Activité 1 : Réseaux et protocoles

I. Réseaux

1. Matériel

Il est possible de faire communiquer deux ordinateurs en les reliant par un simple câble. On dit alors que ces deux ordinateurs sont en réseau.

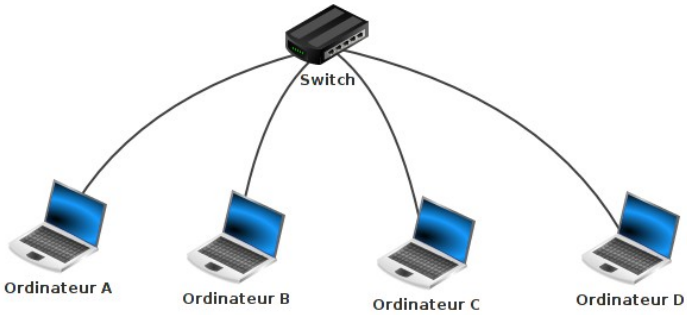
Dans la plupart des cas, le câble reliant les 2 ordinateurs est un câble Ethernet. Ce type de câble possède à ses 2 extrémités des prises RJ45.

Un ordinateur relié à un réseau doit posséder une carte réseau, on identifie cette carte réseau de type Ethernet grâce à la prise RJ45 femelle située souvent à l'arrière de l'ordinateur.

Relier 2 ordinateurs peut avoir un intérêt, mais dans la plupart des cas, un réseau sera constitué d'un plus grand nombre d'ordinateurs. Dans ce cas, il est nécessaire d'utiliser un commutateur réseau, souvent appelé switch (même en français). Un switch est constitué de plusieurs prises RJ45.

Comme nous le montre la photo ci-dessus, il existe des switchs de différentes tailles, certains switchs possèdent 8 prises RJ45 alors que d'autres peuvent en posséder 24.

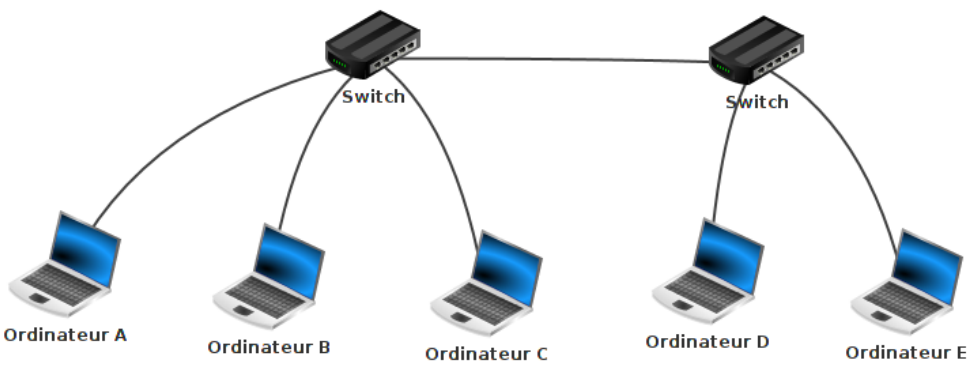
Chaque ordinateur doit être relié au switch par l'intermédiaire d'un câble Ethernet.



Dans l'exemple du schéma ci-contre, les ordinateurs A, B, C et D sont en réseau, chaque ordinateur peut communiquer avec les 3 autres.

Les switchs ayant un nombre de prises RJ45 limité, il peut être nécessaire d'utiliser plusieurs switchs dans un même réseau.

Dans l'exemple du schéma ci-dessus, les ordinateurs A, B, C, D et E sont en réseau. A, B et C sont reliés à un switch, D et E sont reliés à un autre switch. Les 2 switchs étant reliés ensemble.



Depuis le début nous avons uniquement parlé de réseaux filaires, il est aussi possible de mettre plusieurs machines en réseau grâce à des technologies sans fil, par exemple, le wifi. Chaque ordinateur appartenant au réseau sans fil devra posséder une carte réseau wifi. Il sera nécessaire d'utiliser un concentrateur wifi (équivalent du switch en filaire) si l'on désire mettre en réseau plus de deux ordinateurs.

2. 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.

II. L'IP, le MAC et le DNS

1. L'adresse IP

Maintenant que nos ordinateurs sont reliés par l'intermédiaire d'un switch, imaginons que l'ordinateur A "souhaite" entrer en communication avec l'ordinateur C. Quand vous désirez communiquer avec quelqu'un par voie postale, il est nécessaire d'écrire l'adresse de cette personne sur une enveloppe, à chaque habitation correspond donc une adresse postale. Et bien c'est un peu la même chose pour les ordinateurs en réseau, chaque machine possède une adresse, l'adresse IP.
Les adresses IP sont de la forme : "a.b.c.d", avec a, b, c et d compris entre 0 et 255 (a, b, c et d sont codés sur 1 octet). Exemple d'adresse IP : 192.168.0.1
Une partie de l'adresse IP permet d'identifier le réseau auquel appartient la machine (partie réseau) et l'autre partie de l'adresse IP permet d'identifier la machine sur ce réseau (partie hôte).

Exemple : Soit un ordinateur A ayant pour adresse IP 192.168.2.1 Dans cette adresse IP "192.168.2" permet d'identifier le réseau (on dit que la machine A appartient au réseau ayant pour adresse 192.168.2.0, pour trouver l'adresse réseau il suffit de remplacer la partie "machine" de cette adresse IP par un ou des 0) et "1" permet d'identifier la machine sur le réseau.
Toutes les machines appartenant au même réseau devront posséder la même adresse réseau (sinon elles ne pourront pas communiquer ensemble, même si elles sont bien physiquement reliées).
2 exemples, soit 2 machines A et B en réseau :

- la machine A a pour adresse IP 192.168.2.5 et la machine B a pour adresse IP 192.168.2.8. Les 3 premiers octets sont bien identiques ("192.168.2"), A et B ont donc la même adresse réseau "192.168.2.0". Ces 2 machines pourront donc communiquer ensemble
- la machine A a pour adresse IP 192.168.2.5 et la machine B a pour adresse IP 192.168.3.8. Les 3 premiers octets ne sont pas identiques ("192.168.2" pour A et "192.168.3" pour B), A et B n'ont pas la même adresse réseau ("192.168.2.0" pour A et "192.168.3.0" pour B). Ces 2 machines ne pourront donc pas communiquer ensemble

Attention, les adresses IP (a.b.c.d) n'ont forcément pas les parties a, b et c consacrées à l'identification du réseau et la partie d consacrées à l'identification des machines sur le réseau : on rajoute souvent à l'adresse IP un "/" suivit du nombre 8, 16 ou 24

- si ce nombre est 8 (exemple : 192.168.2.1/8), cela signifie que pour une adresse a.b.c.d/8, la partie a est consacrée à l'adresse réseau, le reste (b, c, d) est consacré à la partie hôte de l'adresse IP. On aura donc une adresse réseau de la forme a.0.0.0
- si ce nombre est 16 (exemple : 192.168.2.1/16), cela signifie que pour une adresse a.b.c.d/16, les parties a et b sont consacrées à l'adresse réseau, le reste (c, d) est consacré à la partie hôte de l'adresse IP. On aura donc une adresse réseau de la forme a.b.0.0
- si ce nombre est 24 (exemple : 192.168.2.1/24), cela signifie que pour une adresse a.b.c.d/24, les parties a, b et c sont consacrées à l'adresse réseau, le reste (d) est consacré à la partie machine de l'adresse IP. On aura donc une adresse réseau de la forme a.b.c.0

Exercice 1
Déterminez les adresses réseaux à partir des adresses IP suivantes :
- 147.12.1.24/16
- 192.168.2.45/24
- 5.23.65.87/8

Exercice 2
Soit 2 machines A et B connectées à un switch, dites dans quels cas ces 2 machines pourront communiquer ensemble :
- adresse IP de A : 172.23.4.7/16 ; adresse IP de B : 172.23.5.8/16
- adresse IP de A : 24.2.8.127/8 ; adresse IP de B : 24.23.5.52/8
- adresse IP de A : 193.28.7.2/24 ; adresse IP de B : 193.28.8.3/24

Il est à noter que certaines adresses IP ne sont pas disponibles :

- les adresses IP qui ont tous les octets de la partie "machines" de l'adresse IP à 0 ne sont pas utilisables (ce sont des adresses de test du réseau), par exemple aucune machine ne pourra avoir l'adresse IP 192.168.1.0/24 ou encore l'adresse IP 25.0.0.0/8
- les adresses IP qui ont tous les octets de la partie "machines" de l'adresse IP à 255 ne sont pas utilisables (ce sont des adresses de broadcast qui permettent d'envoyer des données vers toutes les machines d'un réseau), exemples : 192.167.24.255/24, 172.28.255.255/16 ou encore 4.255.255.255/8 sont des adresses de broadcast

Exercice 3
Combien de machines peut-on trouver au maximum :
- dans un réseau d'adresse réseau 192.168.2.0/24 ?
- dans un réseau d'adresse réseau 176.24.0.0/16 ?
- dans un réseau d'adresse réseau 10.0.0.0/8 ?

Le nombre de machines connectées à internet étant en augmentation constante, il y a en ce moment une transition de l'IPv4 (sur 4 octets) vers l'IPv6 (sur 16 octets)

2. 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.

3. 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.

III. Protocoles de communications

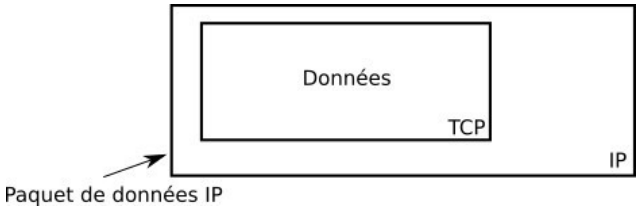
1. Protocoles TCP,IP et TCP/IP

Pour communiquer ensemble, 2 ordinateurs en réseau doivent utiliser des règles communes, l'ensemble de ces règles qui permettent à 2 ordinateurs de communiquer ensemble s'appelle un protocole.

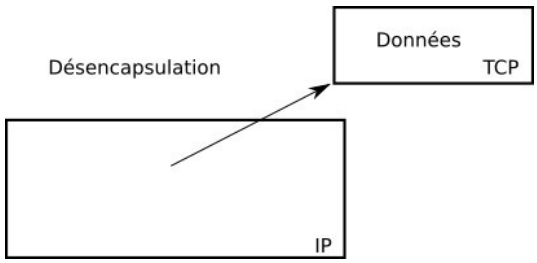
Il existe de nombreux protocoles réseau, nous allons en étudier 2 : le protocole TCP et le protocole IP. Ces 2 protocoles sont tellement liés l'un à l'autre que l'on parle souvent du protocole TCP/IP.

Quand un ordinateur A "désire" envoyer des données à un ordinateur B, l'ordinateur A "utilise" le protocole TCP pour mettre en forme les données à envoyer.

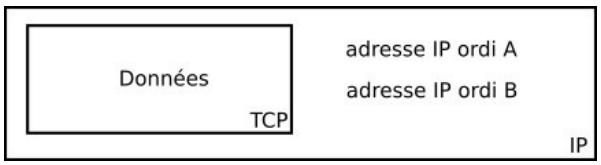
Ensuite le protocole IP prend le relais et utilise les données mises en forme par le protocole TCP afin de créer des paquets des données. Après quelques autres opérations, les paquets de données pourront commencer leur voyage sur le réseau jusqu'à l'ordinateur B. Il est important de bien comprendre que le protocole IP "encapsule" les données issues du protocole TCP afin de constituer des paquets de données.

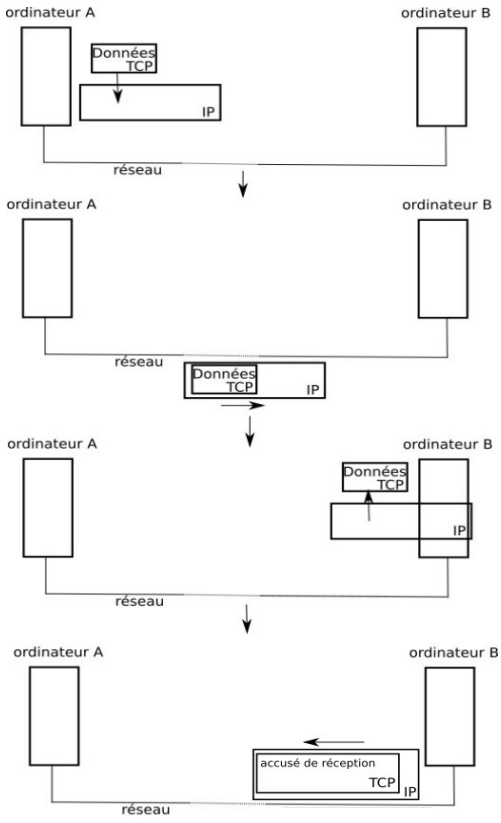


Une fois arrivées à destination (ordinateur B), les données sont "désencapsulées" : on récupère les données TCP contenues dans les paquets afin de pouvoir les utiliser.

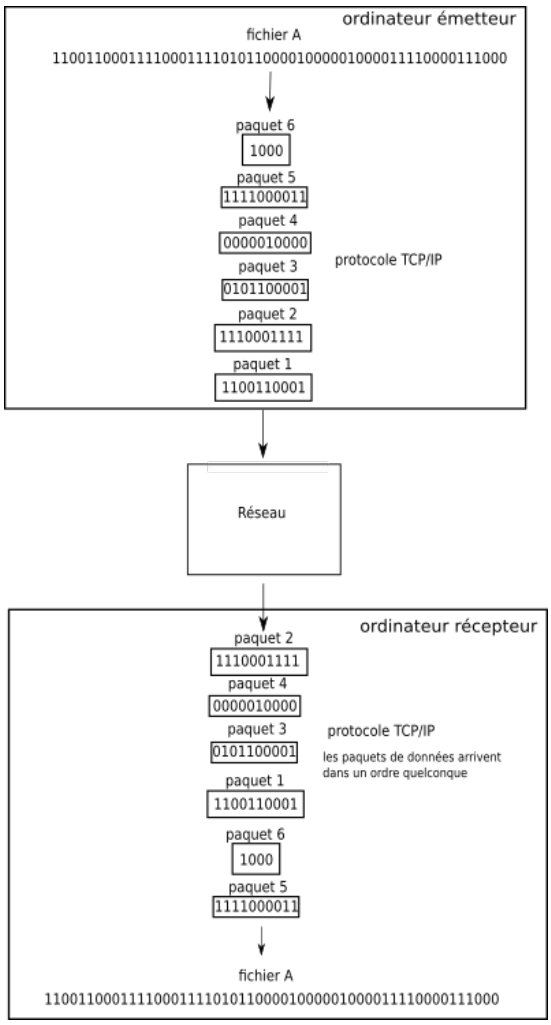


Le protocole IP s'occupe uniquement de faire arriver à destination les paquets en utilisant l'adresse IP de l'ordinateur de destination. Les adresses IP de l'ordinateur de départ (ordinateur A) et de l'ordinateur destination (ordinateur B) sont ajoutées aux paquets de données.





Le protocole TCP permet de s'assurer qu'un paquet est bien arrivé à destination. En effet quand l'ordinateur B reçoit un paquet de données en provenance de l'ordinateur A, l'ordinateur B envoie un accusé de réception à l'ordinateur A (un peu dans le genre "OK, j'ai bien reçu le paquet"). Si l'ordinateur A ne reçoit pas cet accusé de réception en provenance de B, après un temps prédéfini, l'ordinateur A renverra le paquet de données vers l'ordinateur B.
Nous pouvons donc résumer le processus d'envoi d'un paquet de données comme suit :



Il est très important de bien comprendre que TCP/IP repose sur la notion de paquets de données. Si par exemple on désire envoyer un fichier (son, photo, vidéo ou texte, peu importe, dans tous les cas on envoie une succession de bits) en utilisant TCP/IP, les données qui constituent ce fichier ne seront pas envoyées d'un seul tenant, ces données vont être "découpées" en plusieurs morceaux et chaque morceau sera envoyé dans un paquet différent. Une fois tous les paquets arrivés à destination, le fichier d'origine pourra être reconstitué. Pour aller d'un ordinateur A à un ordinateur B, les différents paquets contenant les données qui constituent notre fichier, ne passeront pas forcement par la même route (cette notion de route sera abordée plus tard), ils pourront emprunter des chemins très différents : en exagérant à peine, pour faire le trajet Paris-Los Angeles, certains paquets pourront passer par l'atlantique alors que d'autres passeront par le pacifique. Si un des paquets n'arrive pas à destination, le fichier ne pourra pas être reconstitué, le paquet "perdu" devra être renvoyé par l'émetteur (voir le système d'accusé de réception décrit ci-dessus).

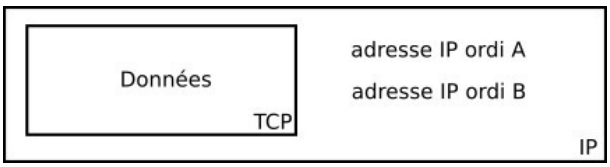
2.Trame Ethernet

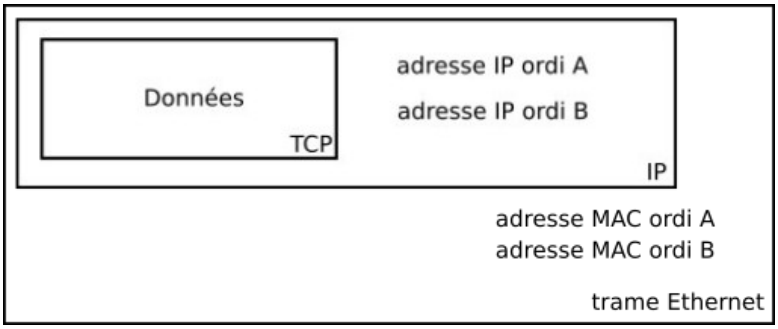
Nous avons eu l'occasion de voir avec les protocoles TCP et IP le processus d'encapsulation des données : "IP encapsule TCP". Les paquets IP ne peuvent pas transiter sur un réseau tel quel, ils vont eux aussi être encapsulés avant de pouvoir "voyager" sur le réseau. L'encapsulation des paquets IP produit ce que l'on appelle une trame.

Si vous utilisez un réseau filaire avec des câbles Ethernet, la trame sera de type Ethernet. Si vous utilisez un réseau sans fil Wifi, la trame sera de type Wifi. Afin de simplifier les choses, dans la suite, nous évoquerons uniquement la trame Ethernet en ayant à l'esprit que ce qui est dit sur la trame Ethernet et aussi valable pour la trame Wifi.

Couche Accès Réseau

Nous avons vu que le paquet IP contient les adresses IP de l'émetteur et du récepteur :





Le paquet IP étant encapsulé par la trame Ethernet, les adresses IP ne sont plus directement disponibles (il faut désencapsuler le paquet IP pour pouvoir lire ces adresses IP), nous allons donc trouver un autre type d'adresse qui permet d'identifier l'émetteur et le récepteur : l'adresse MAC (Media Access Control) aussi appelée adresse physique.

Au moment de l'encapsulation d'un paquet IP, l'ordinateur "émetteur" va utiliser un protocole nommé ARP (Address Resolution Protocol) qui va permettre de déterminer l'adresse MAC de l'ordinateur "destination", en effectuant une requête "broadcast" (requête destinée à tous les ordinateurs du réseau) du type : "j'aimerais connaître l'adresse MAC de l'ordinateur ayant pour IP XXX.XXX.XXX.XXX". Une fois qu'il a obtenu une réponse à cette requête ARP, l'ordinateur "émetteur" encapsule le paquet IP dans une trame Ethernet et envoie cette trame sur le réseau.

Couche application

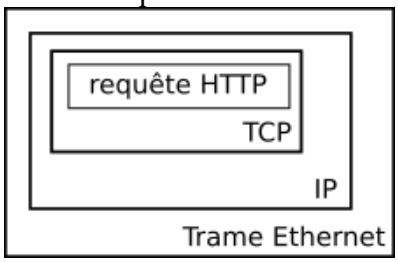
Nous avons vu que le protocole TCP permet de mettre en forme les données à envoyer :

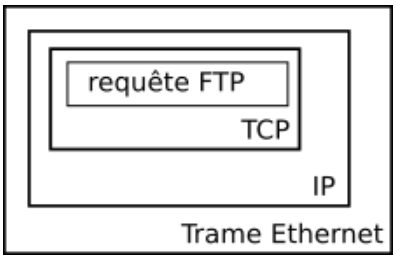
Quelle est la nature de ces données mises en forme par TCP ?

En faite, TCP effectue lui aussi une encapsulation, les données encapsulées par TCP peuvent être de plusieurs natures :

TCP encapsule ainsi différents types de requêtes (et réponses), par exemple HTTP qui sert à accéder aux sites internet, FTP (File Transfer Protocol) qui permet d'envoyer sur un réseau des fichiers (texte, son, image...), SMTP (Simple Mail Transfer Protocol) qui permet d'envoyer des emails, DNS (Domain Name Server) qui permet d'avoir la correspondance entre une adresse IP et une URL,...

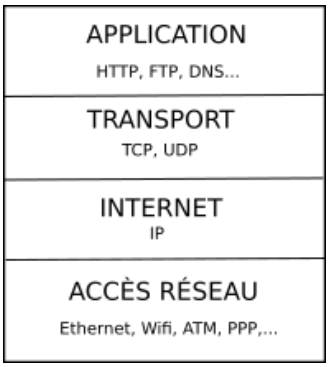
Il est donc aussi possible d'avoir :





On dit que tous ces protocoles (HTTP, FTP, SMTP, DNS,...) appartiennent à la couche "Application" du modèle TCP/IP.

Le modèle des couches TCP/IP



En effet, à chaque phase d'encapsulation on associe ce que l'on appelle une couche :

- comme nous l'avons vu les protocoles HTTP, FTP, SMTP, DNS,... sont associés à la couche "**Application**"
- les protocoles TCP et UDP sont associés à la couche "**Transport**"
- le protocole IP est associé à la couche "**Internet**"
- les trames Ethernet (ou Wifi) sont associées à la couche "**Accès réseau**"

On présente souvent ces différentes couchent sur ce type de schéma :
La couche du "dessous" encapsule la couche située "au dessus"
On nomme ce système de couche "modèle de couches TCP/IP" (car ce modèle repose principalement sur TCP et IP)

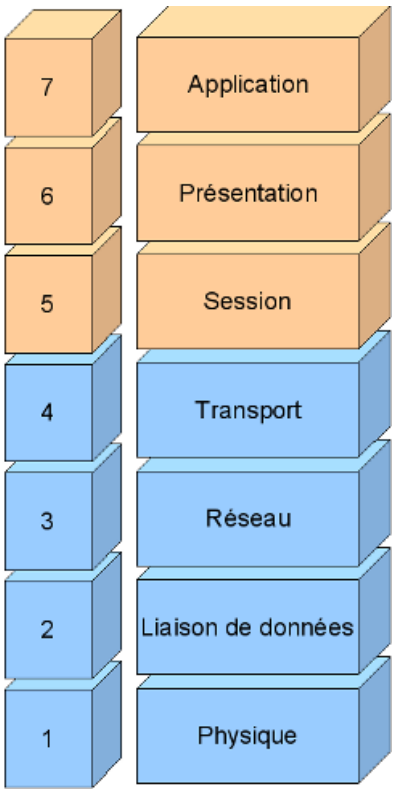
Détails de la trame Ethernet

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 « : ».
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.
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.

3. Le modèle des couches OSI

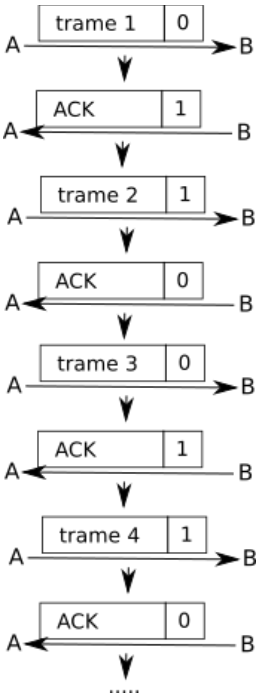
Il existe un autre modèle de couche, le modèle OSI (Open Systems Interconnection), ce système est antérieur au modèle TCP/IP puisqu'il date des années 1970. Ce modèle est composé de 7 couches (alors que le modèle TCP/IP est composé de 4 couches).
Il existe des liens entre le modèle OSI et le modèle TCP/IP (par exemple on retrouve le protocole IP dans la couche 3 du modèle OSI et TCP dans la couche 4), mais parfois comparer les 2 modèles peut être délicat.
Ce modèle est donné ici à titre d'information, mais le principal est de retenir ce qui a été vu sur le modèle TCP/IP.



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

IV. Protocole du bit alterné

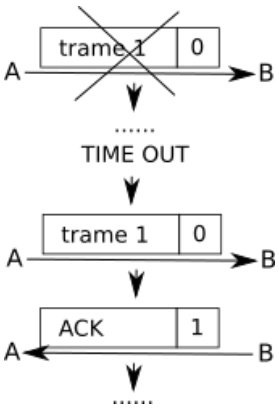
Nous avons vu que le protocole TCP propose un mécanisme d'accusé de réception afin de s'assurer qu'un paquet est bien arrivé à destination. On parle plus généralement de processus d'acquittement. Ces processus d'acquittement permettent de détecter les pertes de paquets au sein d'un réseau, l'idée étant 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.



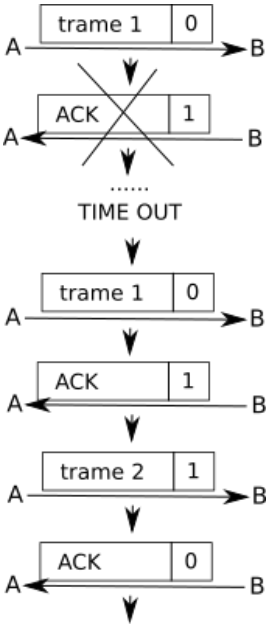
Le principe de ce protocole est simple, considérons 2 ordinateurs en réseau : un ordinateur A qui sera l'émetteur des trames et un ordinateur B qui sera le destinataire des trames. Au moment d'émettre une trame, A va ajouter à cette trame un bit (1 ou 0) appelé drapeau (flag en anglais). B va envoyer 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.
Examinons quelques cas :

- La trame est perdue :
  Au bout d'un certain temps ("TIME OUT") A n'a pas reçu d'accusé de réception, la trame est considérée comme perdue, elle est donc renvoyée.



- L'accusé de réception est perdu :
  A ne reçoit pas d'accusé de réception avec le drapeau à 1, il renvoie donc la trame 1 avec le drapeau 0. B reçoit donc cette trame avec un drapeau à 0 alors qu'il attend une trame avec un drapeau à 1 (puisqu'il a envoyé un accusé de réception avec un drapeau 1), il "en déduit" que l'accusé de réception précédent n'est pas arrivé à destination : il ne tient pas compte de la trame reçue et renvoie l'accusé de réception avec le drapeau à 1. Ensuite, le processus peut se poursuivre normalement.



Exercices

Exercice 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 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 3.
Traduire les adresses IPv4 suivantes en binaire ou en décimal.
1. 192.168.72.1 2. 01010011.1100000.10110011.00000111

Exercice 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.

Exercice5.
Déterminer les plages d'adresses qu'un administrateur réseaux obtiendrait s'il créait huit sous-réseaux sur l'adresse IP 134.240.0.0 /16 en réservant à chaque fois trois bits pour les sous-réseaux. Combien de bits faudrait-il réserver pour 16 sous-réseaux ? Et pour un nombre quelconque de sous-réseaux ?

Exercice 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.