

Couche internet (protocoles IPv4 et IPv6)

IP est le protocole de base d'internet et globalement le seul protocole de la couche internet. Il a cependant deux versions majeures, la version 4 et la version 6.

IPv4 vs IPv6

La version 4 d'IP est celle qui est la plus répandue sur Internet, mais qui est toutefois limitée par le nombre d'adresses possibles, car les adresses sont codées sur 32 bits contre 128 bits pour l'IPv6.

Cela signifie que l'IPv4 à moins de cinq milliards d'adresses possibles. IPv6 a comparativement plus de 7×10^{28} fois plus d'adresses que l'IPv4.

Aujourd'hui toutes les adresses IPv4 ont été assignées, nous allons voir quels stratagèmes ont été utilisés pour faire en sorte que ce ne soit pas un trop gros problème. Mais il est bon de noter que le futur se trouve dans l'IPv6 et qu'il est donc très important de supporter l'IPv6.

CIDR vs classes

Historiquement, les adresses étaient définies suivant des "classes" allant de A à E. La classe A est équivalente à un masque `/8`, la classe B à un masque `/16`, la classe C à un masque `/24`, la classe D pour le multicast et la classe E pour une utilisation future.

Aujourd'hui, on utilise plus tôt le CIDR (Classless InterDomain Routing) qui consiste à préciser le masque avec un `/<nombre>` à la fin d'une IP (comme on a vu plus tôt). Le CIDR a l'avantage de permettre une configuration des réseaux plus précise et d'être plus simple à comprendre.

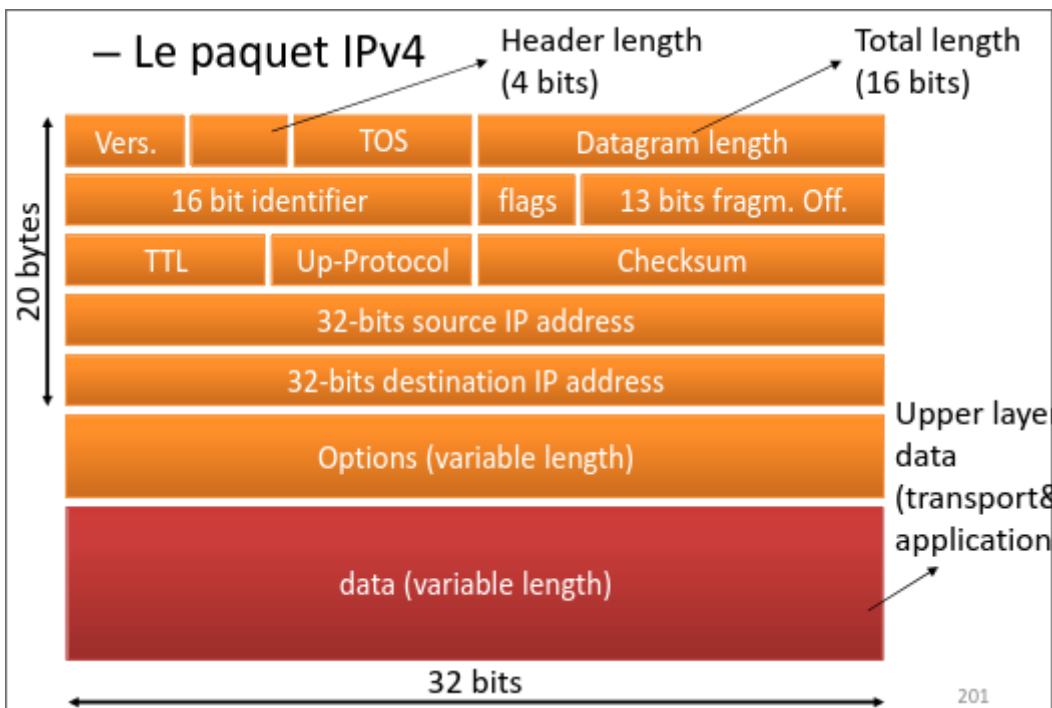
Types d'adresses

Il existe plusieurs types d'adresses :

- Adresses **publiques** qui sont celles utilisées sur Internet et sont achetées à ou allouée par l'IANA (Internet Assigned Number Authority).
- Adresse **loopback** est l'adresse désignant la machine courante, cela permet ainsi d'accéder à un serveur local. Cette adresse est `127.0.0.1` (IPv4) ou `::1` (IPv6) ou `localhost` (qui redirige vers l'adresse IPv4 ou IPv6 dans le fichier d'hôtes).
- Adresses **privées** utilisées sur des réseaux locaux (LAN), elles ne sont pas propagées sur internet et en sont complètement isolées.
- Adresse de **réseau** comme vu plus tôt (préfixe + le reste des bits à 0)
- Adresse de **broadcast** comme vu plus tôt également (préfixe + le reste des bits à 1)

Paquet IPv4

Un paquet IPv4 contient diverses informations :



- La **version** (IPv4 dans ce cas)
- La **longueur d'entête**
- Le **"type of service"** qui indique la priorité du paquet, cette valeur est généralement ignorée
- Le **datagram length** qui indique la longueur totale du paquet sur 16 bits
- L'**identifiant** du paquet
- Des **"flags"** indiquant si le paquet est fragmenté ou non
- Le **fragmentation offset** qui indique le déplacement par rapport au paquet initial
- Le **TTL** (time to live) qui est le temps de survie d'un paquet dans le réseau
- Le **UP-protocol** qui indique le destinataire des données (6 pour TCP, 17 pour UDP)
- Le **Checksum** qui permet de détecter une erreur sur l'entête du paquet, redondant par rapport à TCP

- L'**adresse IP source**
- L'**adresse IP destination**
- Les **options** à ajouter à l'information
- Les données de la couche transport

Fragmentation IPv4

Comme le MSS (Maximum Segment Size) indiquait la taille maximum d'un TPDU de la couche transport, le MTU (Maximum Transert Unit) indique la taille maximale supportée d'un paquet IP, cette taille est imposée par le réseau, donc plusieurs réseaux peuvent avoir des tailles maximales différentes.

Donc si un paquet de longueur 1500 arrive dans un réseau avec un MTU de 600, il va falloir diviser le paquet courant en autres paquets afin de pouvoir le transmettre.

Ainsi le flag permet de savoir si le paquet est fragmenté, l'identifiant permet d'identifier les paquets fragments ensemble. Le fragmentation offset donne l'ordre des fragments. Le dernier fragment a le flag à zéro ce qui indique qu'il n'y a plus de fragments qui suivent.

Eviter les boucles

Pour éviter que des paquets ne bouclent dans le réseau, on utilise la valeur TTL qui indique le temps de vie du paquet en routeur parcouru. Ainsi, la valeur est décrémentée par chaque routeur et si un paquet arrive avec un TTL de un ou inférieur, le paquet est jeté.

ICMPv4

ICMP (Internet Control Message Protocol) permet de "diagnostiquer" certains problèmes réseau via PING et TRACEROUTE.

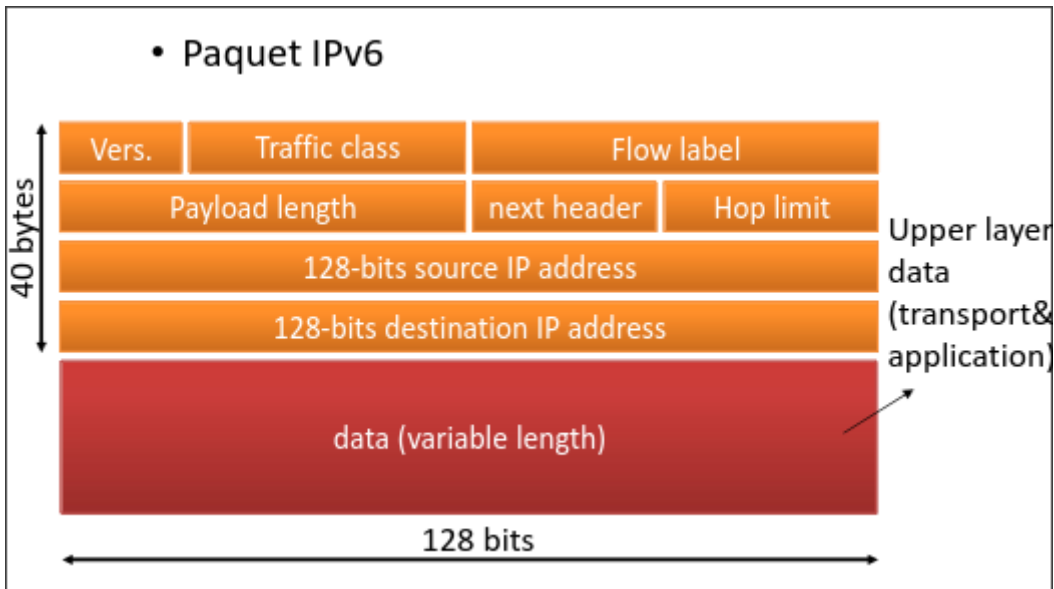
Ping permet de savoir si une machine est capable de recevoir ou répondre au niveau IP, très utile pour vérifier les connexions réseaux, mais souvent limité par les firewalls pour empêcher de pouvoir "tester" les machines du réseau.

Traceroute permet de déterminer le chemin d'une source vers une destination. Cela envoie des paquets IP avec un TTL croissant en partant de 1, qui va donc être rejeté par le routeur qui va ainsi renvoyer un message ICMP `time-exceeded` avec un identifiant du routeur, ce qui permet ainsi de connaître tous les intermédiaires.

Il est parfois même possible, en utilisant certains sites internet, de retrouver les localisations des routeurs par lequel la requête est passée.

Paquet IPv6

IPv6 comme dit précédemment a pour but d'augmenter le nombre d'adresses disponible, améliorer les performances, intégrer de la sécurité, supporter les nouvelles applications en temps réel, facilité la configuration.



Un paquet IPv6 est composé de :

- La **version** (ici IPv6)
- Le **Traffic Class** permettant de marquer les paquets pour obtenir une *qualité de service* particulière
- **Flow label** permettant d'étiqueter un paquet afin de grouper des paquets faisant partie d'un "flow" commun tel qu'un live vidéo par exemple
- Le **payload length** indiquant la taille des données
- Le **next header** qui mentionne une option à traiter ou pour indiquer la couche supérieure à recevoir des données (UDP ou TCP)
- Le **hop limit** qui indique le total de routeurs que le paquet peut traverser, lorsque cette valeur arrive à 0 le paquet est jeté. Similaire au TTL en IPv4
- L'**adresse IP source**
- L'**adresse IP destination**
- Les données de la couche de transport

Différence avec l'IPv4

Il y a donc certaines différences entre les paquets IPv6 et les paquets IPv4 :

- Le checksum n'existe plus, car redondant par rapport à la couche de transport ou d'accès réseau. Cela permet d'améliorer les performances, parce que les routeurs n'ont plus

besoin de vérifier cette valeur

- Disparition des options de taille variable, ces derniers peuvent être placés dans un entête particulière
- Disparition de la fragmentation au niveau des routeurs, IPv6 oblige un MTU de 1280 octets, les paquets peuvent donc être fragmentés. Cela est un grand avantage pour les routeurs qui n'ont plus besoin de fragmenter les paquets, c'est ainsi un gain de performance.

Types d'adresses IPv6

- Adresses **locale-lien** est attachée à l'interface et a une portée limitée au LAN, et ne traverse pas les routeurs. Ce sont des adresses de type `FE80::/10`
- Adresses **locale-unique** sont des adresses attachées à une interface qui peuvent traverser des routeurs mais non utilisable sur internet. Elles sont de type `FC00::/7`
- Adresses **globale-unique** sont des adresses globales, uniques sur Internet et attribuée par le service d'accès Internet. Elles sont de type `2000::/3`
- Adresses **multicast** désignant un groupe de receveurs. Elles sont de type `FF00::/8`
- Adresses **anycast** permettant d'interagir avec n'importe quelle adresse d'un groupe donné (le plus proche selon la politique de routage)

En IPv6, une machine a donc plusieurs adresses, par exemple une adresse globale-unique, une adresse locale-lien et une adresse IPv4 globale.

ICMPv6

ICMPv6 est une évolution d'ICMP pour l'IPv6. Ce protocole permet plusieurs choses :

- Elle permet une gestion des groupes multicast (IGMP en IPv4),
- Retrouver une adresse physique (MAC) en fonction d'une IP (ARP en IPv4),
- Neighbor discovery qui permet de déterminer les adresses local-lien des voisins, routeurs, etc afin de savoir si un voisin est accessible ou non

Elle permet aussi la signalisation des erreurs (destination unreachable, packet too big, time exceeded, parameter problem) ou d'autres messages d'information (ping, gestion de groupes multicast, neighbor discovery).

Neighbor Discovery Protocol (ND)

Le ND est un protocole utilisé pour découvrir les voisins et réaliser de l'auto-configuration des interfaces réseaux (construire l'adresse locale-lien de façon à ce qu'elle soit unique sur le LAN).

Contrairement à DHCP (Dynamic Host Configuration Protocol), qui sert aussi à configurer les hôtes, les adresses ne sont pas distribuées, mais construites. Il est cependant aussi possible de distribuer des adresses en IPv6 en utilisant DHCPv6.

ND prévoit 5 types de messages :

- Sollicitation de routeur, vérification d'un routeur
- Réponse de routeur, un routeur annonce sa présence
- Sollicitation de voisin, vérification d'un voisin
- Réponse de voisin, un voisin indique sa présence
- Redirection, redirige vers un autre routeur

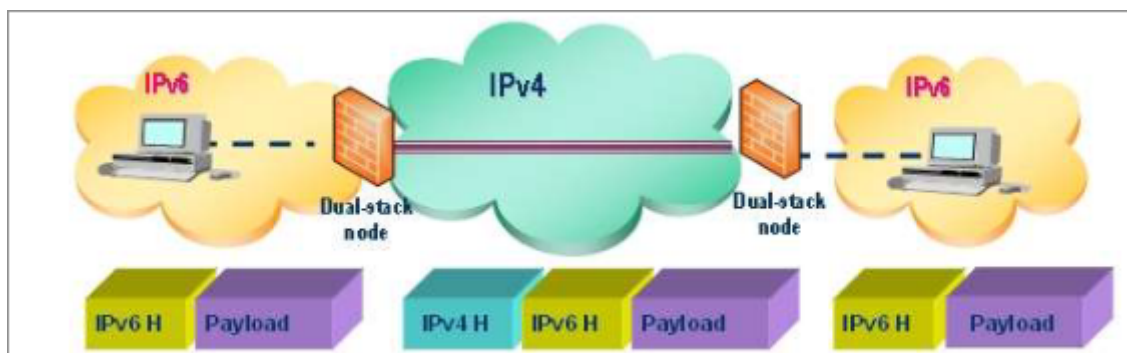
Neighbor solicitation/advertisement permet d'obtenir l'adresse physique (MAC) d'un voisin et de vérifier s'il est accessible.

Transition vers IPv6

La transition vers la version 6 du protocole IP doit être progressive, car il est impossible d'imposer un changement brutal sur plusieurs milliards d'appareils d'un coup. De plus, les coûts pour la transition peuvent être importants parce qu'il faut un logiciel et/ou matériel adapté.

Il existe plusieurs dispositifs pour faire une transition vers l'IPv6 graduelle

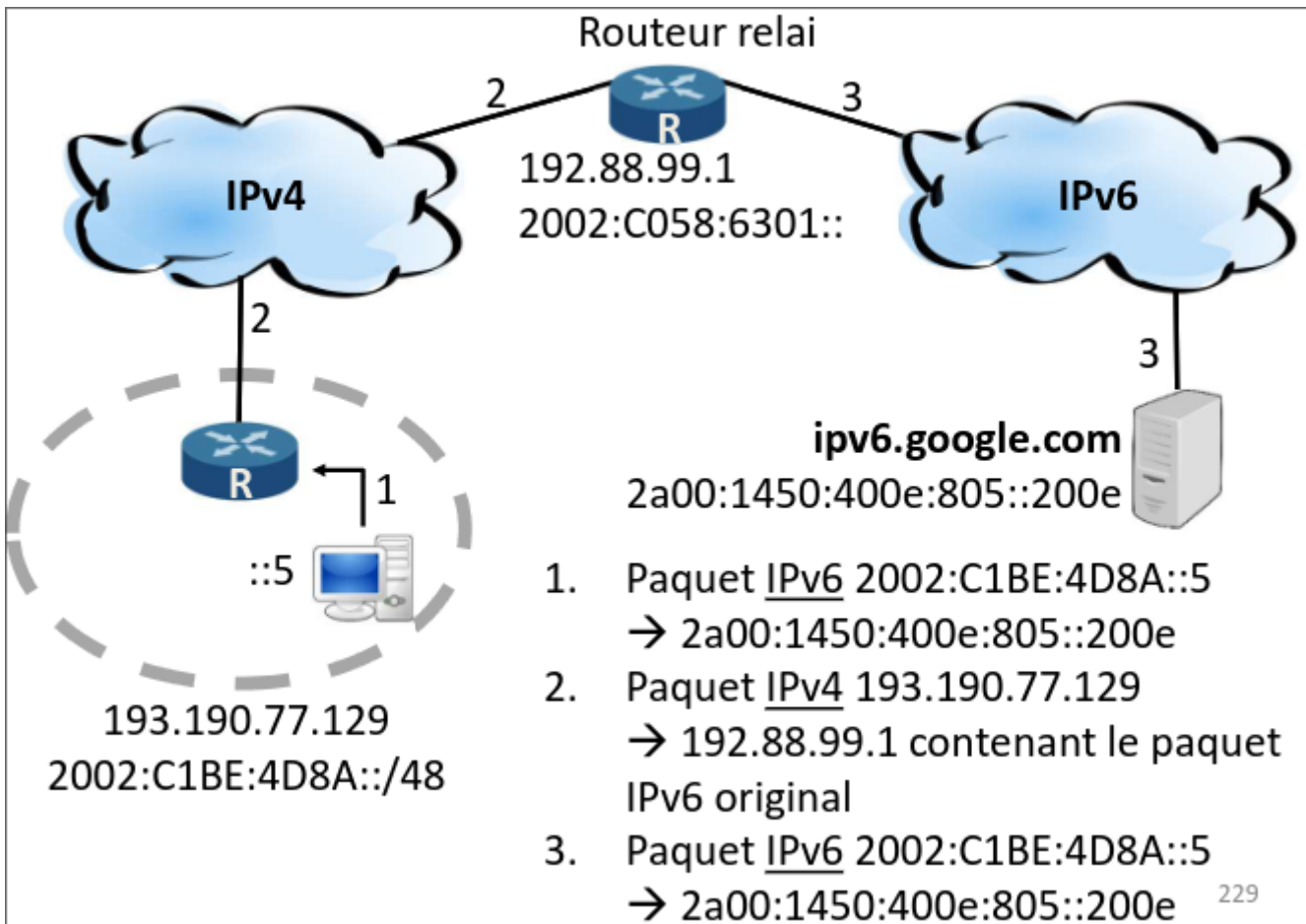
Tunnel-brokers



L'idée ici est de créer un tunnel entre le réseau du client et du fournisseur de service IPv6 (par exemple un site internet). Cela consiste à mettre des paquets IPv6 dans des paquets IPv4.

Un client va donc s'abonner aux services d'un tunnel-broker (par exemple Sixxs), et va envoyer ses paquets IPv6 dans des paquets IPv4 à ce tunnel-broker. Ce dernier va ensuite récupérer les paquets IPv4 pour les envoyer dans le réseau IPv6.

6to4



Une autre idée est d'utiliser des "tunnels automatiques" tel que des routeurs 6to4 qui vont faire le pont entre l'Internet IPv6 et l'Internet IPv4.

Ainsi les paquets IPv6 vont être encapsulés dans des paquets IPv4 et envoyé au routeur relais le plus proche. Ce dernier va ensuite envoyer le paquet IPv6 dans le réseau IPv6 et faire la même chose dans le sens inverse.

Tous les routeurs relais sont identifiés par l'adresse Anycast `192.88.99.1`. Ici le tunnel se fait automatiquement, il n'y a donc pas besoin de s'abonner à un service particulier par exemple.

L'IPv6 d'origine renseignée dans le paquet IPv6 commence toujours par `2002:` pour l'IPv6 et est suivi de l'adresse IPv4 publique. Cela permet ainsi, en utilisant une adresse IPv4 publique, de créer une adresse IPv6 unique.

Le 6to4 a cependant quelques problèmes, par exemple, il est assez difficile de dimensionner les routeurs 6to4 et il est difficile d'assurer une bonne connectivité. Surtout que si un ISP crée un routeur 6to4, il sera également obligé de gérer les clients d'autres ISPs.

Déploiement dual-stack

Le déploiement dual-stack est la méthode de transition la plus "pure" vers l'IPv6 puis ce qu'elle consiste en un fournisseur d'accès Internet qui transforme son infrastructure de manière à supporter nativement à la fois IPv4 et IPv6 (d'où le nom "dual-stack").

Ainsi, le réseau du client, ainsi que le réseau de l'ISP supporte tous les deux l'IPv6 et l'IPv4.

Le problème avec le dual-stack c'est que cela demande souvent une refonte importante de tout le réseau, ce qui n'est parfois pas possible.

6rd

6 Rapid Deployment est une technologie développée par Free. Elle consiste à implémenter une sorte de 6to4 à l'intérieur du réseau de l'ISP.

Ainsi les clients ont des routeurs 6rd qui vont placer les paquets IPv6 dans des paquets IPv4 et va l'envoyer à un routeur 6rd qui va ensuite propager les paquets IPv6 sur le réseau IPv6.

Les machines sont identifiées par des adresses IPv6 locale au réseau de l'ISP, il n'y a donc pas besoin de préfixe comme ce serait le cas pour 6to4 et il n'est ainsi pas nécessaire de modifier tout le réseau existant.

Le 6rd a permis à Free de déployer l'IPv6 à 1.5 million de clients en seulement 5 semaines.

Pallier les problèmes de l'IPv4 en attendant l'IPv6

En attendant que l'IPv6 soit vraiment répandue, il est possible de tout de même palier aux limites d'adressage de l'IPv4.

L'utilisation du CIDR permet par exemple d'affiner les espaces IP adressés et ainsi éviter d'assigner trop d'adresses à une entité.

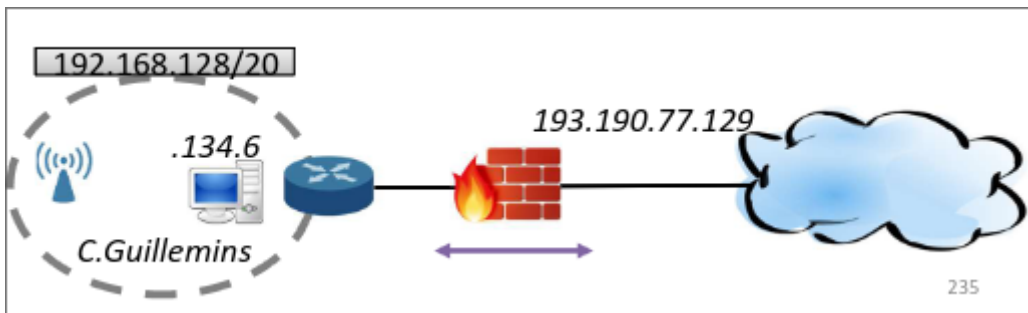
Le **NAT** (Network Address Translator) permet de partager une adresse IP publique entre plusieurs centaines de machines. C'est ce qui est généralement utilisé pour tous les réseaux domestiques.

Le DHCP (Dynamic Host Configuration Protocol) permet de distribuer les adresses au moment de la connexion et ainsi d'en avoir moins pour un certain groupe d'utilisateur.

Fonctionnement du NAT

Le NAT fonctionne en modifiant le port et l'IP source des paquets. Ainsi, lorsqu'un paquet veut sortir du réseau local, le NAT va remplacer l'IP locale par l'IP publique, et le port source par un autre. Quand la réponse du serveur arrive, le NAT va regarder quel IP locale et quel port source correspond au port source transformé, va de nouveau modifier le paquet et l'envoyer à la bonne machine du réseau.

Le routeur peut également parfois faire office de firewall.



Revision #2

Created 2 March 2024 17:55:25 by SnowCode

Updated 3 March 2024 12:45:30 by SnowCode