Ressources Réseau

Sources :
https://openclassrooms.com/
http://www.commentcamarche.net/
https://fr.wikipedia.org/wiki/Suite_des_protocoles_Internet
Vidéo Net Express réalisée par France Télécom....
https://youtu.be/yaBa68xRuQ4

Le sommaire

1 / Les incontournables

1-1 / Quelle différence entre Internet et le Web ?

Internet (pour **Inter Net**work) est le réseau informatique basé sur le protocole de communication IP qui relie des ordinateurs entre eux à l'échelle de la planète.

Le Web (pour **W**orld **W**ide **W**eb) est un type d'utilisation du réseau internet parmi d'autres, comme la téléphonie, l'email ou bien encore le partage de fichiers. Le web est cependant l'application la plus populaire du réseau internet.

Le **Web** est un système de publication et de consultation de documents (textes, sons, images) faisant appel aux techniques de l'hypertexte qui utilisent des renvois permettant de passer directement d'une partie d'un document à une autre, ou d'un document à d'autres documents choisis comme pertinents par l'auteur.

1-2 / L'information binaire, son codage

L'importance du système binaire pour les mathématiques et la logique a été comprise une première fois par le grand mathématicien et philosophe Leibnitz au XVIIe siècle. On trouve cependant des traces du système binaire bien avant, chez les Indiens et les Chinois.

Il faut avant tout se rappeler que les données qui sont le corps des fichiers « sons », « images », « page web » sont formés par des éléments binaires (bit pour **B**inary dig**it**).

On associe généralement ces éléments binaires sous la forme d'octets (mot ou nombre de huit bits).

Deux symboles (bits) sont nécessaires pour construire les nombres de la base 2 (0 et 1).

Petit tableau récapitulatif avec un octet

2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0	
128	**64**	**32**	**16**	**8**	**4**	**2**	**1**	résultat
1	0	0	0	0	0	0	0	128
1	0	1	0	0	0	0	0	160
1	1	1	1	1	1	1	1	255

Nous retrouverons le résultat « 255 », très important dans la suite de notre ressource...
(Les 8 bits de notre octet sont à 1)

1/3 Les LAN et les WAN

Les LAN(Local Area Network)
Ils sont utilisés pour regrouper des machines proches partageant le même but, projet, secteur, etc... Ce genre de réseau comprend les réseaux d'entreprise, les réseaux familiaux... La distance entre de poste dépend certes des média utilisés reste reste généralement faible (même salle, même bâtiment...).

Les WAN (Wide Area Network)
Un réseau étendu (WAN) est composé de plusieurs réseaux locaux reliés les uns aux autres sur de longues distances. Et par exemple serait un bureau d'entreprise connecté à chacun de ses bureaux satellites

Le réseau mondial (Internet) est donc la collaboration de LAN interconnectés en WAN.

2 / L'histoire d'Internet

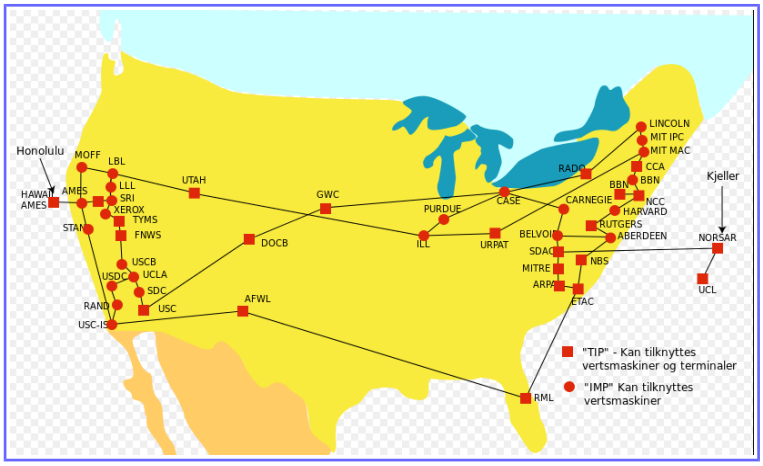
L'histoire d'Internet remonte au développement des premiers réseaux de télécommunication. L'idée d'un réseau informatique, permettant aux utilisateurs de différents ordinateurs de communiquer, se développa par de nombreuses étapes successives.

À l'époque, dans les années 1950, les communications étaient « point à point », c'est-à-dire qu'on ne pouvait communiquer qu'avec une seule machine à la fois.

Les chercheurs universitaires qui devaient communiquer avec plusieurs autres chercheurs lors de réunions, se sont rendu compte qu'il serait intéressant de pouvoir le faire en temps réel plutôt que de passer d'un interlocuteur à l'autre successivement.

ARPANET est le premier réseau à transfert de paquets développé aux États-Unis par la DARPA. Le projet fut lancé en 1969 et la première démonstration officielle date d'octobre 1972.

L'Arpanet, l'ancêtre d'Internet, ne comportait que quatre machines ! Les protocoles utilisés alors ne permettaient pas d'atteindre les buts fixés, à savoir de faire dialoguer des machines provenant de différents réseaux en utilisant différentes technologies de communication.



Sites des États-Unis reliés à ARPANET en 1974.

C'est alors que les chercheurs se sont orientés vers la création d'autres protocoles de communication, et notamment TCP/IP. Internet a continué de croître au fil des années, mais c'est en 1990 qu'une révolution va permettre sa croissance réelle : le langage HTML et le protocole d'échange HTTP qui permettent la création de pages web.

Le réseau Arpanet adopte le 1er janvier 1983 la suite de protocoles TCP/IP qui sera la base d'Internet.

TCP/IP est une suite de protocoles. Le sigle TCP/IP signifie «Transmission Control Protocol/Internet Protocol» et se prononce «T-C-P-I-P».
Il provient des noms des deux protocoles majeurs de la suite de protocoles, c'est-à-dire les protocoles TCP et IP.

TCP/IP représente d'une certaine façon l'ensemble des règles de communication sur internet et se base sur la notion adressage IP, c'est-à-dire le fait de fournir une adresse IP à chaque machine du réseau afin de pouvoir acheminer des paquets de données.

Le réseau TCP/IP est un modèle en couches

Afin de pouvoir appliquer le modèle TCP/IP à n'importe quelles machines, c'est-à-dire indépendamment du système d'exploitation, le système de protocoles TCP/IP a été décomposé en plusieurs modules effectuant chacun une tâche précise. De plus, ces modules effectuent ces tâches les uns après les autres dans un ordre précis, on a donc un système stratifié, c'est la raison pour laquelle on parle de modèle en couches.

3 / Les modèles OSI et TCP/IP

3-1 / Le modèle OSI (rapidement...et pour information)

Nous allons voir comment les chercheurs ont fait pour passer des principes de communication humains à des principes de communication pour ordinateurs.

Ils ont ainsi regroupé l'ensemble de leurs recherches et de leurs résultats dans une norme que devront respecter les personnes se connectant à Internet.

Le rôle du modèle **OSI** (de l'anglais **O**pen **S**ystems **I**nterconnection) consiste à standardiser la communication entre les machines afin que différents constructeurs puissent mettre au point des produits (logiciels ou matériels) compatibles.

Niveau	Modèle OSI	Fonction	Matériel associé
7	Application	La couche application assure l'interface avec les applications. Il s'agit donc du niveau le plus proche des utilisateurs, géré directement par les logiciels.	Le proxy
6	Présentation	La couche présentation définit le format des données manipulées par le niveau applicatif (leur représentation, éventuellement leur compression et leur chiffrement) indépendamment du système.	
5	Session	La couche session définit l'ouverture et la destruction des sessions de communication entre les machines du réseau.	
4	Transport	La couche transport est chargée du transport des données, de leur découpage en paquets et de la gestion des éventuelles erreurs de transmission.	RAS
3	Réseau	La couche réseau permet de gérer l'adressage et le routage des données, c'est-à-dire leur acheminement via le réseau.	Le routeur.
2	Liaison de données	La couche liaison données définit l'interface avec la carte réseau et le partage du média de transmission	Le switch, ou commutateur.
1	Physique	La couche physique définit la façon dont les données sont physiquement converties en signaux numériques sur le média de communication (impulsions électriques, modulation de la lumière, etc.).	Le hub, ou concentrateur en français.

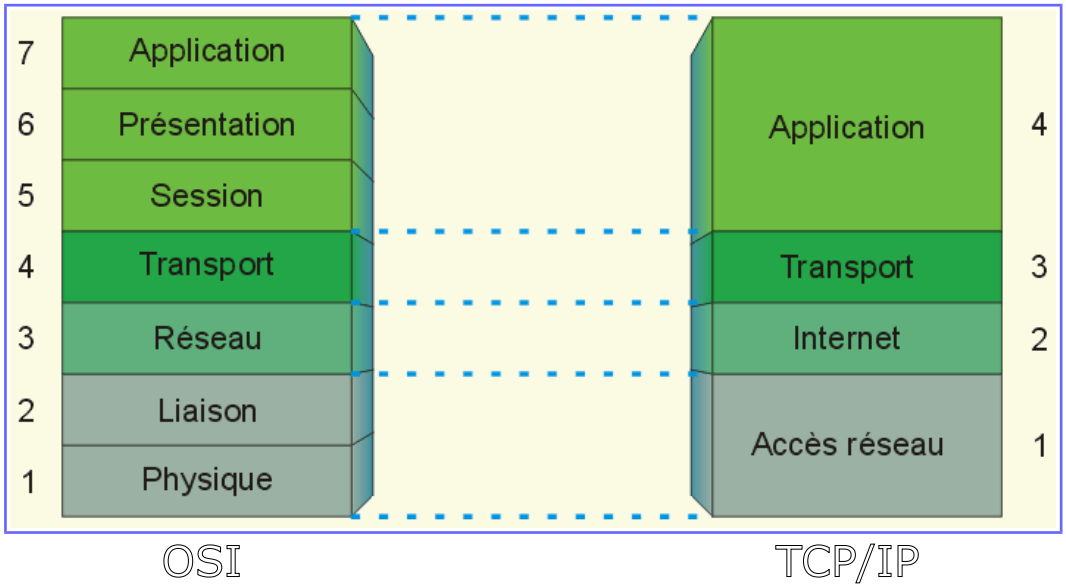
Le modèle OSI est une norme précisant comment les machines doivent communiquer entre elles.

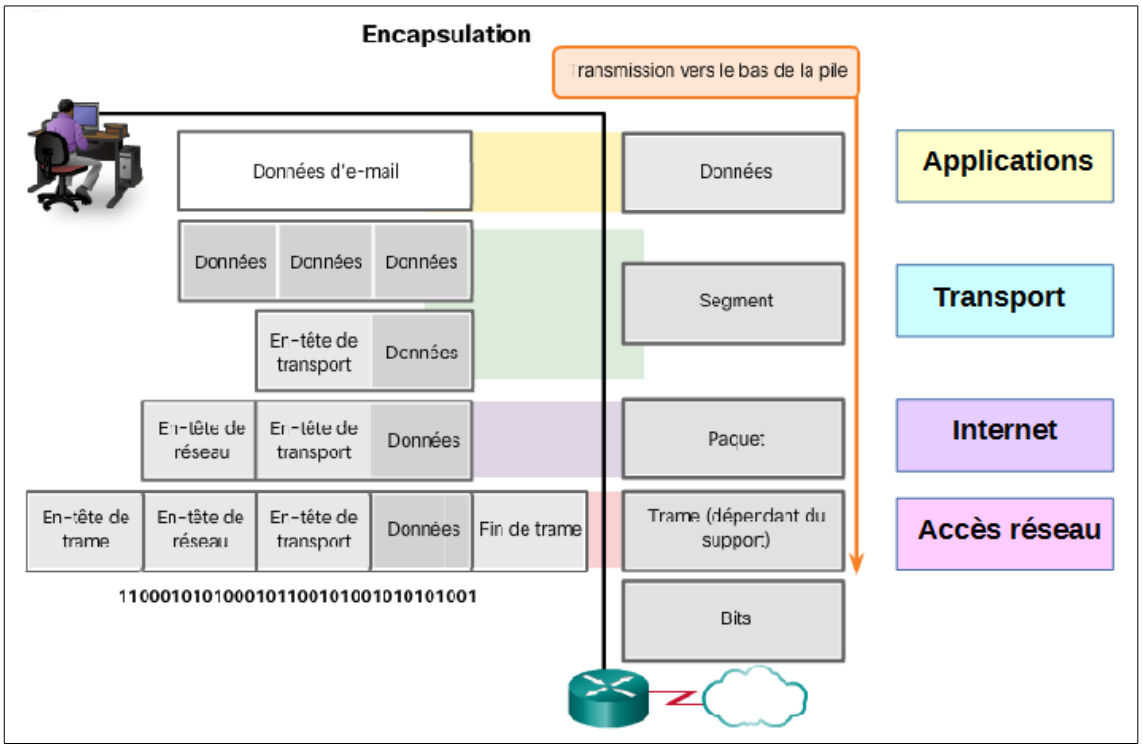
Le modèle OSI possède 7 couches et chaque couche a un rôle particulier à accomplir.
Les couches 1 à 4 sont les couches réseau.
Les couches réseau offrent le service de communication à la couche applicative.
Chaque couche est indépendante des autres.
Chaque couche ne peut communiquer qu'avec une couche adjacente.
Lors de l'envoi de données, on parcourt le modèle OSI de haut en bas, en traversant toutes les couches.

3-2 / Le modèle TCP/IP

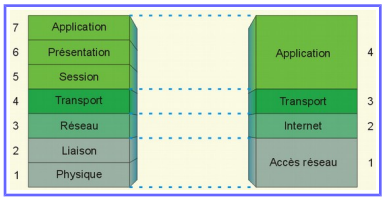
Le modèle TCP/IP, inspiré du modèle OSI, reprend l'approche modulaire (utilisation de modules ou couches) mais en contient uniquement quatre...

Niveau	Modèle OSI	Modèle TCP/IP	Fonction
7	Application	Application (HTTP)	Couche Application : elle englobe les applications standard du réseau (Telnet, SMTP, FTP, ...) Voici les principaux protocoles faisant partie de la suite TCP/IP :
6	Présentation		
5	Session		
4	Transport	Transport (TCP)	La couche Transport : Les protocoles des couches précédentes permettaient d'envoyer des informations d'une machine à une autre. La couche transport permet à des applications tournant sur des machines distantes de communiquer. Le problème consiste à identifier ces applications.
3	Réseau	Internet (IP)	La couche Internet est la couche "la plus importante" (elles ont toutes leur importance) car c'est elle qui définit les datagrammes, et qui gère les notions d'adressage IP.
2	Liaison de données	Accès réseau (LAN)	La couche accès réseau est la première couche de la pile TCP/IP, elle offre les capacités à accéder à un réseau physique quel qu'il soit, c'est-à-dire les moyens à mettre en œuvre afin de transmettre des données via un réseau.
1	Physique		





3-2-1 / La couche 1, la couche accès réseau (TCP/IP)



Le vocable « Ethernet » est souvent employé à contre sens. Peut-être n'est-il pas inutile de préciser un peu, même si, pour l'utilisateur (qui travaille sur la couche supérieure), ce qu'il se passe sur la couche 1 n'a pas beaucoup de répercussions.

Le mot « Ethernet » fait référence au support de propagation des informations utilisé. Historiquement, de trois types (mais d'autres peuvent être utilisés):

Coaxial épais, Coaxial fin (RG58), Paire torsadée.

Pour être tout à fait précis, la norme qui décrit les réseaux de type Ethernet qui sont utilisés sur la majorité des réseaux locaux est la norme IEEE 802.3

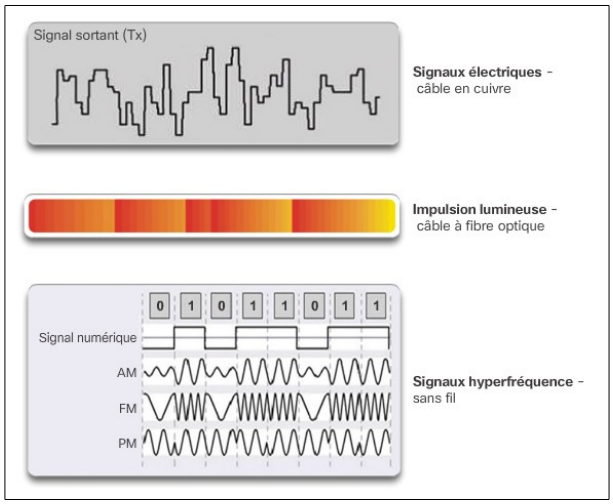
Le rôle principal de la couche 1 est de fournir le support de transmission de la communication.
La couche 1 aura donc pour but d'acheminer des signaux, des 0 et des 1 !

Il existe trois formes élémentaires de support réseau.

Câble en cuivre : les signaux sont des variations d'impulsions électriques.

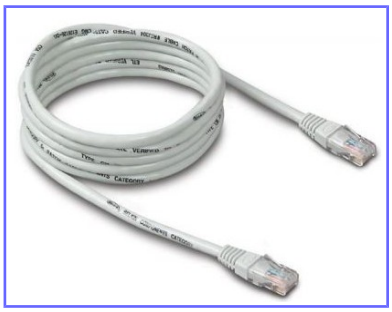
Câble à fibre optique : les signaux sont des variations lumineuses.

Sans fil : les signaux sont des variations de transmission d'hyperfréquences.



Les matériels de connexion sont ceux qui servent à connecter plusieurs machines entre elles, comme les hubs ou les switch

Sur ces switch, on peut raccorder des câbles RJ45 ou de la fibre optique



En réseau, **la topologie** est la manière selon laquelle on branche les machines entre elles.

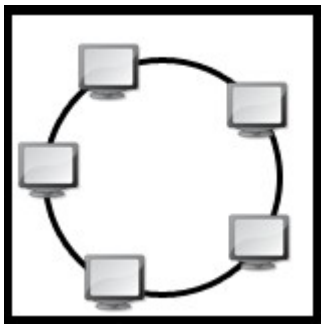
Nous avons plusieurs topologies possibles

1-La topologie en bus (linéaire)
2-La topologie en anneau
3-Le réseau maillé
4-Le réseau hiérarchique (en arbre)

5-La topologie en étoile

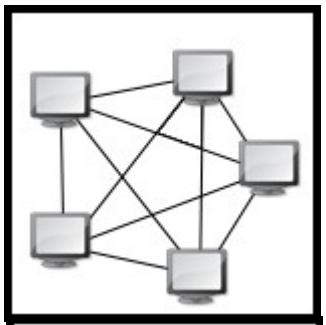
1-La topologie en bus (linéaire)

Sur un bus, une seule machine peut parler à la fois vu qu'il n'y a qu'un seul câble. En gros, on écoute si une machine parle, et si personne ne parle, on parle !



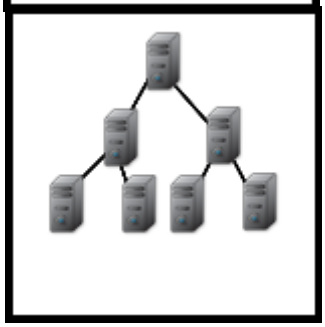
2-Le réseau en anneau

Le mode de communication sur un anneau est assez différent. Il y a un "jeton" qui tourne en permanence sur l'anneau et que les machines peuvent prendre pour envoyer un message.
C'est un peu comme si vous étiez assis en rond avec des amis et que votre seul moyen de communiquer était un panier que vous vous passiez de l'un à l'autre, dans un sens.
Pour parler, il faut prendre le panier et mettre son message dedans. Vous passez le panier à votre voisin qui regarde l'adresse du destinataire. Si c'est lui, il le lit, sinon il passe à son voisin, et ainsi de suite.



3-Le réseau maillé

Cette topologie se rencontre dans les grands réseaux de distribution (Exemple : Internet). L'information peut parcourir le réseau suivant des itinéraires divers, sous le contrôle de puissants superviseurs de réseau, ou grâce à des méthodes de routage réparties.



4-Le réseau hiérarchique (en arbre)

Le sommet, de haut niveau, est connectée à plusieurs nœuds de niveau inférieur, dans la hiérarchie. Ces nœuds peuvent être eux-mêmes connectés à plusieurs nœuds de niveau inférieur. Le tout dessine alors un arbre, ou une arborescence.

5-La topologie en étoile

C'est la topologie la plus courante actuellement.
Omniprésente, elle est aussi très souple en matière de gestion et dépannage de réseau : la panne d'un nœud ne perturbe pas le fonctionnement global du réseau.

En revanche, l'équipement central (un commutateur (switch)) qui relie tous les nœuds constitue un point unique de défaillance : une panne à ce niveau rend le réseau totalement inutilisable.

C'est ce type de topologie qui est utilisée au collège !

Les matériels de connexion sont ceux qui servent à connecter plusieurs machines entre elles, comme les hubs ou les switch

(Les Hubs sont réservés à une utilisation personnelle et locale, pas en réseau sur le collège par exemple....ils ne sont pas « discrets », ils ne cachent rien de vos données !)

L'objectif est de permettre à des machines connectées ensemble de communiquer.

Les adresses MAC

Pour pouvoir parler à une machine en particulier, il faut être capable de l'identifier. Les chercheurs ont donc créé un identifiant particulier à la couche 2 qui permettrait de distinguer les machines entre elles, il s'agit de l'adresse MAC ! (acronyme de **M**edia **A**ccess **C**ontrol)

Une adresse MAC (Media Access Control1) est un identifiant physique stocké dans une carte réseau ou une interface réseau similaire.

À moins qu'elle n'ait été modifiée par l'utilisateur, elle est unique au monde.

Le MAC n'a aucun rapport avec le Mac d'Apple (diminutif de Macintosh).

Toutes les cartes réseau ont une adresse MAC, même celles contenues dans les PC et autres appareils connectés (tablette tactile, smartphone, consoles de jeux...).

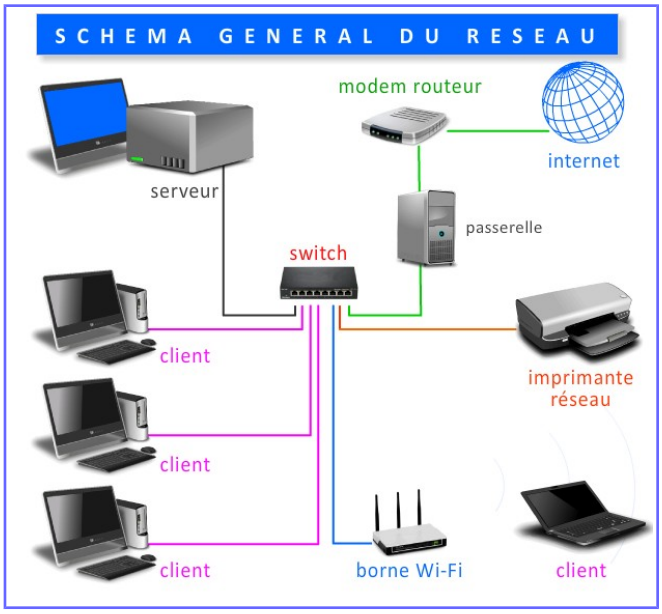
L'adresse MAC est constituée de bit (Le bit est l'unité la plus simple dans un système de numération, ne pouvant prendre que deux valeurs, désignées le plus souvent par les chiffres 0 et 1 et un octet est un regroupement de 8 bits codant une information)

Une adresse MAC-48 est constituée de 48 bits (6 octets) et est généralement représentée sous la forme hexadécimale en séparant les octets par un double point ou un tiret.
Par exemple 5E:FF:56:A2:AF:15.
Cela nous laisse tout de même environ 281 000 milliards d'adresses MAC possibles !

L'aiguillage des trames

Pour envoyer la trame vers la bonne machine, le switch se sert de l'adresse MAC destination contenue dans l'en-tête de la trame.

Il contient en fait une table qui fait l'association entre un port du switch (une prise RJ45 femelle) et une adresse MAC. Cette table est appelée la table CAM.



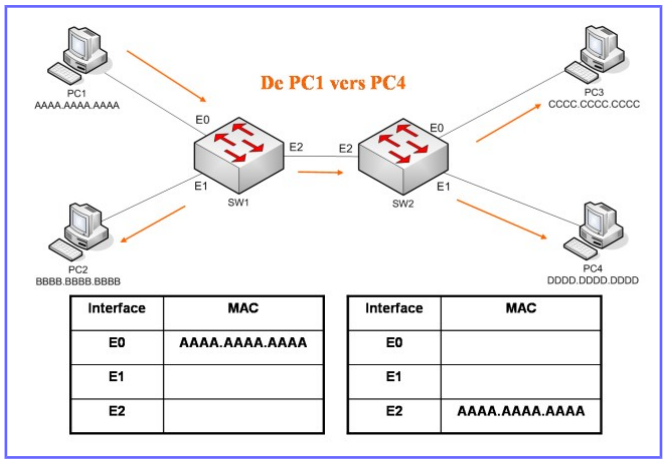
Mais avant toute chose,
Il existe une adresse MAC spéciale

Parmi les adresses MAC, il y en a une particulière, c'est l'adresse dans laquelle tous les bits sont à 1, ce qui donne ff:ff:ff:ff:ff:ff.
Cette adresse est appelée l'adresse de broadcast.

L'adresse de broadcast est une adresse universelle qui identifie n'importe quelle carte réseau.
Elle me permet ainsi d'envoyer un message à toutes les cartes réseaux des machines présentes sur mon réseau, en une seule fois.

Exemple de recherche d'adresse MAC avec un réseau qui comporte 2 switch !

Trame envoyée par PC1 à destination de PC4



Interface	MAC
E0	AAAA.AAAA.AAAA
E1	
E2	

Interface	MAC
E0	
E1	
E2	AAAA.AAAA.AAAA

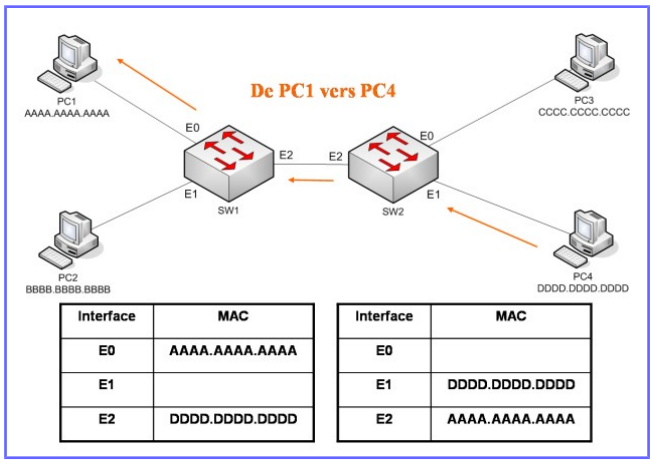
1- la trame sort de la carte réseau de PC1 avec:
adresse MAC source = AAAA.AAAA.AAAA
adresse MAC destination = DDDD.DDDD.DDDD

2- la trame arrive sur le port E0 du switch SW1
le switch extrait l'adresse MAC source et l'insère dans sa table (cf schéma). Maintenant le switch sait que pour joindre cette adresse MAC (AAAA.AAAA.AAAA), il doit commuter les trames vers le port E0. Cette information lui servira donc pour le retour de la trame.
-puis le switch extrait l'adresse MAC destination (DDDD.DDDD.DDDD) et la compare à sa table:
aucune entrée trouvée donc ne sachant pas où envoyer la trame, il la diffuse sur tous les ports exceptés le port de réception E0.

3- la trame arrive sur le port E2 du switch SW2
le switch extrait l'adresse MAC source et l'insère dans sa table (cf schéma). Maintenant le switch sait que pour joindre cette adresse MAC (AAAA.AAAA.AAAA), il doit commuter les trames vers le port E2. Cette information lui servira donc pour le retour de la trame.
puis le switch extrait l'adresse MAC destination (DDDD.DDDD.DDDD) et la compare à sa table: aucune entrée trouvée donc ne sachant pas où envoyer la trame, il la diffuse sur tous les ports exceptés le port de réception E2.

4- la trame arrive sur la carte réseau du PC4: gagné pour la trame aller !

Trame réponse envoyée par PC4 à destination de PC1

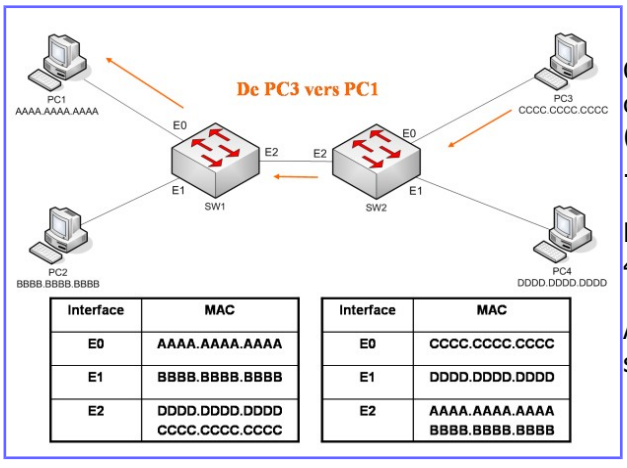


Interface	MAC
E0	AAAA.AAAA.AAAA
E1	
E2	DDDD.DDDD.DDDD

Interface	MAC
E0	
E1	DDDD.DDDD.DDDD
E2	AAAA.AAAA.AAAA

Le fonctionnement est le même que précédemment. On remarque que lorsque la trame arrive sur les Switch, ils insèrent l'adresse MAC source DDDD.DDDD.DDDD dans leur table.

Puis ils extraient l'adresse MAC destination (AAAA.AAAA.AAAA) et la compare à leur table et là ils savent où se situe cette adresse MAC; port E2 pour le switch SW2 et port E0 pour le switch SW1. Ils n'ont plus qu'à commuter la trame UNIQUEMENT sur le port en question.



Interface	MAC
E0	AAAA.AAAA.AAAA
E1	BBBB.BBBB.BBBB
E2	DDDD.DDDD.DDDD CCCC.CCCC.CCCC

Interface	MAC
E0	CCCC.CCCC.CCCC
E1	DDDD.DDDD.DDDD
E2	AAAA.AAAA.AAAA BBBB.BBBB.BBBB

On dit que le switch a convergé quand sa table MAC contient toutes les adresses MAC se trouvant dans le réseau (des PC, des imprimantes, des bornes Wi-Fi, des serveurs, …).

Dans le schéma ci dessus, on voit bien que les adresses des 4 PC sont bien dans chacune des tables de SW1 et SW2.

Au final, lorsqu'une trame arrive sur SW1 ou SW2, ils sauront exactement où commuter cette trame.

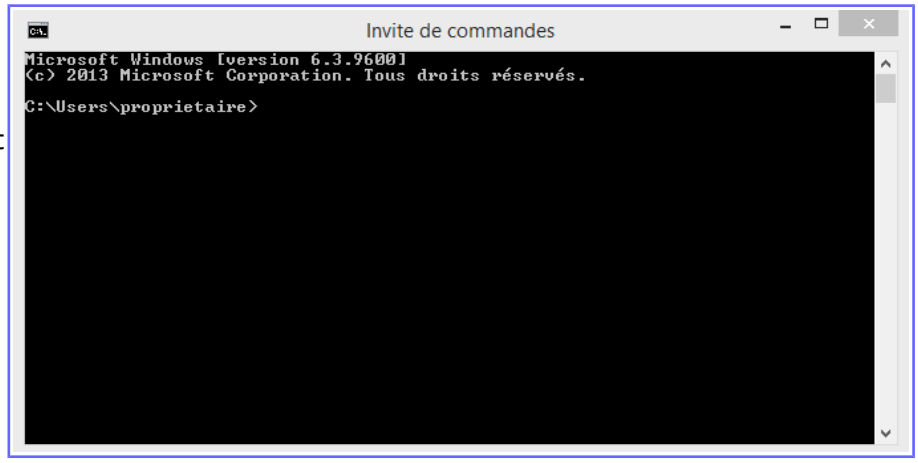
Un peu de pratique

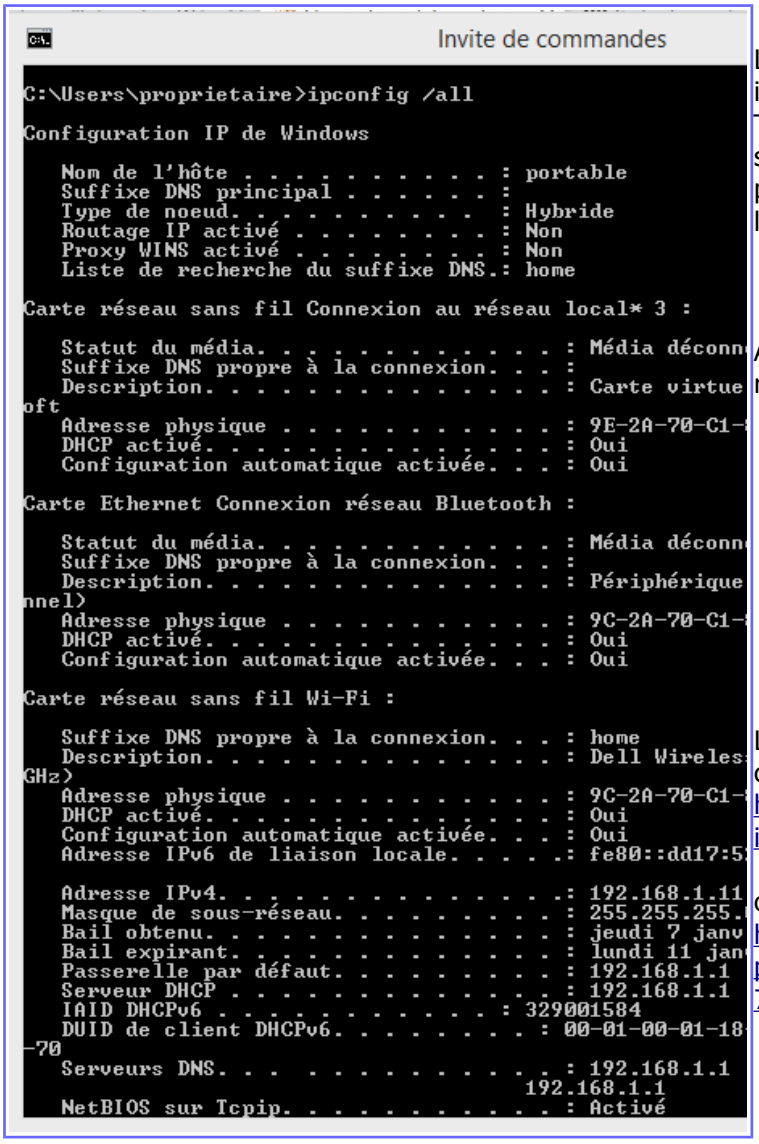
En ligne de commande

Ouvrez une invite de commande

Cliquez sur Démarrer, Exécuter et tapez cmd, puis Ok. Ou sous Windows8 clique droit en bas à gauche sur le logo Windows, puis « invite de commande »

Une fenêtre noire s'affiche, semblable à celle que vous pouvez voir en figure suivante : c'est l'invite de commande !





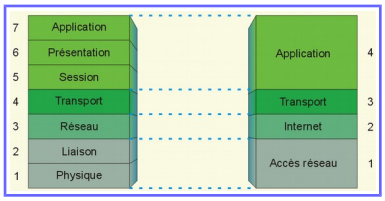
La commande de base pour avoir des informations sur votre carte réseau est ipconfig. Toutefois, pour avoir les informations que nous souhaitons, il va falloir en demander un peu plus à la commande ipconfig en lui mettant l'option /all.

Adresse physique, l'adresse MEC de ma carte réseau 9E-2A-70-C1-xx-xx

Les invites de commande sont à retrouver à cette adresse http://www.commentcamarche.net/faq/13047-invite-de-commande-cmd-sous-windows

ou bien http://www.zebulon.fr/astuces/244-les-principales-commandes-executer-de-windows-7.html

3-2-2 / La couche 2, Internet (TCP/IP)



Le rôle de la couche 2 est d'interconnecter les réseaux.

Internet Protocol. IP
C'est le protocole dont on parle le plus, il est en effet directement impliqué dans la configuration réseau de l'hôte. C'est lui qui, en fonction de l'adresse IP du destinataire acheminera l'information sur la bonne route.
Les considérations relatives à la topologie d'une adresse IP sont vues un peu plus loin dans ce chapitre.
Les concepts du routage sont vus dans le chapitre suivant sur ce site.

Internet Control Message Protocol. ICMP
En termes de sécurité, ce protocole fait peur à beaucoup de monde (parfois à juste titre d'ailleurs), il est cependant fondamental pour le bon fonctionnement de l'Internet. C'est grâce à ce protocole que les anomalies de fonctionnement peuvent être signalées à l'émetteur, afin qu'il puisse essayer d'y remédier.

La couche Internet est la couche "la plus importante" car c'est elle qui définit les datagrammes, et qui gère les notions d'adressage IP.

Elle permet l'acheminement des datagrammes (paquets de données) vers des machines distantes ainsi que de la gestion de leur fragmentation et de leur assemblage à réception.

La couche 2 va donc me permettre de joindre n'importe quel réseau sur Internet, en passant à travers d'autres réseaux. Ma connexion à une machine sur un autre réseau se fera à travers des réseaux, de proche en proche.

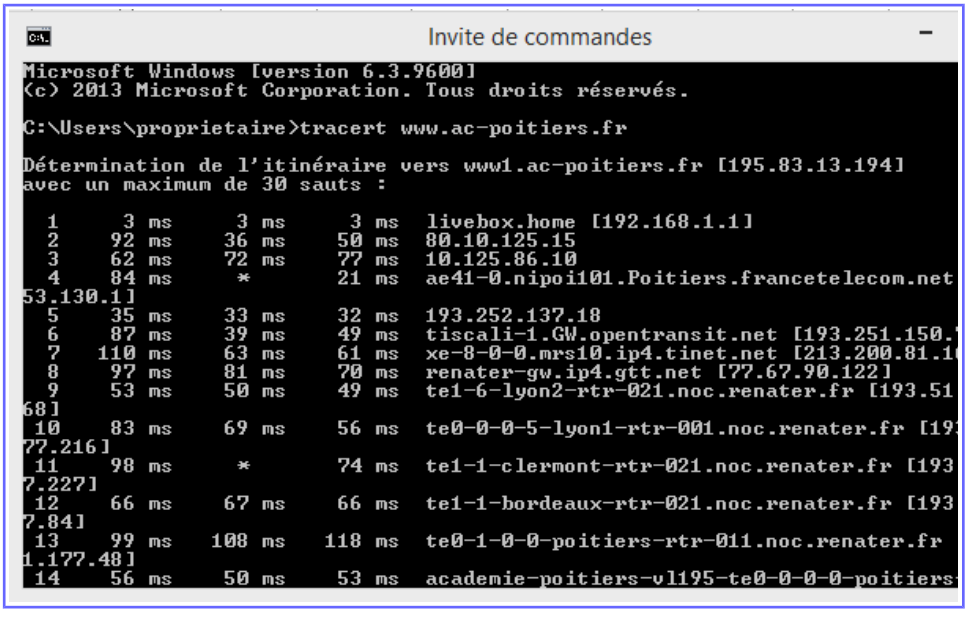
Par exemple, avec la commande tracert, nous allons aller voir le site de l'académie de Poitiers, (adresse IP 192.83.13.194 comme vous pouvez le voir dans la fenêtre ci-dessous)

Et bien, pour partir de la maison (près de Poitiers) je passe par nipoi101, le central téléphonique de Poitiers, j'emprunte le réseau Tiscali, je passe par le réseau Rénater (éducation nationale) puis par Lyon, Clermont, Bordeaux....et Poitiers;)

Simple, non ?

Nous avons traversé de nombreux réseaux...

Et tous avec des adresses...



Les adresses IP

L'adresse IP est en fait l'**adresse du réseau ET de la machine**.

Une adresse IP est codée sur 32 bits (soit 4 octets, car un octet vaut 8 bits).

Afin de simplifier la lecture et l'écriture d'adresses IP pour les humains, nous avons choisi d'écrire les adresses avec la notation en décimal pointée. Cette dernière sépare les 4 octets sous forme de 4 chiffres décimaux allant de 0 à 255.
Cela donne par exemple : 192.83.13.194 pour l'Académie de Poitiers

On en déduit que la plus petite adresse IP est: 0.0.0.0 (quand tous les bits de l'adresse sont à 0) alors que la plus grande vaut : 255.255.255.255 (quand tous les bits sont à 1).

Le masque de sous-réseau

Nous allons en fait ajouter une information supplémentaire à l'adresse IP, le masque de sous-réseau. Et ces deux informations, adresse IP et masque, seront inséparables.

C'est le masque qui va indiquer quelle est la partie réseau de l'adresse, et quelle est la partie machine.

Attention, lire avec attention ce qui va suivre...

Définition : Les bits à 1 dans le masque représentent la partie réseau de l'adresse IP.

On en déduit que les bits à 0 représentent la partie machine de l'adresse.

Prenons un exemple : on associe l'adresse IP 192.168.0.1 au masque 255.255.0.0.
Écrivons maintenant ces deux adresses en binaire pour y voir plus clair :

255.255.0.0 -> 11111111.11111111.00000000.00000000
192.168.0.1 -> 11000000.10101000.00000000.00000001

Le masque nous dit que les bits à 1 représentent **la partie réseau de l'adresse** :

255.255.0.0 -> 11111111.11111111.00000000.00000000
192.168.0.1 -> 11000000.10101000.00000000.00000001

Il nous dit aussi que les bits à 0 représentent la partie machine de l'adresse :

255.255.0.0 -> 11111111.11111111.00000000.00000000
192.168.0.1 -> 11000000.10101000.00000000.00000001

Donc **la partie réseau de l'adresse** est 192.168, et la partie machine est 0.1

(re) Attention, lire avec attention ce qui va suivre;)

Mais parfois le calcul est beaucoup moins simple, reprenons l'exemple de l'adresse précédente mais avec un masque de réseau différent.
L'adresse 192.168.0.1 associée au masque 255.255.240.0

Transformons tout cela en binaire

192.168.0.1 11000000.10101000.00000000.00000001
255.255.240.0 11111111.11111111.11110000.00000000

Nous constatons que la coupure imposée par le masque se fait en plein milieu d'un octet !
On ne peut pas repasser en décimal étant donné que la coupure se fait au milieu d'un octet. En effet, on ne peut malheureusement pas écrire un demi-octet ou une partie d'un octet seulement. On ne peut parler qu'en binaire.

Donc,

La partie réseau de l'adresse est 11000000.10101000.0000 et la partie machine est 0000.00000001.

Les valeurs prises par les octets dans un masque sont spécifiques.

Ainsi, on retrouvera toujours les mêmes valeurs pour les octets d'un masque, qui sont les suivantes :

00000000 -> 0
10000000 -> 128
11000000 -> 192
11100000 -> 224
11110000 -> 240
11111000 -> 248
11111100 -> 252
11111110 -> 254
11111111 -> 255

Calcul de plages d'adresses (toujours attentif?)

Calcul de la première et de la dernière adresse d'une plage
Reprenons le même exemple, l'adresse 192.168.0.1 associée au masque 255.255.240.0

Toutes les machines appartenant à un même réseau ont un point commun :
tous les bits de leur partie réseau sont identiques !

Donc, toutes les machines de ce réseau auront au moins cette partie là commune !
11000000.10101000.0000

Par contre, les bits de la partie machine de l'adresse vont pouvoir varier pour toutes les machines du réseau.

Dans ce réseau, les adresses des machines pourront prendre beaucoup de valeurs, selon que l'on met certains bits de la partie machine à 0 ou 1.
Globalement, les adresses seront :

11000000.10101000.00000000.00000000 -> 192.168.0.0
11000000.10101000.00000000.00000001 -> 192.168.0.1
11000000.10101000.00000000.00000010 -> 192.168.0.2
11000000.10101000.00000000.00000011 -> 192.168.0.3
11000000.10101000.00000000.00000100 -> 192.168.0.4
11000000.10101000.00000000.00000101 -> 192.168.0.5
...
11000000.10101000.00001111.11111110 -> 192.168.15.254
11000000.10101000.00001111.11111111 -> 192.168.15.255

La première adresse du réseau est celle dont tous les bits de la partie machine sont à 0 ; la dernière adresse du réseau est celle dont tous les bits de la partie machine sont à 1.

Calcul du nombre d'adresses dans un réseau

Nous avons vu que dans notre adresse, la partie réseau était fixée et la partie machine pouvait varier.

Il nous suffit de trouver combien de combinaisons sont possibles en faisant varier les bits de la partie machine, et nous aurons alors le nombre d'adresses.

Donc pour trouver le nombre d'adresses dans un réseau, il suffit de connaître le nombre de bits de la partie machine.

Reprenons le même exemple, l'adresse 192.168.0.1 associée au masque 255.255.240.0 et passons l'adresse du masque en binaire

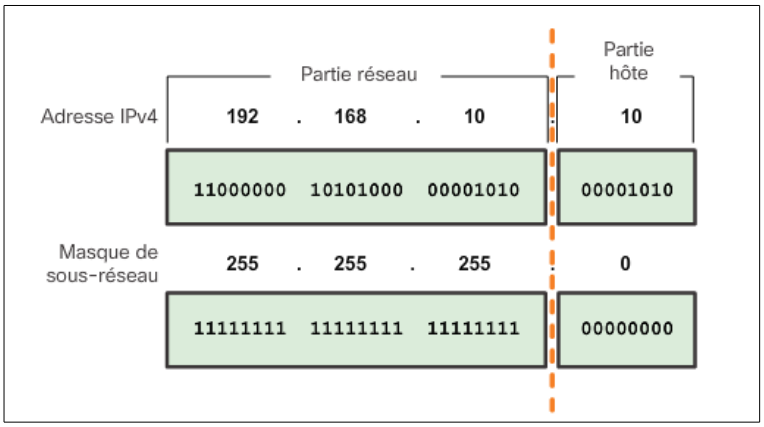
255.255.240.0 11111111.11111111.11110000.00000000

Nous comptons 12 zéros à la fin de l'adresse donc calculons 2^{12} soit 4096 adresses différentes !

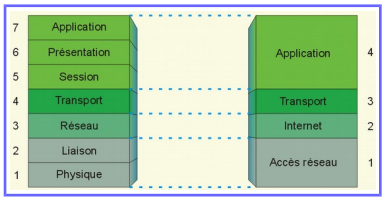
Parmi la plage d'adresses définie par une adresse IP et un masque, deux adresses sont particulières, la première et la dernière.

La première adresse d'une plage est l'adresse du réseau lui-même.
Cette adresse ne pourra donc pas être utilisée pour une machine.

La dernière adresse d'une plage est une adresse spéciale, l'adresse de broadcast.
Cette adresse ne peut pas non plus être utilisée pour une machine. Elle est en fait utilisée pour identifier toutes les machines de mon réseau.



3-2-3 / La couche 3 Transport TCP/IP



TCP et UDP sont les 2 principaux protocoles de la couche transport.
La différence entre TCP et UDP sont fondamentales.

TCP
Dans ce mode, il se met en place un processus de « handshake » (poignée de main) entre le client et le serveur. Ce processus permet d'établir un dialogue à propos du transfert de données. Il y a des accusés réception, des demandes d'émission etc. qui permettent aux applications de savoir exactement où en est le processus de transfert de données.

Ce protocole est très robuste et permet un transfert de données dans de bonnes conditions.

UDP
C'est un mode simple, de type « on envoie les données et on espère qu'elles arriveront »
Dans ce mode, il n'y a pas de « handshake ». Une lettre simple et ici un bon exemple. L'émetteur ne reçoit à priori aucune confirmation de réception.

Ces deux protocoles servent à échanger des paquets d'information entre 2 machines en utilisant leur adresse IP et un numéro de port.

Pour expliquer la différence entre UDP et TCP, on va prendre une analogie :

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 2 machines peuvent dialoguer de manière bidirectionnelle (vous pouvez parler à votre interlocuteur, et c'est réciproque).

TCP sert de socle à de nombreux protocoles de la couche application, par exemple :

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 sert à lire ses emails
SMTP qui sert quant à lui à envoyer des emails

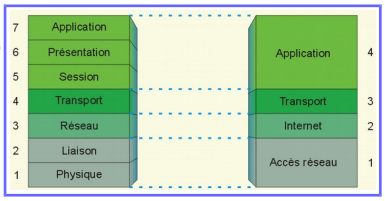
Protocole UDP

UDP est un protocole stateless (sans état), on peut le comparer au courrier : vous placez le message à envoyer dans une enveloppe qui contient toutes les informations nécessaires au routage : l'adresse IP et le port (les coordonnées du destinataire), puis vous envoyez l'enveloppe.

UDP est utilisé par exemple :

DNS, le protocole de résolution des noms de domaines qui permet de connaître l'adresse IP d'un serveur à partir de son nom de domaine (exemple: www.google.fr)

3-2-4 / La couche 4 Applications (TCP/IP)



Ces programmes et les protocoles qu'ils utilisent incluent HTTP (World Wide Web), FTP (transfert de fichiers), SMTP (messagerie), SSH (connexion à distance sécurisée), DNS (recherche de correspondance entre noms et adresses IP) et beaucoup d'autres.

HTTP port TCP 80
SSH port TCP 22
DNS port UDP 53
RIP port UDP 520
FTP port TCP 21

Évitons déjà une confusion
HTTP (Hyper Text Transfert Protocol) est un protocole destiné à transférer du texte (ou des fichiers quelconques, s'ils sont définis par un format MIME) depuis un serveur vers un client.
HTML (Hyper Text Markup Language) est un langage de description de document. Outre les possibilités d'enrichissement du texte comme les attributs gras, italique, souligné....
(le fameux HTML/CSS de vos sites Web)

FTP (transfert de fichiers)
C'est le protocole le plus sûr pour faire du téléchargement de fichiers, même si cette opération peut aussi être réalisée avec HTTP

SMTP (messagerie)
Le protocole SMTP (Simple Mail Transfer Protocol, traduisez Protocole Simple de Transfert de Courrier) est le protocole standard permettant de transférer le courrier d'un serveur à un autre en connexion point à point.

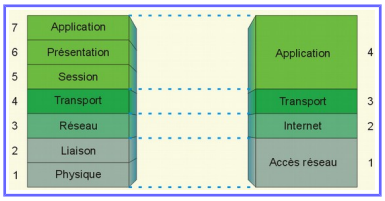
Le protocole POP3
Le protocole POP (Post Office Protocol que l'on peut traduire par "protocole de bureau de poste") permet comme son nom l'indique d'aller récupérer son courrier sur un serveur distant (le serveur POP).

SSH (connexion à distance sécurisée)
SSH - Protocole Secure Shell, Il s'agit d'un protocole permettant à un client (un utilisateur ou bien même une machine) d'ouvrir une session interactive sur une machine distante (serveur) afin d'envoyer des commandes ou des fichiers de manière sécurisée.

DNS (recherche de correspondance entre noms et adresses IP)
Chaque ordinateur directement connecté à internet possède au moins une adresse IP propre. Cependant, les utilisateurs ne veulent pas travailler avec des adresses numériques du genre 66.102.1.94 mais avec un nom de domaine ou des adresses plus explicites, ici www.google.fr
(Pour retrouver l'adresse IP, dans l'invite de commande taper « ping google.fr »)

et...
Serveur DHCP (exercice sur les fiches Cisco)
DHCP signifie Dynamic Host Configuration Protocol. Il s'agit d'un protocole qui permet à un ordinateur qui se connecte sur un réseau d'obtenir dynamiquement (c'est-à-dire sans intervention particulière) sa configuration (principalement, sa configuration réseau). Vous n'avez qu'à spécifier à l'ordinateur de se trouver une adresse IP tout seul par DHCP. Le but principal étant la simplification de l'administration d'un réseau.

4 / Les trames dans le réseau....il faut bien lire et écouter



Sur le schéma de droite, vous avez vos 4 couches TCP/IP, Accès réseau (Ethernet), Internet (IP), transport (TCP ou UDP) et vos applications...

Tout ce beau monde transite sur le réseau en trame (en hexadécimal), comme vous le voyez..ce n'est pas si simple que cela....

No.	Time	Source	Destination	Protocol	Length	Info
35	12.256043	172.16.0.3	172.16.255.255	NBNS	92	Name query NB WPAD<00>
36	40.033085	AsustekC_40:55:9b	Broadcast	ARP	60	Who has 172.16.0.2? Tell 172.16.0.3
37	40.033406	Dell_8d:ed:03	AsustekC_40:55:9b	ARP	60	172.16.0.2 is at 00:25:64:8d:ed:03
38	40.033566	172.16.0.3	172.16.0.2	ICMP	74	Echo (ping) request id=0x0001, seq=17/4352, ttl=128
39	40.033920	Dell_8d:ed:03	Broadcast	ARP	60	Who has 172.16.0.3? Tell 172.16.0.2
40	40.034047	AsustekC_40:55:9b	Dell_8d:ed:03	ARP	60	172.16.0.3 is at 00:1d:60:40:55:9b
41	40.034356	172.16.0.2	172.16.0.3	ICMP	74	Echo (ping) reply id=0x0001, seq=17/4352, ttl=128
42	41.038083	172.16.0.3	172.16.0.2	ICMP	74	Echo (ping) request id=0x0001, seq=18/4608, ttl=128
43	41.038485	172.16.0.2	172.16.0.3	ICMP	74	Echo (ping) reply id=0x0001, seq=18/4608, ttl=128
44	42.052093	172.16.0.3	172.16.0.2	ICMP	74	Echo (ping) request id=0x0001, seq=19/4864, ttl=128
45	42.052504	172.16.0.2	172.16.0.3	ICMP	74	Echo (ping) reply id=0x0001, seq=19/4864, ttl=128
46	43.066080	172.16.0.3	172.16.0.2	ICMP	74	Echo (ping) request id=0x0001, seq=20/5120, ttl=128
47	43.066478	172.16.0.2	172.16.0.3	ICMP	74	Echo (ping) reply id=0x0001, seq=20/5120, ttl=128
48	55.408490	AsustekC_40:55:9b	Broadcast	ARP	60	Who has 172.16.0.1? Tell 172.16.0.3
49	55.408510	AsustekC_e3:9f:c2	AsustekC_40:55:9b	ARP	42	172.16.0.1 is at 90:e6:ba:e3:9f:c2
50	55.408768	172.16.0.3	172.16.0.1	ICMP	74	Echo (ping) request id=0x0001, seq=21/5376, ttl=128
51	55.408847	AsustekC_e3:9f:c2	Broadcast	ARP	42	Who has 172.16.0.3? Tell 172.16.0.1
52	55.409075	AsustekC_40:55:9b	AsustekC_e3:9f:c2	ARP	60	172.16.0.3 is at 00:1d:60:40:55:9b
53	55.409083	172.16.0.1	172.16.0.3	ICMP	74	Echo (ping) reply id=0x0001, seq=21/5376, ttl=128
54	56.419687	172.16.0.3	172.16.0.1	ICMP	74	Echo (ping) request id=0x0001, seq=22/5632, ttl=128
55	56.419752	172.16.0.1	172.16.0.3	ICMP	74	Echo (ping) reply id=0x0001, seq=22/5632, ttl=128
56	57.433696	172.16.0.3	172.16.0.1	ICMP	74	Echo (ping) request id=0x0001, seq=23/5888, ttl=128
57	57.433763	172.16.0.1	172.16.0.3	ICMP	74	Echo (ping) reply id=0x0001, seq=23/5888, ttl=128
58	58.447687	172.16.0.3	172.16.0.1	ICMP	74	Echo (ping) request id=0x0001, seq=24/6144, ttl=128
59	58.447753	172.16.0.1	172.16.0.3	ICMP	74	Echo (ping) reply id=0x0001, seq=24/6144, ttl=128
60	66.514877	172.16.0.2	172.16.0.3	ICMP	74	Echo (ping) request id=0x0001, seq=10/2560, ttl=128
61	71.117747	Dell_8d:ed:03	AsustekC_40:55:9b	ARP	60	Who has 172.16.0.3? Tell 172.16.0.2
62	71.117894	AsustekC_40:55:9b	Dell_8d:ed:03	ARP	60	172.16.0.3 is at 00:1d:60:40:55:9b
63	71.133415	172.16.0.2	172.16.0.3	ICMP	74	Echo (ping) request id=0x0001, seq=11/2816, ttl=128
64	76.125426	172.16.0.2	172.16.0.3	ICMP	74	Echo (ping) request id=0x0001, seq=12/3072, ttl=128
65	81.133051	172.16.0.2	172.16.0.3	ICMP	74	Echo (ping) request id=0x0001, seq=13/3328, ttl=128

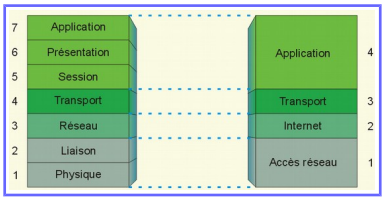
Nous avons au départ, tout en bas la trame Ethernet (nous la (re)verrons dans les exercices sur Cisco Packet Tracer). Elle est constituée de cette façon.

La trame Ethernet
(couche niveau 2 TCP/IP)

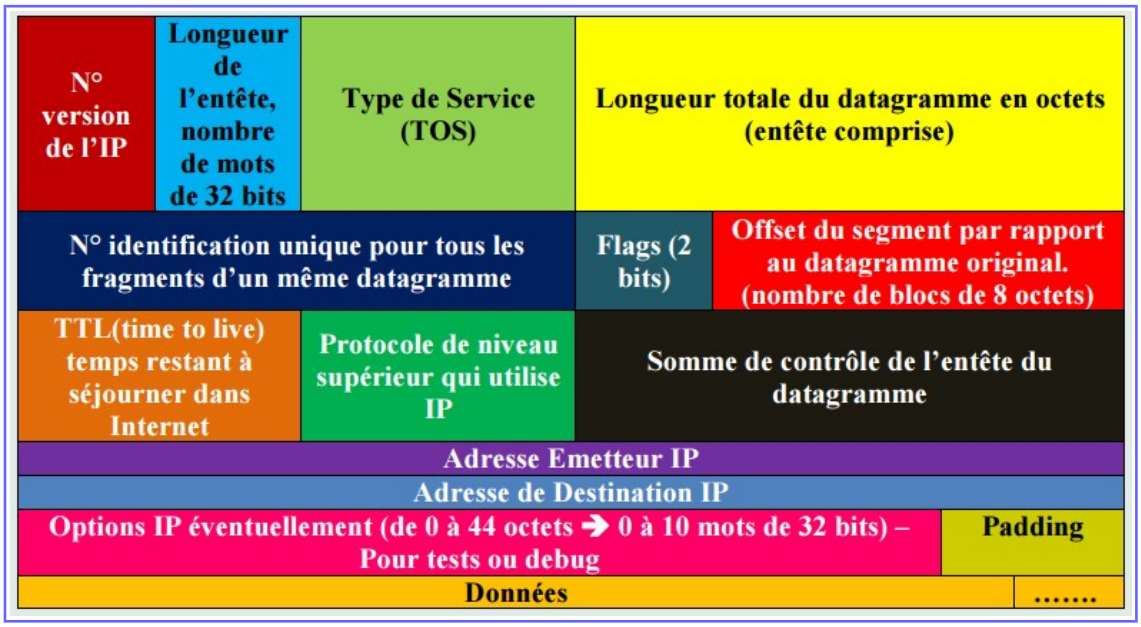
Préambule	SFD	@MAC destination	@MAC source	Type	Données utiles	Bourrage	FCS
7 octets	1 octet	6 octets	6 octets	2 octets	46 à 1500 octets		4 octets

FCS (Field Check Sequence) avec CRC (Cyclic Redundancy Code) – SFD (Start Frame Delimiter)

Au dessus nous allons avoir la trame Internet...

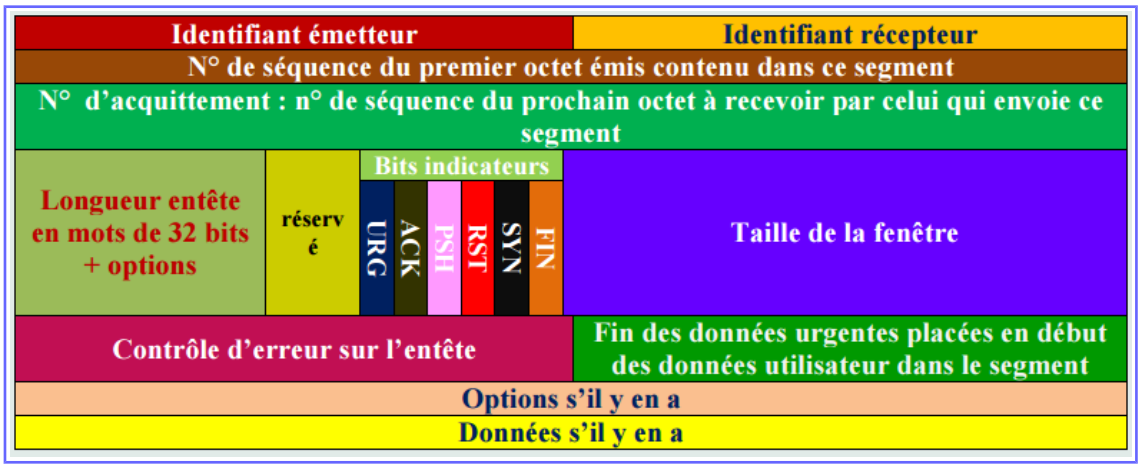


Entête IP
(couche niveau 2 TCP/IP)



Encore au dessus , vous avez la couche transport...

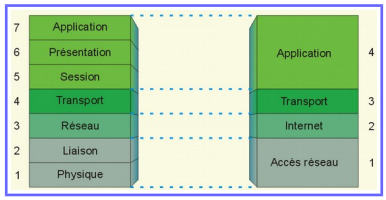
Entête TCP
(Couche niveau 3 TCP/IP)



Nous allons maintenant essayer de comprendre comment tout ceci ne se mélange pas et comment faire pour retrouver ce que vous avez envoyé...

Voici un autre exemple de trame Ethernet en ligne

```
AA AA AA AA AA AA AA AB
08 00 20 0A 70 66 08 00
20 0A AC 96 08 00 45 00
00 28 A6 F5 00 00 1A 06
75 94 C0 5D 02 01 84 E3
3D 05 00 15 0F 87 9C CB
7E 01 27 E3 EA 01 50 12
10 00 DF 3D 00 00 20 20
20 20 20 20 9B 52 46 43
```




```
AA AA AA AA AA AA AA AB
08 00 20 0A 70 66 08 00
20 0A AC 96 08 00 45 00
00 28 A6 F5 00 00 1A 06
75 94 C0 5D 02 01 84 E3
3D 05 00 15 0F 87 9C CB
7E 01 27 E3 EA 01 50 12
10 00 DF 3D 00 00 20 20
20 20 20 20 9B 52 46 43
```


AA AA AA AA AA AA AA AB Synchronisation

08 00 20 0A 70 66 Adresse MAC de destination (constructeur =080020)

08 00 20 0A AC 96 Adresse MAC source (même constructeur)

08 00 → Type (ici IP). Si < à 1500 c'est une longueur)

46 octets inférieur à 1500 donc, datagrammes IP

----------contenu du datagramme IP----------

4 Version IP (ipv4)

5 Longueur de l'entête (5*32 bits = 160 bits ou 5*4 octets = 20 octets)

00 Pas de qualité de service

00 28 Longueur totale (ici 28 en hexadécimal vaut 2*16 en décimal soit 40 octets)

A6 F5 Id du datagramme (numéro quelconque, ne sert que si le datagramme est amené à être fragmenté)

00 00 Drapeau + déplacement (0=inutile, 0=DF (fragmentation autorisée), 0=MF (pas de fragments à suivre, donc dernier fragment) 0000000000000= déplacement soit place du 1er octet transporté, ici 1er fragment) [Il s'agit d'un datagramme non fragmenté]

1A TTL (1A = 1*16 + 10 = 26 routeurs ou secondes)

06 Protocole (ici TCP)

75 94 Bloc de contrôle d'erreur (sur l'en-tête du datagramme)

C0 5D 02 01 @IP émetteur 192.92.2.1 classe C [pas dans le même réseau]

84 E3 3D 05 @IP destinataire 132.227.61 classe B

----------contenu = segment TCP d'une longueur de 20 octets (40-20)----------

00 15 Port source, ici 21 donc serveur ftp

0F 87 Port destination 3975, port quelconque du client

9C CB 7E 01 Numéro de séquence (n° du 1er octet transporté émis (tiré au hasard))

27 E3 EA 01 Numéro de séquence (n° du 1er octet attendu en réception)

5 Longueur de l'entête du segment (20 octets): on peut donc en déduire que ce segment ne contient pas de données

012 = 0000 0001 0010 Drapeaux (ici réponse 'ok' d'ouverture de connexion)

0	0	0	0	0	0	0	1	0	0	1	0
6 bits réservés						URG (urgent)	ACK (accusé de réception)	PSH (livraison immédiate)	RST (réinitialisation de la connexion)	SYN (ouverture ou réponse d'ouverture de connexion)	FIN (clôture de la connexion)

10 00 Taille de la fenêtre, ici 4096 octets. Quantité de données que l'émetteur est autorisé à envoyer sans accusé de réception

DF 3D BCE (Bloc de contrôle d'erreur sur le segment entier)

00 00 Pointeur vers les données urgentes (inutile ici, puisqu'il n'y a pas de données urgentes bit URG=0)

----------Fin du segment TCP (sans données)----------
----------Fin des données du datagramme IP----------

20 20 20 20 20 20 6 octets de bourrage pour amener la trame Ethernet à la longueur minimale autorisée

9B 52 46 43 Bloc de contrôle d'erreur de la trame Ethernet

----------Fin de la trame Ethernet----------

Vous avez un autre exemple
http://coursjmm.perso.sfr.fr/Les_trames_reseaux.pdf