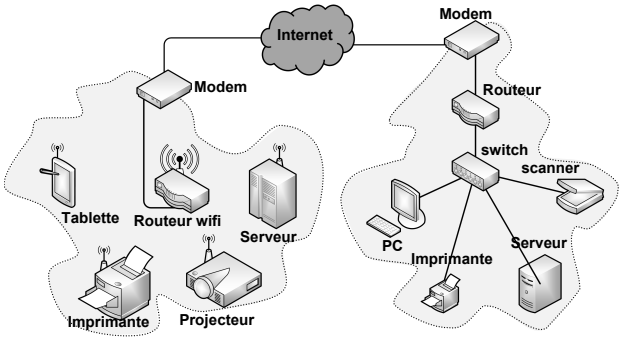
Chapitre 13 : Architecture des réseaux

I. Introduction

Internet constitue le plus grand réseau mondial de transmission de données. Il résulte de l'interconnexion d'innombrables réseaux de tailles variées, permettant aux ordinateurs, appelés hôtes, d'échanger des informations. Chaque hôte peut être à la fois émetteur et récepteur, assurant ainsi la circulation continue des données à travers cette vaste infrastructure de communication universelle.

La connexion Internet repose sur trois éléments complémentaires :

- **Connexion physique :** elle assure le transfert des signaux via les supports de transmission (câbles, fibres optiques, ondes radio).
- **Connexion logique :** elle est établie grâce aux protocoles de communication qui définissent les règles d'échange des données.
- **Applications logicielles :** comme les navigateurs web, elles exploitent ces protocoles pour rendre l'information lisible et compréhensible par l'utilisateur.

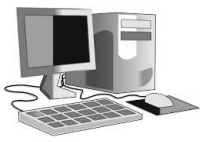


II. Terminologie liée aux réseaux informatiques

1. Equipements utilisés

Les équipements de réseau se répartissent en deux grandes catégories :

➲ **Équipements d'utilisateur final (hôtes) :** ce sont les terminaux directement utilisés par les usagers, tels que les ordinateurs, imprimantes, smartphones ou scanners. Ils constituent les points d'entrée et de sortie de l'information.



PC bureau

Imprimant

scanner

Projecteur

Smartphone

➲ **Équipements intermédiaires de réseau :** Les éléments intermédiaires d'un réseau informatique acheminent, filtrent et contrôlent le trafic entre appareils connectés. Ils assurent une communication efficace et sécurisée. Parmi eux figurent les plus utilisés tels que les commutateurs, routeurs, points d'accès et pare-feu.

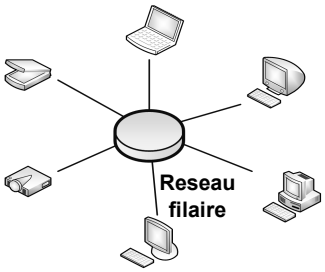
	**Switch (commutateur réseau)** Un switch est un dispositif qui relie plusieurs appareils sur un réseau local (LAN) et qui transmet les données uniquement aux destinataires appropriés, améliorant ainsi l'efficacité du réseau.		**Routeur réseau** Un routeur relie plusieurs réseaux informatiques et choisit le chemin optimal pour transmettre les paquets de données, en se basant principalement sur l'adresse IP de destination.
	**Passerelle réseau (Gateway)** Une passerelle relie des réseaux utilisant des protocoles, formats ou architectures différents. Elle traduit les données, assurant ainsi une communication fluide et compatible entre systèmes hétérogènes.		**Firewall (pare-feu)** Un pare-feu est un dispositif matériel ou logiciel qui filtre le trafic réseau selon des règles de sécurité, protégeant contre les intrusions, attaques DDoS et autres menaces potentielles.

	**Répéteur (Repeater)** Un répéteur amplifie et retransmet les signaux électriques ou optiques d'un réseau afin d'étendre sa portée et de réduire l'affaiblissement du signal sur de longues distances.		**Hub (concentrateur réseau)** Un hub connecte plusieurs appareils d'un réseau local en diffusant toutes les données reçues à chaque périphérique, sans distinction, ce qui peut provoquer des collisions et ralentir les performances globales du réseau.

2. Topologies physiques des réseaux

La topologie physique d'un réseau décrit l'organisation réelle de son infrastructure. Elle précise la manière dont les câbles, fibres ou supports de transmission relient les différents équipements. Cette configuration détermine la structure du réseau, influence ses performances, sa fiabilité ainsi que la facilité de maintenance.

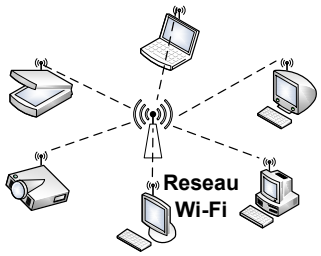
Topologie en étoile :



Dans cette configuration, **tous les hôtes** sont reliés à un **point central** (commutateur ou concentrateur).

☑ **Avantage** : la coupure d'un câble n'affecte que l'équipement concerné, le reste du réseau continue de fonctionner.

✗ **Inconvénient** : lorsque le nombre de stations augmente, le coût du câblage et de l'équipement central devient important.

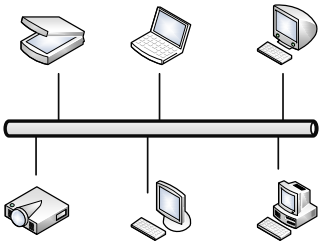


Topologie en bus :

Dans ce type de réseau, toutes les stations partagent une **seule ligne** de transmission appelée **bus**. Les extrémités sont terminées par des bouchons qui absorbent les signaux pour éviter les réflexions.

☑ **Avantage :** simplicité et faible coût de mise en œuvre.

✗ **Inconvénient :** une rupture du bus rend l'ensemble du réseau inutilisable.

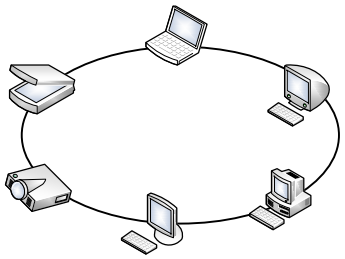


Topologie en anneau :

La topologie en anneau, ou en boucle, relie les stations par des liaisons point à point formant un cercle fermé. Les données circulent dans une seule direction, de station en station, jusqu'à atteindre leur destinataire.

☑ **Avantage :** temps de transmission prévisible.

✗ **Inconvénient :** une panne sur une station ou un lien peut perturber tout le réseau.

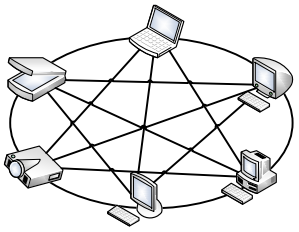


Topologie maillée :

Dans une topologie maillée, chaque équipement est relié à tous les autres par des liaisons directes. Cette organisation assure une forte robustesse : si une liaison est rompue, les données peuvent suivre un autre chemin.

☑ **Avantage :** grande fiabilité et tolérance aux pannes.

✗ **Inconvénient :** coût élevé et complexité de câblage.



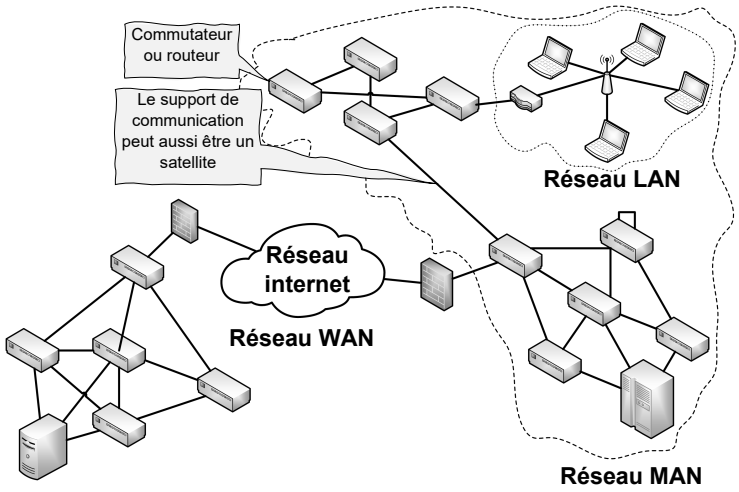
3. Types de réseaux

Les réseaux informatiques se différencient essentiellement par leur étendue géographique et leurs performances de transmission. On distingue généralement trois grandes catégories, chacune adaptée à un contexte d'utilisation particulier :

➲ **LAN (Local Area Network) :** réseau local limité à une zone restreinte (bâtiment, école, entreprise). Il relie ordinateurs et périphériques pour partager des ressources.

➲ **MAN (Metropolitan Area Network) :** réseau métropolitain couvrant une ville ou une grande agglomération. Il regroupe plusieurs LAN, par exemple une banque reliant ses différentes agences dans la même ville.

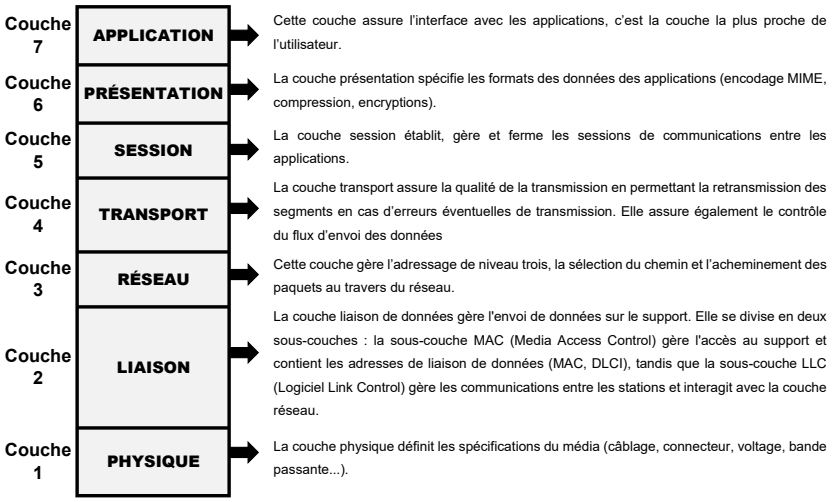
➲ **WAN (Wide Area Network) :** réseau étendu reliant de vastes zones géographiques, à l'échelle nationale ou internationale. Il interconnecte des sites distants via diverses technologies (fibre, satellite, etc.). Internet en est l'exemple le plus connu.



III. Modèles en couches

1. Modèle OSI (Open System Interconnection)

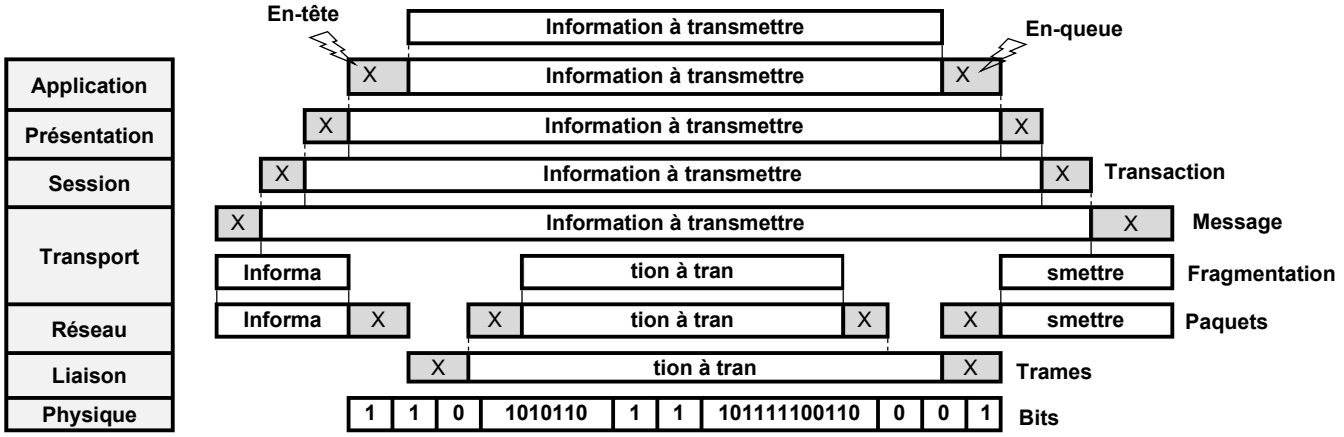
Le modèle **OSI**, proposé par l'**ISO** en 1984, constitue une **référence universelle** pour la communication entre systèmes informatiques. Il définit un cadre à **sept couches hiérarchisées**, chacune remplissant une fonction précise, afin d'assurer la **compatibilité** et l'**interopérabilité** entre matériels et logiciels de réseaux hétérogènes.



2. Encapsulation des données

L'encapsulation est le processus par lequel chaque couche du modèle OSI ajoute ses propres informations de protocole (en-têtes, parfois pieds de trame) aux données avant leur transmission sur le réseau.

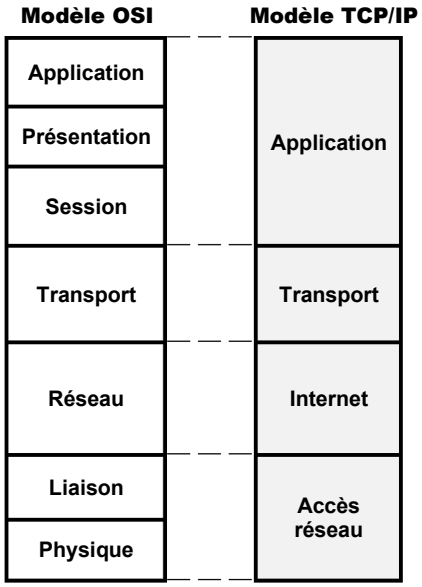
À la réception, l'opération inverse, appelée désencapsulation, permet à chaque couche de retirer son en-tête pour restituer les données originales à l'application.



Ainsi, les hubs, Switchs, routeurs, passerelles, répéteurs et pare-feu interviennent à différents niveaux, assurant la transmission, la sécurité et l'interopérabilité entre réseaux, garantissant une communication fluide et fiable.

3. Modèle TCP/IP

Contrairement au modèle OSI, devenu surtout un cadre théorique, le modèle TCP/IP s'impose aujourd'hui comme la référence des réseaux modernes. Basé sur les protocoles **TCP (Transmission Control Protocol)** et **IP (Internet Protocol)**, il a profondément transformé l'interconnexion des systèmes d'information. Ce modèle simplifié regroupe les fonctions essentielles en **quatre couches principales** :



- Constitution des applications réseaux :

Les applications réseaux reposent sur des protocoles de haut niveau permettant d'exploiter les ressources des réseaux informatiques. Parmi les plus utilisés, on retrouve :

- Le courrier électronique (**SMTP**),
- Le transfert de fichiers (**FTP**),
- Les connexions à distance (**TELNET**),
- Le World Wide Web (**HTTP**),
- Ainsi que des protocoles de sécurité (**SSL**, **TLS**).

- Elle assure **l'envoi des messages** vers le **destinataire** :

- **TCP :** fiable, avec contrôle d'erreurs.
- **UDP :** rapide, sans garantie de livraison.

- Elle gère l'adressage et le routage des paquets :

- **IP (IPv4 / IPv6) → adressage et routage des paquets.**
- **ICMP → messages de contrôle et de diagnostic (ping)**
- **ARP → résolution d'adresse (IP → MAC) dans un réseau local.**

- Comment transmettre des paquets de données ?

- Constitution des trames (Ethernet, Wi-Fi).
- Gestion des erreurs (détection/correction).
- Organisation de l'accès au support.
- Transmission sur câbles ou ondes.

IV. Couche physique

La couche physique est la première et la plus basse couche du modèle OSI. Elle définit les règles permettant de transmettre des bits (0 et 1) sous forme de signaux électriques, optiques ou électromagnétiques sur un support de communication. Son rôle est de transformer les données numériques en signaux adaptés au média choisi : câble cuivre, fibre optique ou ondes radio. Elle prend en charge la **synchronisation** entre émetteur et récepteur, le choix des niveaux de tension, la fréquence, la durée des impulsions, ainsi que les aspects mécaniques des connecteurs et des câbles. Elle définit également les techniques de modulation et d'encodage.

Remarque : *Cette partie a déjà été traitée dans le chapitre précédent consacré à la* ***transmission de l'information****.*

V. Étude de la couche Liaison

La couche liaison de données assure une transmission fiable entre machines connectées. Elle **encapsule** les paquets en **trames**, ajoute les **adresses MAC** et les codes de **contrôle,** puis gère la **détection** et la **correction d'erreurs**. Elle régule également le **flux de transmission**, délimite les trames et contrôle l'accès au support partagé comme Ethernet ou Wi-Fi. Ainsi, elle **organise** et **sécurise** l'échange de données entre la couche physique et la couche réseau.

Dans notre cours, nous nous intéressons particulièrement aux **trames Ethernet**, qui constituent l'unité de base de transmission dans un réseau local. La couche liaison gère l'**adressage physique**, assuré par les adresses MAC permettant d'identifier l'émetteur et le récepteur. Elle intègre également le **CRC (Cyclic Redundancy Check)**, un mécanisme essentiel de détection d'erreurs garantissant l'intégrité des données échangées entre machines connectées.

1. Trame Ethernet

Une trame Ethernet est l'unité de base d'échange sur un réseau local. Elle enveloppe les données, transporte les adresses MAC source et destination, précise le protocole encapsulé, et inclut un CRC pour détecter d'éventuelles erreurs durant la transmission.

Préambule	MAC destination	MAC source	Type	Données	CRC
8 octets	6 octets	6 octets	2 octets	46 à 1500 octets	4 octets

- **Préambule** : pour la synchronisation d'horloge et ses octets vaut 1010 1010 sauf le dernier vaut 1010 1011.
- **MAC destination :** adresse physique du destinataire.
- **MAC source :** adresse physique de l'émetteur.
- **Type :** le type de protocole inséré dans le champ de données (0x0800 : IPv4, 0x86DD : IPv6, 0x809B : AppleTalk, 0x0806 : ARP, 0x8035 : RARP).
- **Données :** contient les données de la couche 3.
- **CRC :** Il constitue la séquence de contrôle de la trame, ce qui permet à l'adaptateur qui reçoit cette trame de repérer toute éventuelle erreur qui aurait pu se glisser dans son contenu.

2. Adresse physique ou adresse MAC de la carte réseau

Les adresses MAC (source et destination) sont des identifiants physiques de **48 bits** (6 octets) portés par la carte réseau. Les **3 premiers octets** forment l'**OUI** (*Organizationally Unique Identifier*) attribué par l'IEEE au fabricant ; les **3 octets suivants** sont assignés par ce fabricant pour distinguer chaque interface. Cette organisation garantit l'**unicité mondiale** des adresses MAC.

Identificateur d'organisation OUI (3 octets)	Numéro d'identifiant de la carte réseau (3 octets)

Exemple : Trame ETHERNET

MAC Dest... MAC source type

AA AA AA AA AA AA AA AB 00 01 02 AF F5 E2 00 60 08 61 04 7B 08 00 45 00 00 3D DC 56 00 00 80 11 AA 42 0A 0A 9F 02 0A 0A 01 01 0A 79 00 35 00 29 A1 E4 00 02 01 00 00 01 00 00 00 00 00 00 02 77 70 08 6E 65 74 73 63 61 70 65 03 63 6F 6D 00 00 01 00 01

CRC

Question : Indiquer les informations partager dans cette trame Ethernet :

MAC destinataire	MAC source	Type de protocole (couche 3)	Données CRC
00 01 02 AF F5 E2	00 60 08 61 04 7B	0800 (IPv4)	00 01 00 01

3. Contrôle par redondance cyclique CRC

Le **CRC (Cyclic Redundancy Check)** est une méthode de **détection d'erreurs** sur des trames Ethernet. L'émetteur calcule un **reste** selon une division binaire particulière et l'ajoute à la trame (champ **CRC**). Le récepteur refait le calcul : si le reste vaut **0**, on considère la trame intègre.

Données B : $[b_{n-1}\ b_{n-2}\ldots b_2\ b_1\ b_0]$	CRC (reste) : $[r_{k-1}\ r_{k-2}\ldots r_2\ r_1\ r_0]$

Le principe repose sur l'idée qu'à tout mot binaire $b_{n-1}\ b_{n-2}\ldots b_0$ on peut associer un polynôme, en prenant chaque bit b_i comme coefficient du terme x^i, tel que : $B(x) = b_{n-1}.x^{n-1} + b_{n-1}.x^{n-1} + \cdots + b_2.x^2 + b_1.x + b_0$

À l'émission, on multiplie le polynôme du message **B(x)** par x^k, puis on divise ce produit par le polynôme générateur **G(x)** (de degré **k**). Le reste de cette division, appelé **CRC**, est ensuite ajouté au mot binaire comme champ de contrôle d'erreur.

Remarque : Le polynôme générateur G(x) est commun entre l'émetteur et le récepteur. C'est une convention fixée par la norme du protocole (Ethernet, USB, CAN, etc.).

Exemple : soit une donnée binaire à émettre $B = 101001_{(2)}$ avec $G = 1011_{(2)}$

➔ Construction des polynômes :

- La longueur de B est n + 1= **6 bits** → ordre de B(x) : **n = 5**.

  D'où : $B(x) = 1.x^5 + 0.x^4 + 1.x^3 + 0.x^2 + 0.x^1 + 1.x^0 \Rightarrow \boxed{B(x) = x^5 + x^3 + 1}$

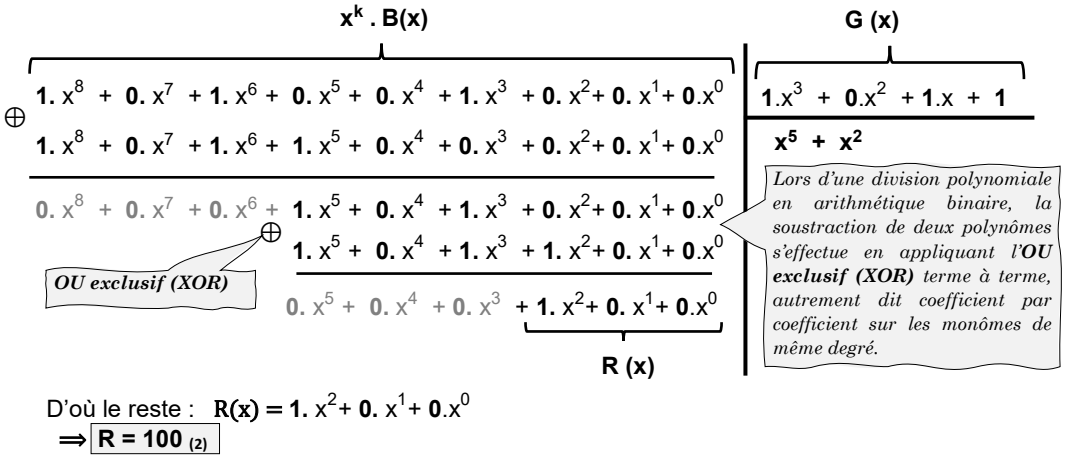
- La longueur de G est k + 1= **4 bits** → ordre de G(x) : **k = 3**.

  D'où : G(x) = **1**. x^3 + **0**. x^2 + **1**. x^1 + **1**. x^0 ⟹ **$G(x) = x^3 + x + 1$**

➔ Décalage : Polynôme $x^k.B(x)$:

On a **k = 3** ⟹ **$x^3.B(x) = x^3 . (x^5 + x^3 + 1)$** ⟹ **$x^3.B(x) = x^8 + x^6 + x^3$**

➔ Division euclidienne : $x^k.B(x)$ / G(x) :



D'où le reste : **$R(x) = 1. x^2 + 0. x^1 + 0.x^0$**

⟹ **$R = 100_{(2)}$**

➔ Le message transmis T(x) :

Le message à transmettre est la combinaison entre B(x) et R(x) : **T(x) = B(x) || R(x)** :

Donc : T = (101001) || (100) ⟹ finalement : **T = 101001100**

Cette technique offre une très forte capacité de détection des erreurs sur le support de transmission. Les polynômes générateurs G(x) sont **normalisés**. Leur **degré** se choisit selon le contexte : plus le risque d'erreur ou la **taille du bloc** à protéger est élevé, plus ce degré doit être grand. Les principaux polynômes employés sont :

- Pour le USB, Bluetooth (CRC-16) : **$G(x) = x^{16} + x^{12} + x^5 + 1$**
- Ethernet (CRC-32) : **$G(x) = x^{32} + x^{26} + x^{23} + x^{22} + x^{16} + x^{12} + x^{11} + x^{10} + x^8 + x^7 + x^5 + x^4 + x^2 + x + 1$**

VI. Étude de la couche Réseau

La couche réseau occupe une place essentielle dans l'acheminement des données à travers les réseaux informatiques. Elle garantit que les paquets atteignent leur destination en gérant l'**adressage logique**, le **routage** et certains aspects liés au contrôle de trafic et à la sécurité. Elle constitue ainsi un maillon central dans la communication entre machines distantes. Dans ce cours, nous limiterons notre étude aux notions d'**adresses IP**, en nous focalisant sur le protocole **IPv4**.

1. Adressage IP

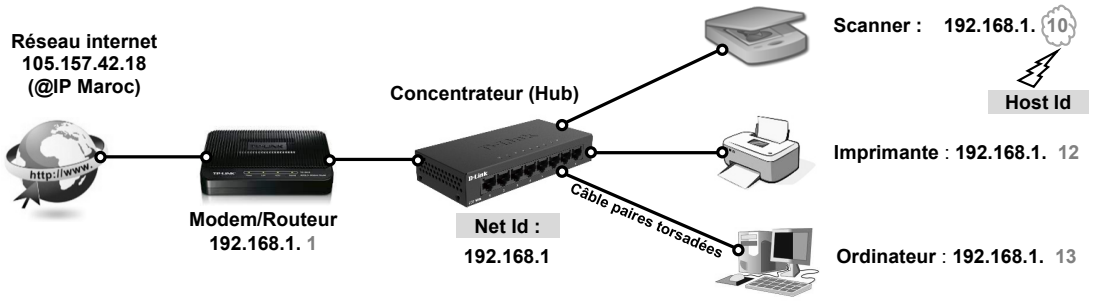
L'adressage IP est le mécanisme qui attribue à chaque machine ou périphérique connecté à un réseau une adresse unique, appelée adresse IP. Cette adresse permet d'identifier l'émetteur et le destinataire des données, d'assurer le routage par les routeurs et de garantir une communication fiable. En IPv4, elle est codée sur 32 bits (4 octets) : Ex **192 . 168 . 1 . 13**.

192								168								1								13							
1	1	0	0	0	0	0	0	1	0	1	0	1	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	1	1	0	1

Une adresse IP se compose de deux éléments :

- **Le Net ID**, qui correspond à la partie fixe permettant d'identifier le réseau.
- **Le Host ID**, qui désigne la partie variable servant à identifier chaque machine (hôte) au sein de ce réseau.

Exemple : **Un réseau local LAN connecté au réseau WAN (l'internet)**



Ce schéma montre l'adressage IP dans un réseau local : le routeur (192.168.1.1) connecte Internet au hub, qui diffuse le **Net ID 192.168.1** vers tous les périphériques. Chaque machine est distinguée par un **Host ID** unique (ex. 10, 13).

2. Classe d'adressage IP

L'**ICANN (Internet Corporation for Assigned Names and Numbers)** est l'autorité internationale chargée d'attribuer les numéros aux différents réseaux. Les administrateurs réseau se chargent ensuite d'attribuer les adresses complètes aux machines. Selon la taille et l'importance du réseau, plusieurs **classes d'adresses** existent. On distingue généralement trois classes principales :

2.1. Classe A

La classe A correspond aux réseaux de très grande envergure. Elle a historiquement été attribuée à de grandes organisations et institutions, comme le ministère de la Défense américain ou encore des entreprises telles qu'IBM, DEC et HP. La majorité de ces réseaux se trouvent aux États-Unis.

Net Id								Host Id																			
1er octet								2ème octet								3ème octet								4ème octet							
0	Y	Y	Y	Y	Y	Y	Y	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X

Nombre de réseaux possibles	Nombre de machines possibles	Adresse min	Adresse max
$2^7 - 2 = 126$	$2^{24} - 2 = 16\,777\,214$	0.0.0.0	127.255.255.255

(-2) : la 1ère et dernière adresse ne s'affectent pas aux machines et elles sont réservées pour d'autre cas particuliers

2.2. Classe B

La classe B est destinée aux réseaux de taille intermédiaire, tels que ceux utilisés par les universités, grandes écoles ou entreprises de dimension nationale et internationale. Elle offre un bon compromis entre nombre de réseaux disponibles et nombre d'hôtes par réseau.

Net Id																Host Id															
1er octet								2ème octet								3ème octet								4ème octet							
1	0	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X

Nombre de réseaux possibles	Nombre de machines possibles	Adresse min	Adresse max
$2^{14} - 2 = 16\,384$	$2^{16} - 2 = 65\,534$	128.0.0.0	191.255.255.255

2.3. Classe C

La classe C est réservé aux réseaux de petite taille, souvent utilisés par les petites entreprises ou les réseaux locaux. Elle permet de disposer d'un grand nombre de réseaux, chacun pouvant accueillir un nombre limité d'hôtes.

Net Id																								Host Id							
1er octet								2ème octet								3ème octet								4ème octet							
1	1	0	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	X	X	X	X	X	X	X	X

Nombre de réseaux possibles	Nombre de machines possibles	Adresse IP min	Adresse IP max
$2^{21} - 2 = 2\,097\,150$	$2^8 - 2 = 254$	192.0.0.0	223.255.255.255

➲ Cas particulier

En plus des classes d'adresses A, B et C, certaines adresses IP ne sont pas utilisées pour des communications publiques. Elles sont réservées à des usages spécifiques (privés, tests ou internes) :

- **255.255.255.255** : adresse de diffusion (*broadcast*), utilisée lorsqu'une machine envoie un message à toutes les autres machines d'un même réseau.
- **127.0.0.0 :** appelée adresse de rebouclage (*loopback*), elle désigne la machine locale (*localhost*) et permet de tester TCP/IP sans passer par une interface réseau physique.
- **0.0.0.0 :** utilisée par une machine qui ne connaît pas encore son adresse IP au démarrage.

➲ Adressages privés réservées à l'usage privé :

Classe	Adresse min	Adresse max
A	10.0.0.0	10.255.255.255
B	172.16.0.0	172.31.255.255
C	192.168.0.0	192.168.255.255

3. Masque de sous réseau

Le masque de sous-réseau (ou masque IP) est un élément essentiel dans la gestion des adresses IP. Il permet de séparer une adresse IP en deux parties distinctes : la **partie réseau**, représentée par des « 1 », et **la partie hôte**, représentée par des « 0 ». Grâce à ce mécanisme, on distingue l'adresse du réseau et celle des machines qui y sont connectées.

Les masques de sous-réseau par défaut, associés aux classes d'adresses standard, sont :

Classe	Masque sous réseau	
A	**/8** soit **255.0.0.0**	**/8** désigne le nombre des «1» est **8**.
B	**/16** soit **255.255.0.0**	
C	**/24** soit **255.255.255.0**	

Remarque : Un « **ET logique** » entre l'adresse IP et le masque permet d'identifier le réseau ou sous-réseau de la machine pour orienter l'information.

Exemple 1 : Considérons une machine ayant l'adresse IP 192.168.1.1 avec le masque 255.255.255.0.

Adresse IP	192.168.12.1	11000000.10101000.00001100.00000001
Masque	255.255.255.0	11111111.11111111.11111111.00000000
« ET logique »	192.168.12.0	← 11000000.10101000.00001100.00000000

Donc l'identifiant réseau : 192.168.12.0

Exemple 2 : Considérons deux machines souhaitant échanger des données.

	Machine n°1	Machine n°2
Adresse IP	**192.59.66.200**	**192.59.66.17**
Masque	255.255.255.0	255.255.255.0
« ET logique »	192.59.66.0	192.59.66.0

Ces deux hôtes peuvent-ils échanger des données sans intermédiaire ? Les deux machines appartient au même réseau, elles peuvent donc communiquer directement.

4. Protocoles de la couche réseau

La couche réseau du modèle OSI garantit l'acheminement des paquets entre machines, indépendamment du support. Elle repose sur divers protocoles définissant adressage, routage et contrôle des communications.

Parmi l'ensemble des protocoles existants, trois sont fondamentaux pour comprendre le fonctionnement des réseaux actuels :

- **IPv4**, qui constitue le protocole principal d'**adressage et d'acheminement des paquets**.
- **ICMP**, utilisé pour la **gestion des erreurs et le diagnostic** des connexions.
- **ARP**, permet de trouver **l'adresse MAC** associée à une **adresse IP**.

On s'intéresse ici à la trame IPv4, chargée d'assurer l'adressage des hôtes ainsi que l'acheminement des paquets de données à travers le réseau. Sa structure, présentée ci-dessous, permet d'organiser les informations nécessaires au routage et au contrôle de la transmission.

<table>
<tr><th>0</th><th>1</th><th>2</th><th>3</th><th>4</th><th>5</th><th>6</th><th>7</th><th>8</th><th>9</th><th>10</th><th>11</th><th>12</th><th>13</th><th>14</th><th>15</th><th>16</th><th>17</th><th>18</th><th>19</th><th>20</th><th>21</th><th>22</th><th>23</th><th>24</th><th>25</th><th>26</th><th>27</th><th>28</th><th>29</th><th>30</th><th>31</th></tr>
<tr><td colspan="4">Version d'IP</td><td colspan="4">Longueur de l'en-tête</td><td colspan="8">Type de service</td><td colspan="16">Longueur totale en octet</td></tr>
<tr><td colspan="16">Identification (pour les fragments)</td><td colspan="3">Flag</td><td colspan="13">Fragment offset</td></tr>
<tr><td colspan="8">Durée de vie</td><td colspan="8">Protocole **</td><td colspan="16">Somme contrôle de l'entête</td></tr>
<tr><td colspan="32">Adresse IP source</td></tr>
<tr><td colspan="32">Adresse IP destination</td></tr>
<tr><td colspan="32">Option + Bourrage</td></tr>
<tr><td colspan="32">Données</td></tr>
</table>

** Indique le protocole de la couche supérieure — transport — (**TCP = 6**, **UDP = 17**, **ICMP = 1**).

Remarque : En IPv4, la taille maximale du champ de données peut atteindre **64 Ko**. Toutefois, les réseaux ne supportent pas des trames aussi longues. Chaque trame possède une taille maximale appelée **MTU (Maximum Transmission Unit)**, fixée à **1500 octets** pour Ethernet. Lorsque la taille d'un paquet (datagramme) dépasse la valeur du MTU, celui-ci est automatiquement découpé en plusieurs fragments pour être transmis.

VII. Étude de la couche Transport

La couche transport du modèle OSI gère la transmission de données entre applications. Elle segmente les messages en paquets, contrôle les erreurs et régule le flux pour assurer une communication efficace. Deux protocoles dominent : **TCP**, garantissant fiabilité et ordre des données utilisé par exemple dans la transmission des E-mails et **UDP**, privilégiant rapidité et simplicité, souvent utilisé pour le multimédia en temps réel.

1. Protocole UDP (User Datagram Protocol)

Le protocole **UDP (User Datagram Protocol)**, défini dans la RFC768, appartient à la couche transport du modèle TCP/IP. Contrairement à TCP, il fonctionne en mode non connecté et ne garantit ni l'ordre ni la réception des paquets, ce qui en fait un protocole non fiable. Cependant, il assure une vérification simple des données par checksum. Sa légèreté et sa rapidité le rendent adapté aux applications multimédias et temps réel. Le **datagramme UDP** est encapsulé dans un paquet IP. Il comporte un en-tête suivi des données proprement dites à transporter.

<table>
<tr><th>0</th><th>1</th><th>2</th><th>3</th><th>4</th><th>5</th><th>6</th><th>7</th><th>8</th><th>9</th><th>10</th><th>11</th><th>12</th><th>13</th><th>14</th><th>15</th><th>16</th><th>17</th><th>18</th><th>19</th><th>20</th><th>21</th><th>22</th><th>23</th><th>24</th><th>25</th><th>26</th><th>27</th><th>28</th><th>29</th><th>30</th><th>31</th></tr>
<tr><td colspan="16">Port Source</td><td colspan="16">Port destination</td></tr>
<tr><td colspan="16">longueur</td><td colspan="16">Somme de contrôle</td></tr>
<tr><td colspan="32">Données (longueur variable)</td></tr>
</table>

L'en-tête UDP contient quatre champs : **port source** (origine du paquet), **port de destination** (cible du paquet), **longueur** (taille totale du segment, minimum **8 octets**) et **somme de contrôle (checksum)**. Ce dernier garantit l'intégrité en incluant un pseudo en-tête IP, illustrant l'interdépendance entre les couches IP et UDP.

2. Protocole TCP (Transmission Control Protocol)

Le protocole TCP (Transmission Control Protocol), défini dans la RFC793, appartient à la couche transport du modèle TCP/IP. Il est fiable, orienté connexion, et découpe les flux d'octets en segments adaptés à la MTU. Son fonctionnement repose sur trois étapes : établissement de la connexion, transfert des données, puis terminaison. Il garantit une transmission sans perte, ordonnée et contrôlée entre applications

<table>
<tr><td>0</td><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td><td>7</td><td>8</td><td>9</td><td>10</td><td>11</td><td>12</td><td>13</td><td>14</td><td>15</td><td>16</td><td>17</td><td>18</td><td>19</td><td>20</td><td>21</td><td>22</td><td>23</td><td>24</td><td>25</td><td>26</td><td>27</td><td>28</td><td>29</td><td>30</td><td>31</td></tr>
<tr><td colspan="16">Port source</td><td colspan="16">Port de destination</td></tr>
<tr><td colspan="32">Numéro de séquence</td></tr>
<tr><td colspan="32">Numéro d'acquittement</td></tr>
<tr><td colspan="4">Taille de l'en-tête</td><td colspan="3">Réservé</td><td colspan="3">ECN</td><td colspan="2">URG</td><td colspan="2">ACK</td><td colspan="2">PSH</td><td colspan="2">RST</td><td colspan="2">SYN</td><td colspan="2">FIN</td><td colspan="16">Fenêtre</td></tr>
<tr><td colspan="16">Somme de contrôle</td><td colspan="16">Pointeur de données urgentes</td></tr>
<tr><td colspan="24">Options</td><td colspan="8">Remplissage</td></tr>
<tr><td colspan="32">Données</td></tr>
</table>

L'en-tête TCP contient plusieurs champs essentiels. On y retrouve les **ports source** et **destination**, les **numéros de séquence** et **d'acquittement** qui assurent l'ordre des données, ainsi que la **taille de l'en-tête**. Des indicateurs comme les **drapeaux (URG, ACK, PSH, RST, SYN, FIN)** permettent de gérer l'établissement, le contrôle et la fin de connexion. La **fenêtre** définit la quantité de données acceptées **sans accusé de réception**. La **somme de contrôle (checksum)** garantit l'intégrité, complétée par le **pointeur urgent**, les **options** et les **données applicatives** de la couche supérieure.

VIII. Étude de la couche Application

La couche application du modèle TCP/IP constitue le niveau le plus proche de l'utilisateur. Elle regroupe l'ensemble des protocoles permettant aux applications d'échanger des données sur un réseau, tels que HTTP, FTP, SMTP ou DNS. Cette couche ne se limite pas au simple transfert d'informations : elle définit aussi les règles de communication entre programmes. Dans le modèle OSI, elle correspond à la combinaison des couches **Application, Présentation** et **Session**, réunies dans TCP/IP pour plus de simplicité.

Les protocoles les plus utilisés au sein de la couche application du modèle TCP/IP et leurs principales fonctions sont présentés ci-dessous :

- **HTTP (HyperText Transfer Protocol) :** protocole utilisé pour transférer des pages web et du contenu multimédia entre un serveur et un navigateur.
- **HTTPS (HyperText Transfer Protocol Secure) :** version sécurisée de HTTP, qui chiffre les données échangées grâce au protocole SSL/TLS pour garantir confidentialité et intégrité.
- **DNS (Domain Name System) :** service qui traduit les noms de domaine (ex. www.exemple.com) en adresses IP afin de localiser les serveurs sur Internet.
- **DHCP (Dynamic Host Configuration Protocol) :** protocole qui attribue automatiquement une adresse IP et d'autres paramètres réseau aux machines d'un réseau.
- **FTP (File Transfer Protocol) :** protocole destiné au transfert de fichiers entre un client et un serveur.
- **SSH (Secure Shell) :** protocole sécurisé permettant d'accéder à distance à une machine et d'y exécuter des commandes de manière chiffrée.
- **SMTP (Simple Mail Transfer Protocol) :** protocole utilisé pour l'envoi de courriers électroniques vers un serveur de messagerie.

Références bibliographiques :

- **C. François**, Les grandes fonctions de la chaîne d'information - IUT, BTS, CPGE, FRANCE : Ellipses, 2016
- **Fraisse, P.**, **Protière, R.**, & **Marty-Dessus, D**. (1999). Télécommunications 1 : Transmission de l'information. Paris : Ellipses.
- **M, RAHBAOUI**. Introduction aux réseaux TCP/IP [PDF]. ENSET Rabat, Année universitaire 2015/2016