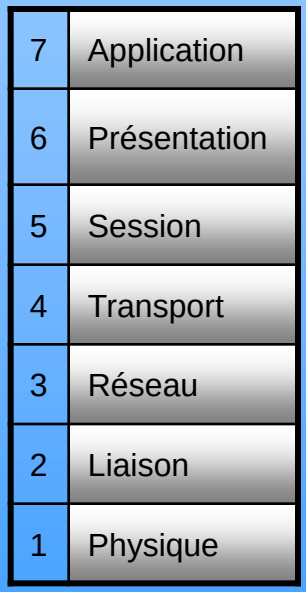
IPv6 : Internet Protocol version 6

Historique

- IPv6 est un protocole réseau sans connexion de la **couche 3** du modèle OSI
- IPv6 est l'aboutissement des travaux menés au sein de l'IETF au cours des années 1990 pour **succéder à IPv4** et ses spécifications ont été finalisées en décembre 1998
- Grâce à **des adresses de 128 bits** au lieu de 32 bits, IPv6 dispose d'un **espace d'adressage bien plus important qu'IPv4**. Cette quantité d'adresses considérable permet une **plus grande flexibilité** dans l'assignation des adresses et une meilleure agrégation des routes dans la table de routage d'Internet.
- La traduction d'adresse, qui a été rendue populaire par le manque d'adresses IPv4, n'est plus nécessaire !



Raisons du développement d'un nouveau protocole IP

- Le protocole IPv4 permet d'utiliser un peu plus de quatre milliards d'adresses différentes pour connecter les ordinateurs et les autres appareils reliés au réseau
- Une partie des quatre milliards d'adresses IP théoriquement disponibles ne sont pas utilisables pour numéroter des machines, soit parce qu'elles sont destinées à des usages particuliers (par exemple, le multicast ou les réseaux privés), soit parce qu'elles ont été attribuées de façon inefficace
- Au début des années 1990, devant l'épuisement de l'espace d'adressage, notamment des réseaux de classe B, les registres Internet régionaux font leur apparition et le découpage des adresses en classe est aboli au profit du plus flexible CIDR. L'attribution des adresses est rendue plus efficace et tient compte des besoins réels, tout en permettant un certain niveau d'agrégation, nécessaire au bon fonctionnement du routage sur Internet, ces deux principes étant antagonistes.
- La demande croissante en adresses pour les nouvelles applications, les équipements mobiles et les équipements connectés en permanence conduisent à l'utilisation de plus en plus fréquente des adresses privées, de la traduction d'adresse réseau (NAT) et à l'attribution dynamique des adresses.
- En dépit de ces efforts, **l'épuisement des adresses IPv4 publiques est inévitable**. C'est la raison principale du développement d'un nouveau protocole Internet mené au sein de l'Internet Engineering Task Force (IETF) dans les années 1990.

Généralités

- IPv6 dispose de mécanismes d'assignation automatique des adresses et facilite la renumérotation. **La taille du sous-réseau**, variable en IPv4, **a été fixée à 64 bits en IPv6**. Les mécanismes de sécurité comme IPsec font partie des spécifications de base du protocole. L'en-tête du paquet IPv6 a été simplifiée et des types d'adresses locales facilitent l'interconnexion de réseaux privés.
- Le déploiement d'IPv6 sur Internet est compliqué en raison de l'incompatibilité des adresses IPv4 et IPv6. Les traducteurs d'adresses automatiques se heurtent à des problèmes pratiques importants. Pendant une phase de transition où coexistent IPv6 et IPv4, les hôtes disposent d'une double pile, c'est-à-dire qu'ils disposent à la fois d'adresses IPv6 et IPv4, et des tunnels permettent de traverser les groupes de routeurs qui ne prennent pas encore en charge IPv6.
- En 2010, le déploiement d'IPv6 est encore limité, la proportion d'utilisateurs Internet en IPv6 étant estimé entre 0,25 et 1 %2,3, et ce en dépit d'appels pressants à accélérer la migration adressés aux fournisseurs d'accès à Internet et aux fournisseurs de contenu de la part des registres Internet régionaux et de l'ICANN, l'épuisement des adresses IPv4 publiques disponibles étant imminent.
- Pourquoi IPv6 ne s'appelle-t-il pas IPv5 ?La version 5 d'IP était une version d'expérimentation du protocole Internet Stream Protocol, qui n'a jamais été massivement déployé.

Fonctionnement IPv6

- Le fonctionnement d'IPv6 est très similaire à celui d'IPv4. Les protocoles TCP et UDP sont pratiquement inchangés. Ceci est résumé par la formule « 96 bits de plus, rien de magique »
- Une adresse IPv6 est longue de 128 bits, soit 16 octets, contre 32 bits pour IPv4. La notation décimale pointée employée pour les adresses IPv4 (par exemple 172.31.128.1) est abandonnée au profit d'une écriture hexadécimale, où les 8 groupes de 2 octets (16 bits par groupe) sont séparés par un signe deux-points :
  - *2001:0db8:0000:85a3**:0000:0000:**ac1f:8001*
- On peut omettre les zéros à gauche dans chaque groupe, et remplacer une seule séquence de zéros par un signe « :: ». L'adresse peut être abrégée en :
  - *2001:db8:0:85a3**::**ac1f:8001*

Adresses Globales unicast : Découpage géographique grâce aux préfixes

- Chacun des fournisseurs dispose d'une fraction réservée de l'espace d'adressage (adresses unicast = 1/8 de cet espace). Les 5 premiers bits qui suivent le préfixe 0010 (2000::/3) sont utilisés pour indiquer dans quel " registre " se trouve le fournisseur d'accès. Actuellement, trois registres sont opérationnels, pour l'Amérique du nord, l'Europe et l'Asie. Jusqu'à 29 nouveaux registres pourront être ajoutés ultérieurement.
- Chaque registre est libre de diviser les 15 octets restants comme il l'entend. Une autre possibilité est d'utiliser un octet pour indiquer la nationalité du fournisseur et de laisser toute liberté aux octets suivant pour définir une structure d'adresses spécifique.
- Le modèle géographique est le même que celui du réseau Internet actuel, dans lequel les fournisseurs d'accès ne jouent pas un grand rôle. Dans ce cadre, IPv6 peut gérer 2 types d'adresses.

Préfixe IPv6

- Les réseaux sont notés en utilisant la notation CIDR : la première adresse du réseau est suivie par une barre oblique et un nombre qui indique la taille en bits du réseau. La partie commune des adresses est appelée préfixe. Par exemple :
  - Le préfixe *2001:db8:85a3::/48* représente l'ensemble des adresses qui commence à *2001:db8:85a3:0:0:0:0:0* et finit à *2001:db8:85a3:ffff:ffff:ffff:ffff:ffff*.
  - Le préfixe *fc00::/7* représente les adresses de *fc00:0:0:0:0:0:0:0* à *fdff:ffff:ffff:ffff:ffff:ffff:ffff:ffff*

Adressage IPv6

Certains préfixes d'adresses IPv6 jouent des rôles particuliers :

Type d'adresses IPv6	
Préfixe	**Description**
::/8	Adresses réservées
2000::/3	Adresses unicast routables sur Internet
fc00::/7	Adresses locales uniques
fe80::/10	Adresses locales lien
ff00::/8	Adresses multicast

Les adresses unicast Locales (ULA)

- Les adresses unicast Locales (ULA) utilisent le préfixe FC00::/7, elles sont destinées à l'équivalent des adresses ip privées IPV4.
  Elles peuvent être réutilisées par d'autres organisations sans qu'il y ait de conflit. Elles ne peuvent pas être propagées hors des limites des organisations, ce qui les rend bien adaptées à celles qui utilisent des gardes-barrières pour protéger leur réseau privé du réseau Internet.
  Si elles sont correctement générées (tirage aléatoire des 40 bits suivant le préfixe FD00::/8) elles permettront d'interconnecter des réseaux par vpn avec moins d'une chance sur mille milliards de conflit .

- Les adresses de liens locaux (préfixe FE80::/10) n'ont qu'une spécification locale sur l'interface.

- Toutes ces adresses , si elles utilisent la procédure de création automatique ont généralement 8 octets qui représentent le réseau et 8 octets représentant l'interface sur ce réseau .

Adresse multicast

- Préfixe FF00::/8Les adresses de diffusion multidestinataire disposent d'un champ Drapeau (4 bits) et d'un champEnvergure (4 bits) à la suite du préfixe, puis d'un champ Identificateur de groupe (112 bits). L'un des bits du drapeau distingue les groupes permanents des groupes transitoires.

- Le champ Envergure permet une diffusion limitée sur une zone

Adresse anycast

- En plus de supporter l'adressage point à point classique (unicast) et l'adressage de diffusion multidestinataire (multicast) IPv6 supporte un nouveau type d'adressage de diffusion au premier vu (anycast).

- Cette technique est similaire à la diffusion multidestinataire dans le sens ou l'adresse de destination est un groupe d'adresses, mais plutôt que d'essayer de livrer le datagramme à tous les membres du groupe, il essai de le livrer à un seul membre du groupe, celui le plus proche ou le plus à même de le recevoir.

Adressage IPv6

- Parmi les adresses réservées :
  - ::/128 est l'adresse non spécifiée. On peut la trouver comme adresse source dans une phase d'acquisition de l'adresse réseau.
  - ::1/128 est l'adresse localhost, semblable à 127.0.0.1 en IPv4
- Parmi les adresses de 2000::/3 sont distinguées :
  - Les adresses permanentes (2001::/16) ouvertes à la réservation depuis 1999 ;
    - 2001::/32 est utilisé pour Teredo ;
    - 2001:db8::/32 est réservé pour la documentation par la RFC 3849 ;
  - Les adresses 6to4 (2002::/16) permettant d'acheminer le trafic IPv6 via un ou plusieurs réseaux IPv4 ;
  - Toutes les autres adresses routables (plus des trois quarts) sont actuellement réservées pour usage ultérieur.

Adressage IPv6

- **Scope :**
  - Le *scope* d'une adresse IPv6 consiste en son domaine de validité et d'unicité.
  - On distingue :
  - Les adresses unicast :
    - l'adresse *loopback* ::1/128 a une validité limitée à l'hôte,
    - les adresses link-local, uniques sur un lien donné,
    - les autres adresses, y compris les adresses locales uniques, ont un scope *global*, c'est-à-dire qu'elles sont uniques dans le monde et peuvent être utilisées pour communiquer avec d'autres adresses globalement uniques, ou des adresses link-local sur des liens directement connectés,
  - Les adresses anycast, dont le scope est identique aux adresses unicast,
  - Les adresses multicast ff00::/8, pour lesquels les bits 13 à 16 déterminent le scope : local, lien, organisation ou global.
  - Toutes les interfaces où IPv6 est actif ont au moins une adresse de scope link-local (fe80::/10).

Adressage IPv6

- Exemple adresse IPv6 globale unicast :
  - Free : 2a01::/3
  - Orange : 2001::/3

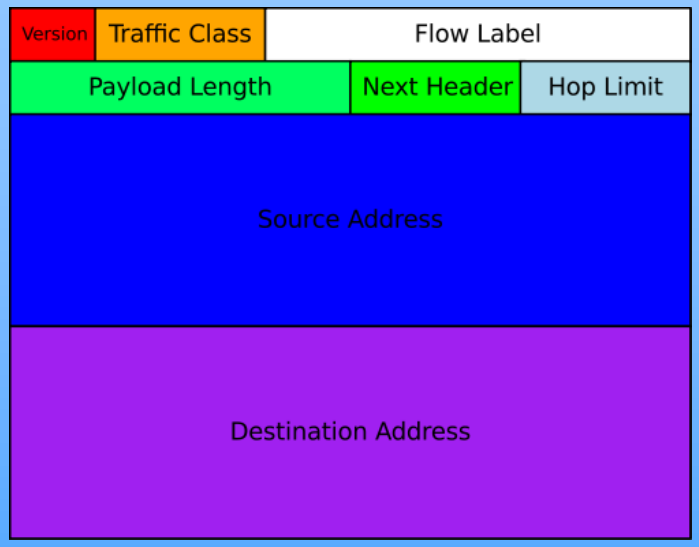
Les principales améliorations d’IPv6

- Les spécifications principales d'IPv6 sont publiées en 1995 par l'IETF. Parmi les nouveautés, on peut citer :
  - l'augmentation de 232 (soit environ 4×109) à 2128 (soit environ 3,4×1038) du nombre d'adresses disponibles, soit 667 millions de milliards d'adresses IP disponibles par mm^2 de la surface de la Terre ;
  - des mécanismes de configuration et de renumérotation automatique ;
  - IPsec, QoS et le multicast font partie de la spécification d'IPv6, au lieu d'être des ajouts ultérieurs comme en IPv4 ;
  - la simplification des en-têtes de paquets, qui facilite notamment le routage.

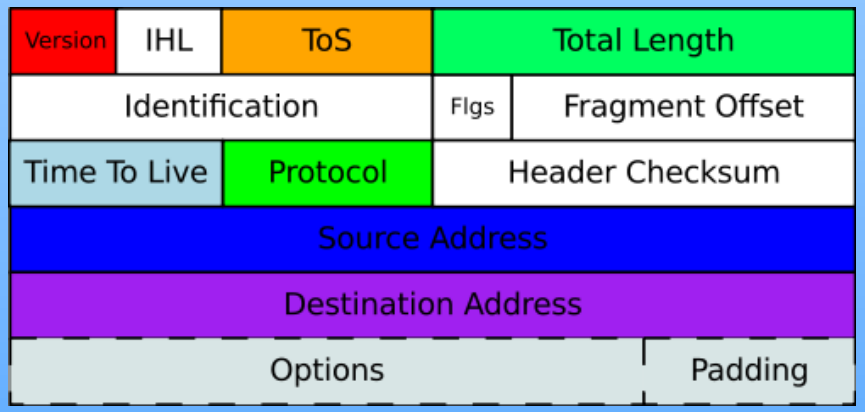
En-tête IPv6

- L'en-tête du paquet IPv6 est de taille fixe à 40 octets, tandis qu'en IPv4 la taille minimale est de 20 octets, des options pouvant la porter jusqu'à 60 octets, ces options demeurant rares en pratique.

En-tête IPv6



En-tête IPv6



En-tête IPv4

En-tête IPv6

- La signification des champs est la suivante :
  - Version (4 bits) : fixé à la valeur du numéro de protocole internet, 6
  - Traffic Class (8 bits) : utilisé dans la qualité de service
  - Flow Label (20 bits) : permet le marquage d'un flux pour un traitement différencié dans le réseau.
  - Payload length (16 bits) : taille de la charge utile en octets.
  - Next Header (8 bits) : identifie le type de header qui suit immédiatement selon la même convention qu'IPv4.
  - Hop Limit (8 bits) : décrémenté de 1 par chaque routeur, le paquet est détruit si ce champ atteint 0 en transit.
  - Source Address (128 bits) : adresse source
  - Destination Address (128 bits) : adresse destination.

Comparaison avec IPv4

- la taille de l'en-tête est fixe, le champ IHL (IP Header Length) est donc inutile,
- il n'y a pas de somme de contrôle sur l'en-tête. En IPv4, cette somme de contrôle inclut le champ TTL et oblige les routeurs à le recalculer dans la mesure ou le TTL est décrémenté. Ceci simplifie le traitement des paquets par les routeurs.
- les éventuelles informations relatives à la fragmentation sont repoussées dans un en-tête qui suit.
- le champ Time to Live est renommé en Hop Limit, reflétant la pratique

Teredo (protocole)

- Le protocole Teredo, « Tunneling IPv6 over UDP through NAT », définit une méthode permettant d'accéder à l'Internet IPv6 derrière un équipement réalisant du NAT. Il fait partie des mécanismes de transition d'IPv4 vers IPv6 et consiste à encapsuler les paquets IPv6 dans des datagrammes UDP sur IPv4 entre le client et le relais Teredo, avec l'aide d'un serveur Teredo.

Teredo : But

- 6to4, le protocole d'encapsulation IPv6 sur IPv4 le plus courant, nécessite que le matériel au bout du tunnel d'encapsulation ait une adresse IPv4 publique. Pourtant actuellement et pour combler l'épuisement des adresses IPv4, la plupart de ses hôtes sont reliés au réseau IPv4 par un périphérique faisant du NAT. Ainsi, l'adresse publique est assignée à ce périphérique NAT et c'est donc lui qui doit implémenter le protocole 6to4. Malheureusement, une grande partie de ces équipements ne peuvent pas être mis à jour pour fournir le support de 6to4 pour des raisons techniques ou économiques.
- Teredo permet de résoudre ce problème en encapsulant les paquets IPv6 dans des datagrammes UDP/IPv4, que la plupart des NAT peuvent transmettre correctement. Ainsi, les hôtes IPv6 derrière des NAT peuvent être utilisés comme points de terminaison du tunnel Teredo, même quand ils n'ont pas une adresse IPv4 publique dédiée. En effet, un hôte implémentant le protocole Teredo peut acquérir une connectivité IPv6 sans la coopération de l'environnement du reste du réseau local.
- Teredo est destiné à être une mesure temporaire : à long terme, tous les hôtes IPv6 devraient utiliser la connectivité IPv6 native. Le protocole Teredo comprend des dispositions pour une procédure en coucher de soleil: les implémentations de Teredo doivent fournir un moyen de pouvoir arrêter d'utiliser la connectivité Teredo lorsque IPv6 sera disponible et permettra une connectivité moins compliquée.

ICMPv6 : Internet Control Message Protocol V6

- L’ICMP pour IPv6 (Internet Control Message Protocol Version 6) fait partie à part entière de l'architecture IPv6 et doit être complètement supportée par toutes les implémentations d'IPv6. ICMPv6 combine des fonctions antérieurement subdivisées à travers différents protocoles, tels qu’ICMPv4 (Internet Control Message Protocol version 4), IGMP (Internet Group Membership Protocol), et ARP (Address Resolution Protocol), et il introduit quelques simplifications en éliminant des types de messages obsolètes qui ne sont plus utilisés.

ICMPv6 : Internet Control Message Protocol V6

- L’ICMP pour IPv6 (Internet Control Message Protocol Version 6) fait partie à part entière de l'architecture IPv6 et doit être complètement supportée par toutes les implémentations d'IPv6. ICMPv6 combine des fonctions antérieurement subdivisées à travers différents protocoles, tels qu’ICMPv4 (Internet Control Message Protocol version 4), IGMP (Internet Group Membership Protocol), et ARP (Address Resolution Protocol), et il introduit quelques simplifications en éliminant des types de messages obsolètes qui ne sont plus utilisés.

ICMPv6 : Internet Control Message Protocol V6

- L'Internet Protocol, version 6 (IPv6) est une nouvelle version d'IP. IPv6 utilise le protocole ICMP comme défini pour IPv41, avec quelques changements. Le protocole résultant est appelé ICMPv6. Cet article décrit le format d'un ensemble de messages de contrôle utilisés par ICMPv6.
- ICMPv6 est un protocole générique ; par exemple, il est utilisé pour rapporter des erreurs trouvées dans le traitement de paquets, effectuer des diagnostics, effectuer une découverte de voisinage, et rapporter l'appartenance à un multicast. Pour cette raison, les messages ICMPv6 sont catégorisés en deux classes : error messages et information messages. Les datagrammes ICMP sont transportés à l'intérieur de datagrammes IPv6 dans lequel un en-tête d'extension peut aussi être présent. Un message ICMP est identifié par sa valeur 58 positionnée dans le champ Next Header de l'en-tête IPv6.

Traceroute v6

- Protocole analogue à tracert pour IPv4.
- Commande : traceroute6 URL
- Répertoire des routeurs traversés pour atteindre l’URL de destination

DHCPv6

- Fourni une adresse IPv6 unicast lien local à un client. Protocole basé sur UDP.

Fragmentation et option jumbo

- En IPv4, les routeurs qui doivent transmettre un paquet dont la taille dépasse le MTU du lien de destination ont la tâche de le fragmenter, c'est-à-dire de le segmenter en plusieurs paquets IP plus petits. Cette opération complexe est coûteuse en termes de CPU pour le routeur ainsi que pour le système de destination et nuit à la performance des transferts, d'autre part les paquets fragmentés sont plus sensibles aux pertes : si un seul des fragments est perdu, l'ensemble du paquet initial doit être retransmis.
- En IPv6, les routeurs intermédiaires ne fragmentent plus les paquets et renvoient un paquet ICMPv6 Packet Too Big en lieu et place, c'est alors la machine émettrice qui est responsable de fragmenter le paquet. L'utilisation du Path MTU discovery est cependant recommandé pour éviter toute fragmentation.
- Ce changement permet de simplifier la tâche des routeurs, leur demandant moins de puissance de traitement.

Fragmentation et option jumbo

- La MTU minimale autorisée pour les liens a également été portée à 1 280 octets (contre 68 pour l'IPv414). Si des liens ne peuvent pas soutenir ce MTU minimal, il doit exister une couche de convergence chargée de fragmenter et de réassembler les paquets.
- Comme pour IPv4, la taille maximale d'un paquet IPv6 hors en-tête est de 65535 octets. IPv6 dispose cependant d'une option jumbo permettant de porter la taille maximale d'un paquet à 4 Go et profiter ainsi des réseaux avec un MTU plus élevé.

Neighbor Discovery Protocol

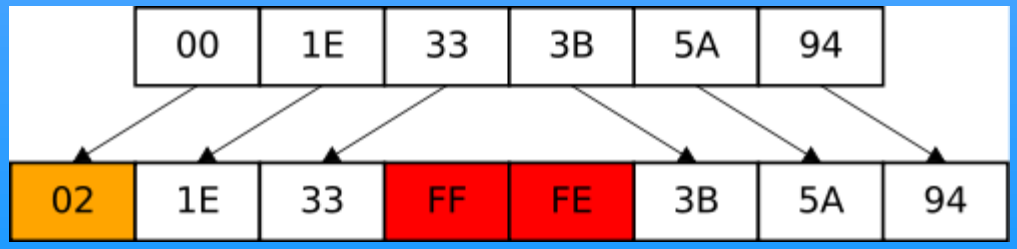
- Le Neighbor Discovery Protocol associe les adresses IPv6 a des adresses MAC sur un segment comme ARP pour IPv4. Il permet également de découvrir les routeurs et les préfixes routés, le MTU, de détecter les adresses dupliquées, les hôtes devenus inaccessibles et l'autoconfiguration des adresses et éventuellement les adresses des serveurs DNS récursifs. Il est basé sur ICMPv6.

Assignation des adresses IPv6

Dans un sous-réseau, il existe plusieurs méthodes d'assignation des adresses :

- Configuration manuelle
  - l'administrateur fixe l'adresse. Les adresses constituées entièrement de 0 ou de 1 ne jouent pas de rôle particulier en IPv6.
- Configuration automatique
  - autoconfiguration sans état (Stateless Address Autoconfiguration, SLAAC) basée sur l'adresse MAC qui utilise le Neighbor Discovery Protocol (NDP).
  - autoconfiguration avec tirage pseudo aléatoire.
  - assignation par un serveur DHCPv6.

L'utilisation de l'adresse MAC d'une carte réseau pour construire une adresse IPv6 a suscité des inquiétudes quant à la protection des données personnelles16 dans la mesure où l'adresse MAC permet d'identifier de façon unique le matériel. Pour pallier cet inconvénient, il est possible d'utiliser des adresses temporaires générées de façon pseudo-aléatoire et modifiées régulièrement ou bien d'utiliser un service d'attribution automatique des adresses IPv6 par un serveur, de façon similaire à ce qui existe pour IPv4, avec DHCPv6.



Construction d'une adresse d'interface EUI-64 modifiée à partir d'une adresse MAC.