Version beta

Internet Protocol

(Pour mieux comprendre, faire une similitude avec la vie réelle. A la fin de chaque partie, pose une question de révision. Chaque personne qui achète et lit mes ouvrages, après un test et petite formation pratique, s'il a été choisi, peut obtenir un brevet. Pour des questions et critiques mettre mon E-mail).

Chaque appareil (ordinateur, téléphone, serveur etc.) connecté à internet est identifié d'une façon unique grâce à l'adresse IP.

Elle est comparée à l'adresse d'un domicile, qui est une adresse qui identifie de façon unique une résidence (maison, appartement etc.). Si une personne veut vous envoyer une lettre via la poste, elle vous parviendra précisément grâce à cette adresse.

Ou encore, si vous faites un achat en ligne, pour vous livrer le produit dans votre emplacement exact, il faut fournir votre adresse.

Cela se passe de la même manière sur Internet. L'adresse IP sert d'adresse pour la livraison de toutes les informations jusqu'à leur destination.

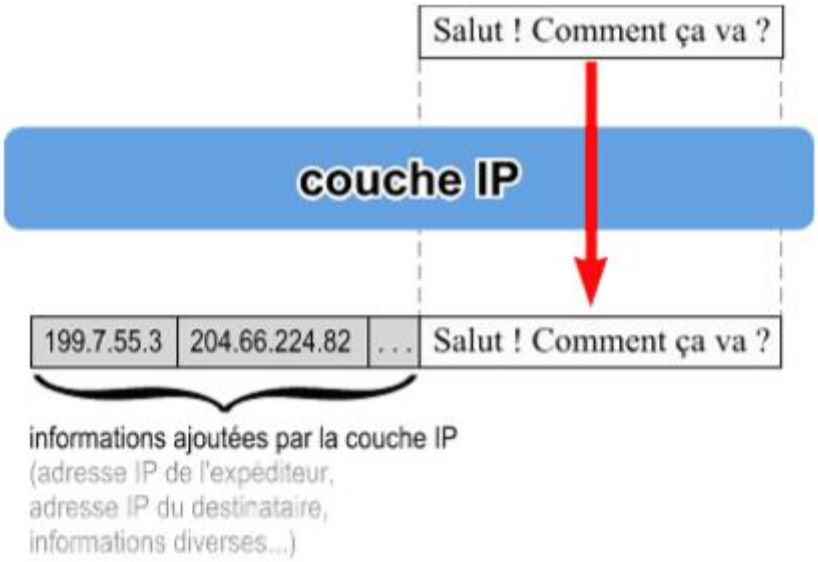
Quelles sont les règles pour envoyer une lettre par la poste ?

- Placer la lettre dans une enveloppe
- Sur le recto, il faut inscrire l'adresse du destinataire
- Au dos, il faut écrire l'adresse de l'expéditeur

Ces règles sont utilisées par tous ceux qui veillent envoyer une lettre par la poste. C'est ce qu'on appelle **un protocole**.

De même sur Internet, (si vous voulez envoyer un message, vous aurez juste à le taper via une application appropriée, puis IP mettra tous les informations nécessaires enfin qu'il arrive à destination) chaque message est enveloppé par la **couche réseau (IP)** qui y ajoute différente informations :

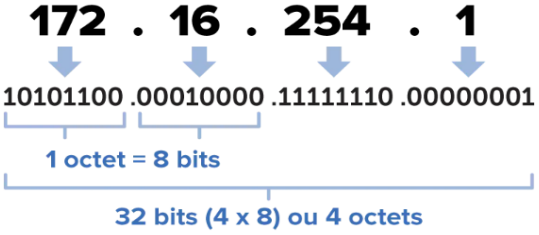
- L'adresse de l'expéditeur (la vôtre)
- L'adresse IP du destinataire
- Différentes données supplémentaires, dont nous verrons dans les lignes suivantes, qui permettent de bien contrôler l'acheminement du paquet (ou information).



Une adresse IP ou Internet Protocol adress est un numéro unique attribué à chaque appareil lorsqu'il se connecte à Internet.

Adresse IPv4 versus IPv6

Deux versions d'Internet Protocol sont actuellement utilisées : IP version 4 (IPv4) et IP version 6 (IPv6). Elles ont deux fonctions principales : l'identification et la localisation.



(Prendre plutôt une image pour IPv4 et IPv6)

La principale différence entre IPv4 et IPv6 est le nombre d'adresse possibles. IPv4 n'en permet qu'environ 4 milliards (2^{32}= 4 294 967 296), car elle utilise seulement 32 bits (4 octets × 8 bits). IPv6 a été introduite préventivement en 1995 pour garantir suffisamment d'adresses disponibles dans un futur proche. IPv6 utilise 128 bits (16 octets × 8 bits), ce qui correspond à 2^{128}= 3,4 $\times 10^{38}$ adresses possibles.

Adresses IP publique et Adresse IP privée

Adresse IP publique

Il est impossible d'aller sur internet sans adresse IP publique. Pour utiliser internet, tous les appareils connectés doivent posséder une adresse IP publique. Une adresse IP permet à deux appareils, l'envoyeur et le destinataire de la communication internet, de trouver et d'échanger des informations entre eux. Sans IP, pas de communication.

La stabilité d'internet dépend du faite que chaque adresse publique soit unique. L'organisme qui s'en occupe est appelé IANA (internet assigned numbers authority) autrefois appelé interNIC (internet network information center). Il gère l'ensemble des adresses IP publique enfin de s'assurer qu'il n'y ait pas deux adresses publiques identique. Il y a plusieurs moyens pour obtenir une adresse ou une plage d'adresse IP publique.

Parmi eux nous avons :

- Fournisseur d'Accès Internet (FAI)
  (Les entreprises et les utilisateurs internet à domicile reçoivent leurs adresses IP de leur FAI : free, orange etc.)
- ISP (internet service provider)
- LIR (local internet registry)
- RIR (regional internet registry).

Problématique des adresses IP publique

Il y a une croissance très rapide d'internet, qu'il y a un manque d'adresse IP publique. Pour remédier à ce problème, il y a des nouveaux (mécanismes) :

- NAT (Network Adress Translation)
- CIDR (classless interdoamin routing)
- VLSM (variable lenght subnet mask)
- IPv6 (Internet Protocol version 6).

Adresse IP privée

Les adresses IP privées (par **IETF** Interne Engineering Task Force) sont en interne pour l'entreprise. Tant qu'un hôte privé ne se connecte pas à internet, il peut utiliser n'importe quelle adresse IP privée si celle-ci ne pas attribuée à

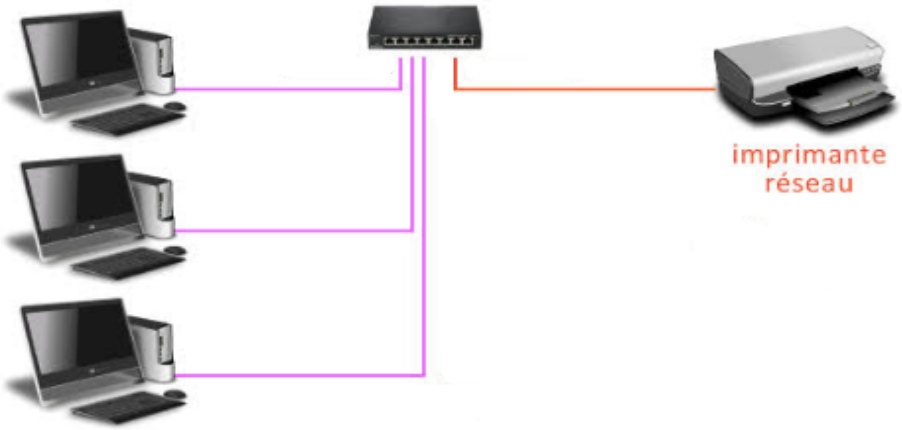
une autre machine. Les routeurs internet sont configurés pour éliminer tous les adresses privées. (**pack bon internet**), donc elles ne sont pas routable sur internet.

Alors si un réseau utilisant les adresses privées veut se connecter à Internet, il faudra faire ce qu'on appelle la translation des adresses privées en adresses publiques. Ce processus est appelé le NAT. Le périphérique réseau qui s'occupe du NAT est le routeur ou le firewall.

Adresses IP publiques versus adresse privées

Contrairement aux adresses IP publiques, les adresses IP privées sont utilisées par le réseaux privés pour identifier et partage des informations entre les ordinateurs et les appareils (comme une imprimante réseau par exemple) qui ne sont pas directement connectés à Internet.

Chaque appareil sur votre réseau à domicile a une adresse IP unique de façon à ce qu'il puisse communiquer ensemble. Cependant, en dehors de ce réseau local, personne ne peut les voir ou établir une connexion.



Votre routeur attribue une adresse IP privée à tout ce qui se passe sur votre réseau domestique via le protocole DHCP. Certaines gammes de numéro ne peuvent être utilisées que comme adresses IP privées. Comment reconnaître des adresses IP publiques et privées ?

Classe des adresses IP

Pour accueillir de réseau de différent taille, les adresses IP sont divisées en catégorie qu'on appelle '' classe ''. Les hôtes IP utilisent les adresses IP de classe A, B et C pour les communications UNICAST c'est-à-dire d'un hôte vers un seul autre hôte, et ces classes sont réservées pour utilisateurs d'Internet (entreprises, fournisseurs d'accès, etc.

Classe A

Est un bloc d'adresse conçu pour supporter des **réseaux extrêmement grands** avec 16 777 214 adresses hôtes dans le réseau.
(Image)

La plage IP va de 1.0.0.0 à 127.255.255.255

Classe B

Conçu pour répondre aux besoins de **réseaux moyens** de plus de 65 534 hôtes.
(Image)

La plage IP va de 128.0.0.0 à 191.255.255.255

Classe C

Il est plus utilisé car elle est destinée **aux petits réseaux** avec un maximum de 254 hôtes par réseaux
(Image)

De 192.0.0.0 à 223.255.255.255

(Il existe deux autres classes qui ne sont pas destiné pour des Hôtes IP.)

Classe D

Il est dédié aux applications multicast, par exemple pour le streaming.
De 224.0.0.0 à 239.255.255.255

Classe E

Est Un bloc d'adresse expérimentale
De 240.0.0.0 à 255.255.255.255

N.B : Les classes D et E sont de cas particulier, elles ne sont jamais assignées aux hôtes.

- Une adresse IP ne peut pas commencer par 0 (ex. 0.10.50.1), car la plage d'adresse valide est entre 1 à 223.

- Pour calculer les nombres de machines utilisable dans l'adresse IPv4 et IPv6, on utilise la formule 2^n, **n** qui est le nombre de bit utilisé dans chaque version (IPv4=32 bits et IPv6=128 bit).

Donc pour reconnaître les adresses IP publiques et privées :

catégorie	adresses publiques	adresses privées
classe A	De 1.0.0.0 à 129.255.255.255	De 10.0.0.0 à 10.255.255.255
classe B	De 128.0.0.0 à 191.254.255.255	De 172.16.0.0 à 172.31.255.255
classe C	De 192.0.0.0 à 223.255.255.255	De 192.168.0.0 à 192.168.255.255

L'adresse 192.65.25.428 est-il valide ? Pourquoi ?

Octet

Un octet est une séquence de huit bits. C'est donc un nombre codé avec huit bits. Ainsi, si on convertie sa valeur en décimal, on obtient un nombre qui peut varier entre 0 et 255 (en binaire 00000000 et 11111111). Donc, dans une adresse IP, on ne peut trouver qu'un nombre compris entre 0 et 255. Une adresse IP comme 192.65.25.428 ne peut pas être valide car son dernier octet n'est pas compris entre 0 et 255. Une adresse IPv4 est composée de 4 octets écrits en notation décimale, séparés par des points : 50.25.145.8. Elle peut aussi s'écrire en binaire : 00110010.00011001.10010001.00001000.

Pour apprendre la conversion facile, cliquez sur les liens ci-dessous :

Les adresses IPv4 réservées

Hormis les adresses IP privées et publiques, nous avons les adresses IP réservées c'est-à-dire qui ne peuvent pas être attribué à un hôte.

Adresse de Broadcast locale

Si un périphérique IP veut communiquer avec tous les autres du même réseau local, alors il enverra un paquet à destination de l'adresse 4 fois 255 c'est-à-dire tous les octets sont à 255 (255.255.255.255), et ce paquet sera diffusé sur l'ensemble du réseau.
Comme il s'agit d'une diffusion locale, il ne pourra pas passer un routeur. Donc le routeur supprimera le paquet. (Comment ?) Cette adresse en 4 fois 255 est aussi appelé '' Broadcast IP universel''.

Adresse de Broadcast d'un réseau

Admettons que nous avons un réseau 192.168.1.0 avec un masque en /24, c'est-à-dire en 3 fois 255.0. Avec ce masque, cela signifie que la plage IP va de 192.168.1.0 à 255
Une adresse de Broadcast est une adresse spéciale qui permet de communiquer avec tous les hôtes de ce même réseau. Ce paquet ne sera propagé que dans les machines du même sous-réseau. Elle correspond à l'adresse la plus élevée de la plage IP du réseau, c'est-à-dire celle où les bits de

la partie hôtes sont tous à 1. Par exemple, pour une adresse réseau de 192.168.1.0, celle du broadcast sera 192.168.1.255.
Dans la classe c, si l'ensemble des adresses sont utilisées, un ping de l'adresse de Broadcast recevra une réponse de 254 hôtes. Si nous utilisons un réseau de la classe A par exemple le 10.0.0.0 avec un masque par défaut en /8. L'adresse de Broadcast serait donc la 10.3 fois 255 (10.255.255.255). Si l'ensemble des adresses de cette classe sont utilisées, cela signifierait qu'un ping de l'adresse de broadcast recevrait une réponse de plus de 16 millions d'hôtes.

L'adresse de broadcast peut être acheminée via l'intranet de son entreprise et aussi sur Internet.

Adresse de loopback

Elle est utilisée pour permettre au système de pouvoir tester sa propre carte réseau (test de boucle local) et pour faire de diagnostic. La plage de cette adresse va de 127.0.0.0 à 127.255.255.255. Une interface loopback est une interface virtuelle c'est-à-dire qui n'existe pas. On l'utilise principalement sur le routeur pour jouer le rôle de la corbeille du réseau. Les paquets qui comportent des erreurs seront envoyés directement sur cette adresse de loopback qui les supprimera automatiquement quand ils atteindront leurs durées de vie.

L'adresse réseau

Par exemple l'adresse 192.168.1.0 ne peut pas être affectée ou utilisé par un hôte, car il s'agit de l'adresse du **réseau local** privée de la classe C. L'adresse de ce réseau permettra à un routeur de transmettre un paquet IP sur le réseau approprié en fonction de sa table de routage.

Route par défaut

L'adresse 4 fois 0, c'est-à-dire où tous les octets sont à 0 (0.0.0.0) est une adresse non routable utilisée pour désigner une destination invalide, inconnue ou non atteignable. Cette plage d'adresse va de 0.0.0.0 à 0.255.255.255

Liste des adresses réservées

Adresse de Broadcast locale	255.255.255.255
Adresse de Broadcast d'un réseau	De X.255.255.255 à X.X.X.255
Adresse de loopback	De 127.0.0.0 à 127.255.255.255
L'adresse réseau	De X.0.0.0 à X.X.X.0
Route par défaut	De 0.0.0.0 à 0.255.255.255

Comment savoir avec exactitude les nombres des machines (hôtes) utilisables pour une adresse IP ?

Masque de sous-réseau

Le masque de sous-réseau (désigné par *subnet mask, netmast* ou *address mask* en anglais) est une suite de 4 octets (32 bits) comme l'adresse IPv4. Chacun de ces bits peuvent prendre la valeur de 0 ou 1**. Les bits à 1 représentent la partie réseau de l'adresse, et les bits à 0 la partie machine**. Ainsi, on associe une adresse IP et un masque de sous-réseau pour savoir dans une adresse IP quelle est la partie réseau et la partie machine. Donc le masque de sous-réseau sert à séparer une adresse IP en deux parties : réseau et machine. C'est seulement grâce à lui qu'on peut déterminer avec précision le nombre des machines et des sous-réseaux d'une adresse IP, ce qui fait qu'il soit inséparable avec celle-ci. Une adresse IP seule ne voudra rien dire puisqu'on ne saura pas quelle est la partie réseau et la partie machine. De même, un masque de sous-réseau seul n'aura pas de valeur puisqu'on n'aura pas d'adresse sur laquelle l'appliquer. Voyons-le d'une manière pratique.

Chaque classe d'adresse IP a son masque de sous-réseau par défaut. Pour : 1) la classe A c'est 255.0.0.0, 2) la classe B c'est 255.255.0.0 et 3) la classe C c'est 255.255.255.0. Comme nous l'avons vu ci-haut, en convertissant ces adresses en binaire, les bits à 1 représentent la partie réseau de l'adresse, et les bits à 0 la partie machine.

(Image).

Caractéristique IP

Protocole IP (sont des règles utilisées par tout le monde p.12 réseau info livre ex enveloppe).
Il fait partie de la couche internet de TCP/IP, il est très important car il s'occupe de transport de datagramme IP (paquets de donnée), et non la livraison. Donc il permet le transfert d'un message, en le découpant en plusieurs morceaux transmis séparément.
Un paquet est inclus dans un en-tête (Header). Ce paquet comprend les informations nécessaires pour acheminer et reconstituer le message.
Chaque hôte doit avoir une adresse unique pour pouvoir communiquer dans un réseau IP.

EN-TÊTE IPv4

Avant de pouvoir envoyer un paquet IP, il faut lui ajouter un en-tête qui contiendra l'ensemble des informations nécessaire pour qu'il puisse arriver à destination.
Certain champs sont statiques (ex. version)
Certain sont modifiable tout au long du chemin (ex. TTL)

L'ensemble de champs d'un en-tête

Voici la description de chaque champ :

- **Version** : indique la version du protocole (IPv4 ou IPv6)
- **IHL** : indique la longueur de l'en-tête
- **ToS** : permet de marqué un paquet comme plus important qu'un autre.
- **TPL** : décrit la longueur du paquet. Elle comprend l'en-tête est les données qui sont dans le champ Data.
- **Fragment ID** : permet d'identifier si le paquet a été fragmenté
- **Flag** : défini divers indicateurs de contrôle qui concerne la fragmentation.
- **Fragment offset** : est aussi lié à la fragmentation. Elle définit l'endroit où la fragmentation a été faite
- **TTL (time to live)** : comprend le nombre de routeur que le paquet peut encore traversé avant d'être détruit. Ça permet d'éviter que le paquet tourne indéfiniment dans le réseau, à cause d'un problème de routage. C'est comme la date périnatale (d'expiration).
  EX : 60. Après chaque routeur -1, jusqu'à 0.
- **Protocole** : elle indique le protocole utilisé pour les données du paquet, c'est-à-dire ce qui se trouve dans le champ data
- **Checksum** : permet de contrôler l'intégrité de l'en-tête. S'il estime que le paquet a été modifié dans la route, alors il sera détruit
- **Source IP** (adresse source) : est celle de celui qui a émis le paquet.
- **Option** : comprend diverse paramètres facultative utilisé très rarement
- **Data** : correspond aux données du paquet.

Lien :