

CHAPITRE 1

Les concepts de base dans l'optimisation des réseaux informatique.

I.1. Introduction

Les réseaux sont nés du besoin de transporter une information d'une personne à une autre. Pendant longtemps, cette communication s'est faite directement par l'homme, comme dans le réseau postal, ou par des moyens sonores ou visuels. Il y a un peu plus d'un siècle, la première révolution des réseaux a consisté à automatiser le transport des données.

Aujourd'hui, les réseaux informatiques qui permettaient à leur origine de relier des terminaux passifs à de gros ordinateurs centraux autorisent à l'heure actuelle l'interconnexion de tous types, d'ordinateurs que ce soit de gros serveurs, des stations de travail, des ordinateurs personnels ou de simples terminaux graphiques. Les services qu'ils offrent font partie de la vie courante des entreprises et administrations (banques, gestion, commerce, bases de données, recherche, etc...) et des particuliers (messagerie, loisirs, services d'informations par minitel et Internet ...).

I.2. Les différents systèmes de numération

I.2.1. Représentation des données pour un système informatique

Un ordinateur pourrait se résumer à un ensemble de commutateurs électriques pouvant prendre deux états :

- En fonction (le courant passe)
- Hors fonction (le courant ne passe pas)

Pour les différentes tâches qu'ils effectuent de nos jours, les ordinateurs utilisent le système de **numérotation binaire**. Du fait que les humains fonctionnent avec le système décimal, l'ordinateur doit pouvoir effectuer cette traduction afin de pouvoir traiter les informations des utilisateurs. Ces nombres binaires sont exprimés en **bits**, qui constituent la plus petite unité d'information d'un ordinateur. Un groupe de 8 bits correspond à un **octet**, qui représente un caractère de données. Pour un ordinateur, un octet représente également un emplacement de mémoire adressable. Du fait de la taille des informations contenues dans les ordinateurs actuels, différentes unités de mesure ont été mises en place :

Unité	Définition	Octets	Bits	Exemples
Bit (b)	Chiffre binaire 1 ou 0	1 bit	1 bit	+5 volts ou 0 volts
Octet (o)	8 bits	1 octet	8 bits	01001100 correspond à la lettre L en ASCII
Kilo-octet (Ko)	1 kilo-octet =1 024 octets	1024 octets	8192 bits	mail type : 2ko premiers PC : 64Ko de Ram

Méga-octet (Mo)	1 méga-octet =1024 kilo octets	1 048 576 octets	8 388 608 bits	disquette = 1,44 Mo CD-ROM = 650 Mo
Giga-octet (Go)	1 giga-octet =1024 méga octets	1 048 576 kilo-octets	Env. 8 milliards de bits	disque dur type = 4 Go
Téra-octet (To)	1 téra-octet =1024 giga octets	1 048 576 méga-octets	Env. 8 trillions de bits	quantité théorique de données transmissibles par une fibre optique en 1 seconde

Tableau 1.1 Les différentes unités de mesure

I.2.2. Les différents systèmes de numération

L'homme est habitué dès le plus jeune Age à utiliser un système de numérotation pour représenter des valeurs. Ce système comporte 10 symboles : 0 1 2 3 4 5 6 7 8 9 et se nomme « **système de numérotation décimal** ». Une valeur est de ce fait une notion abstraite pouvant être exprimée selon différents systèmes :

Par exemple, nous savons qu'un ordinateur fonctionne avec des commutateurs électriques pouvant avoir 2 états : en fonction et hors fonction. L'ordinateur va donc utiliser un système de numérotation avec deux symboles : 0 et 1. C'est ce que l'on appelle le **système binaire**. Il fonctionne de manière analogue au système décimal sauf qu'il n'utilise que 2 symboles.

Exemple : 1011 qui en décimal équivaut à la valeur 11

Autres systèmes, le **système hexadécimal**, comportant 16 symboles 0 1 2 3 4 5 6 7 8 9 A B C D E F. Les 6 lettres correspondent en décimal à 10 11 12 13 14 15.

Exemple : A2F54B qui équivaut en décimal à la valeur 10679627

Voici les différents systèmes que nous utiliserons ainsi que leur spécificité :

Nom	Symboles utilisés	Référence
binaire	0 1	2
octal	0 1 2 3 4 5 6 7	8
décimal	0 1 2 3 4 5 6 7 8 9	10
Hexa ² décimal	0 1 2 3 4 5 6 7 8 9 A B C D E F	16

Tableau 1.2 : les différents systèmes de numérotation

I.2.3. Méthodes de conversion de base

Le système décimal repose sur les puissances de 10. Chaque symbole composant un nombre décimal représente une puissance de 10 ; chacun ayant pour exposant sa position dans le nombre en partant de la droite ; multiplié par le symbole occupant cette position.

Exemple : $25642 = 2 \times 10^4 + 5 \times 10^3 + 6 \times 10^2 + 4 \times 10^1 + 2 \times 10^0$

Pour convertir une valeur exprimée dans un système en une valeur utilisant le système de numérotation décimal, l'algorithme est le suivant :

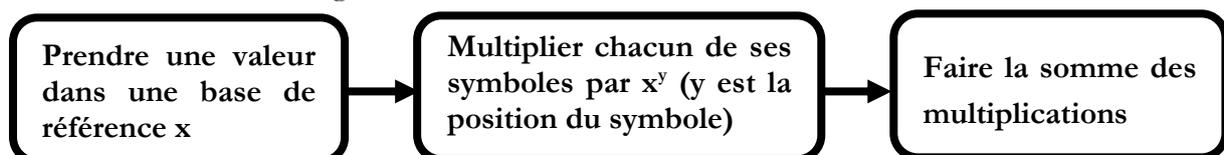


Figure 1.1 : algorithme de conversion d'un système en base x vers le système décimal

Exemple de conversion Octal → Décimal

$20165 \text{ (octal)} \rightarrow 2 \times 8^4 + 0 \times 8^3 + 1 \times 8^2 + 6 \times 8^1 + 5 \times 8^0 = 8192 + 0 + 64 + 48 + 5 = 8309 \text{ (dec)}$

Exemple de conversion Hexadécimal → Décimal

$$A2F54B \text{ (hexadécimal)} \rightarrow A(10) \times 16^5 + 2 \times 16^4 + F(15) \times 16^3 + 5 \times 16^2 + 4 \times 16^1 + B(11) \times 16^0$$

$$\rightarrow 10485760 + 131072 + 61440 + 1280 + 64 + 11 = 10679627 \text{ (dec)}$$

I.2.4. Représentation numérique des données informatiques

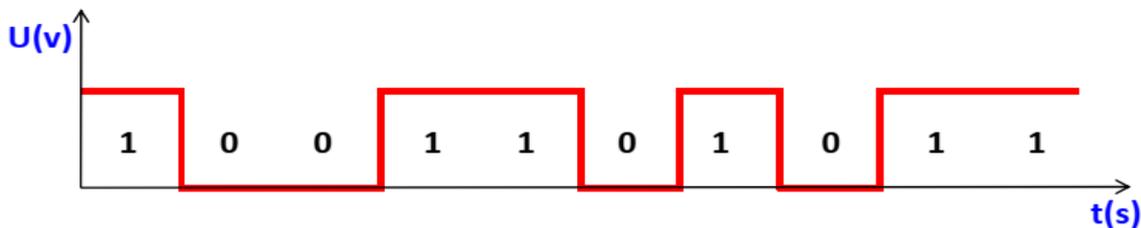
Les ordinateurs sont composés d'un ensemble de commutateurs électriques qui jouent le rôle des interrupteurs et pouvant prendre deux états:

- **Courant passe** : En fonction qui correspond à (1)
- **Courant ne passe pas** : Hors fonction qui correspond à (0)

Exemple:

Le signal correspondant à une suite binaire de 10 bits (1001101011). Dans ce cas de figure, le signal peut prendre deux valeurs:

- En informatique on note **0** ou **1**.
- En électronique on donne les deux tensions (ex: **0** volt et **+5** volts)

**I.3. Système de communication**

Les besoins de communication de données informatiques entre systèmes plus ou moins éloignés sont multiples : transmission de messages, partage de ressources, transfert de fichiers, consultation de bases de données, gestion de transactions, lecture de vidéos ou de musiques, réseaux sociaux, réservations et paiements en ligne...

Pour communiquer, ces systèmes disposent de trois blocs fonctionnels (figure 1.2)

- les applications qui veulent échanger des données ;
- les fonctions destinées à établir et à gérer la communication ;
- les fonctions assurant la transmission des données.
- Il est important de noter que ce sont les applications qui sont à l'origine de la demande et de la procédure de communication. En revanche, l'établissement de la connexion entre les systèmes informatiques s'effectue à partir du réseau.
- C'est tout d'abord la connexion entre les deux systèmes qui est établie à travers le réseau (**phase 1**). Puis la communication est établie, vérifiant que les systèmes peuvent dialoguer : même « langage », mémoire disponible, services applicatifs présents (**phase 2**). Les applications peuvent alors échanger leurs informations (**phase 3**). Pour comprendre le rôle de chacun de ces blocs, une analogie simple avec le réseau téléphonique peut être faite :

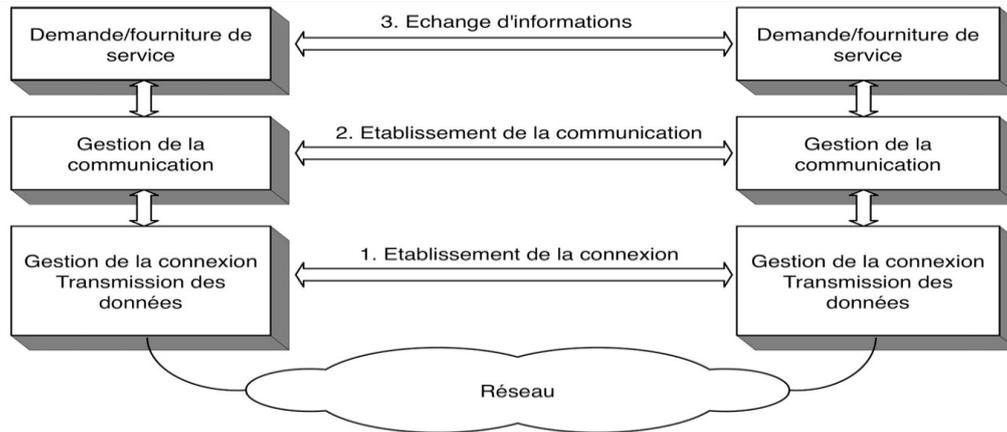


Figure 1.2 : Architecture des systèmes de communication.

Phase 1 : ➔ à l'initiative de l'appelant, la demande de connexion est initiée par la prise du combiné (la tonalité confirme que le réseau est disponible) et la numérotation,

➔ l'opérateur est chargé d'établir la connexion entre les deux postes téléphoniques,

➔ le combiné distant sonne, informant le destinataire de la demande de connexion. Celui-ci répond en décrochant son combiné, **la connexion physique est établie ;**

Phase 2 : ➔ s'ils sont disponibles et s'ils parlent la même langue, les deux interlocuteurs peuvent être mis en relation par l'intermédiaire d'un secrétariat ou d'un standard par exemple, **la communication est établie ;**

Phase 3 : ➔ les deux interlocuteurs dialoguent.

Matériellement, un réseau de transmission comprend des **équipements de raccordement** pouvant être externes (comme un modem, un routeur, un point d'accès sans fil ou encore une box Internet qui inclut ces trois fonctions) ou internes (carte réseau Ethernet ou WiFi par exemple). Ces équipements sont connectés entre eux par des lignes ou **supports physiques** de transmission (figure 1.3).

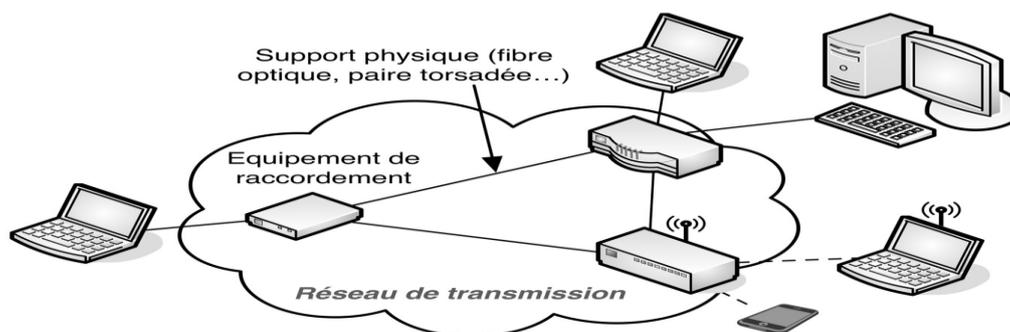


Figure 1.3 : Architecture d'un réseau de transmission.

I.4. La terminologie de base des réseaux

I.4.1. Qu'est-ce qu'un réseau ?

Définition 1.1 (réseau)

Un **réseau** est un système complexe d'objets et de personnes interconnectés. On trouve les réseaux partout dans notre vie, que nous pouvons classer selon diverses catégories :

➔ **Communications** : Internet, téléphone, services postal, télévision, radio...

➔ **Transport** : Réseau autoroutier, transport aérien, transport maritime...

→ **Société** : Villes, amis, famille...

→ **Biologie** : Neurologie, système cardio-vasculaire...

→ **Services publics** : Eau potable, réseau électrique, réseau téléphonique (mobile et fixe)...

I.4.2. Réseau informatique

Définition 1.2 (Réseau informatique)

Un **réseau informatique** est un ensemble d'équipements reliés entre eux pour échanger des données numériques, la connexion entre les différents composants d'un réseau s'effectue à l'aide des supports pouvant être des câbles sur lesquels circulent des signaux électriques, l'air (ou le vide) où circulent des ondes radio, ou des fibres optiques qui propagent des ondes lumineuses.

La communication se fait selon des règles bien définies (les protocoles).

Les utilisateurs peuvent se connecter à un réseau informatique afin d'échanger de données avec d'autres utilisateurs (courriers électroniques, messages instantanés, vidéo conférence...), solliciter des données ou des services auprès d'un serveur (consulter une boîte email, recherche sur Google...).

Pour une entreprise, le réseau informatique lui permet de partager efficacement éléments comme les fichiers, les imprimantes, les données des clients...

I.4.3. Les composants de base d'un réseau

Quel que soit le réseau informatique, son infrastructure comprend, entre autres, trois catégories de composant réseau :

- **Hôtes** (ou périphériques finaux): sont des machines capables d'envoyer et de recevoir des données directement sur le réseau (ordinateur, serveur, imprimante réseau, ...). Chaque hôte a une adresse IP.
- **Périphériques partagés** : Ne sont pas directement connectés au réseau, l'accès au réseau se fait à travers les hôtes (Webcam, imprimante, ...).
- **Périphériques réseau (ou périphériques intermédiaires)**: Permettent de relier les hôtes individuels au réseau ou connecter plusieurs réseaux (commutateurs, concentrateurs, routeurs, point d'accès wifi, pare-feu, ...).
- **Supports réseau (ou médias)**: Permet l'interconnexion (physiquement) des hôtes et les périphériques réseau entre eux (câble en cuivre, fibre optique, l'air (sans fil)).

I.4.4. Les types de réseaux informatiques

En fonction de la localisation, la distance et le débit, les réseaux informatiques peuvent être classés en plusieurs types. Dont voici une première classification selon la distance entre les communicants :

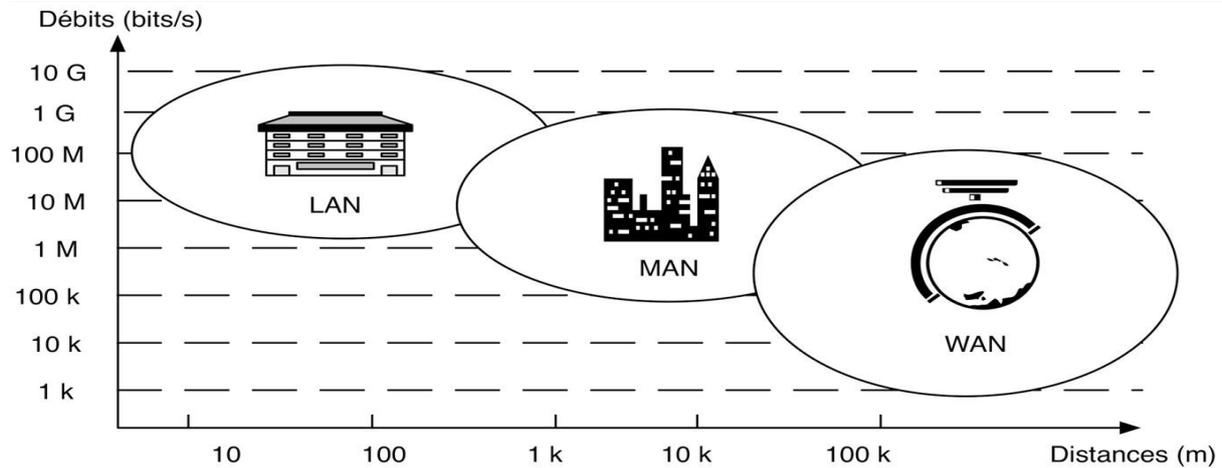


Figure 1.4 : Types de réseaux

Réseau personnel (PAN) : (ou Personal Area Network) souvent de faible portée (généralement dans un espace d'une dizaine de mètres), on utilise surtout les technologies USB, Bluetooth, Infrarouge et wifi.

Exemple de réseau PAN : souris, clavier, imprimante, télécommande, partage via Bluetooth...

Réseau local (LAN) : (ou Local Area Network) est un réseau permettant l'interconnexion des ordinateurs au sein d'une même entreprise ou d'une organisation, il peut s'étendre en moyenne de 10 mètres à 1 kilomètre. Si la technologie utilisée est sans fil, on l'appelle **LAN sans fil (WLAN)**.

Exemple de réseau LAN : salle informatique, école, un immeuble, campus...

Réseau métropolitain (MAN) : (ou Metropolitan Area Network) interconnecte plusieurs LAN s'étendant sur des régions géographiquement proches (situés dans une même ville ou de quelques dizaines de kilomètres), plus vaste que LAN, mais plus petit que WAN.

Exemple de réseau MAN : réseau reliant les différentes annexes et facultés d'une université,...

Réseau étendu (WAN) : infrastructure réseau permettant relier des LAN sur des zones étendues comme entre : villes, des états, des provinces, des pays ou des continents, généralement géré par des opérateurs téléphoniques.

Exemple de réseau WAN : Internet

Réseau de stockage (SAN) : infrastructure réseau conçue pour prendre en charge des serveurs de fichiers dédiés au stockage, récupération et réplication de données. Cette infrastructure nécessite des serveurs haut de gamme avec plusieurs disques durs (baies de disques).

Réseau privé virtuel (VPN) : est réseau permettant de construire un tunnel sécurisé au sein de l'internet, cela afin de connecter d'une façon sécurisée deux réseaux éloignés.

Exemple de réseau VPN : un télétravailleur peut utiliser un réseau VPN peut accéder à distance au réseau intranet de son entreprise.

Internet : est un ensemble mondial de réseaux interconnectés et dont personne n'est propriétaire, qui garantit l'échange d'informations sur différents types de supports et technologies (fils téléphonique, fibre optique, sans fil, satellite, ...).

Intranet : Ce terme est souvent utilisé pour faire référence un réseau LAN privé qui appartient à une entreprise ou une organisation auquel peuvent accéder uniquement ses employés. n'est généralement accessible que depuis l'entreprise.

I.5. La bande passante

Définition 1.3 (bande passante)

La bande passante d'un réseau est sa capacité ou la quantité de données maximale pouvant être transférée en une période de temps donné. Se mesure en bit par seconde (**bits/s**).

I.5.1. L'importance de la bande passante

Plusieurs facteurs rendent la bande passante importante :

- Elle est limitée par des facteurs physiques et technologiques.
- Elle n'est pas gratuite (il faut l'acquérir auprès d'un fournisseur d'Internet).
- Elle est indispensable pour analyser les performances d'un réseau.
- Les besoins en bande passante ne cessent de croître.
- Elle est essentielle à une bonne compréhension de circulation des données sur le réseau (problème de congestion).

I.5.2. Les unités de la bande passante

L'unité de la bande passante est le bit par seconde (bit/s), ce qui mesure la quantité de bits d'information que l'on peut transférer d'un endroit à l'autre en une seconde.

Ce tableau montre les différentes unités utilisées pour mesurer la bande passante :

Unité	Abréviation	Equivalence
Bits par seconde	bits/s	1bit/s = Unité fondamentale
Kilobits par seconde	Kbits/s	1 kbits = 1 000 bits/s = 10^3 bits/s
Mégabits par seconde	Mbits/s	1 Mbits = 1 000 000 bits/s = 10^6 bits/s
Gigabits par seconde	Gbits/s	1 G bits = 1 000 000 000 bits/s= 10^9 bits/s

I.6. Le débit

Définition 1.4 (débit)

Le débit est la bande passante réelle mesurée à un moment précis de la journée, le débit est souvent inférieur à bande passante prise en charge par les médias utilisés.

Les facteurs influençant le débit :

- Type des périphériques réseau (commutateur, concentrateur, routeurs, ponts, ...)
- Type de média (câble, fibre optique, sans fil)
- Nombre d'utilisateurs sur le réseau
- Topologie de réseau (bus, anneau, étoile...)
- Votre ordinateur (Carte réseau, Vitesse CPU, RAM, ...)
- Le serveur interrogé
- Type de données transmises
- L'heure de jour

I.6.1. Calcul du temps de transfert des données

Nous distinguons deux mesures permettant de calculer le temps nécessaire pour le téléchargement d'un fichier :

- Temps théorique : (ou Téléchargement idéal)

$$T = \frac{\text{Taille du fichier (bits)}}{\text{Bande passante(bits/ s)}}$$

- Temps réel : (ou Téléchargement type)

$$T = \frac{\text{Taille du fichier (bits)}}{\text{Débit réel au moment de transfert(bits/ s)}}$$

Exemple :

Pour télécharger le fichier de **1 Go**, nous ne disposons que d'un débit de **512 kbit/s** à cet instant. Combien de temps (réel) faut-il pour le télécharger ?

Taille de fichier en bit : 1GO = 1 × 1024 × 1024 × 1024 × 8 bits = 8 589 934 592 bits

Débit en bit : 512 Kbits/s = 512 × 1000 bits/s = 512 000 bits/s

$$T = \frac{8\,589\,934\,592 \text{ (bits)}}{512\,000 \text{ (bits/ s)}} = 16777s = 4h\ 39\ \text{min}\ 37s$$

I.7. Modèles OSI & TCP-IP

I.7.1. Normalisation & Norme

Normalisation : a pour objet de fournir des documents de référence comportant des solutions à des problèmes techniques et commerciaux concernant les produits, biens et services qui se posent de façon répétée dans des relations entre partenaires économiques, scientifiques, techniques et sociaux.

Norme : est un document qui définit des exigences, des spécifications, des lignes directrices ou des caractéristiques à utiliser systématiquement pour assurer l'aptitude à l'emploi des matériaux, produits, processus et services.

Les Normes internationales garantissent des produits et services sûrs, fiables et de bonne qualité. Pour les entreprises, elles sont des outils stratégiques permettant d'abaisser les coûts, en augmentant la productivité et en réduisant les déchets et les erreurs.

I.7.2. Notion de protocole

Définition 1.5 (protocole)

Un **protocole** décrit un ensemble de règles utilisées par les équipements pour établir une communication ou échanger des données. Ces protocoles peuvent concerner la **connexion** des équipements, la gestion de la **communication** ou la nature des **informations** échangées.

Pour chacun des blocs fonctionnels décrits précédemment, un ensemble de protocoles sont définis :

- au niveau de la gestion de la **connexion**, des protocoles décrivent les opérations qui s'enchaînent pour assurer l'ouverture, la gestion et la fermeture de cette connexion (l'internaute connecte le modem ADSL de sa box, son FAI – Fournisseur d'Accès Internet – l'authentifie puis lui fournit un accès...);

- au niveau de la **communication**, des protocoles tels TCP gèrent le transport des données entre deux machines en s'appuyant sur la connexion précédemment établie ;
- au niveau du **service**, des protocoles décrivent les commandes et les réponses permettant de transférer et de traiter les données. Par exemple, dans le cas de HTTP, il s'agit de l'envoi d'une page web d'un serveur vers le navigateur d'un client.

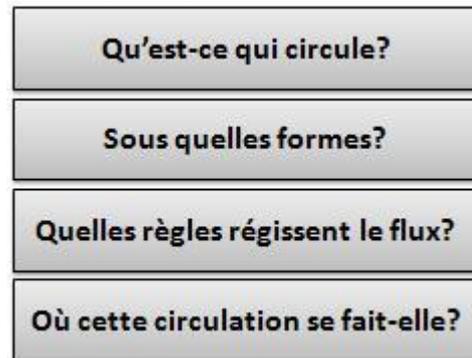
I.7.3. Système en couche

Le but de ce modèle en couche est de séparer le problème en différentes parties (couches) selon leur niveau d'abstraction, c.-à-d. d'analyser la communication en découpant les différentes étapes en 7 couches ; chacune de ces couches remplissant une tâche bien spécifique :

Exemple :

Analyse d'un réseau en couche

- Quelles sont les informations qui circulent ?
- Sous quelle forme circulent-elles ?
- Quel chemin empruntent-elles ?
- Quelles règles s'appliquent aux flux d'informations ?



I.7.4. Modèle OSI (Open Systems Interconnections)

La première évolution des réseaux informatiques a été des plus anarchiques, chaque constructeur développant presque sa propre technologie. Le résultat de cela était une quasi-impossibilité de connecter différents réseaux entre eux. Pour pallier à cela, l'ISO (Institut de normalisation) décida de mettre en place un modèle de référence théorique décrivant le fonctionnement des communications réseau : Le modèle OSI a été développé en 1984 par ISO (Organisation internationale de normalisation) afin de faire face à l'incompatibilité entre les réseaux des différents constructeurs de l'époque (ex: SNA, DecNET, ...) . Parmi ses objectifs:

- Utilisé comme modèle de référence.
- Permet aux réseaux des différents constructeurs de s'interconnecter.
- Séparer les communications en 7 couches selon leur niveau d'abstraction.
- Analyser les communications réseaux en étapes.
- Identifications des informations circulant dans le réseau.
- Sélection des chemins pour atteindre le destinataire.
- Unification des règles régissant le réseau.

Les couches du modèle OSI

Le modèle OSI comporte sept couches représentées de la manière suivante :

La couche application : La couche la plus proche de l'utilisateur. Elle fournit des services réseau aux applications de l'utilisateur. Elle crée une interface **directe** avec le reste du modèle OSI par le biais d'applications réseau (navigateur Web, messagerie électronique, protocole FTP (Filezilla), Telnet, etc.).

- Pour vous souvenir des fonctions de cette couche, pensez aux **navigateurs**.
- Unité de données : **Données**

La couche présentation : Elle assure que les informations envoyées par la couche application de l'émetteur sont lisibles par la couche application du récepteur. Cette étape comporte : le **cryptage, compression et décompression** des données.

- Pour vous souvenir des fonctions de cette couche, pensez à un **format de données courant**.
- Unité de données : **Données**

La couche session : Elle permet l'ouverture, la gestion et la fermeture d'une session entre deux applications communicantes. Elle synchronise également le **dialogue** entre les couches de présentation des deux hôtes et gère l'échange des données. Permet **l'aiguillage** des données selon les applications qui utilisent le même réseau simultanément.

- Pour vous souvenir des fonctions de cette couche, pensez aux **dialogues** et aux **conversations**.
- Unité de données : **Données**

La couche transport : segmente les données envoyées de l'émetteur et à la couche transport du récepteur de reconstituer le flux de données en les remettant dans le bon ordre, cette couche permet également :

- ✓ Contrôle du transport de bout en bout de manière fiable et précise.
- ✓ Contrôle du flux d'informations.
- ✓ Assure le Découpage, le réassemblage des informations et la cohérence des données.
- ✓ Protège les couches supérieures des détails d'implémentation du transport.
- Pour vous souvenir des fonctions de cette couche, pensez à qualité de service (QoS) et la fiabilité.
- Unité de données : **Segment**

La couche réseau : Elle gère **l'acheminement des données** à travers le réseau en assurant le routage des paquets de données entre les nœuds du réseau. Elle assure la **connectivité** et la **sélection du chemin** entre deux systèmes hôtes pouvant être situés sur des réseaux géographiquement éloignés.

- Pour vous souvenir des fonctions de cette couche, pensez à **la sélection du chemin, au routage et à l'adressage (IP)**.
- Unité de données : **Paquet**

La couche liaison de données : Assure un **transfert fiable** des données sur une liaison physique. Ainsi, Elle s'occupe de **l'adressage physique (MAC)**, de la **topologie du réseau**, de l'accès au réseau, de la notification des erreurs, de la livraison ordonnée des trames et du contrôle de flux.

- Pour vous souvenir des fonctions de cette couche, pensez aux **trames et aux adresses MAC**.
- Unité de données : **Trame**

La couche physique : décrivent les moyens mécaniques, électriques, fonctionnels et méthodologiques permettant d'activer, de gérer et de désactiver des connexions physiques pour la

transmission de bits vers et depuis un périphérique réseau. Les données sont transmises sous forme **binaire** et traduites par des **impulsions électriques** ou **lumineuses**.

- Pour vous souvenir des fonctions de cette couche, pensez aux **signaux** et aux **médias**.
- Unité de données : **Bit**

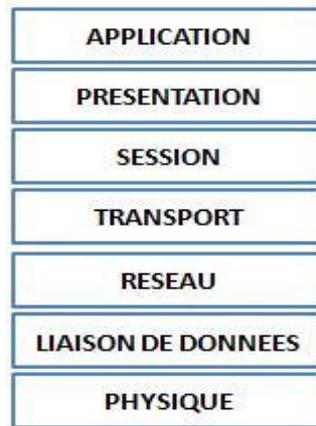


Figure 1.5 : Les sept couches du modèle de référence OSI de l'ISO.

Unité de données de protocole (PDU : Protocol Data Unit) & Services

PDU: unité d'information échangée entre deux couches homologues.

(N)-PDU: unité de données pour une couche **N** comprenant: **(N+1)-PDU** et une information de contrôle **(N)-PCI** (Protocol control information ou **en-tête**).

(N)-SDU(**N-Service Data Unit**) : Ensemble de données provenant de la couche supérieure (**(N+1)-PDU**) et qui doivent être transportées par la couche **N**.

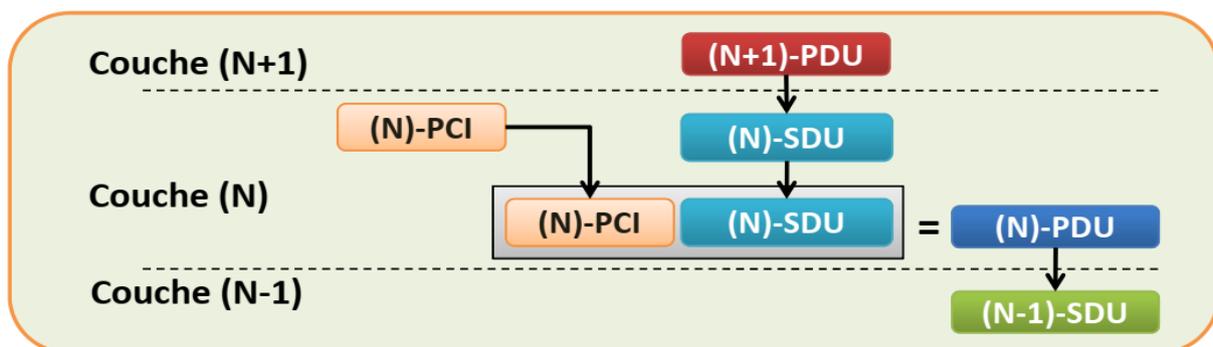


Figure 1.6 : Constitution d'un PDU

Protocoles & Services

Protocole (N) : Ensemble de règles et de conventions régissant une communication entre deux couches homologues de niveau **N**.

Services (N) : Ensemble d'actions effectuées au niveau de la couche **N** afin de rendre service à la couche **N+1**.

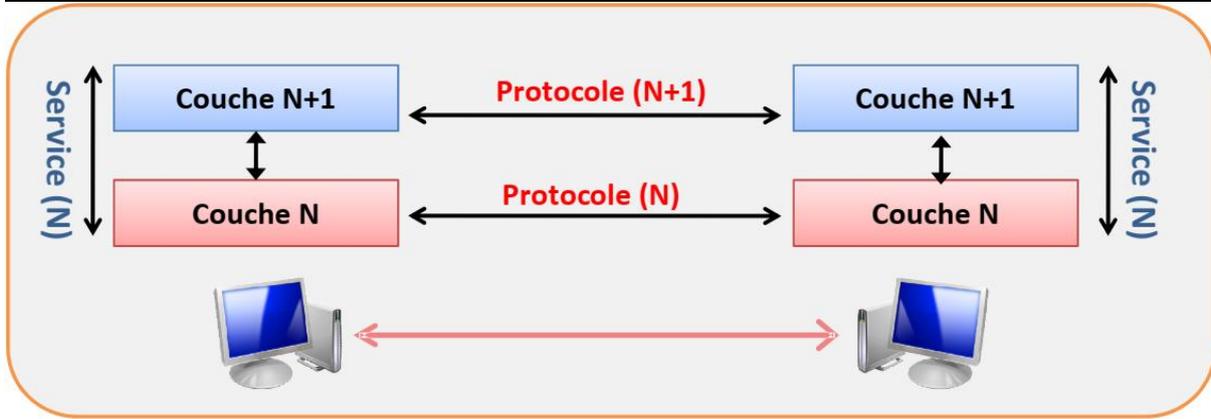


Figure 1.7 : Protocole et services

Encapsulation

Définition 1.6 (L'encapsulation)

L'encapsulation : processus qui consiste à ajouter un bloc de données (des informations spécifiques) (**en-tête**, ...) à une unité de donnée d'un protocole (**Protocol Data Unit (PDU)**) à chaque passage par une couche d'abstraction.

L'encapsulation est exécutée lors de l'envoi par l'émetteur.

- Les données passent de la couche la plus haute vers la couche la plus basse.

La **décapsulation** est exécutée lors de la réception par le récepteur.

- Les données passent de la couche la plus basse vers la couche la plus haute.

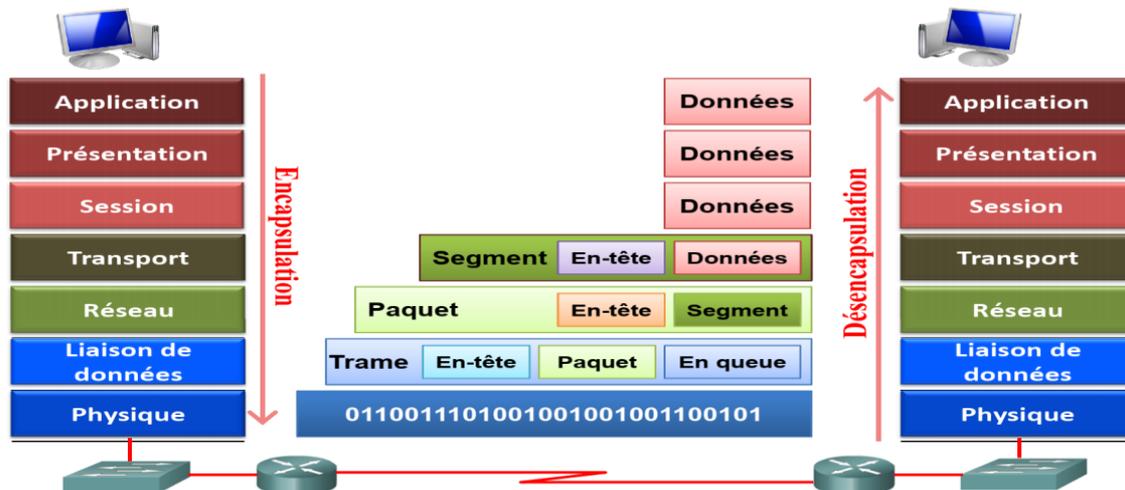


Figure 1.8 : Encapsulation et dés-encapsulation des données par le modelé OSI.

I.7.5. Modèle TCP/IP (Transmission control protocol / Internet protocol)

Le modèle TCP/IP crée par le ministre de la défense américain, et parmi ses objectifs :

- Qu'il soit capable de **résister à toutes les conditions**, même en guerre.
- **Communication décentralisée** : le réseau doit être capable de résister à toute attaque.
- **Compatibilité** avec toute sorte de liaisons: câbles, fibre optique, satellite,....
- Communication en **4 couches**.

- Les réseaux actuels sont construits avec **TCP/IP** (c'est sur lui que repose l'internet actuel)
- Le modèle **TCP/IP** est basé sur le **modèle de référence OSI**, mais avec des services différents.
- **TCP/IP** a été développé en tant que norme ouverte

Comparaison du modèle TCP/IP et du modèle OSI

- **OSI** et **TCP/IP** : sont tous les deux des modèles de communication en couche et utilisent l'encapsulation des données.
- **TCP** regroupe certaines couches du modèle **OSI**.
- **OSI** n'est qu'un modèle de référence (théorique), tandis que **TCP** c'est sur lui que repose le réseau internet actuel.



Figure 1.9 : Comparaison OSI - TCP/IP

Modèle TCP/IP: Protocoles

En pratique le modèle TCP / IP est implémenté par un ensemble de protocoles répartis à travers les 4 couches. Le schéma suivant essaie de donner quelques exemples de protocoles correspondant à chacune des couches du modèle TCP/IP.

Exemple d'application

- Messagerie : SMTP, POP, IMAP, etc.
- Transfert de fichier : TCP, UDP.
- Navigateur web: HTTP, HTTPS, etc.

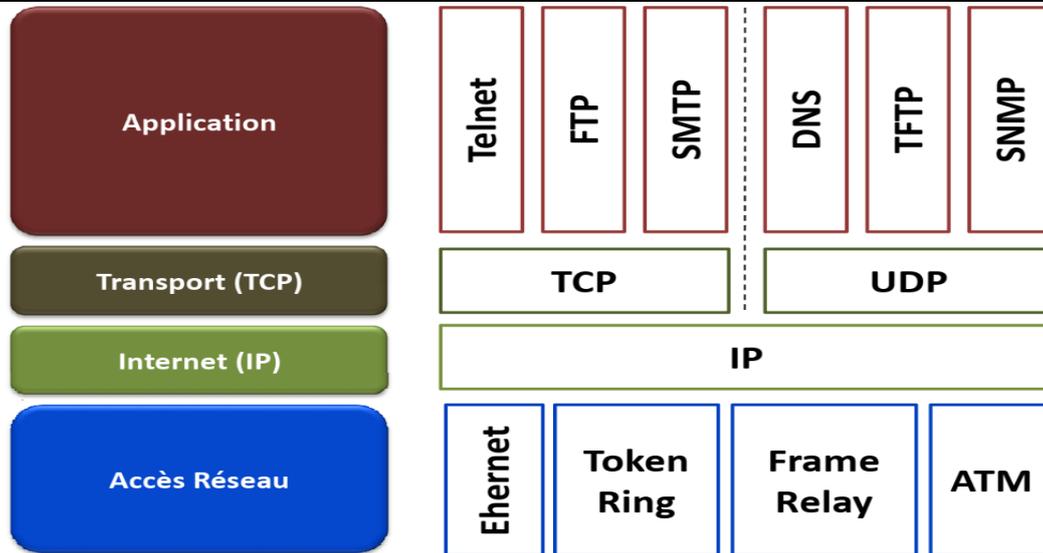


Figure 1.10 : Comparaison OSI - TCP/TP

Protocoles orientés & non-orientés connexion

Nous pouvons classer les protocoles (de la couche application) en deux catégories:

Protocoles orientés connexion: on parle également d'une communication en mode connecté (ou avec connexion), ce mode de communication passe en trois phases:

- Etablissement de la connexion entre les deux entités communicantes
- Le transfert de données et contrôle de données
- La fermeture de la connexion.

TCP est un exemple de protocole orienté connexion

Protocoles non-orientés connexion: s'appelle aussi communication en mode non-connecté (ou sans connexion):

- Transfert de données sans connexion
- Pas de contrôle de flux
- Pas de garanti sur la bonne livraison des données

UDP est un exemple de protocole non-orienté connexion

I.8. Les topologies

Définition 1.7 (topologie)

Une **topologie** définit la façon dont les unités de réseaux sont connectées entre elles, Nous distinguons deux types de topologies:

La topologie physique : désigne les connexions physiques et identifie la façon dont les périphériques finaux et les périphériques d'infrastructure tels que les routeurs, les commutateurs et les points d'accès sans fil sont interconnectés.

La topologie logique : décrit comment les équipements communiquent entre eux. Ainsi que la manière dont un réseau transfère les trames d'un nœud à l'autre.

I.8.1. La topologie en bus

Perspective physique: tous les hôtes sont reliés directement au même câble (généralement coaxial).

Perspective logique: les données envoyées par un hôte peuvent être vues par tous les hôtes de réseau.

Remarque : C'est la topologie la plus simple. En revanche, elle représente quelques faiblesses: En cas de rupture de câble commun tout le réseau tombe en panne.

I.8.2. La topologie en anneau

Perspective physique: les hôtes sont chaînés sous forme d'un anneau (en boucle).

Perspective logique: chaque hôte passe les données à ses voisins (dans un sens unique), chacun à son tour.

Remarque : Le mécanisme de communication sur le réseau est matérialisé par un **jeton d'anneau** qui passe de poste en poste permettant le transport des données sur le réseau. Ce protocole est connu sous terme de **Token Ring**.

I.8.3. La topologie en étoile

Perspective physique: les hôtes sont reliés à un périphérique réseau central (généralement un commutateur ou concentrateur).

Perspective logique: toutes les données passent obligatoirement par l'équipement central.

Remarque : Une topologie étendue est une topologie dont plusieurs topologies en étoiles reliées par un périphérique réseau central (généralement un routeur, commutateur ou concentrateur). C'est la topologie la plus couramment utilisée.

I.8.4. La topologie complète (maillée)

Perspective physique: chaque hôte est connecté avec tous les autres.

Perspective logique: dépend de l'équipement utilisé.

Remarque : Cette topologie est utilisée dans des structures qui n'acceptent pas des ruptures de communication (ex: contrôle des centres nucléaire, routeur assurant la connexion internet).

I.8.5. La topologie hiérarchique

Perspective physique: les hôtes sont constitués d'un ensemble de réseaux étoiles reliées entre eux en niveaux formant une arborescence.

Perspective logique: le flux de données est hiérarchique.

I.8.6. Les structures de réseau hybride

Une **structure de réseau hybride** est un mélange de différentes structures de réseau. Lorsqu'il s'agit d'un réseau de grande taille, cette structure peut comporter à la fois les différentes topologies de base (en anneau, en étoile, en bus...).

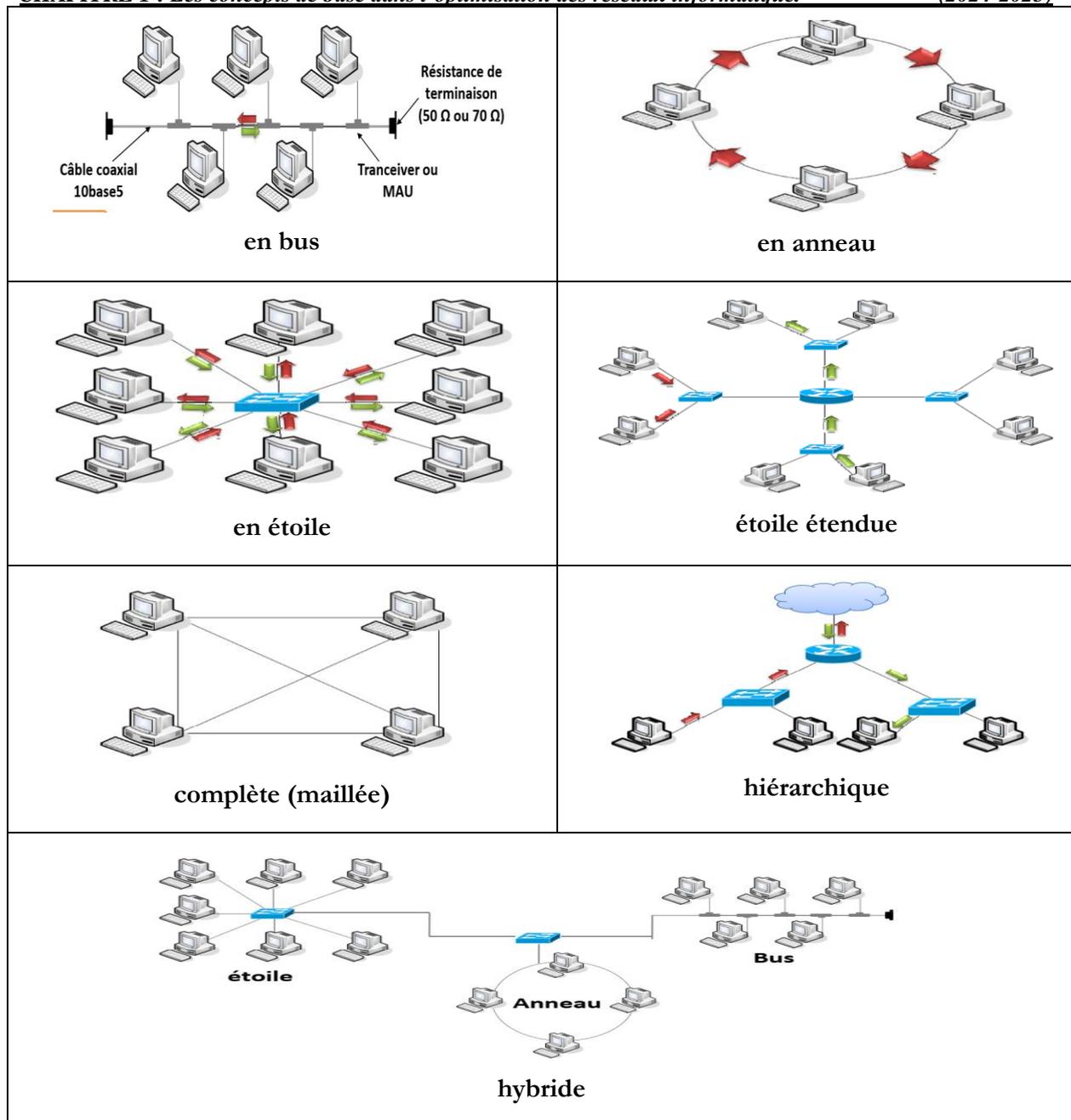


Figure 1.11 : Les différentes topologies

I.9. Les adresses IP (Internet Protocol)

Le mécanisme de l'adressage est fondamental dans les réseaux. Sans lui, les machines qui les constituent ne pourraient pas s'identifier et se contacter les unes les autres, ce qui veut dire qu'aucun réseau ne pourrait exister.

Actuellement, un système d'adressage est standard dans le monde entier : l'adressage **IP** (Internet Protocol). Le terme Internet ne désignant pas l'Internet en particulier, mais n'importe quel internetwork (réseau de réseaux) en général. Les machines que l'on peut joindre par leur adresse IP s'appellent des **hôtes** (hosts). Ce terme s'applique à toute entité dotée d'une ou plusieurs adresses de réseau. Les serveurs, les postes de travail, les imprimantes de réseau, les routeurs, les téléphones IP (Voice over IP) et beaucoup de switches sont des hôtes.

I.9.1. Format d'un datagramme IP (paquet)

Les paquets de la couche réseau transmis par IPv4 sont appelés des datagrammes et comporte en général deux parties :

- **En-tête IP** : indique les données caractérisant le paquet.
- **Données** : contient les données provenant de la couche supérieure, à savoir le segment de la couche Transport.

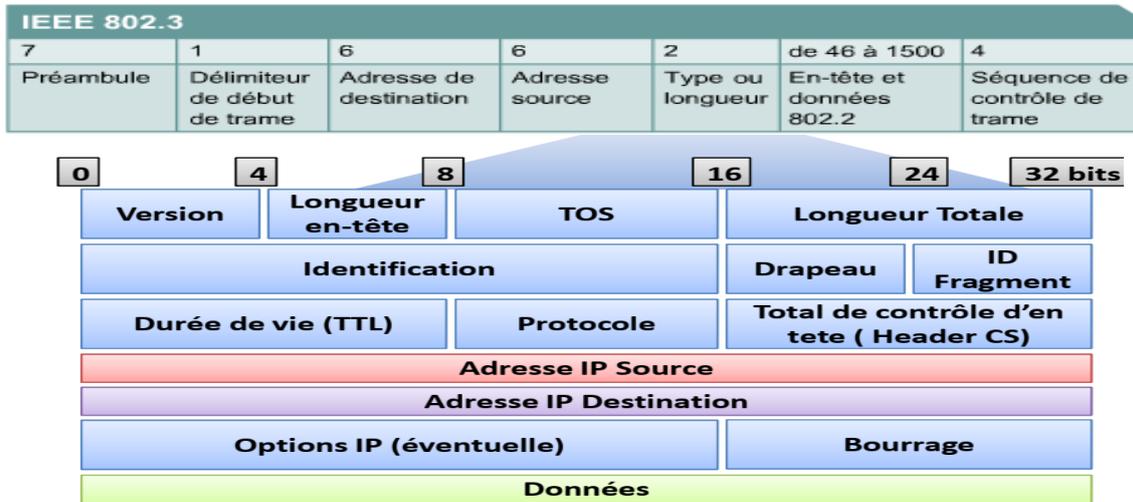


Figure 1.12 : Datagramme IP

I.9.2. Structure de l'adresse IP

L'adressage utilisé dans Internet est un adressage logique. Chaque équipement possède un nom symbolique auquel on fait correspondre l'adresse logique appelée **adresse IP**.

Une **adresse IP** (Internet Protocol) est un nombre de **32 bits** noté sous forme de **4** nombres entiers séparés par des points attribués à chaque hôte et aux routeurs afin de l'identifier sur le réseau auquel il est connecté. On en distingue deux parties :

- **Identificateur de réseau NetID**: c'est la partie des bits à gauche, identique pour toutes adresses d'un même réseau.
- **Identificateur d'hôte Host-ID**: c'est la partie droite, il identifie un hôte ou un routeur au sein d'un réseau.

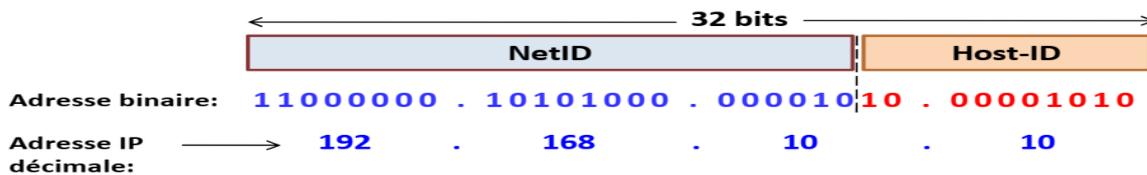


Figure 1.13 : Adresse IP

I.9.3. Masque de sous-réseau

Le masque est une suite de 32 bits défini par **une suite de 1 consécutifs suivi des 0**, et représenté sous forme de 4 nombres entiers séparés par des points. Les masques permettent d'indiquer quelle partie de l'adresse IP correspond à la partie réseau **NetID** et quelle partie correspond à la partie hôte **host-ID**. Le masque est configuré toujours en conjonction avec l'adresse IP, il permet à l'hôte de déterminer le sous-réseau auquel il appartient (NetID).

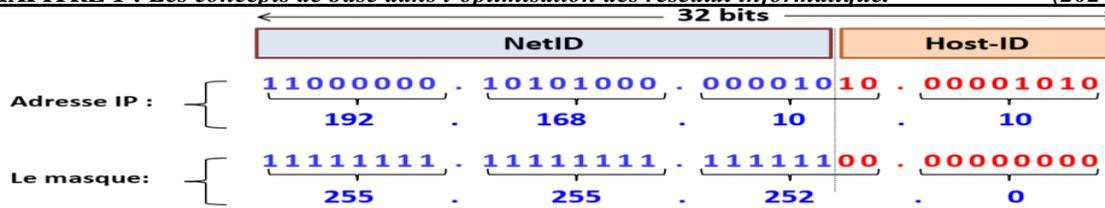


Figure 1.14 : Masque de sous-réseau

I.9.4. L'adresse IP & le masque sous-réseau

Le masque est configuré toujours en conjonction avec l'adresse IP. On retrouve l'adresse de réseau (**NetID**) en effectuant un **ET logique** bit à bit entre une adresse complète et le masque associé. Ce qui permet à l'hôte de déterminer le réseau auquel il appartient.

Exemple : Et logique entre l'adresse IP machine et le masque du réseau.

Adresse IP	134.157.1.151	1000110.10011101.00000001.10010111
Masque	255.255.255.128	11111111.11111111.11111111.10000000
ET logique		1000110.10011101.00000001.10000000
Adresse du réseau	134 . 157 . 1 . 128	

CIDR (Classless Inter-Domain Routing) (ou **préfixe réseau**): une forme plus courte du masque notée par un « / » suivi du nombre de bits à 1 dans le masque.

Exemple : Le masque 255.255.255.128 en notation CIDR est : /25



I.9.5. Les classes d'adresses IP

A l'origine, plusieurs groupes d'adresses ont été définis dans le but d'optimiser l'acheminement des paquets entre les réseaux (routage), on distingue cinq classes d'adresses IP :

Classes	1 ^{er} Octet	Plages d'adresses	Masque par défaut	Identificateur
A	0	0.0.0.0 127.255.255.255	255.0.0.0	R.H.H.H
B	10	128.0.0.0 191.255.255.255	255.255.0.0	R.R.H.H
C	110	192.0.0.0 223.255.255.255	255.255.255.0	R.R.R.H
D	1110	224.0.0.0 239.255.255.255	aucun	multicast
E	1111	240.0.0.0 255.255.255.255	aucun	Réservées aux expérimentations

Figure 1.15 : Les classes d'adresses IP

Remarque : La notion de classe est **obsolète** depuis le milieu des années 1990, ce système a été remplacé par la notation **CIDR**.

I.9.6. Les adresses privées

Les **adresses privées** sont parfois utilisées par les hôtes qui utilisent la **traduction d'adresse réseau (NAT)** ou un **serveur proxy** pour se connecter à un réseau public ou par des hôtes qui

ne se connectent pas du tout à Internet. Autrement dit, une adresse privée n'est pas routée sur Internet.

	De	A	Nombre de réseaux	Nombre d'adresses par réseau
Classe A	10.0.0.0	10.255.255.255	1	2 ²⁴ -2 soit 16 777 216
Classe B	172.16.0.0	172.31.255.255	16	2 ¹⁶ -2 soit 65534
Classe C	192.168.0.0	192.168.255.255	256	2 ⁸ -2 soit 254

I.9.7. Les adresses particulières

Adresse réseau: les bits de la partie host-ID sont tous à 0

Première adresse d'hôte : tous les bits d'host-ID à 0 sauf le bit le plus à droite de la partie host-ID à 1.

Dernière adresse d'hôte : tous les bits d'host-ID à 1 sauf le bit le plus à droite de la partie host-ID à 0.

Adresse IP	192.168.10.152	11000000.10101000.00001010.10011000
Masque	255.255.255.0	11111111.11111111.11111111.00000000
Adresse du réseau		11000000.10101000.00001010.00000000 192 . 168 . 10 . 0
Première adresse		11000000.10101000.00001010.00000001 192 . 168 . 10 . 1
Dernière adresse		11000000.10101000.00001010.11111110 192 . 168 . 10 . 254

Adresse de diffusion (broadcast): tous les bits d'host-ID sont à 1.

Adresse IP	172.18.32.200	10101100.00010010.00100000.11001000
Masque	255.255.0.0	11111111.11111111.00000000.00000000
Adresse du réseau		10101100.00010010.00000000.00000000 172 . 18 . 0 . 0
Adresse de diffusion		10101100.00010010.11111111.11111111 172 . 18 . 255 . 255

L'adresse de bouclage ou boucle locale (Loopback): Désigne la machine locale, elle commence par 127.X.X.X

Exemple: L'adresse de localhost : 127 . 0 . 0 . 1

I.9.8. Segmentation d'un réseau en sous-réseaux « Subnetting »

Définition 1.8 (Subnetting)

Le **subnetting** est une opération qui consiste à diviser un réseau plus large en plusieurs sous-réseaux de petite taille. Cela consiste tout simplement à emprunter quelques bits dans la partie **host-ID** pour créer des sous-réseaux.

Le **subnetting** permet une segmentation des domaines de **broadcast**, ce qui constitue une façon permettant la gestion du trafic dans un réseau.

Au moins *deux bits* doivent rester dans la partie **host-ID**.

- Avant la division en sous-réseaux:



- Après la division en sous-réseaux:



I.9.9. Pourquoi créer des sous-réseaux?

Plusieurs raisons peuvent amener à diviser un réseau en plus sous-réseaux:

- **Permet de limiter la propagation des broadcasts:** des diffusions trop importantes dans des réseaux avec une grande quantité de machines.
- **Limiter la consommation des adresses IP:** l'allocation des plages d'adresses IP selon le besoin.
- **Optimisation des tables de routage:** réduire le nombre d'entrées des tables de routage.
- **Sécurité et confidentialité:** on peut vouloir isoler certains utilisateurs de certaines ressources.

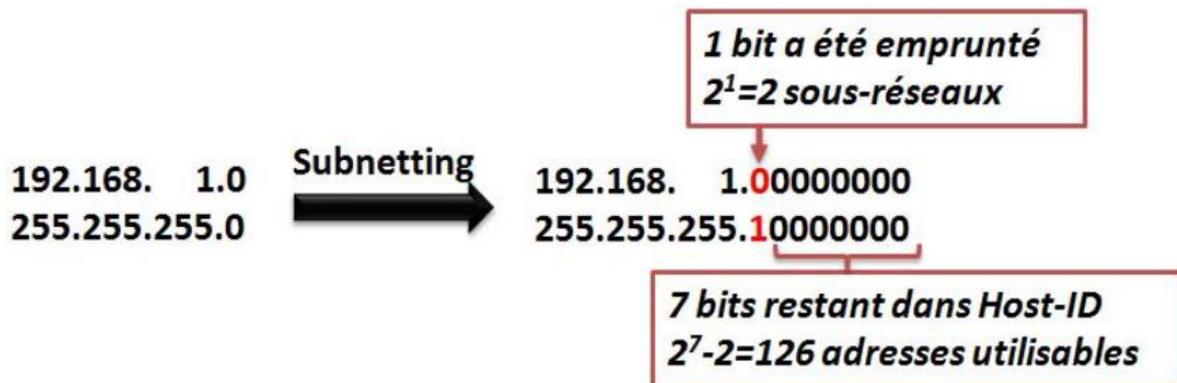
I.9.10. Calculer les sous-réseaux

Nombre de sous-réseaux et d'adresses machines

Ce calcul dépend de nombre de bits empruntés pour la création des sous-réseaux. Etant donné que nous avons emprunté **n** bits pour les sous-réseaux et avec **m** bits restant dans la partie **host-ID**. Le nombre de sous-réseaux et d'hôtes par sous-réseau seront calculés de cette façon :

- **Nombre de sous-réseaux:** 2^n (où **n** le nombre de bits empruntés).
- **Nombre d'hôtes par sous-réseau:** $2^m - 2$ (où **m** le nombre de bits restant dans la partie **host-ID**).

Exemple : Calcul du nombre de sous-réseaux et d'adresses par sous-réseau



Remarque : Étant donné que les hôtes ne peuvent pas utiliser l'adresse réseau ni l'adresse de diffusion d'un sous-réseau, ces deux adresses ne peuvent pas être attribuées à des hôtes. Cela signifie, Dans cet exemple, que chaque sous-réseau dispos de 126 adresses d'hôte valides ($2^7 - 2$). L'emprunt de 1 bit permet donc la création de 2 sous-réseaux dont chacun peut prendre en charge un total de 126 hôtes.

Les différentes étapes de choix d'un sous-réseau:

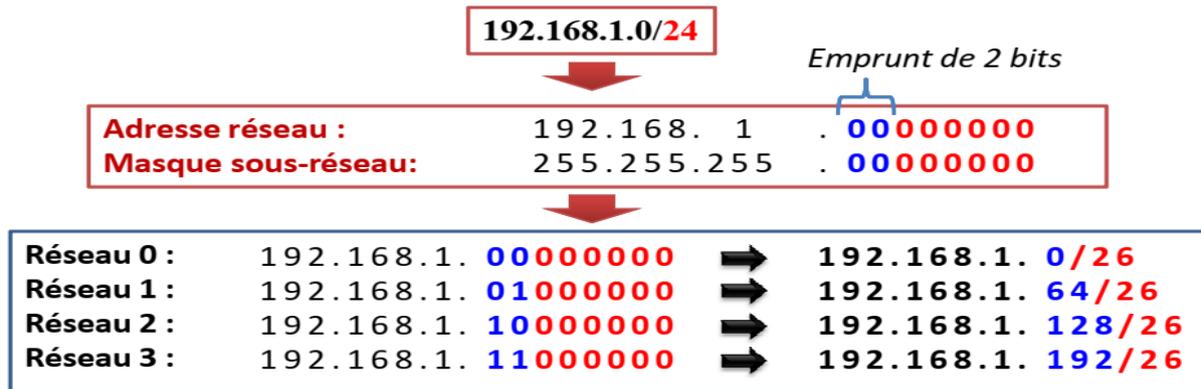
- Empruntez le nombre de bits suffisants.

- Calculez le nouveau masque de sous réseau.
- Identifiez les différentes adresses sous-réseaux.
- Identifiez les adresses de réseau et de broadcast.
- Déterminez les plages d'adresses utilisables par les hôtes.

Plages d'adresses

Etant donné une segmentation du réseau **192.168.1.0/24** en **4** sous-réseaux.

- Nombre de sous-réseaux = $2^n=4 \Rightarrow n=2$ (nombre de bit à emprunter)
- Nombre d'hôtes par sous-réseau = $2^6-2= 62$ (adresses utilisables)



- Les quatre sous-réseaux utilisent le même masque /26:

255.255.255.11000000 ➔ 255.255.255.192

- Plage d'adresses du sous-réseau: **192.168.1.0/26**
 - Adresse Réseau: 192.168.1.0000000 192.168.1.0
 - Première adresse: 192.168.1.0000001 192.168.1.1
 - Dernière adresse: 192.168.1.00111110 192.168.1.62
 - Adresse diffusion: 192.168.1.00111111 192.168.1.63
- Plage d'adresses du sous-réseau: **192.168.1.64/26**
 - Adresse Réseau: 192.168.1.01000000 192.168.1.64
 - Première adresse: 192.168.1.01000001 192.168.1.65
 - Dernière adresse: 192.168.1.01111110 192.168.1.126
 - Adresse diffusion: 192.168.1.01111111 192.168.1.127
- Plage d'adresses du sous-réseau: **192.168.1.128/26**
 - Adresse Réseau: 192.168.1.10000000 192.168.1.128
 - Première adresse: 192.168.1.10000001 192.168.1.129
 - Dernière adresse: 192.168.1.10111110 192.168.1.190
 - Adresse diffusion: 192.168.1.10111111 192.168.1.191
- Plage d'adresses du sous-réseau: **192.168.1.192/26**
 - Adresse Réseau: 192.168.1.00000000 192.168.1.192
 - Première adresse: 192.168.1.00000001 192.168.1.193
 - Dernière adresse: 192.168.1.00111110 192.168.1.254
 - Adresse diffusion: 192.168.1.00111111 192.168.1.255

192.168.1.0/24

