Séquence 1 : Introduction et architecture matérielle

Activité 4 : Mise en œuvre des réseaux informatiques

1. Introduction aux réseaux

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.

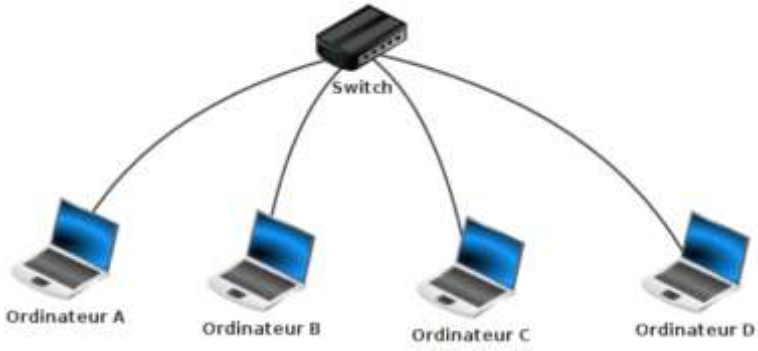
Dans la plupart des cas, le câble reliant les 2 ordinateurs est un câble Ethernet. Ce type de câble possède à ses 2 extrémités des prises RJ45 (il existe d'autres types de câbles qui permettent de mettre 2 ordinateurs en réseau, mais l'utilisation de câbles Ethernet est tellement majoritaire que nous ne nous intéresserons pas aux autres types de câbles).

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.

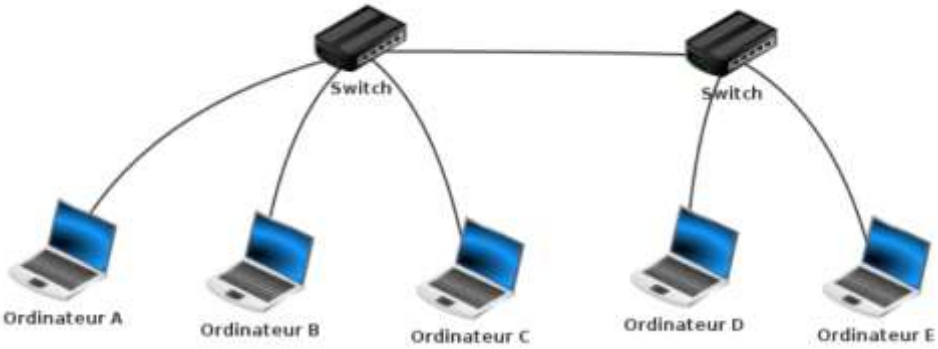
Comme nous le montre la photo ci-dessus, il existe des switchs de différentes tailles, certains switchs possèdent 8 prises RJ45 alors que d'autres peuvent en posséder 24.

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



Dans l'exemple du schéma ci-dessus, 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 (les différents composants du réseau sont reliés par des câbles), il est aussi possible de mettre plusieurs machines en réseau grâce à des technologies sans fil (utilisation des ondes radio pour transmettre l'information entre les différents composants du réseau), par exemple, le wifi (il existe d'autres technologies sans fil que le wifi, mais elles ne seront abordées ici). Chaque ordinateur appartenant au réseau sans fil devra posséder une carte réseau wifi (aujourd'hui tous les ordinateurs portables vendus sont par défaut équipés d'une telle carte). Il sera nécessaire d'utiliser un concentrateur wifi (équivalent du switch en filaire) si l'on désire mettre en réseau plus de deux ordinateurs.

Maintenant que nos ordinateurs sont reliés par l'intermédiaire d'un switch (ou d'un concentrateur wifi), 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. Pendant très longtemps il a existé différentes technologies de réseau et donc différents types d'adresse. Aujourd'hui, on trouve presque exclusivement qu'un seul type d'adresse : les adresses IP (nous étudierons donc uniquement ce type d'adresse).

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). Voici un exemple d'adresse IP : 192.168.0.1

Une partie de l'adresse IP permet d'identifier le réseau auquel appartient la machine et l'autre partie de l'adresse IP permet d'identifier la machine sur ce réseau.

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).

Prenons 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. Il y a de nombreuses années, les adresses ont été découpées en trois classes :

- Certaines adresses ont les parties a, b et c consacrées à l'identification du réseau et la partie d consacrée à l'identification des machines sur le réseau (on parle d'adresse IP de classe C)
- Certaines adresses ont la partie a et b consacrées à l'identification du réseau et les parties c et d consacrées à l'identification des machines sur le réseau (on parle d'adresse IP de classe B)
- Certaines adresses ont la partie a consacrée à l'identification du réseau et les parties b, c et d consacrées à l'identification des machines sur le réseau (on parle d'adresse IP de classe A)

Nous avons donc :

- Réseau de classe A : adresse réseau : a.0.0.0 (avec a qui doit être compris entre 1 et 126)
- Réseau de classe B : adresse réseau : a.b.0.0 (avec a qui doit être compris entre 128 et 191)
- Réseau de classe C : adresse réseau : a.b.c.0 (avec a qui doit être compris entre 192 et 223)

Cette partition étant peu flexible, elle a progressivement été remplacée par un découpage plus fin où la séparation réseaux/machine peut se trouver à l'intérieur d'une partie, dépendant de ce que l'on appelle le « masque de sous-réseau », mais cette notion ne sera pas abordée que la semaine prochaine.

Remarque : vous avez sans doute remarqué que l'on passe de "126" pour la "fin" des réseaux de classe A à "128" pour le "début" des réseaux de classe B, le "127" est réservé et ne peut être utilisé (nous aurons l'occasion de revenir là-dessus plus tard).

1.1 Exercice 1

Déterminer les adresses réseaux à partir des adresses IP suivantes :

- 147.12.1.24
- 192.168.2.45
- 5.23.65.87

1.2 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 ; adresse IP de B : 172.23.5.8
- Adresse IP de A : 24.2.8.127 ; adresse IP de B : 24.23.5.52
- Adresse IP de A : 193.28.7.2 ; adresse IP de B : 193.28.8.3

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

- Une adresse réseau ne peut pas être attribuée à une machine, par exemple aucune machine ne pourra avoir l'adresse IP 192.168.1.0 ou encore l'adresse IP 25.0.0.0
- 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, 172.28.255.255 ou encore 4.255.255.255 sont des adresses de broadcast

1.3 Exercice 3

Combien de machines peut-on trouver au maximum :

- Dans un réseau de classe A ?
- Dans un réseau de classe B ?
- Dans un réseau de classe C ?

2. Les protocoles 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.

2.1 Historique

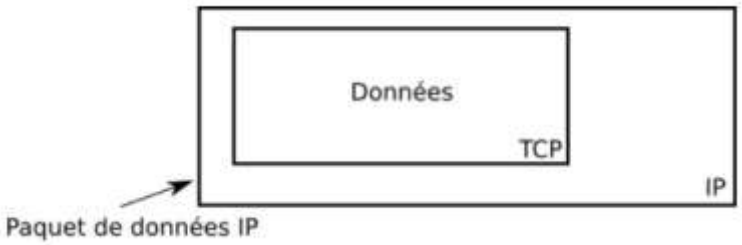
La DARPA (Defense Advanced Research Projects Agency) voit le jour en 1958, cette agence gouvernementale américaine a pour but de veiller à la constante suprématie des États unis en matière technologique et scientifique. En 1962 la DARPA soutient le projet du professeur Licklider qui a pour but de mettre en réseau les ordinateurs des universités américaines afin que ces dernières puissent échanger des informations plus rapidement (même à des milliers de kilomètres de distance). En 1968, ARPAnet, 1er réseau informatique à grande échelle de l'histoire voit le jour. Le 29 octobre 1969, le 1er message (le mot "login") est envoyé depuis l'université de Californie à Los Angeles vers l'université de Stanford via le réseau ARPAnet (les 2 universités sont environ distantes de 500 Km). C'est un demi-succès, puisque seules les lettres "l" et "o" arriveront à bon port. En 1972, 23 ordinateurs sont connectés à ARPAnet (on trouve même des ordinateurs en dehors des États unis). En parallèle au projet ARPAnet, d'autres réseaux voient le jour, problème, ils utilisent des protocoles de communication hétéroclite (UUCP, NCP ou encore X.25) et 2 ordinateurs appartenant à 2 réseaux différents sont incapables de communiquer entre eux puisqu'ils n'utilisent les mêmes protocoles. En 1974 Vint Cerf et Bob Khan vont mettre au point le protocole TCP qui sera très rapidement couplé au protocole IP pour donner TCP/IP. TCP/IP, grâce à sa simplicité, va très rapidement s'imposer comme un standard : les différents réseaux (ARPAnet et les autres) vont adopter TCP/IP. Cette adoption va permettre d'interconnecter tous ces réseaux (2 machines appartenant à 2 réseaux différents vont pouvoir communiquer grâce à cette interconnexion). Internet

était né (le terme Internet vient de "internetting" qui signifie "Connexion entre plusieurs réseaux"). TCP/IP est donc au cœur d'Internet, voilà pourquoi aujourd'hui, la plupart des machines utilisent TCP/IP.

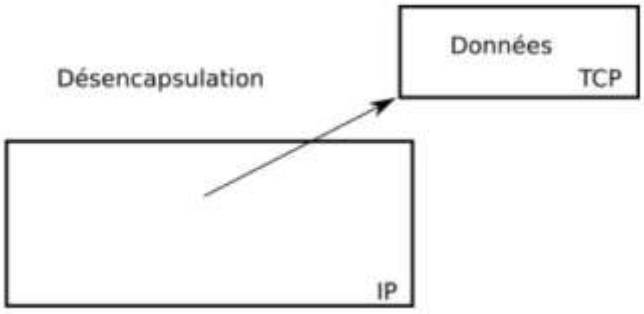
2.2 Principes de base

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.

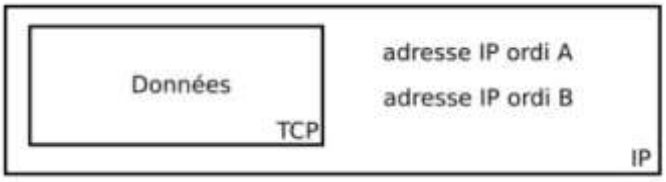
Ensuite le protocole IP prend le relai et utilise les données mises en forme par le protocole TCP afin de créer des paquets des données. Après quelques autres opérations qui ne seront pas évoquées ici, les paquets de données pourront commencer leur voyage sur le réseau jusqu'à l'ordinateur B. Il est 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.



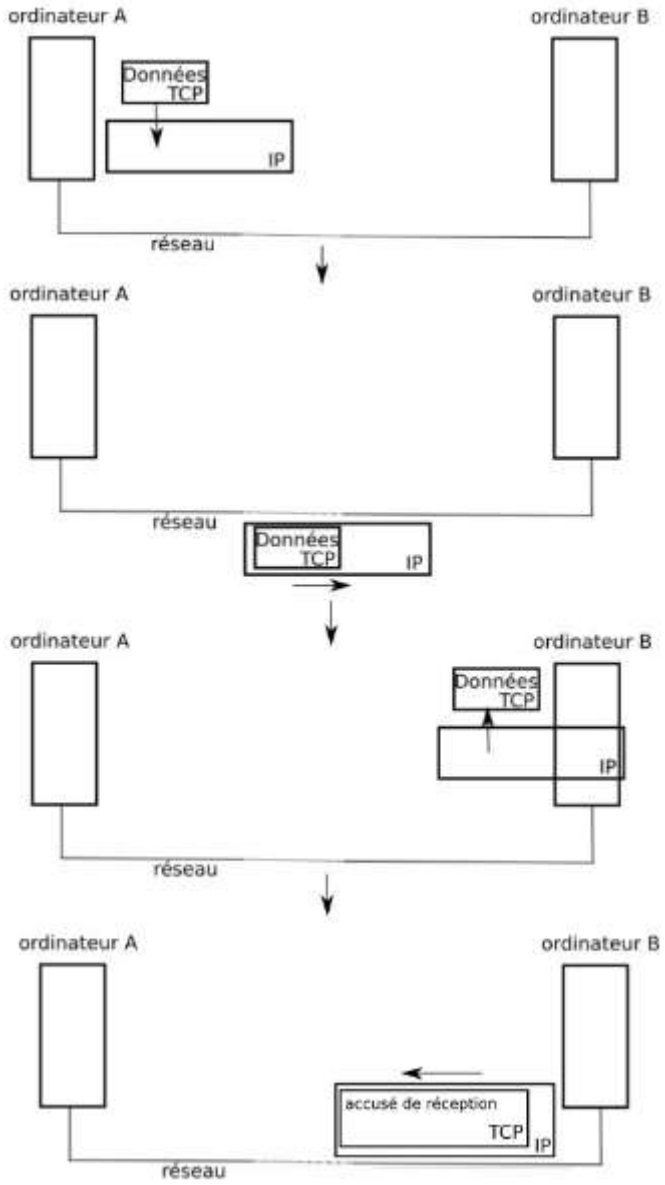
Le protocole IP s'occupe uniquement de faire arriver à destination les paquets en utilisant l'adresse IP de l'ordinateur de destination. Les adresses IP de l'ordinateur de départ (ordinateur A) et de l'ordinateur destination (ordinateur B) sont ajoutées aux paquets de données.



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

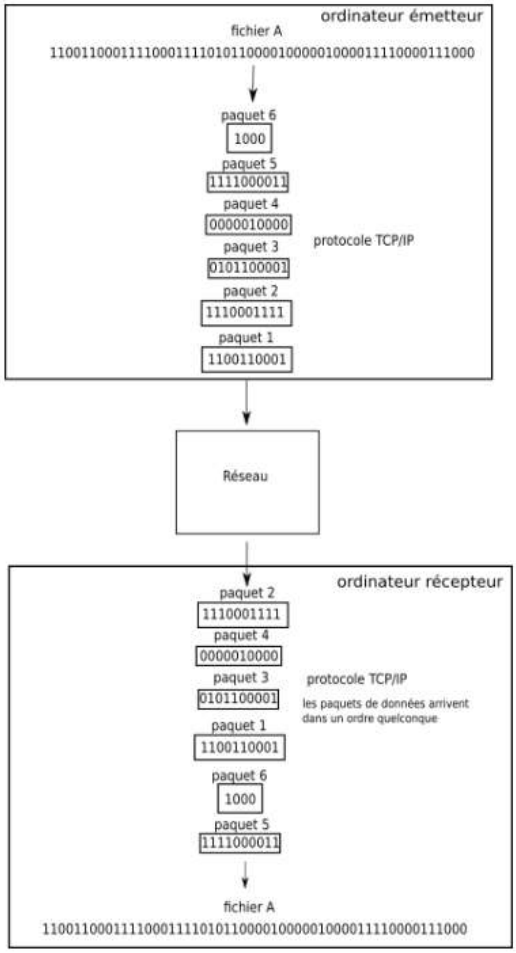
accusé de réception à l'ordinateur A (un peu dans le genre "OK, j'ai bien reçu le paquet"). Si l'ordinateur A ne reçoit pas cet accusé de réception en provenance de B, après un temps prédéfini, l'ordinateur A renverra le paquet de données vers l'ordinateur B.

Nous pouvons donc résumer le processus d'envoi d'un paquet de données comme suit :



À noter qu'il existe aussi le protocole UDP qui ressemble beaucoup au protocole TCP. La grande différence entre UDP et TCP est que le protocole UDP ne gère pas les accusés de réception. Les échanges de données avec UDP sont donc moins fiables qu'avec TCP (un paquet "perdu" est définitivement "perdu" et ne sera pas renvoyé) mais beaucoup plus rapides (puisqu' il n'y a pas d'accusé de réception à transmettre). UDP est donc très souvent utilisé pour les échanges de données qui doivent être rapides, mais où la perte d'un paquet de données de temps en temps n'est pas un gros problème (par exemple le streaming vidéo).

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).



3. Le modèle TCP/IP

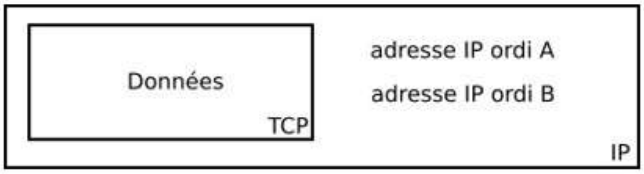
3.1 Trame Ethernet

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

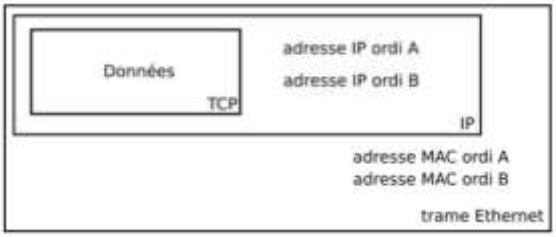
encapsulés avant de pouvoir "voyager" sur le réseau. L'encapsulation des paquets IP produit ce que l'on appelle une trame. Il n'est pas question d'étudier en détail ce qu'est une trame, vous devez juste savoir qu'il existe de nombreux types de trames : ATM, token ring, PPP, Ethernet, Wifi... Nous allons uniquement évoquer les 2 dernières : la trame Ethernet et la trame Wifi.

Si vous utilisez un réseau filaire avec des câbles Ethernet (avec des prises RJ45), la trame sera de type Ethernet (ce qui est le cas pour le réseau du lycée). Si vous utilisez un réseau sans fil Wifi, la trame sera de type Wifi. En fait, la trame Wifi ressemble beaucoup à la trame Ethernet, on peut même dire que la trame Wifi est la variante sans-fil de la trame Ethernet, 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.

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.



Une adresse MAC est codée sur 6 octets. on écrit traditionnellement les adresses MAC en hexadécimal, chaque octet étant séparés par 2 points (exemple d'adresse MAC : 00:E0:4C:68:02:11)

L'adresse MAC est liée au matériel, chaque carte réseau (Ethernet ou Wifi) possède sa propre adresse MAC, il n'existe pas dans le monde, 2 cartes réseau (Ethernet ou Wifi) qui possèdent la même adresse MAC. Les 3 premiers octets d'une adresse MAC ("00:E0:4C" dans l'exemple ci-dessus) désignent le constructeur du matériel, par exemple, "00:E0:4C" désigne le constructeur "realtek semiconductor corp".

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 connaitre 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.

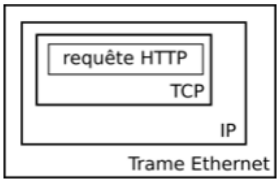
3.2 Couche application

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 ?

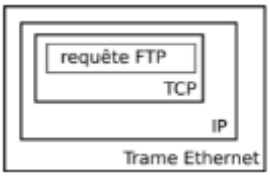
En fait, TCP effectue lui aussi une encapsulation, les données encapsulées par TCP peuvent être de plusieurs natures :

Nous étudierons prochainement le protocole HTTP. Les requêtes et les réponses HTTP sont encapsulés par TCP, au bout du compte et en résumé, nous avons donc :



TCP encapsule aussi d'autres types de requêtes (et réponses), par exemple 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.

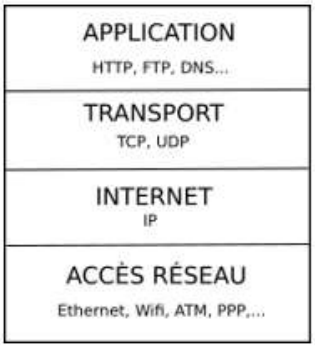
3.3 Le modèle des couches TCP/IP

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 "dessus" encapsule la couche située "en dessous"

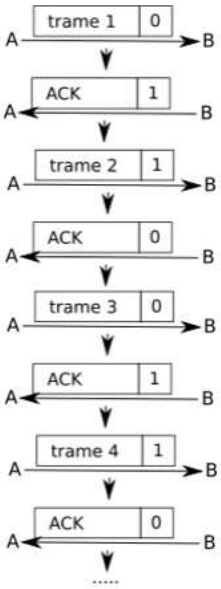
On nomme ce système de couche "modèle de couches TCP/IP" (car ce modèle repose principalement sur TCP et IP).

4. Le 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 n°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).

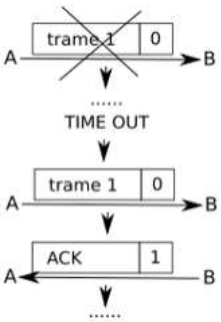
La règle est relativement simple : la première trame envoyée par A aura pour drapeau 0, dès cette trame reçue par B, ce dernier va envoyer un accusé de réception avec le drapeau 1 (ce 1 signifie "la prochaine trame que A va m'envoyer devra avoir son drapeau à 1"). Dès que A reçoit l'accusé de réception 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.

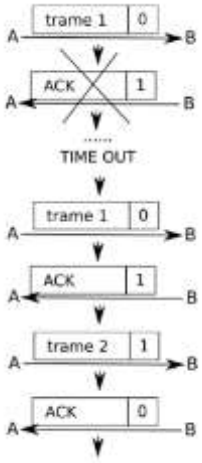
Examinons quelques cas :

- 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.

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.

4.1 Exercice 1

Essayez de déterminer une ou plusieurs situations où le protocole de bit alterné est inefficace.

Bibliographie :

https://pixees.fr/informatiquelycee/n_site/nsi_prem.html