Chapitre 4

Réseaux

4.1 Un peu d'histoire

Le réseau ARPANET (Advanced Research Projects Agency Network) est crée aux États-Unis dans les années 1960. Le projet débute en 1966 et sa première démonstration publique a lieu en 1972. Il s'agit du premier réseau informatique à transfert de paquets et est donc considéré comme l'ancêtre d'internet. Il reliait initialement les quelques ordinateurs présents dans les universités américaines afin de partager leurs ressources et d'unifier les techniques de connexion d'un terminal à un autre ordinateur distant et de constructeur différent. De quelques dizaines à ses débuts, le nombre de nœuds du réseaux atteint une centaine dans la deuxième moitié des années 1970 et continue de croître.

En 1974, le protocole TCP/IP est crée afin d'uniformiser le réseau et définitivement adopté par ARPANET en 1983. Ce protocole sera à la base d'Internet. Le réseau se divise en deux, un à usage militaire et l'autre à usage universitaire. Durant les années 1990, les connexions grandissantes d'autres pays au réseau et l'arrivée d'acteurs privés et particuliers achève la transformation d'ARPANET en l'Internet que nous connaissons aujourd'hui. Celui-ci n'a alors cesser de croître depuis.

4.2 Les réseaux informatiques

Un réseau informatique est un ensemble de machines (ordinateurs, téléphones, etc) reliées entre elles et s'échangeant des informations par le biais d'installation matérielles (contrôleurs Ethernet, câbles Ethernet, fibres optiques, bornes WIFI, commutateurs, routeur, etc) et logicielles (pilotes des interfaces, firmwares des équipement, etc). Par exemple le réseau au sein d'un domicile, d'une entreprise, d'un lycée, etc. Le réseau doit permettre d'offrir à ses utilisateurs des services tels que : la mise à disposition d'imprimantes, l'accès à internet, l'échanges de fichiers, de courriels... Les contraintes sont nombreuses : un réseau doit être en capacité de transporter n'importe quel type d'information, de n'importe quelle taille, n'importe où tout en conciliant sécurité et fiabilité.

Internet désigne le réseau reliant l'ensemble de ces réseaux informatiques. Les ordinateurs reliés entre eux au sein de ces réseau et donc d'internet le sont par des moyens filaires (fibre optique, ADSL, etc.) ou non filaires (Wifi, Bluetooth, etc.). Internet est avant tout définit par ses protocoles, pas réellement par ses moyen physique de connexion.

4.2.1 Tailles de réseaux

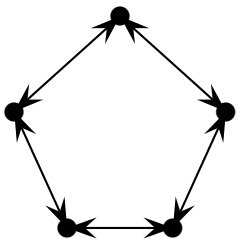
On distingue plusieurs tailles de réseaux, lesquels peuvent être intégré dans un des réseaux plus grands.

Nom	Signification	Échelle
PAN	Personal Area Network	1m
LAN	Local Area Network	10m - 100m
MAN	Metropolitan Area Network	1km - 10km
WAN	Wide Area Network	1km - 100km

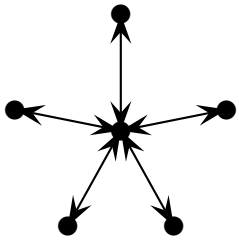
Le PAN peut par exemple représenter un téléphone connecté à un ordinateur par Bluetooth afin de partager une connexion Internet. Le LAN peut représenter l'ensemble des appareils connectés au sein d'un foyer ou des ordinateurs connectés dans une salle de classe. Le WAN correspond des tailles de réseaux d'entreprises ou d'institutions occupant de grands espaces ; par exemple, EDF, SNCF, etc possèdent des réseaux informatiques très étendus.

4.2.2 Topologies

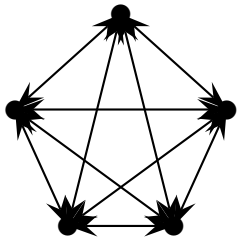
Il existe de nombreuses formes de réseaux. En voici quelques-unes parmi les plus connues.



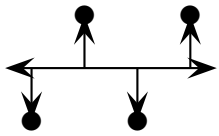
En anneau



En étoile / centralisé



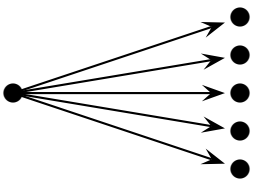
Pair-à-pair



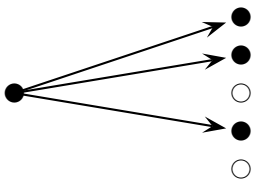
En bus

4.2.3 Modes de fonctionnement

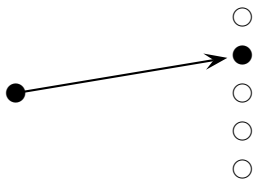
Pour les réseaux de petites tailles (PAN et LAN) on peut envoyer une information à tous les équipements (broadcast), ou certains seulement (multicast). Pour les grands réseau tel qu'internet par exemple, on communique avec un seul équipement (unicast) via de nombreux supports. Il doit exister au moins un chemin entre deux équipements.



Broadcast



Multicast



Unicast

4.3 L'IP, le routage, le MAC et le DNS

4.3.1 Adresses IP

L'adressage des machines sur le réseau est assuré par le protocole IP (Internet Protocol). Une adresse IP est codée sur quatre octets, donc quatre nombres compris entre 0 et 255, par exemple 66.178.234.0. Elle peut identifier une machine ou un sous-réseau, ce qui est souvent le cas dans la mesure où le nombre d'adresses IPv4 s'épuise à cause de l'augmentation constante de machines connectées à internet.

Deux approches visent à contourner ce problème :

— une transition de l'IPv4 (sur 4 octets) vers l'IPv6 (sur 16 octets) ;

— l'utilisateur de sous-réseaux grâce à des « masques de sous-réseaux » (que l'on verra plus bas).

Les adresses IP sont réparties en cinq catégories.

Classe	IP	Utilisation
A	0.0.0.0 à 126.255.255.255	Privées et publiques
B	128.0.0.0 à 191.255.255.255	Privées et publiques
C	192.0.0.0 à 223.255.255.255	Privées et publiques
D	224.0.0.0 à 239.255.255.255	Multicast
E	240.0.0.0 à 255.255.255.255	Réservées par l'IETF

Une adresse IP publique est unique à l'échelle planétaire et sert à identifier un sous-réseau ou une machine sur internet mais pas au sein d'un sous-réseau.

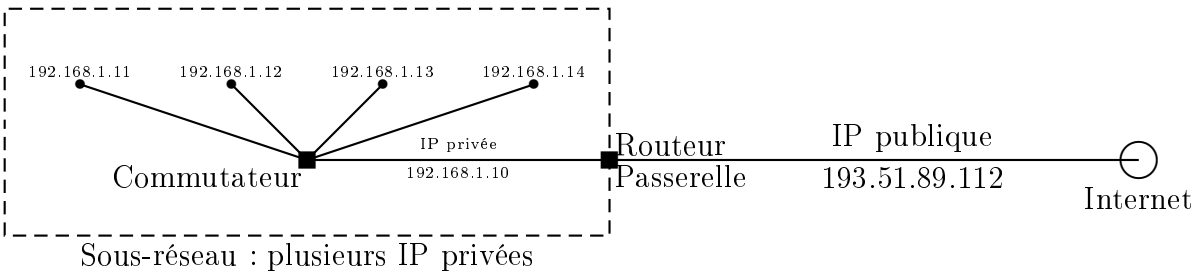
Une adresse IP privée est une adresse IP au sein d'un réseau local. Elle est unique au sein du réseau local mais ne l'est pas à l'échelle planétaire, elle n'est donc pas utilisable sur internet. Chacune des classes A, B et C possède une plage d'adresses privées :

Classe A : 10.0.0.0 à 10.255.255.255 ;

Classe B : 172.16.0.0 à 172.31.255.255 ;

Classe C : 192.168.0.0 à 192.168.255.255.

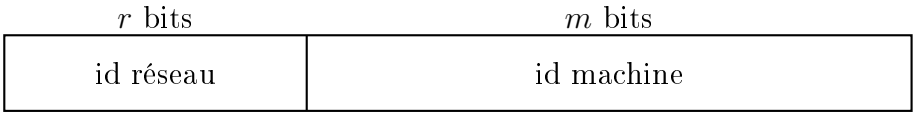
On peut donc retrouver plusieurs machines ayant la même adresse privée à condition que celles-ci soient dans des sous-réseaux différents.



Remarque : les adresses allant de 127.0.0.0 à 127.255.255.255 sont réservées pour des tests.

4.3.2 Masque de sous-réseau

L'adresse IP se décompose en deux parties : un identifiant réseau et un identifiant machine appartenant à ce réseau. Le tout étant codé sur 32 bits, on pourrait écrire $r + m = 32$.



Une machine connectée à un sous-réseau doit connaître son adresse IP et le nombre de bits attribués au réseau et au sous-réseau. C'est le masque de sous-réseau qui permet de déterminer le nombre de bits attribués au réseau ou au sous-réseau et donc par complémentarité à la machine. Il s'agit d'un mot de 32 bits obéissant aux règles suivantes :

— des 1 à la place des identifiants de réseau et sous-réseau ;

— des 0 à la place de l'identifiant machine.

Exemples :

— 11111111.11111111.11111111.00000000 donne 255.255.255.0 ; on a 24 bits de sous-réseau et 8 de machines, ce qui donne $2^8 = 256$ adresses machines possibles.

— 11111111.11111111.11111110.00000000 donne 255.255.254.0 ; on a 23 bits de sous-réseau et 9 de machines, ce qui donne $2^9 = 512$ adresses machines possibles.

Le nombre de bits attribués au réseau et au sous-réseau suit l'adresse IP en en étant séparé par un slash. Par exemple :

$$192.168.34.0 \ / \ 24$$

signifie qu'il y a 24 bits réservés au réseau et sous-réseau, donc 8 pour la machine.

Pour obtenir l'adresse du sous-réseau, on applique l'opération booléenne ET au masque et à l'adresse IP. Pour obtenir l'adresse de la machine, on applique cette même opération cette fois-ci entre l'adresse IP et le complément à 1 du masque.

Exemple : Considérons l'adresse IP 143.200.34.2 / 19. Son masque de sous-réseau est 255.255.224.0 ; appliquons à l'adresse IP. Convertis en binaire, ces deux adresses donnent avec l'opération ET :

$$\begin{array}{rl} & 10001111.11001000.00100010.00000010 \\ \& & 11111111.11111111.11100000.00000000 \\ = & 10001111.11001000.00100000.00000000 \end{array}$$

On obtient donc 143.200.32.0 comme adresse de sous-réseau. En prenant le complément à un du masque (i.e. en inversant tous ses bits), on obtient alors :

$$\begin{array}{rl} & 10001111.11001000.00100010.00000010 \\ \& & 00000000.00000000.00011111.11111111 \\ = & 00000000.00000000.00000010.00000010 \end{array}$$

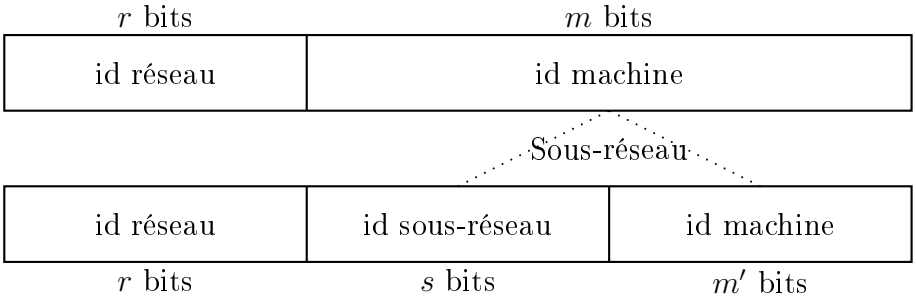
Ce qui donne 0.0.2.2 pour l'adresse machine.

Remarques :

— En réalité, les masques de sous-réseaux 0.0.0.0 et 255.255.255.255 ne comptent pas dans le nombre de machine à considérer dans les calculs ci-dessus. En effet, 255.255.255.255 désigne un réseau à une seule machine ou le réseau en entier et peut servir d'adresse de broadcast. 0.0.0.0 est utilisée par une machine pour connaître son adresse IP lors d'un processus d'amorçage.

— Le découpage par multiple de 8 bits n'est pas obligatoire même s'il facilite le travail des routeurs.

Il est possible de diviser l'adresse du sous-réseau pour créer plusieurs sous-réseaux distincts en changeant la valeur du masque de sous-réseau. Pour cela, on décompose l'identifiant machine en deux identifiants : un pour le sous-réseau et l'autre pour la machine. Toujours codé sur 32 bits, on pourrait écrire $r + s + m' = 32$. Cela permet d'affecter des bits à l'identification du sous-réseau sans toucher à d'identifiant du réseau qui doit demeurer intact.



Exemple : Un administrateur gère un réseau 192.44.78.0/24 qu'il aimerait décomposer en quatre sous-réseaux.

Pour cela, il réserve les deux premiers bits de l'identifiant machine pour identifier ses nouveaux sous-réseaux.

Sous-réseau	1	2	3	4
Identification	00	01	10	11

Toute adresse IP d'un même sous-réseau aura donc 24 bits en commun ainsi que les deux bits identifiant le sous-réseau. Le masque de sous-réseau peut ainsi être codé de la façon suivante : 11111111.11111111.11111111.11000000 en binaire, ce qui correspondra à 255.255.255.192 en décimal et donc à un / 26. Les sous-réseaux seront :

— 192.44.78.0/26 (les adresses de 192.44.78.0 à 192.44.78.63) ;

— 192.44.78.64/26 (les adresses de 192.44.78.64 à 192.44.78.127) ;

— 192.44.78.128/26 (les adresses de 192.44.78.128 à 192.44.78.191) ;

— 192.44.78.192/26 (les adresses de 192.44.78.192 à 192.44.78.255).

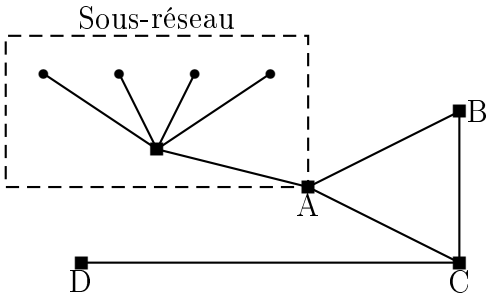
62 adresses de chaque sous-réseau seront utilisables pour numéroter des interfaces.

Remarque : de l'extérieur, l'ensemble des sous-réseaux est vu comme un unique réseau.

★ Calculateur de masque IPv4 du CNRS Grenoble.

4.3.3 Routage

Un routeur permet d'acheminer un « paquet » vers une destination au sein du réseau en utilisant une table de routage selon le principe des plus proches voisins.



Exemple de topologie

Tables de routage

Routeur A	
Pour	Envoyer à
B	B
C	C
D	C

Routeur B	
Pour	Envoyer à
A	A
C	C
D	C

Routeur C	
Pour	Envoyer à
A	A
B	B
D	D

Routeur D	
Pour	Envoyer à
A	C
B	C
C	C

Pour envoyer des données vers une autre machine, il faut d'abord pouvoir la localiser. On a deux possibilités :

— les deux machines font partie du même réseau local : c'est un **routage direct**.

— les deux machines ne font pas partie du même réseau local : c'est un **routage indirect**. Il faut alors passer par un intermédiaire qui permet de rejoindre l'extérieur du réseau : un routeur (aussi appelé passerelle ou gateaway en anglais).

Pour déterminer si le routage est direct ou indirect, il suffit de comparer les parties réseau des adresses IP du destinataire et de l'émetteur. Si elles sont identiques, les deux machines sont dans le même réseau et les données peuvent directement être envoyées. Sinon, elles doivent être remises au routeur pour un routage indirect. Le routeur se charge d'envoyer les données à un autre routeur selon se table de routage comme dans l'exemple ci-dessus.

4.3.4 Adresses MAC

L' adresse IP est une adresse de réseau données par l'administrateur réseau à une machine lorsque celle-ci s'y connecte. Elle est propre à la machine le temps qu'elle y est connectée mais cesse de l'être quand elle se déconnecte. Pour que le réseau puisse identifier uniquement la machine, on utilise une adresse MAC ; il s'agit d'une adresse matérielle unique : celle de la carte réseau de la machine. Le protocole ARP (Adress Résolution Problem) fournit une correspondance dynamique entre les deux adresses et s'assure qu'à chaque adresse IP du réseau correspond bien une machine.

4.3.5 L'annuaire d'internet : le DNS

Une adresse IP est un outil pour les machines mais pas pour les humains ; en effet, il est difficile de retenir que son site préféré a pour adresse 113.45.666.1 ! Les humains utilisent des adresses symboliques tels que mouette.org qui sont plus faciles à retenir.

La correspondance entre les adresses symboliques et IP est effectuée par les serveurs DNS (Domain Name System). L'annuaire DNS est organisé en domaines et sous-domaines, par

exemple .org est un domaine et wikipedia.org un sous domaine de celui-ci. Lorsque l'on saisit une adresse symbolique, une requête est envoyée à un serveur DNS qui renvoie l'IP correspondante et notre ordinateur se connecte alors à l'aide de l'IP.

Exemple de lecture d'une adresse symbolique

$$\text{https ://} \underbrace{\text{fr}}_{3} . \underbrace{\text{wikipedia}}_{2} . \underbrace{\text{org}}_{1} / \underbrace{\text{wiki}}_{4} / \underbrace{\text{Loutre}}_{5}$$

Le https : ne fait pas partie de l'adresse symbolique, il désigne en fait le protocole de connexion https (hypertext transfer protocol secure). Une adresse symbolique ne se lit pas tout à fait de gauche à droite mais comme suit.

1. Le .org est le domaine de premier niveau, il indique ici que nous sommes une adresse d'une organisation non gouvernementale.
2. Le sous-domaine wikipedia.
3. Une fois dans le domaine wikipedia.org, le fr indique que nous sommes sur la partie française du site.
4. Dans la partie française de wikipedia.org, on va dans le dossier wiki.
5. Dans ce dossier, on va sur la page loutre.

4.4 Modèle de couche OSI

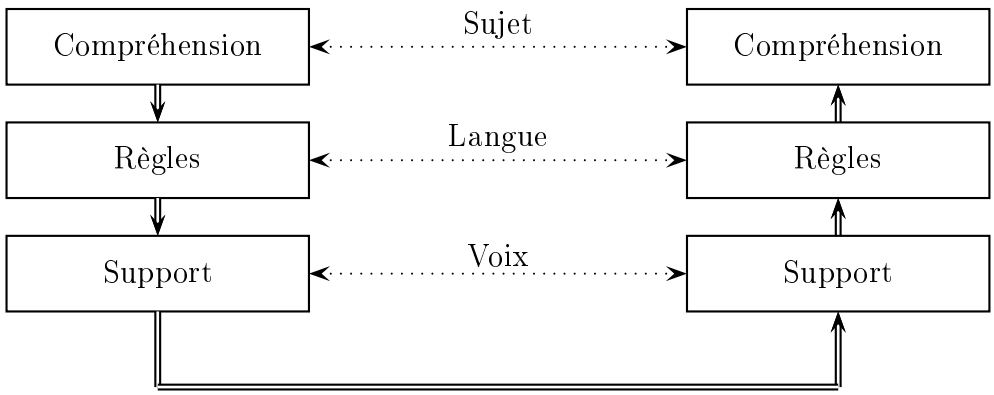
4.4.1 Notions de protocoles de communication

Pour pourvoir communiquer, deux interlocuteurs doivent respecter des règles communes :

Niveau de compréhension / connaissance identique : le sujet traité doit être accessible aux deux interlocuteurs ; un exposé sur la résolution d'une équation aux dérivées partielles sur un domaine multicouche irrégulier s'annonce ardu pour le spectateur non initié.

Règles de communication identiques : le sujet doit être traité avec des règles de communication communes aux deux interlocuteurs ; imaginez l'exposé ci-dessus en anglais.

Support de communication identique : la méthode d'expression doit être comprise des deux interlocuteurs ; imaginez que vous êtes sourd et que vous essayez de suivre l'exposé ci-dessus alors qu'il est intégralement oral, même en comprenant parfaitement l'anglais et le sujet, cela sera impossible.



Dans l'exemple précédent chaque niveau constitue une couche de communication. En informatique, on appelle **couche réseau** une entité qui fournit les moyens électriques et/ou fonctionnels nécessaires à l'activation, au maintien et à la désactivation des connexions destinées à la transmission de données numériques (ensemble de bits) entre deux entités de liaison de données.

4.4.2 Protocole OSI

Le modèle OSI (Open Systems Interconnection) est un protocole ISO de communication constitué de 7 couches permettant d'organiser la communication entre deux machines au sein d'un réseau. Un protocole de communication est une spécification standardisée qui permet la communication entre deux équipements. Il définit les règles et les procédures par lesquelles une information est transmise.

Couche	Nom	Description
7	Application	Point d'accès aux services du réseau (HTTPS, SMTP, SSH, etc)
6	Présentation	Conversion et chiffrement des données (formats, compression, etc)
5	Session	Établissement ou terminaison de la connexion, synchronisation
4	Transport	Découpage / reconstitution des données en segments (TCP, UDP)
3	Réseau	Routage des paquets grâce à l'IP
2	Liaison	Adressage physique (MAC) et trames (LAN)
1	Physique	Transmission binaire (Wifi, Éthernet, etc)

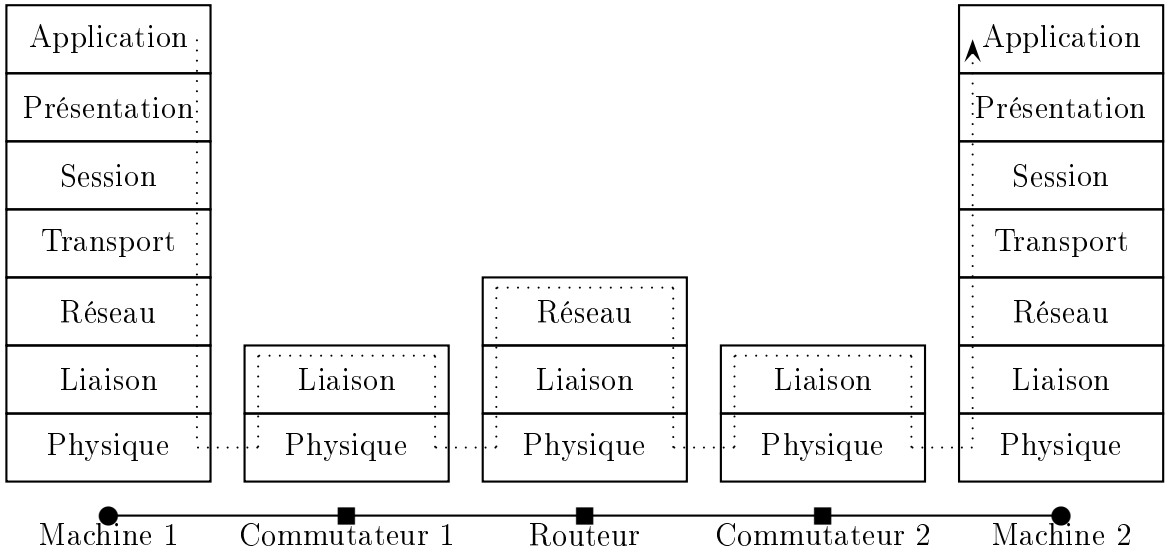
Couches 7,6 et 5 : le message qui est au bon format doit être utilisé pour réaliser une certaine tâche. Il doit donc être transmis vers un destinataire, qui peut par exemple être repéré par une adresse de courriel pour POP (ou IMAP) et SMTP. Ce sont les **couches hautes**.

Couche 4 : le message est découpé en segments numérotés, avec un numéro de port correspondant à l'application utilisée (80 pour HTTP ; 443 pour HTTPS ; 25 pour SMTP...). On vérifie à ce niveau si l'ordre est respecté, si chaque segment a été reçu, quel est l'état de la connexion (en écoute, en attente de fermeture). On est entré dans les **couches matérielles** ou **basses**.

Couche 3 : les segments sont encapsulés dans des paquets IP qui contiennent en plus les adresses logiques de la source et du destinataire, la longueur du paquet et sa durée de vie. À ce stade, on teste si la source et le destinataire sont dans le même réseau, sinon la source au niveau de cette couche devient un routeur (passerelle) disposant d'une table de routage.

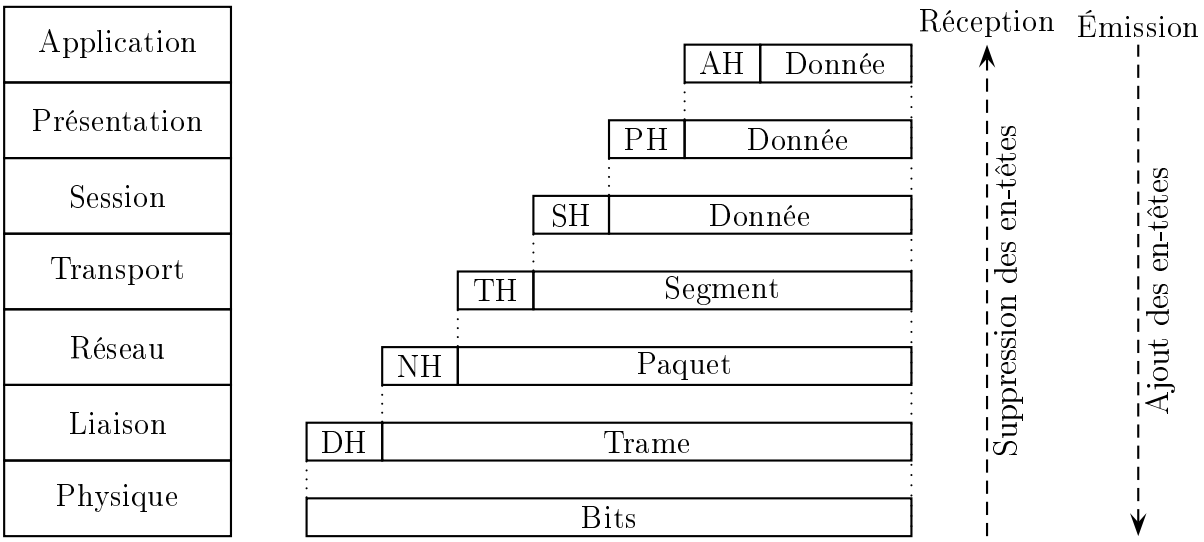
Couche 2 : elle est atteinte lorsque le dernier routeur et le destinataire sont dans le même réseau. Une machine contient une carte réseau physique associée à une interface réseau logique qui lui donne un nom et une adresse unique fournie par le fabricant (adresse MAC, Media Access Control). Le paquet, encapsulé dans une trame qui contient les adresses source et destination à l'intérieur d'un réseau local (LAN) est le plus souvent transmis à tous les membres du réseau (broadcast).

Couche 1 : le message transite par ondes radio (Wifi), signaux électriques (câble) ou lumineux (fibre). Il peut être déformé en réception, les couches supérieures vont alors effectuer des contrôles et des corrections.



4.4.3 Encapsulation

L'encapsulation, en informatique et spécifiquement pour les réseaux informatiques, est un procédé consistant à inclure les données de la couche d'un protocole donné vers la couche d'un protocole de plus bas niveau. C'est un système de poupées russes. Voici un schéma de l'encapsulation du modèle OSI.



DH : en-tête de liaison ; **TH :** en-tête de transport ; **PH :** en-tête de présentation ;
NH : en-tête de réseau ; **SH :** en-tête de session ; **AH :** en-tête d'application.

4.5 Trame Ethernet et protocole TCP/IP

4.5.1 Trame Ethernet et protocole TCP/IP

Plus rigoureux et publié après son concurrent direct (1984), le modèle en couche OSI n'est que peu utilisé en réalité. C'est le modèle TCP/IP, plus souple et publié plus tôt (1976) qui l'emporte en terme d'utilisation. Ce dernier est comme le modèle OSI un modèle en couche mais n'en comporte que quatre :

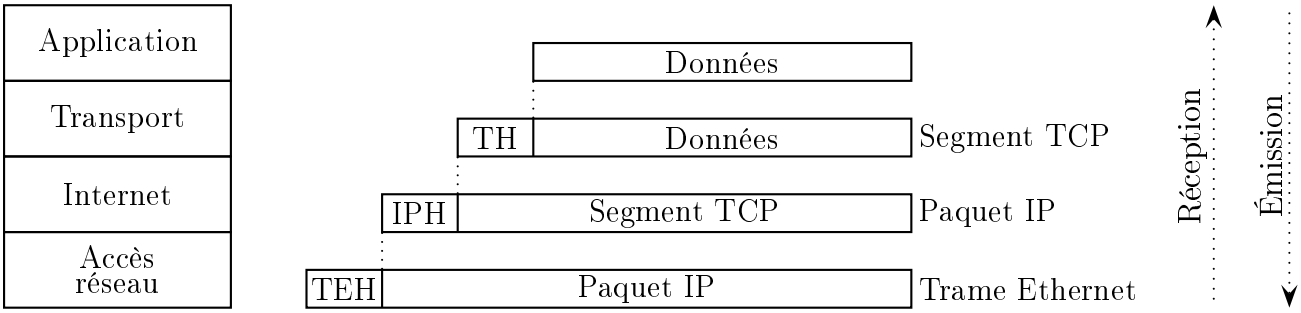
1. Application.
2. Transport.
3. Internet.
4. Accès réseau.

TCP/IP		OSI	
1	Application	1	Application
		2	Présentation
		3	Session
2	Transport (TCP)	4	Transport
3	Internet (IP)	5	Réseau
4	Accès réseau	6	Liaison
		7	Physique

L'information numérique qui chemine sur un réseau TCP/IP est une succession de bits appelée **Trame Ethernet**.

4.5.2 Encapsulation

Comme pour le modèle OSI, le protocole TCP/IP a un processus d'encapsulation des données à chaque couche.



TH : en-tête de transport ; elle contient les adresses de port de la source et de la destination plus d'éventuelles autres informations.

IPH : en-tête de session ; elle contient les adresses IP de la source et de la destination plus d'éventuelles autres informations.

TEH : en-tête de la trame Ethernet ; elle contient les adresses MAC de la source et de la destination plus d'éventuelles autres informations.

4.5.3 Détails de la trame Ethernet

Préambule	Adr. dest.	Adr. scr.	E.T.	Données	CRC
8o	6o	6o	2o	46 à 1500o	4o

Préambule : Annonce le début de la trame et permet aux récepteurs de se synchroniser. Il contient 8 octets dont la valeur est 10101010 (on alterne des 1 et des 0), sauf pour le dernier octet dont les 2 derniers bits sont à 1.

Adresse MAC destinataire : Adresse MAC de l'interface (carte d'accès) Ethernet destinataire de la trame. On représente une adresse Ethernet comme ses 6 octets en hexadécimal séparés par des « : ». Exemple : 08 :00 :07 :5c :10 :0a.

Une seule trame peut avoir plusieurs destinataires. En effet, le format des adresses MAC permet de coder 3 types de destinations :

- unicast : (mono-diffusion) un destinataire unique (celui qui possède cette adresse MAC) ;
- multicast : (mutil-diffusion) un groupe d'interfaces est destinataire ;
- broadcast : (diffusion générale) c'est l'adresse ff : ff : ff : ff : ff : ff . Elle correspond à toutes les interfaces Ethernet actives sur un réseau Ethernet (tous les équipements se reconnaissent dans cette adresse).

Adresse MAC source : Adresse MAC de la carte Ethernet émettrice de la trame. C'est forcément une adresse unicast.

Ether Type : Indique quel protocole est concerné par le message. Quelques types courants (en hexadécimal) :

- 0x0800 : IPv4 ;
- 0x0806 : ARP (Adress Resolution Protocol) ;
- 0x8035 : RARP (Reverse ARP) ;
- 0x86DD : IPv6 ;
- 0x880B : PPP (Point-to-Point Protocol).

Données : Données véhiculées par la trame. Sur la station destinataire de la trame, ces octets seront communiqués à l'entité (protocole) indiquée par le champ EtherType.

CRC : (Cyclic Redundancy Code) Champ de contrôle de la redondance cyclique. Permet de s'assurer que la trame a été correctement transmise et que les données peuvent donc être délivrées au protocole destinataire.

4.5.4 Détails de la couche de transport

L'adresse physique MAC permet à deux hôtes sur le même réseau de communiquer et l'adresse IP permet deux hôtes sur des réseaux différents de communiquer. Cependant, comment l'ordinateur sait-il au quel de ses logiciels il doit distribuer les données qu'il a reçu du réseau ou d'une autre machine ? Pour résoudre ce problème, le système d'exploitation attribue

aléatoirement un numéro de port supérieur à 1024 à chaque logiciel dans l'ordinateur. Ce numéro de Port est encapsulé dans un segment TCP ou un datagramme UDP dans chaque paquet IP pour pouvoir s'adresser à tel ou tel logiciel. Les ports réservés sont compris entre 0 et 1023.

TCP et UDP (User Datagram Protocol) sont les 2 principaux protocoles de la couche transport. La différence entre TCP et UDP sont fondamentales. Ces deux protocoles servent à échanger des paquets d'information entre 2 machines en utilisant leur adresse IP et un numéro de port.

Protocole TCP : TCP fonctionne un peu comme le téléphone : il faut d'abord établir une connexion TCP entre les 2 machines, ce qu'on pourrait comparer à composer le numéro de téléphone. Une fois que la communication est établie, les deux machines peuvent dialoguer de manière bidirectionnelle (vous pouvez parler à votre interlocuteur, et c'est réciproque) tant que vous ne fermez pas la connexion TCP (i.e. tant que vous ne raccrochez pas le combiné téléphonique). TCP sert de socle à de nombreux protocoles de la couche application :

- HTTP, qui sert à accéder aux sites internet (autrement dit : le web) ;
- FTP, qui sert à échanger des fichiers entre 2 ordinateurs ;
- POP3 et IMAP qui servent à réceptionner les mails ;
- SMTP qui sert quant à lui à envoyer des mails.

Protocole UDP : UDP fonctionne un peu comme le courrier : vous placez le message à envoyer dans une enveloppe qui contient toutes les informations nécessaires au routage : l'adresse IP et le port (i.e. les coordonnées du destinataire), puis vous envoyez l'enveloppe. Il est par exemple utilisé dans les protocoles DNS. À l'inverse de TCP, il n'y a donc pas de connexion entre les deux machines et pas de vérification des données transférées ni de leur réception.

4.6 Protocole du bit alterné

Nous avons vu que le protocole TCP propose un mécanisme d'accusé de réception afin de s'assurer qu'un paquet est bien arrivé à destination. On parle plus généralement de processus d'acquittement. Ces processus d'acquittement permettent de détecter les pertes de paquets au sein d'un réseau, l'idée étant qu'en cas de perte, l'émetteur du paquet renvoie le paquet perdu au destinataire. Nous allons ici étudier un protocole simple de récupération de perte de paquet : le protocole de bit alterné.

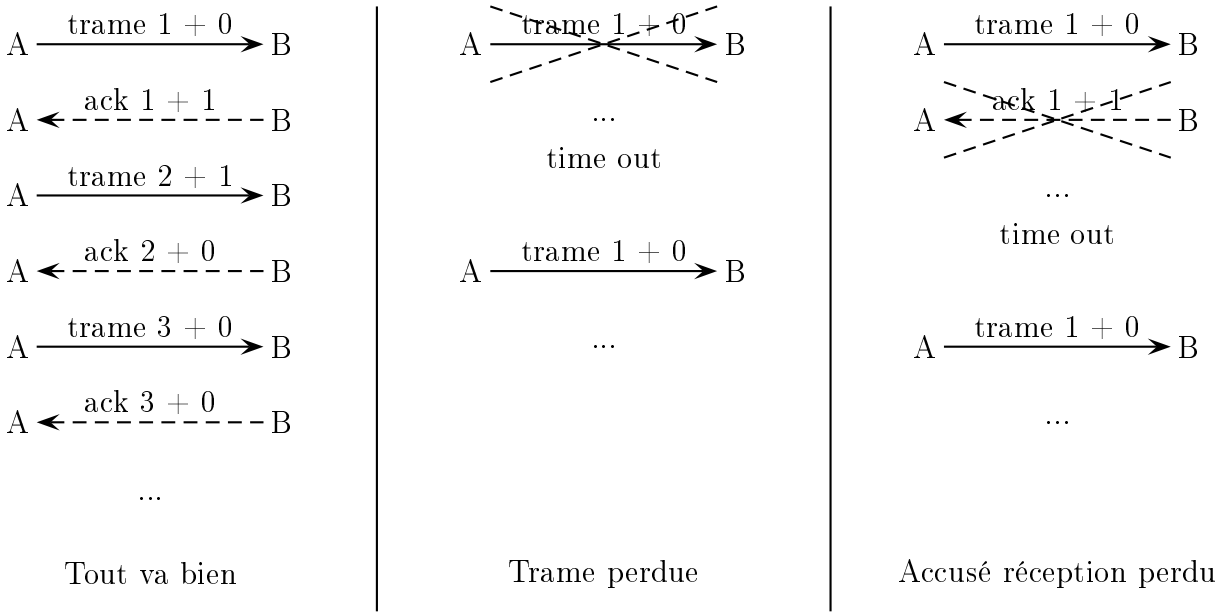
Le protocole de bit alterné est implémenté au niveau de la couche de liaison de données du modèle OSI (couche 2), il ne concerne donc pas les paquets, mais les trames (on parle de paquets uniquement à partir de la couche Réseau (couche 3) du modèle OSI).

Le principe de ce protocole est simple, considérons 2 ordinateurs en réseau : un ordinateur A qui sera l'émetteur des trames et un ordinateur B qui sera le destinataire des trames. Au moment d'émettre une trame, A va ajouter à cette trame un bit (1 ou 0) appelé drapeau (flag en anglais). B va envoyer un accusé de réception (acknowledge en anglais souvent noté ACK) à destination de A dès qu'il a reçu une trame en provenance de A. À cet accusé de réception on associe aussi un bit drapeau (1 ou 0). La règle est relativement simple :

- la première trame envoyée par A aura pour drapeau 0 ;
- dès cette trame reçue par B, ce dernier va envoyer un accusé de réception avec le drapeau 1 (ce 1 signifie "la prochaine trame que A va m'envoyer devra avoir son drapeau à 1") ;

— dès que A reçoit l'accusé de réception avec le drapeau à 1, il envoie la 2e trame avec un drapeau à 1, et ainsi de suite...

Le système de drapeau est complété avec un système d'horloge côté émetteur. Un « chronomètre » est déclenché à chaque envoi de trame, si au bout d'un certain temps, l'émetteur n'a pas reçu un acquittement correct (avec le bon drapeau), la trame précédemment envoyée par l'émetteur est considérée comme perdue et est de nouveau envoyée.



Dans certaines situations, le protocole de bit alterné ne permet pas de récupérer les trames perdues, c'est pour cela que ce protocole est aujourd'hui remplacé par des protocoles plus efficaces, mais aussi plus complexes.

★ Vidéo de Monsieur Bidouille partie 1 et partie 2 reprenant les principaux éléments du chapitre.

4.7 Attendus et savoir-faire

— Connaître la définition d'une adresse IPv4, savoir si adresse est valide, en donner des exemples.

— Appliquer un masque de sous-réseau à une adresse IPv4.

— Diviser une plage d'adresses IP en sous-réseaux distincts.

— Déterminer si le routage en deux machines est direct ou indirect.

— Connaître les différentes couches du protocole TCP/IP et le processus d'encapsulation qui lui est associé.

— Exécuter le protocole du bit alterné.

4.8 Exercices

4.8.1 Démarrage

Exercice 4.1. Les adresses IPv4 suivantes sont-elles valides ?

1. 192.168.72.1
2. 235.89.143.264
3. 1.0.134.214
4. 230.198.103

Exercice 4.2. Combien d'adresses possibles peuvent être codées en IPv4 ? En IPv6 ? Combien de machines pourrait-on mettre par mètres carrés sur Terre en IPv6 ?

Exercice 4.3. Traduire les adresses IPv4 suivantes en binaire ou en décimal.

1. 192.168.72.1
2. 01010011.1100000.10110011.00000111

Exercice 4.4. Quelles sont les adresses réseaux et machines associées aux adresses IP suivantes ?

1. 208.0.178.34 /19.
2. 208.0.178.34 /20.
3. 208.0.178.34 /21.

4.8.2 Approfondissement

Exercice 4.5. Un administrateur réseaux souhaite créer huit sous-réseaux sur l'adresse IP 134.240.0.0 /16 en réservant à chaque fois trois bits pour les sous-réseaux.

1. Déterminer les plages d'adresses des huit sous-réseaux.
2. Combien de machines peut contenir chaque sous-réseau ?
3. Combien de bits faudrait-il réserver pour 16 sous-réseaux ? Et pour un nombre quelconque de sous-réseaux ?

Exercice 4.6. Les machines d'adresses suivantes peuvent-elles communiquer par routage direct ou indirect ?

1. 172.2.246.3 /20 et 172.2.252.1 /20.
2. 172.2.246.3 /20 et 172.2.230.1 /20.

4.8.3 Entraînement

Exercice 4.7. Quelles sont les adresses réseaux et machines associées aux adresses IP suivantes ?

1. 208.0.178.185 /27.
2. 208.0.178.185 /25.

Exercice 4.8. Déterminer les plages d'adresses qu'un administrateur réseaux obtiendrait s'il créait trois sous-réseaux sur l'adresse IP 134.240.0.0 /16.

Exercice 4.9. Les machines d'adresses suivantes peuvent-elles communiquer par routage direct ou indirect ?

1. 208.0.178.185 /27 et 208.0.178.163 /27.
2. 208.0.178.185 /27 et 208.0.178.152 /27.