en un format convenable pour la transmission et adapté au support. Le **décodage** consiste en le processus inverse, il permet d'interpréter les informations reçues.

6.1.2 Le formatage et l'encapsulation des messages

Les messages envoyés doivent correspondre à un certain **format** selon leur type. L'**encapsulation** consiste à placer le format du message dans une trame avant de transmettre le message et la **décapsulation** est le processus inverse à la réception de celui-ci. Un message mal formaté ne sera pas livré ni traité par le destinataire.

6.1.3 La taille des messages

La **taille des messages** est limitée par ce que le destinataire peut traiter et comprendre en une seule fois, il faut donc décomposer un grand message en plusieurs trames qui doivent respecter des impératifs strictes sous peine de ne pas être livrées. L'hôte recompose le message après avoir désencapsulé les trames.

6.1.4 La synchronisation des messages

La **méthode d'accès** détermine le moment où le périphérique peut communiquer sur le réseau pour éviter que deux communications se collisionnent et que les communications doivent recommencer.

6.1.5 Le contrôle de flux

Le **contrôle du flux** permet aux périphériques de se mettre d'accord sur la synchronisation du flux pour parvenir à communiquer.

6.1.6 Le délai d'attente de la réponse

Les périphériques sont prévus pour agir d'une certaine façon si après un **délai d'attente** trop important ils n'ont pas reçu de réponse.

6.1.7 Les options de remise de messages

Les **options de remise de messages** servent à indiquer si le message à un seul, un groupe ou tout les hôtes comme destinataire ou à préciser qu'un message ne requiert pas d'accusé de réception.

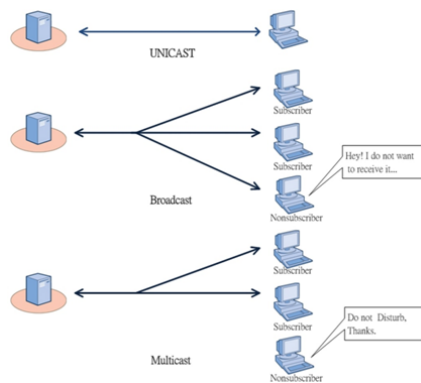


FIGURE 8 – Les différents types de casts

7 Les protocoles de communications

Pour pouvoir communiquer il faut une suite de protocole qui est mise en place par les périphériques dans le logiciel et/ou dans le matériel. On représente cette

suite par une pile dont les couches supérieures dépendent des couches inférieures.

Comme on peut le voir dans la figure 9 on a le protocole **HTTP** (*Hypertext Transfer Protocol*) qui décrit les requêtes et les réponses entre le client et le serveur.

Il dépend donc du protocole **TCP** (*Transmission Control Protocol*) qui va diviser les transmissions HTTP en petit paquets et contrôle la taille et le débit des échanges.

Le protocole TCP dépend du protocole **IP** (*Internet Protocol*) qui encapsule les paquets produits par le TCP et qui les adresse au bon destinataire en utilisant le meilleur chemin.

Enfin il faut bien un support physique et c'est là qu'intervient la couche **Ethernet** qui se charge aussi de la communication sur une liaison de données.

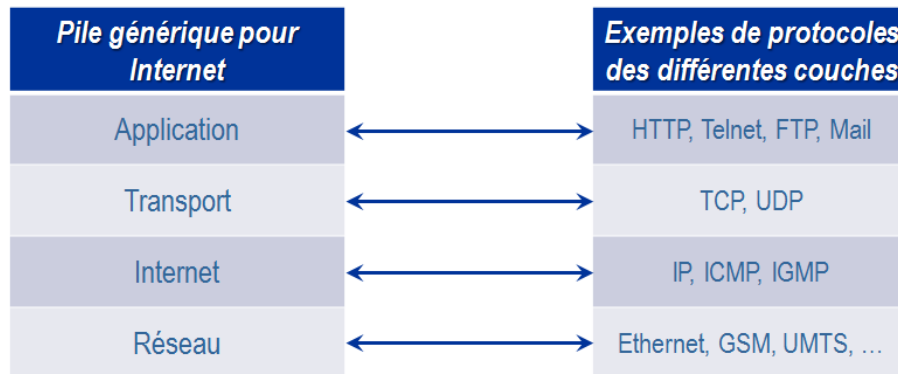


FIGURE 9 – Exemples de pile de protocoles

Les suites de protocoles peuvent être une norme ouverte et autorisée par un organisme ou propriétaire comme l'AppleTalk.

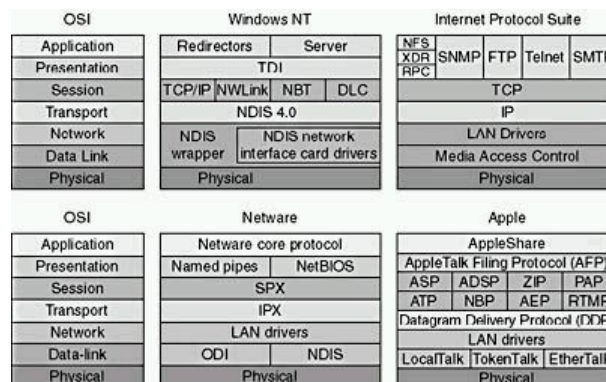


FIGURE 10 – Comparaison des suites de protocoles norme ouverte et propriétaire

7.1 La suite de protocoles TCP/IP

Dans le **modèle TCP/IP** les **protocoles TCP/IP** se trouvent de la couche Internet à la couche application. Les couches inférieures sont chargées de transmettre les paquets sur le réseau physique.

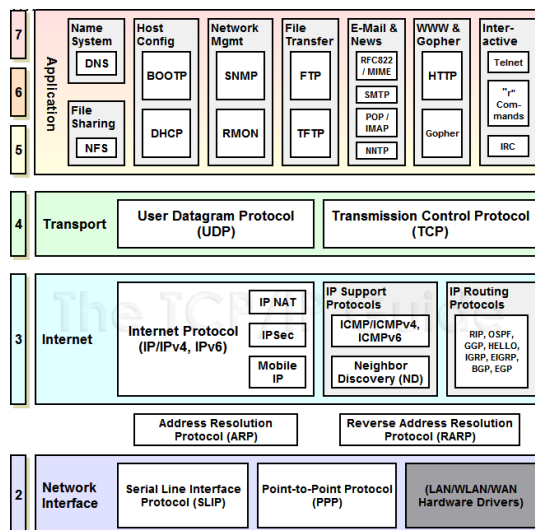


FIGURE 11 – Les différents protocoles du modèle TCP/IP

7.1.1 Couche application

- **DNS** (*Domain Name System/Service*) : Traduit les noms de domaines en adresse IP.
- **DHCP** (*Dynamic Host Configuration Protocol*) : Attribue dynamiquement les adresse IP à la connexion.
- **SMTP** (*Simple Mail Transfer Protocol*) : Permet le transfert d'e-mail à un serveur de messagerie.
- **POP** (*Post Office Protocol*) : Permet de récupérer des e-mails depuis un serveur de messagerie.
- **IMAP** (*Internet Message Access Protocol*) : Permet d'accéder à des e-mails sur un serveur de messagerie.
- **FTP** (*File Transfer Protocol*) : Permet d'accéder aux fichier sur un autre hôte et de transférer des fichiers.
- **TFTP** (*Trivial File Tranfer Protocol*) : Un version simplifiée de FTP qui ne requiert pas d'identifiants de connexion.
- **HTTP** (*HyperText Tranfert Protocol*) : Permet d'échanger du text et des multimédias.

7.1.2 Couche transport

- **UDP** (*User Datagram Protocol*) : Permet d'envoyer des paquets sans-connexion et sans confirmation entre les processus.
- **TCP** (*Transmission Control Protocol*) : Permet un connection fiable entre les processus.

7.1.3 Couche Internet

- **IP** (*Internet Protocol*) : Transforme les segments de messages en paquets et indique l'adresse du destinataire.
- **NAT** (*Network Address Translation*) : Convertit les adresses IP privées en adresses IP publiques.
- **ICMP** (*Internet Control Message Protocol*) : Permet au destinataire de signaler une erreur dans le paquet à la source.
- **OSPF** (*Open Shortest Path First*) : Permet de faire du routage dynamique.
- **EIGRP** (*Enhanced Interior Gateway Routing Protocol*) : Permet aussi de faire du routage dynamique mais par Cisco.

7.1.4 Couche d'accès au réseau

- **ARP** (*Address Resolution Protocol*) : Fournit un mappage dynamique entre une adresse IP et une adresse MAC.
- **PPP** (*Point to Point Protocol*) : Encapsule les paquets pour les transmettre en série.
- **Ethernet** : Définit les règles de câblage et de signalisation de cette couche.
- **Pilotes d'interface** : Permet à un ordinateur de contrôler une interface sur un périphérique réseau.

7.2 Les organismes de normalisations

Les **organismes de normalisations** sont des associations à but non lucratif qui développent de nouvelles normes. Voici les plus connues :

- L'*Internet Society* (**ISOC**) qui promeut l'évolution et l'utilisation d'Internet ouvert dans le monde.
- L'*Internet Architecture Board* (**IAB**) s'occupe de la gestion du développement et de la surveillance des normes Internet.
- L'*Internet Engineering Task Force* (**IETF**) développe et s'assure de la maintenance de TCP/IP et produisent des Request for Comments (**RFC**) pour décrire les processus et technologies d'Internet. Il est constitué de groupes de travail missionnés qui se dissolvent une fois leur mission réussie.
- L'*Internet Research Task Force* (**IRTF**) développe Internet et TCP/IP mais sur le long terme.

Il existe aussi l'Institute of Electrical and Electronic Engineers (**IEEE**) constitué de 400 000 spécialistes de l'électronique. Il gère des normes affectant de nombreux secteurs comme leurs normes 802 qui traitent des LAN et MAN filaire et sans fil. En voici quelques exemples :

- **802.1** : Un groupe de travail sur les protocoles LAN de couches supérieures.
- **802.3** : Un groupe de travail sur Ethernet et définit le MAC.
- **802.11** : Un groupe de travail sur les WLAN et définit les couches physiques et de liaison de données MAC du modèle OSI.
- **802.15** : Un groupe de travail sur WPAN.

Enfin il y a l'organisation internationale de normalisation (**ISO**) surtout célèbre pour le modèle **OSI** (*Open Systems Interconnection*), même si on lui a

finalement préféré le modèle **TCP/IP**.

Il existe aussi des organisme de normalisation commerciaux. Les principaux sont :

- L'*Electronic Industries Alliance* (**EIA**) concerne les entreprise électronique et est connue pour ses normes de cables, de connecteur et les racks 19 pouces.
- Le *Telecommunications Industry Association* (**TIA**) s'occupe de nombreuses normes de communications.
- Le *secteur de la normalisation des télécommunications de l'Union Internationale des Télécommunications* (**ITU-T**) définit des normes de compression vidéo, de TV sur IP, de DSL et les indicatifs téléphoniques internationaux.
- L'*Internet Corporation for Assigned Names and Numbers* (**ICANN**) gère le protocole DNS, l'attribution d'adresses IP et les identificateurs de protocole TCP et UDP.
- L'*Internet Assigned Numbers Authority* (**IANA**) est une composante de l'ICANN qui gère les noms de domaines, les IP et les identificateurs de protocole.

7.3 Les modèles de référence et de protocoles

Un **modèle** comme TCP/IP ou OSI permet de visualiser les interaction des protocoles et leurs fonctionnement. Il permet de concevoir un protocole plus facilement grâce aux interactions entre les couches et évite qu'un changement dans une couche ne se répercute dans les autres. Il encourage la concurrence car les produit concurrent peuvent fonctionner ensembles car il fournit un langage commun pour décrire les fonction et les fonctionnalités réseaux.

Un **modèle de protocole** suit la structure d'une suite de protocole donnée. La suite de protocole hiérarchisée comporte normalement toutes les fonctions requises pour un interface entre un humaine et le réseau. Le **modèle TCP/IP** décrit les fonctions qui interviennent à chaque couches de la suite TCP/IP.

Un **modèle de référence** décrit les opérations à effectuer à chaque couches mais pas leur mise en oeuvre. Il permet de mieux comprendre les fonctions et les processus impliqués. Le modèle **OSI** ne spécifie pas l'implémentation et ne possède pas suffisamment de détails pour définir précisément les services de l'architecture réseau.

7.4 Le modèle OSI

1. La **couche application** relie les réseaux humains.
2. La **couche présentation** permet de représenter les données de façon commune entre les services de la couche application.
3. La **couche session** permet à la couche présentation d'échanger des données.
4. La **couche transport** segmente, transfert et réassemble les données.
5. La **couche réseau** permet d'échanger des paquets entre périphériques finaux.

6. La **couche liaison de données** permet d'échanger des trames entre périphériques sur un support commun.
7. La **couche physique** permet de gérer des connexions physiques pour le transfert de bits.

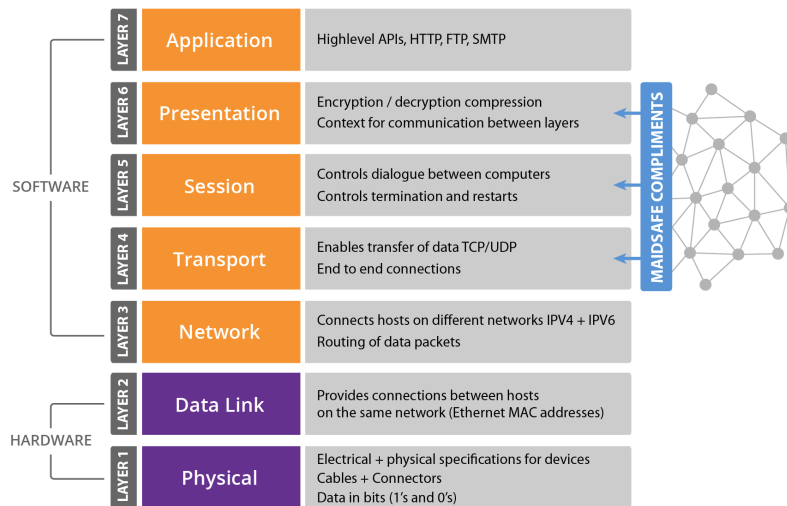


FIGURE 12 – Modèle OSI

Le **PDU** (*Protocol Data Unit*) est l'unité de données de protocole.

Peer-to-Peer Communications

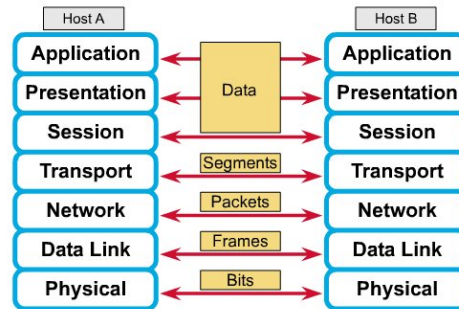


FIGURE 13 – PDU du modèle OSI

7.5 Le modèle TCP/IP

Le modèle TCP/IP est une norme ouverte, elle est donc décrite dans un RFC disponible au public.

Les différences notables sont :

- Au niveau de la **couche d'accès réseau** la suite TCP/IP ne spécifie pas de protocole pour la transmission physique des données.

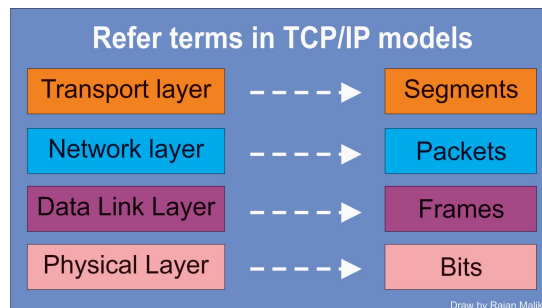


FIGURE 14 – PDU du modèle TCP/IP

- Au niveau de la **couche d'application** TCP/IP propose plusieurs protocoles qui ont été basés sur les couches 5, 6 et 7 du modèle ISO.



FIGURE 15 – Comparaison des modèles OSI et TCP/IP

7.6 Adresses réseau et adresses de liaison de données

Les protocoles possèdent des adresses sources et de destinations mais ne les utilisent pas de la même façon.

Sur la couche réseau on trouve dans un paquet IP :

L'**adresse IP source** est l'adresse IP du périphérique expéditeur. L'**adresse IP de destination** est l'adresse du récepteur, elle est utilisée par les routeurs pour transférer le paquet IP vers sa destination.

Sur la couche liaison de données on retrouve :

L'**adresse de liaison de données source** est l'adresse physique de la carte réseau de l'expéditeur

L'**adresse de liaison de données de destination** est l'adresse physique du routeur du tronçon suivant ou du destinataire.

Pour obtenir l'adresse MAC Ethernet d'un autre périphérique, l'hôte utilise le protocole ARP. Dans la RAM se trouve une table ARP qui contient le

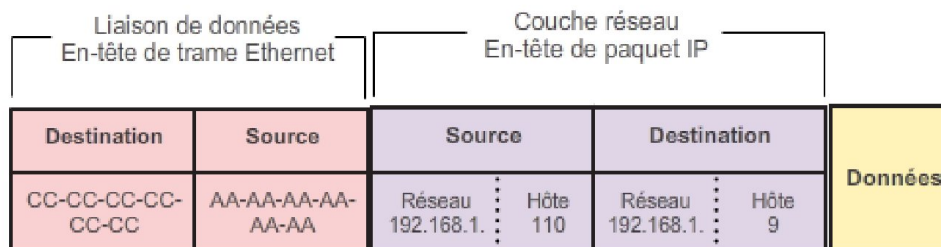


FIGURE 16 – Composition d'un paquet

mappage des adresses MAC et des adresses IP correspondantes. Il est soit créé de façon dynamique soit à chaque échange avec un nouvel hôte. La demande de ligne ARP se fait par multidiffusion et elles ont bien sûr une date limite.

Il est possible de devoir configurer les tables ARP manuellement avec des entrées statiques pour éviter les empoisonnement ARP.

Pour accéder aux ressources distantes, l'hôte doit passer par le routeur ou passerelle par défaut. L'adresse IP est donc celle de l'hôte distant mais l'adresse mac est d'abord celle du routeur puis de chaque périphérique intermédiaire avant d'arriver au destinataire.