IPv6

IPv6 (*Internet Protocol version 6*) est un protocole réseau sans connexion de la couche 3 du modèle OSI (Open Systems Interconnection).

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 dans la RFC 2460[1] en décembre 1998. IPv6 a été standardisé dans la RFC 8200[2] en juillet 2017.

Grâce à des adresses de 128 bits au lieu de 32 bits, IPv6 dispose d'un espace d'adressage bien plus important qu'IPv4 (près de 100 milliards de milliards de fois plus). Cette quantité d'adresses considérable permet une plus grande flexibilité dans l'attribution 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.

IPv6 dispose également de mécanismes d'attribution 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 simplifié 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 (RFC 4966[3]). 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 2011, seules quelques sociétés ont entrepris de déployer la technologie IPv6 sur leur réseau interne Google[4] notamment.

Au début de l'année 2016, le déploiement d'IPv6 est encore limité, la proportion d'utilisateurs Internet en IPv6 étant estimée à 10 %[5] 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.

Sommaire

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. Au début d'Internet, dans les années 1970, il était pratiquement inimaginable qu'il y aurait un jour suffisamment de machines sur un unique réseau pour que l'on commence à manquer d'adresses disponibles.

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.

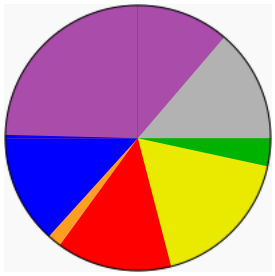
Jusqu'aux années 1990, les adresses sont distribuées sous forme de *classes*, des blocs de 16 millions (*Classe A*), 65 536 (*Classe B*) ou 256 adresses (*Classe C*) sont attribués aux demandeurs, parfois bien au-delà des besoins réels. Par exemple les premières grandes organisations connectées à Internet se sont vu attribuer 16 millions d'adresses.

Au début des années 1990, devant l'épuisement de l'espace d'adressage, notamment des réseaux de classe B (RFC 1338[7]), les registres Internet régionaux font leur apparition et le découpage des adresses en classes 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.

Le 3 février 2011, l'Internet Assigned Numbers Authority (IANA) annonce que les cinq derniers blocs d'adresses ont été distribués de façon égale aux cinq registres Internet régionaux (RIR) et que, par conséquent, elle ne dispose plus de blocs d'adresses libres[8]. Le 15 avril 2011, APNIC, le RIR qui dessert la zone Asie-Pacifique, a annoncé qu'il ne disposait plus que d'un bloc /8 (16,7 millions d'adresses) et ne distribue désormais qu'une quantité limitée d'adresses aux demandeurs[9]. Le RIPE NCC, qui dessert l'Europe et le Moyen-Orient, a fait de même le 14 septembre 2012[10]. Les autres RIR épuiseront les allocations d'adresses IPv4 pour les registres Internet locaux (LIR) entre 2013 et 2015. Les LIR commenceront à manquer d'adresses IPv4 à attribuer à leurs clients en 2012.

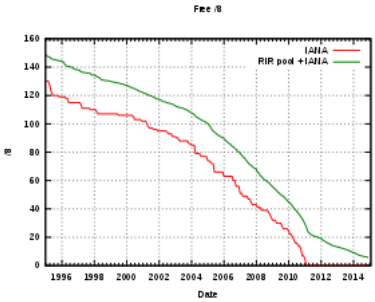


Distribution de l'espace d'adressage IPv4[6]. Le 3 février 2011, il ne reste plus aucun bloc d'adresses libre.

IPv6 améliore aussi certains aspects du fonctionnement d'IP, à la lumière de l'expérience acquise.

Les spécifications principales d'IPv6 sont publiées en 1995 par l'IETF. Parmi les nouveautés, on peut citer :

- l'augmentation de 2^{32} (soit environ $4{,}3\times10^{9}$)[11] à 2^{128} (soit environ $3{,}4\times10^{38}$)[12] du nombre d'adresses disponibles. Pour épuiser la totalité de ce stock d'adresses, il faudrait placer 667 millions de milliards d'appareils connectés sur chaque millimètre carré 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.



Épuisement des adresses IPv4 depuis 1995.

Historique

Au début des années 1990, il est devenu clair que le développement d'Internet allait aboutir à l'épuisement des adresses disponibles (RFC 1752[13]). En 1993, l'IETF lance un appel à propositions (RFC 1550[14]) et annonce la création d'un groupe de travail *IP Next Generation (IPng)*[15].

D'abord nommé *Simple Internet Protocol Plus* (SIPP, RFC 1710[16]), puis *IP Next Generation* (IPng), celui-ci a été choisi en 1994 parmi plusieurs candidats et a reçu en 1995 son nom définitif d'IPv6 (IP version 6[17]), la version 5 d'IP ayant été réservée pour le *Internet Stream Protocol Version 2 (ST2)* par la RFC 1819[18]. Les spécifications d'IPv6 sont initialement publiées en décembre 1995 dans la RFC 1883[19] et finalisées dans la RFC 2460[20] en décembre 1998.

Fonctionnement d'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[21] ».

Adresse IPv6

Une adresse IPv6 est longue de 128 bits, soit 16 octets, contre 32 bits / 4 octets 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

Il est permis d'omettre de un à trois chiffres zéros non significatifs dans chaque groupe de quatre chiffres hexadécimaux. Ainsi, l'adresse IPv6 ci-dessus est équivalente à la suivante :

2001:db8:0:85a3:0:0:ac1f:8001

De plus, une unique suite de un ou plusieurs groupes consécutifs de 16 bits tous nuls peut être omise, en conservant toutefois les signes deux-points de chaque côté de la suite de chiffres omise, c'est-à-dire une paire de deux-points « :: » (RFC 2373[22]). Ainsi, l'adresse IPv6 ci-dessus peut être abrégée en la suivante :

2001:db8:0:85a3::ac1f:8001

Une même adresse IPv6 peut être représentée de plusieurs façons différentes, comme 2001:db8::1:0:0:1 et 2001:db8:0:0:1::1. La RFC 5952[23] recommande une représentation canonique.

Les réseaux sont identifiés en utilisant la notation CIDR : la première adresse du réseau est suivie par une barre oblique « / » puis par un entier compris entre 0 et 128, lequel indique la longueur en bits du *préfixe* du réseau, à savoir de la partie commune des adresses déterminées par ledit réseau.

Voici des exemples d'adresses réseau IPv6 avec leurs ensembles d'adresses déterminées :

- Le préfixe 2001:db8:1f89::/48 représente l'ensemble des adresses qui commence à 2001:db8:1f89:0:0:0:0:0 et finit à 2001:db8:1f89:ffff:ffff:ffff:ffff:ffff.
- Le préfixe 2000::/3 représente les adresses de 2000:0:0:0:0:0:0:0 à 3fff:ffff:ffff:ffff:ffff:ffff:ffff:ffff[Ex 1].
- 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.
- Le préfixe fe80::/10 représente les adresses de fe80:0:0:0:0:0:0:0 à febf:ffff:ffff:ffff:ffff:ffff:ffff:ffff.

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

Deux des adresses réservées de ::/8 peuvent être remarquées :

- ::/128 est l'adresse non spécifiée. On peut la trouver comme adresse source initiale, à l'instar de 0.0.0.0 en IPv4, dans une phase d'acquisition de l'adresse réseau ;
- ::1/128 est l'adresse de boucle locale (dite aussi localhost). Elle est semblable à 127.0.0.1 en IPv4[24].

Les adresses de 2000::/3 peuvent être distinguées comme suit :

- Les adresses permanentes (2001::/16) sont ouvertes à la réservation depuis 1999 :
  - La plage 2001::/32 est utilisée pour Teredo ;
  - La plage 2001:db8::/32 est dédiée à un adressage de réseau IPv6 au sein de la documentation technique impliquant de tels réseaux. Cet usage réservé est spécifié dans la RFC 3849[25] ;
- Les adresses 6to4 (2002::/16) permettent d'acheminer le trafic IPv6 *via* un ou plusieurs réseaux IPv4 ;
- Toutes les autres adresses routables (plus de trois quarts de la plage 2000::/3) sont actuellement réservées à un usage ultérieur

Structure de l'adresse IPv6 unicast globale

Structure des adresses unicast globales

champ	*préfixe de routage global*	*identificateur de sous-réseau*	*identificateur d'interface*
bits	n	64-n	64

Le préfixe de routage global, de taille variable, représente la *topologie publique* de l'adresse, autrement dit celle qui est vue à l'extérieur d'un site. La partie *sous-réseau* constitue la *topologie privée*. La RFC 4291[26] indique que toutes les adresses unicast globales doivent avoir une taille d'identificateur d'interface (IID) égale à 64 bits, à l'exception de celles qui débutent par 000 en binaire. Pour les liens point-à-point, il est cependant possible d'utiliser un /127 (RFC 6164[27]). La RFC 7421[28] explique le choix architectural de cette taille uniforme d'identificateur d'interface qui semble dépasser largement les besoins d'adressage dans un sous-réseau.

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).

Indice de zone

Il peut exister plusieurs adresses link-local sur des liaisons différentes d'une même machine, on lève les ambiguïtés en fournissant un *indice de zone* (RFC 4007[29]) qu'on ajoute à l'adresse après un signe pourcent : fe80::3%eth0 correspondra à l'adresse link-local fe80::3 sur l'interface eth0 par exemple.

Attribution des blocs d'adresses IPv6

Dans l'espace d'adresse unicast global (2000::/3), l'IANA attribue des blocs dont la taille varie de /12 à /23 aux registres Internet régionaux[30], comme le RIPE NCC en Europe. Ces derniers distribuent des préfixes /32 aux *registres Internet locaux* qui les attribuent ensuite sous forme de bloc /48 à /64 aux utilisateurs finaux (RFC 6177[31][32]).

Chaque utilisateur final se voit attribuer un bloc dont la taille varie de /64 (un seul sous-réseau) à /48 (65 536 sous-réseaux), chacun des sous-réseaux pouvant accueillir un nombre d'hôtes virtuellement illimité (2^{64}). Dans le bloc 2000::/3 qui représente 1/8e de l'espace d'adressage disponible en IPv6, on peut donc créer 2^{29}, soit 500 millions de blocs /32 pour des fournisseurs d'accès à Internet, et 2^{45}, soit 35 000 milliards de réseaux d'entreprise typiques (/48).

En-tête IPv6

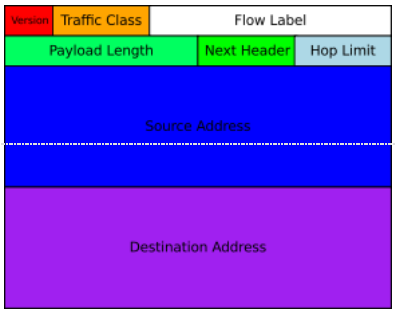
L'en-tête du paquet IPv6 est de taille fixe à 40 octets, tandis qu'en IPv4 la taille minimale est de 20 octets, des options pouvant la porter jusqu'à 60 octets, ces options demeurant rares en pratique.

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.

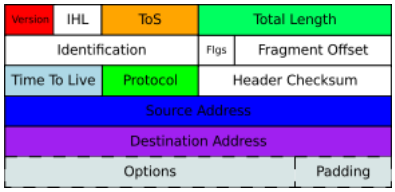
Il est possible qu'un ou plusieurs en-têtes d'extension suivent l'en-tête IPv6. L'en-tête de routage permet par exemple à la source de spécifier un chemin déterminé à suivre.



En-tête IPv6.

Comparaison avec IPv4

- La taille de l'en-tête est fixe, le champ IHL (IP Header Length) est donc inutile.
- Le champ *Time to Live* (TTL) est renommé en *Hop Limit*, reflétant la pratique, la RFC 791[33] prévoyait en effet que le champ *TTL* reflétait le *temps* en secondes.
- 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 où le TTL est décrémenté. Ceci simplifie le traitement des paquets par les routeurs.
- Le champ *Payload length* n'inclut pas la taille de l'en-tête standard, contrairement au champ *Total length* d'IPv4. Tous les en-têtes optionnels sont inclus dans la *payload length* tel que définit dans la RFC 2460[20].
- Les éventuelles informations relatives à la fragmentation sont repoussées dans un en-tête qui suit.
- Les en-têtes optionnels IPv6 doivent tous être analysés un par un pour en déterminer la fin et savoir où commence la charge utile (*payload*) de niveau 4 dans le paquet IPv6 ; en conséquence, les décisions de routage basées sur le contenu des en-têtes de paquets au niveau 4 (par exemple l'identification du numéro de port TCP, UDP, ou type de requête ICMPv6) ne peut se faire sans avoir analysé la chaîne complète des en-têtes optionnels (même seulement pour ne pas en tenir compte) ; ceci inclut notamment les options de fragmentation qui pourraient avoir été insérées par l'émetteur du paquet. Cela pose des difficultés de mise en œuvre dans certains routeurs ou pare-feux pouvant notamment conduire à des problèmes de performance[34, 35].
- Le protocole de résolution de niveau 2 (ARP) de type broadcast est remplacé par NDP qui est en fait une utilisation d'ICMPv6 en multicast, avec quasiment un groupe multicast distinct par hôte[36] ; cela peut entrainer des dysfonctionnements liés à des filtrages[37] d'une part, à des problèmes de performances sur certains équipements[38] d'autre part.



En-tête IPv4.

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 recommandée pour éviter toute fragmentation.

Ce changement permet de simplifier la tâche des routeurs, leur demandant moins de puissance de traitement.

La MTU minimale autorisée pour les liens a également été portée à 1 280 octets (contre 68 pour l'IPv4[39]). 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 65 535 octets. IPv6 dispose cependant d'une option *jumbogram* (RFC 2675[40]) permettant de porter la taille maximale d'un paquet à 4 Go et profiter ainsi des réseaux avec un MTU plus élevé.

En-têtes d'extension

L'en-tête IPv6 peut être suivi d'un certain nombre d'en-tête d'extensions. Ceux-ci se succèdent, chaque en-tête indiquant la nature du suivant. Quand ils sont présents, leur ordre est le suivant :

En-têtes d'extension IPv6

Nom	Type	Taille	Description	RFC
Options Hop-By-Hop	0	variable	Contient les options qui doivent être honorées par tous les routeurs de transit, par exemple l'option jumbogram.	RFC 2460[41], RFC 2675[42]
Routage	43	variable	Permet de modifier le routage à partir de la source, qui est utilisé notamment par Mobile IPv6	RFC 2460[41], RFC 3775[43], RFC 5095[44]
Fragment	44	64 bits	Contient les informations relatives à la fragmentation.	RFC 2460[41]
Authentication Header (AH)	51	variable	Contient les informations nécessaires à l'authentification de l'en-tête, voir IPsec.	RFC 4302[45]
Encapsulating Security Payload (ESP)	50	variable	Contient les informations relatives au chiffrement du contenu, voir IPsec.	RFC 4303[46]
Options de destination	60	variable	Options qui doivent être traitées par la destination finale.	RFC 2460[41]
No Next Header	59	vide	Indique qu'il n'y a aucune charge utile qui suit.	RFC 2460[41]

Les autres valeurs possibles suivent la même convention que le champ *Protocol* dans l'en-tête IPv4[47].

Neighbor Discovery Protocol

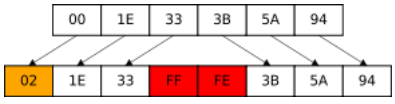
Le Neighbor Discovery Protocol (ND, RFC 4861[48]) associe les adresses IPv6 à des adresses MAC sur un segment, comme ARP pour IPv4. Il permet également de découvrir les routeurs et les préfixes routés, le MTU, de détecter les adresses dupliquées, les hôtes devenus inaccessibles et l'autoconfiguration des adresses et éventuellement les adresses des serveurs DNS récursifs (RDNSS, RFC 5006[49]). Il s'appuie sur ICMPv6.

Attribution des adresses IPv6

Dans un sous-réseau, il existe plusieurs méthodes d'attribution 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



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

- autoconfiguration sans état (*Stateless Address Autoconfiguration*, SLAAC) basée sur l'adresse MAC qui utilise le Neighbor Discovery Protocol (NDP) (RFC 4862[50]).
- autoconfiguration avec tirage pseudo aléatoire (RFC 4941[51]),
- utilisation d'adresses générées cryptographiquement (CGA, RFC 3972[52]), qui lient l'adresse à la clé publique du client et qui peuvent être utilisées par SEND,

- attribution par un serveur DHCPv6 (RFC 3315[53]).

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 personnelles[54] 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 (RFC 4941[51]) 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.

Multicast

Le multicast, qui permet de diffuser un paquet à un groupe, fait partie des spécifications initiales d'IPv6. Cette fonctionnalité existe également en IPv4 où il a été ajouté par la RFC 988[55] en 1986.

Il n'y a plus d'adresse broadcast en IPv6, celle-ci étant remplacée par une adresse multicast spécifique à l'application désirée. Par exemple, l'adresse ff02::101 permet de contacter les serveurs NTP sur un lien. Les hôtes peuvent ainsi filtrer les paquets destinés à des protocoles ou des applications qu'ils n'utilisent pas, et ce sans devoir examiner le contenu du paquet.

Au niveau ethernet, une série de préfixes OUI est réservée aux adresses IPv6 multicast (33:33:xx). L'adresse MAC du groupe multicast consistera en ces 16 bits que l'on fait suivre par les 32 derniers bits de l'adresse IPv6 multicast. Par exemple, l'adresse ff02::3:2 correspondra à l'adresse MAC 33:33:00:03:00:02. Bien que de nombreux groupes multicast partagent la même adresse MAC, ceci permet déjà un filtrage efficace au niveau de la carte réseau.

Bien que la prise en charge de multicast au niveau des liens soit obligatoire pour IPv6, le routage des paquets multicast au-delà du segment requiert l'utilisation de protocoles de routage comme PIM, à la discrétion du fournisseur d'accès à Internet.

Le protocole Multicast Listener Discovery permet d'identifier les groupes actifs sur un segment, à l'instar d'IGMP pour IPv4.

Les commutateurs ethernet les plus simples traitent les trames multicast en les diffusant comme des trames broadcast. Ce comportement est amélioré avec *MLD snooping* qui limite la diffusion aux seuls hôtes manifestant un intérêt pour le groupe, à l'instar d'*IGMP Snooping* pour IPv4.

Alors qu'en IPv4 il est difficile de réserver des adresses multicast globales, la RFC 3306[56] associe un bloc d'adresses multicast /96 pour chaque préfixe routable sur Internet, c'est-à-dire que chaque organisation dispose automatiquement de 4 milliards d'adresses multicast publiques. La RFC 3956[57] simplifie également la réalisation de points de rendez-vous pour les interconnexions multicast.

DNS

Dans le Domain Name System les noms d'hôtes sont associés à des adresses IPv6 grâce à l'enregistrement AAAA.

```
www.ipv6.ripe.net.          IN   AAAA   2001:610:240:22::c100:68b
```

L'enregistrement inverse est réalisé sous ip6.arpa en inversant l'adresse écrite sous forme canonique (RFC 3596[58]) :

```
b.8.6.0.0.0.1.c.0.0.0.0.0.0.0.0.2.2.0.0.0.4.2.0.0.1.6.0.1.0.0.2.ip6.arpa. IN   PTR    www.ipv6.ripe.net.
```

La première mouture de la norme prévoyait d'utiliser le suffixe *ip6.int*.

Le mécanisme utilisé pour construire le nom de domaine inverse est similaire à celui employé en IPv4, à la différence que les points sont utilisés entre chaque *nibble* (groupe de 4 bits), ce qui allonge le domaine.

Les plus complexes bitlabels (RFC 2673[59]), DNAME et A6 (RFC 2874[60]), qui permettent de s'affranchir de la contrainte de la délégation sur une frontière de nibble, sont considérés comme expérimentaux et leur support est rare (RFC 3363[61], l'enregistrement A6, inusité, est relégué à l'état « historique » par la RFC 6563[62] en 2012).

La résolution inverse peut être utilisée par des systèmes de contrôle d'accès ainsi que par des outils de diagnostic comme traceroute.

Traduction d'adresse

Le recours à la traduction d'adresse est découragé en IPv6 pour préserver la transparence du réseau[63], son utilisation n'est plus nécessaire pour économiser des adresses.

IPv6 et mobilité

IPv6 prévoit des mécanismes pour conserver une même adresse IPv6 pour une machine pouvant être connectée à des réseaux différents, tout en évitant autant que possible le routage triangulaire.

Technologies de transition pour l'accès à l'Internet IPv6

Les adresses IPv4 et IPv6 ne sont pas compatibles, la communication entre un hôte ne disposant que d'adresses IPv6 et un hôte ne disposant que d'adresses IPv4 constitue donc un problème. La transition consiste à doter les hôtes IPv4 d'une *double pile*, c'est-à-dire à la fois d'adresses IPv6 et IPv4.

La manière la plus simple d'accéder à IPv6 est lors de l'abonnement de choisir un FAI qui offre de l'IPv6 *nativement*, c'est-à-dire sans recours à des tunnels.

À défaut, et pendant une phase de transition, il est possible d'obtenir une connectivité IPv6 via un tunnel. Les paquets IPv6 sont alors encapsulés dans des paquets IPv4, qui peuvent traverser le réseau du FAI jusqu'à un serveur qui prend en charge IPv6 et IPv4, et où ils sont décapsulés. Le recours à des tunnels, et donc à un réseau overlay, est de nature à nuire aux performances.

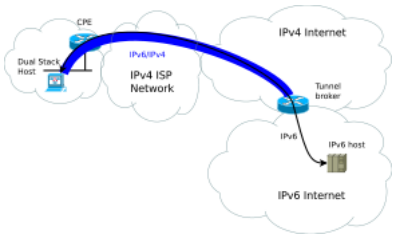


Schéma de fonctionnement d'un tunnel statique.

Tunnels statiques

Plusieurs services du type « *tunnel broker* » sont disponibles, nécessitant en général une inscription. On peut citer SixXS[64], ou Hurricane Electric[65].

Les protocoles utilisés peuvent être :

- 6in4 (RFC 4213[66]) fait usage du numéro de protocole 41 d'IP et est donc parfois bloqué par des pare-feux et les NAT.
- AYIYA[67] permet le transport sur UDP ou TCP et gère le changement d'adresse IP
- GRE utilise le numéro de protocole 47.

Le Tunnel Setup Protocol (RFC 5572[68]) facilite la création des tunnels et permet la mobilité et l'authentification. Le *Tunnel Information and Control protocol*, utilisé par AICCU **(en)**, automatise la création des tunnels.

Tunnels automatiques

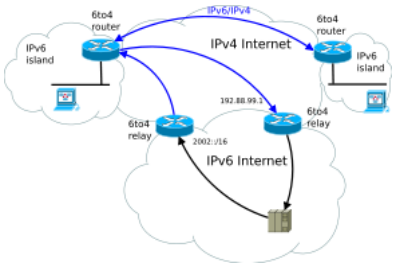


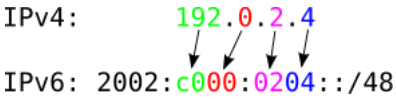
Schéma de fonctionnement de 6to4.

- 6to4 (RFC 3056[69]) si une adresse IPv4 publique (de préférence fixe) est disponible, 6to4 est simple à mettre en place. Pour l'accès aux adresses IPv6 hors du préfixe 2002::/16 (réservé pour 6to4), une adresse relais anycast est réservée, 192.88.99.1.
- 6rd (RFC 5569[70]) est similaire au précédent. Il ne fait pas usage du préfixe 2002::/16 mais d'un préfixe spécifique au fournisseur d'accès.
- 6over4 (RFC 2529[71]) permet la connexion à travers un réseau IPv4 qui prend en charge le multicast
- ISATAP (RFC 5214[72]), une amélioration du précédent qui ne requiert pas le support multicast.
- Teredo (RFC 4380[73]) utilisable dans un réseau d'adresses IPv4 privées, relié à Internet via un routeur assurant une traduction d'adresses. Une implémentation de Teredo fait partie de la pile IPv6 des systèmes Windows, et une implémentation pour Linux et les systèmes BSD est miredo[74].

Passerelles applicatives

Il est possible de faire usage de serveurs qui disposent d'une double pile et qui font office de passerelle applicative (Application-Level gateway, ALG), un serveur mandataire web par exemple.

NAT-PT combine la traduction d'adresse réseau et un serveur DNS pour permettre la communication entre des systèmes IPv4 et des systèmes IPv6. Il est défini dans la RFC 2766[75] mais a été rendu obsolète par la RFC 4966[76] en raison de problèmes causés.



Encodage d'une adresse IPv4 dans le préfixe 6to4.

Multihoming

Le multihoming consiste, pour un réseau, à disposer de plusieurs fournisseurs de transit dans le but d'augmenter la fiabilité de l'accès Internet. En IPv4, ceci est généralement accompli en disposant d'un numéro d'AS propre, d'une plage d'adresse IP de type *Provider Independent* (PI) et en utilisant BGP pour échanger des routes de façon dynamique avec chacun des fournisseurs d'accès.

Cette façon de réaliser le multihoming consomme des numéros d'AS et augmente la taille de la table de routage Internet en raison de préfixes PI qu'il n'est pas possible d'agréger

La standardisation du multihoming en IPv6 a tardé, une des ambitions initiales de l'architecture IPv6 étant de n'utiliser que des adresses de type *Provider Aggregatable* (PA) pour réduire la taille de la table de routage Internet. Dans cette optique, le multihoming était réalisé en attribuant autant d'adresses PA qu'il y a de fournisseurs, les mécanismes d'IPv6 comme l'attribution automatique et la durée de vie limitée des adresses facilitant les changements d'adresses liées aux changements de fournisseurs. Par conséquent, les registres Internet régionaux ne distribuaient pas de bloc PI pour IPv6 jusqu'à récemment.

En 2009, les RIR, comme le RIPE NCC, ont modifié leur politique en acceptant d'attribuer des blocs PI aux entreprises qui veulent se connecter à plusieurs fournisseurs[77], la taille minimale du bloc PI est de /48, alors que la taille des blocs PA est /32. Ceci permet de réaliser le multihoming de la même façon qu'en IPv4.

D'autre approches possibles sont basées sur la séparation de l'identificateur et du localisateur (*Identifier / Locator Separation*) :

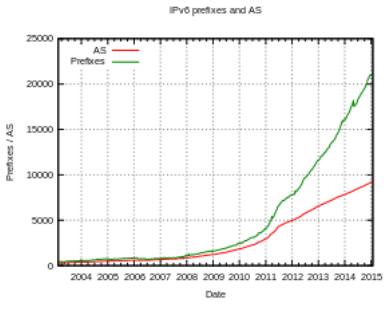
- SHIM6 (RFC 5533[78])
- Host Identity Protocol (RFC 4423[79], RFC 5102[80])
- Stream Control Transmission Protocol
- GSE/8+8[81, 82].
- Locator/Identifier Separation Protocol (LISP)[83]
- NPTv6, soit la traduction de préfixe (RFC 6296[84])

Ceci est un sujet de recherche confié au groupe de travail *Routing Research* de l'Internet Research Task Force (en)[85].

Déploiement d'IPv6

L'Internet IPv6

Dans une première phase, les fournisseurs d'accès à Internet utilisent des tunnels qui encapsulent les paquets IPv6 dans des paquets IPv4 (via 6in4 ou GRE) pour traverser les groupes de routeurs qui ne prennent pas en charge IPv6. Lorsque c'est possible, les échanges se font *nativement*, avec IPv4 et IPv6 qui coexistent sur les mêmes liaisons. Pour autant que les routeurs soient mis à jour pour la prise en charge d'IPv6, il n'est pas nécessaire de disposer d'une infrastructure séparée pour IPv6, les routeurs traitant à la fois le trafic IPv4 et IPv6.



Nombre de préfixes et d'AS IPv6 sur Internet, de 2003 à aujourd'hui. À titre de comparaison, il y a environ 50 000 AS visibles dans la default-free zone en 2015.

Prise en charge d'IPv6 par le DNS

Depuis juillet 2004, l'ICANN accepte d'intégrer des serveurs de noms avec des adresses IPv6 (*glue records*) dans la zone racine[86]. Les premiers domaines de premier niveau qui disposent d'un serveur DNS IPv6 sont .kr et .jp, .fr suit peu après[87].

En février 2008, l'ICANN a ajouté des adresses IPv6 à six des treize serveurs racine du DNS[88] et « i » a été ajouté en 2010. D'autre part, en 2010, 228 des 283 domaines de premier niveau disposent d'au moins un serveur avec une adresse IPv6[89]. Les agents d'enregistrement doivent cependant mettre à jour leurs logiciels pour la prise en charge des délégations vers des serveurs IPv6 et les éventuels *glue AAAA* records[90].

Les principaux serveurs de noms comme BINDv9 prennent en charge les records AAAA ainsi que le transport des requêtes sur IPv6.

La taille des paquets DNS en UDP est limitée à 512 octets (RFC 1035[91]), ce qui peut poser des problèmes au cas où la réponse est particulièrement volumineuse. La norme prévoit alors qu'une connexion TCP est utilisée, mais certains pare-feux bloquent le port TCP 53 et cette connexion consomme plus de ressources qu'en UDP. Ce cas se pose notamment pour la liste de serveurs de noms de la zone racine. L'extension EDNS0 (RFC 2671[92]) permet d'utiliser une taille de paquets plus élevée, sa prise en charge est recommandée pour IPv6 comme pour DNSSEC.

Prise en charge d'IPv6 par les protocoles de routage

Les protocoles de routage comme BGP (RFC 2545[93]), OSPFv3 (RFC 5340[94]), IS-IS (RFC 5308[95]) et MPLS (RFC 4798[96]) ont été mis à jour pour IPv6.

Prise en charge d'IPv6 sur les couches liaison et transport

Les protocoles TCP et UDP fonctionnent comme en IPv4. Le pseudo en-tête utilisé pour le calcul du code de contrôle est cependant modifié et inclut les adresses IPv6 source et destination. L'utilisation du code de contrôle est obligatoire également pour UDP. Des modifications mineures ont été apportées pour la prise en charge des paquets jumbo (RFC 2675[42]).

Les protocoles de la couche de liaison de type IEEE 802 sont adaptés pour le transport d'IPv6. Au niveau ethernet par exemple, la valeur du champ *type* attribué à IPv6 est 0x86DD (RFC 2464[97]).

Sur les réseaux NBMA (en) comme X.25 ou Frame Relay, des adaptations sont prévues pour permettre le fonctionnement du *Neighbor Discovery*.

Le consortium CableLabs (en) a publié les spécifications IPv6 qui concernent les modems câble dans DOCSIS v3.0 en août 2006. Il n'y a pas de prise en charge IPv6 dans la version DOCSIS 2.0. Une version dite « DOCSIS 2.0 + IPv6 » existe cependant et ne nécessite qu'une mise à jour micrologicielle.[98]

Pour les technologies xDSL, la RFC 2472[99] définit l'encapsulation de IPv6 sur PPP. Le BRAS doit également prendre en charge IPv6.

En général, les équipements qui travaillent sur la couche de liaison, comme les commutateurs ethernet, n'ont pas besoin de mise à jour pour la prise en charge d'IPv6, sauf éventuellement pour le contrôle et la gestion à distance et l'optimisation de la diffusion multicast avec MLD snooping.

Les systèmes d'accès doivent généralement être revus pour IPv6, les outils d'attribution des adresses et les bases de données d'enregistrement des adresses notamment.

Prise en charge d'IPv6 dans les systèmes d'exploitation et les logiciels

Depuis le début du XXIe siècle, tous les principaux systèmes d'exploitation (GNU/Linux, Mac OS X, Microsoft Windows, BSD, Solaris, HP-UX, etc.) ont été mis à jour pour la prise en charge d'IPv6, et c'est également le cas d'autres systèmes embarqués, tels que Symbian, QNX, Android, Windows Mobile ou Wind River.

Windows Vista prend en charge IPv6 dans sa configuration par défaut, expose les réglages IPv6 dans l'interface graphique sur le même plan que les réglages IPv4, et utilise une nouvelle pile TCP/IP *dual stack* au lieu d'une pile indépendante pour IPv6. Cette prise en charge sert de base à HomeGroup et DirectAccess dans Windows 7.

Au niveau des routeurs, Cisco offre la prise en charge IPv6 depuis 2001 avec IOS 12.2, c'est également le cas des versions récentes de logiciels par principaux vendeurs comme Juniper Networks, Alcatel-Lucent ou Redback Networks.

Certains CPE restent cependant encore incompatibles avec IPv6, ce qui rend nécessaire la configuration de tunnels.

Les applications reliées au réseau doivent être modifiées pour être compatibles avec IPv6. L'ampleur de la mise à jour du code source varie en fonction de l'usage qui est fait des adresses par les applications. Il peut s'agir d'un remplacement simple mais aussi de modifications plus complexes si l'adresse est stockée dans une base de données ou est utilisée dans un contrôle d'accès.

Quand il n'est pas possible de mettre l'application à jour rapidement, des techniques de transition permettent à des applications IPv4 de communiquer avec des clients IPv6 :

- *Bump in the Stack* (RFC 2767[100])
- *Bump in the API* (RFC 3338[101]) - L'outil IPv6 CARE en fournit une implémentation pour les systèmes UNIX.

De nombreuses applications ont déjà été portées[102] C'est en particulier le cas des navigateurs web comme Internet Explorer (depuis la version 7, partiellement pour la version 6), Mozilla Firefox (1.0), Opera (7.20b), Safari et Google Chrome, du client de messagerie Mozilla Thunderbird (1.0), serveur web Apache (1.3.27/2.0.43), du serveur de mail Exim (4.20), etc.

Déploiement d'IPv6 chez les fournisseurs d'accès à Internet en France

Renater a commencé à expérimenter IPv6 en 1996 avec le réseau G6bone, le pendant français du réseau 6bone mondial qui a démarré la même année. Ce réseau de test utilisait essentiellement des tunnels. Le service pilote IPv6 du réseau Renater 2 offre des connexions natives IPv6 sur ATM en 2002.

Fournisseur d'accès à internet	Date de déploiement	Longueur du préfixe attribué	MTU	Notes
Nerim	mars 2003	/48	1 500 en PPPoA, 1492 en PPPoE	
Free	décembre 2007[103]	/61[104]	1 480 en ADSL dégroupé, non disponible en non dégroupé	6rd en ADSL
FDN	novembre 2008	/48	1 492 en PPPoE	
SFR	fin 2011 (beta en juin 2011) fin 2013 (FTTH)	/64[105]	?	tunnel L2TP[106]
Numericable	début 2012	?	?	DOCSIS 3.0[107]
OVH	mi-2012	/56	1 500 en IPoE (dégroupé), 1 492 en PPPoE	délégation de préfixe (RFC 3633[108]) par DHCPv6[109]
Orange	tests de Wanadoo en 2005 ; proposé en offre sur mesure depuis 2010 sur le marché entreprise sous la marque Orange Business Services, tests internes depuis juillet 2014, le déploiement IPv6 pour le grand public a commencé depuis début 2016 pour les clients fibre et VDSL[110].	/56	1 500	La Livebox Play est annoncé comme compatible IPv4 et IPv6[111]
Bouygues Telecom	prévu pour l'ADSL dégroupé en 2017[112], le FTTH en 2018	/60[113]	1 500	délégation de préfixe IPv6 sur la Bbox en 2018[114]
Zeop	22 juillet 2014	/56	1 500	Premier opérateur IPv6 à la Réunion[réf. nécessaire]
Quantic Telecom	2013	/48[115]	?	?
K-Net	2012	/56	1 500	

Déploiement d'IPv6 chez les fournisseurs d'accès à Internet en Suisse

En Suisse, outre l'exploitant des réseaux des universités Switch, plusieurs opérateurs alternatifs ont déployé IPv6 pour leurs clients résidentiels dès la normalisation du protocole, l'un des plus importants étant Init7.

L'opérateur historique, Swisscom, a mené des expériences de déploiement en 2003 et 2004 dans le cadre de la Swiss IPv6 Task Force dont il assurait la direction, mais seul le réseau international de la société (IP-Plus) a conservé IPv6 en production. En 2011, Swisscom a initié[116] un pilote ouvert à tous ses clients pour le déploiement d'IPv6 résidentiel via la technologie 6rd, chaque client disposant d'un /60 pour son usage personnel.

Les autres grands opérateurs suisses, à savoir Sunrise, Cablecom, et Orange n'ont pas encore annoncé officiellement de plans en juillet 2011, mais France Telecom avait annoncé[117] en octobre 2009 utiliser la Suisse comme pays pilote pour ses déploiements.

Déploiement d'IPv6 en Europe

En 2000, le programme 6INIT permet l'interconnexion des réseaux nationaux de la recherche et de l'enseignement (NREN) européens grâce à des PVC IPv6 sur ATM à travers le réseau de recherche européen TEN 155[118]. En 2003, le réseau GÉANT, qui succède à TEN 155, utilise une double pile (IPv4 + IPv6). Dix-huit des NREN sont connectés nativement en IPv6.

La Commission européenne s'est fixé comme objectif de recevoir des engagements des 100 principaux opérateurs de sites web de l'Union européenne avant la fin de l'année 2008 et a publié un plan d'action[119] en mai 2009.

En 2010, le RIPE NCC (Europe) est la région qui annonce le plus grand nombre de préfixes IPv6[120].

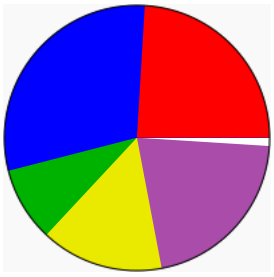
Le projet *IPv6 Ripeness*[121] du RIPE vise à observer le déploiement d'IPv6 en Europe en attribuant des étoiles aux registres Internet locaux quand certains indicateurs de déploiement sont atteints. Les étoiles sont attribuées pour chacun des critères suivants :

- une allocation IPv6,
- le bloc d'adresse IPv6 est visible dans la table de routage Internet,
- le bloc fait l'objet d'un enregistrement *route6* dans la base de données du RIPE,
- la zone DNS inverse correspondant au bloc est déléguée.

En janvier 2013, 57 % des LIR ont obtenu un bloc d'adresse IPv6, et 19 % ont atteint le niveau le plus élevé de quatre étoiles[122].

Résultat de l'enquête *IPv6 Ripeness* du RIPE en avril 2010, sur 6 748 registres locaux.

Pas d'IPv6 (72,3 %)
1 étoile (9,5 %)
2 étoiles (4 %)
3 étoiles (5,9 %)
4 étoiles (8,3 %)



Résultats en juin 2015 sur 11 813 registres locaux.

Pas d'IPv6 (24 %)
1 étoile (30 %)
2 étoiles (9 %)
3 étoiles (15 %)
4 étoiles (21 %)

Déploiement d'IPv6 dans le monde

En 1996, le réseau de test 6bone a permis les expérimentations de la technologie IPv6 (RFC 2471[124]). Ce réseau était construit sur des tunnels, et les routes échangées par le protocole BGP4+. Les participants se voyaient octroyer un préfixe /24, /28 ou /32 dans le bloc 3ffe::/16[125]. Le réseau a été démantelé en 2006 (RFC 3701[126]) au profit de connexions natives.

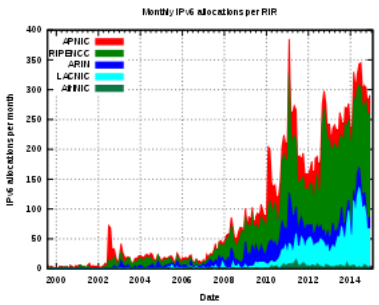
Aujourd'hui, de nombreux serveurs web acceptent les connexions via IPv6[127]. Google est par exemple accessible en IPv6 depuis mars 2008[128], c'est également le cas de YouTube et Facebook depuis 2010.

Existent également des serveurs en IPv6 proposant des services courants, tels que FTP, SSH, SMTP, IMAP ou IRC.

En 2009, plusieurs opérateurs mondiaux ont commencé à déployer IPv6[129, 130, 131].

Au Japon, NTT commercialise différentes offres de services IPv6[132] et commercialise également le *Flet's phone*.

Les règlements des marchés publics rendent la prise en charge d'IPv6 obligatoire, notamment dans les États de l'Union européenne et aux États-Unis[133].



Nombre mensuel d'allocations de blocs IPv6 par chacun des RIR depuis 1999.

Aux États-Unis, Comcast a commencé[134] en 2010 des tests de diverses technologies autour d'IPv6, sur son réseau de production, en prévision du déploiement définitif et de l'épuisement des adresses IPv4. IPv6 est également utilisé par le département de la défense des États-Unis d'Amérique.

La Chine populaire considère avec intérêt l'IPv6. Elle vise à un début d'utilisation commerciale de l'IPv6 à partir de 2013, et à une utilisation et une interconnexion plus large d'ici 2015[135]. Les adresses IPv6 chinoises ne représentent que 0,29 % des adresses IPv6 mondiales[136], en 2011. Alors que la Chine est à la troisième place à un niveau mondial[137].

IPv6 s'impose parfois comme unique moyen d'interconnexion avec les terminaux mobiles itinérants en Asie ; il le sera aussi rapidement en Europe quand les anciennes solutions d'interconnexion basées sur les protocoles GSM devront être remplacées par des solutions IP. De plus, l'évolution des usages mobiles allant vers une connectivité IP permanente, il deviendra alors très difficile d'adresser un nombre très important de terminaux mobiles (smartphones), avec un adressage IPv4 (même avec NAT).

Un rapport de l'OCDE publié en avril 2010[86] indique que le niveau d'adoption d'IPv6 est encore faible, avec de 0,25 à 1 % des utilisateurs qui font usage d'IPv6. Le trafic IPv6 natif représente 0,3 % du trafic de l'AMS-IX. À la fin de l'année 2009, 1 851 numéros d'AS IPv6 étaient visibles, ce nombre ayant doublé en deux ans.

En décembre 2010, Google estime que le nombre d'utilisateurs IPv6 de son service de recherche Internet serait de 0,25 % environ[5].

Le cas de Wikipédia

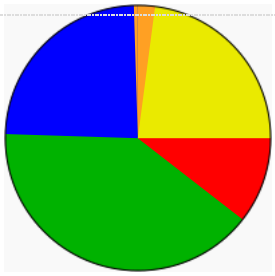
Les équipes de Wikipédia préparent cet aspect technique depuis 2008[138, 139, 140], après une tentative en 2006[141]. Une page de suivi a été créée pour en suivre l'évolution[142] Après une participation de la fondation à la journée de test de 2011[143]. Wikipedia permet à ses utilisateurs de profiter pleinement de ses services à l'aide de l'IPv6[144, 145] lors de la journée de lancement[146, 147].

Journée mondiale IPv6

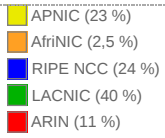
Le 8 juin 2011 l'Internet Society (ISOC) a organisé une journée mondiale IPv6 pendant laquelle les fournisseurs et les sites ont été encouragés à tester la technologie à grande échelle[148]. Google, Facebook, Yahoo!, Akamai et Limelight Networks ont participé à cet événement. Google a estimé que 99,95 % des utilisateurs ne seraient pas affectés par ce test[149]. Des statistiques présentées par Yahoo montrent que 0,022 % des utilisateurs de leur site ont été affectés, tandis que 0,229 % ont utilisé IPv6[150].

Évolution législative

En France, la loi pour une république numérique rend obligatoire la compatibilité avec l'IPv6 des produits vendus à partir du 1er janvier 2018[151].



Répartition de la taille des allocations de blocs IPv6 aux registres Internet régionaux en 2012 (source OCDE). Il y avait plus de 17000 allocations à ce moment[123].



Freins au déploiement d'IPv6

Critiques opérationnelles

Certains, comme Randy Bush, ont critiqué la façon dont la phase de transition vers IPv6 a été élaborée, en indiquant que les difficultés et les coûts de la transition ont été minimisés, que les adresses IPv6 sont distribuées de façon trop généreuse, que le niveau actuel de trafic ne permet pas d'affirmer que les routeurs sont capables des mêmes performances qu'avec IPv4, que l'adaptation des protocoles est incomplète (notamment SNMP et les pare-feu) et que les bénéfices escomptés (en termes d'élimination de NAT et d'agrégation de la table de routage Internet) ont été surestimés[152].

D'autre part, certains systèmes d'exploitation qui disposent d'une double pile sans toutefois disposer de connectivité IPv6 fonctionnelle peuvent créer des délais anormaux lors de l'accès à des serveurs qui disposent à la fois d'une adresse IPv6 et d'une adresse IPv4[153], l'adresse IPv6 étant utilisée en priorité avant de recourir à l'adresse IPv4 après un délai déterminé.

En 2011, la politique de *peering* de certains fournisseurs d'accès aboutit au partitionnement de l'Internet IPv6. Les utilisateurs de Hurricane Electric (AS 6939) ne peuvent pas communiquer avec ceux de Cogent (AS 174) ni ceux de Level 3 (AS 3356) par exemple. Ce problème affecte occasionnellement aussi l'Internet IPv4[154, 155].

Logo de la journée mondiale du lancement IPv6 du 6 juin 2012.

Freins au déploiement

Les freins au déploiement d'IPv6 sont, entre autres, les suivants :

- Pour les équipements anciens :
  - Le fabricant a cessé ses activités ;
  - Le fabricant ne fournit pas de mise à jour pour IPv6 ou réclame des prix élevés pour le faire;
  - La mise à jour logicielle est impossible (le code étant en mémoire morte) ;
  - L'équipement n'a pas les ressources requises pour le traitement d'IPv6 ;
  - IPv6 est disponible mais avec des performances dégradées.
- Pour les équipements récents :
  - Le prix de vente est plus élevé pour le consommateur ;
  - Le développement de logiciel compatible IPv6 est coûteux.
- L'indifférence des utilisateurs finaux :
  - Les utilisateurs ne manifestent pas d'intérêt à défaut de nécessité ;
  - Les applications fonctionnent correctement en IPv4 actuellement ;
  - La formation à la nouvelle technologie coûte cher

Concernant le développement de la prise en charge IPv6 chez les fournisseurs de contenu et d'accès, on compare parfois le problème à celui de l'œuf et de la poule[156] :

- Les fournisseurs d'accès disent qu'il n'y a pas de contenu disponible spécifiquement en IPv6 ;
- Les fournisseurs de contenu disent qu'il n'y a pas de demande.

Selon une étude publiée en octobre 2009[157], les fournisseurs identifient les points suivants comme les principaux obstacles :

- Les coûts ;
- La prise en charge par les fabricants ;
- L'absence de rentabilité ;
- Le manque de familiarité.

Les principaux facteurs de développement sont :

- Tenir le rôle de précurseur ;
- S'assurer que les produits sont compatibles IPv6 ;
- Désir de profiter des avantages d'IPv6 dès que possible ;
- Prévoir l'épuisement des adresses IPv4.

Concernant les problèmes rencontrés par les FAI qui ont déployé IPv6 :

- Le manque de demande de la part des utilisateurs ;
- Le manque de familiarité avec la technologie.

IPv6 dans les produits destinés au public

En général, les produits du marché destinés au grand public n'ont pas de possibilité de mise à jour[réf. nécessaire]

En 2014, la prise en charge d'IPv6 n'est pas encore un critère de choix pour le consommateur final. Quand une application majeure ne sera plus accessible en IPv4, l'importance de ce critère sera sans doute revue. Les entreprises sont cependant plus attentives à ce problème et évitent d'investir dans des équipements qui pourraient s'avérer incompatibles avec IPv6.

Les clients ne disposant que d'une adresse IPv6 pourraient apparaître vers 2014, le problème de la connectivité vers les serveurs Internet qui ne disposent que d'une adresse IPv4 se posera concrètement dès lors pour les clients internet qui ne sont pas dotés d'une double pile (adresses IPv4 et IPV6). L'accès aux serveurs IPv6 depuis des clients IPv4 présente également un défi technique.

Ainsi, des problèmes sont déjà[Quand ?] visibles concernant notamment les accès Internet mobile, qui souvent n'attribuent que des adresses IPv4 privées non routables, mais connectées à des serveurs proxy HTTP fournis par l'opérateur de réseau d'accès, avec des performances parfois décevantes et des problèmes de restriction des protocoles de communication supportés par ce type de tunnels mais aussi de stabilité des sessions temporaires. D'autres solutions utilisant un NAT dynamique connaissent un autre problème lié à la famine des ports disponibles dans les routeurs NAT partagés par plusieurs clients IPv4 pour une utilisation optimale avec les applications de plus en plus interactives du web actuel et qui nécessitent de nombreux ports pour chaque utilisateur; les autres solutions basées sur la traduction de protocole dans un tunnel (6to4 ou Teredo) posent également des problèmes similaires de performance et de coût de mise en œuvre, que seul un déploiement en IPv6 natif pourrait résoudre avec un meilleur compromis entre performances, coût de mise en œuvre et coûts d'exploitation : puisque déjà des problèmes très fréquents[réf. souhaitée] existent sur les accès mobiles 3G, et sont constatés par les clients de ces réseaux même pour une utilisation très modérée[réf. souhaitée] (alors que le coût d'accès est déjà élevé), le passage au palier suivant des réseaux 4G+ (LTE par exemple) ne pourra pas être économiquement viable sans un passage au routage IPv6 natif[réf. nécessaire], sans tunnel ni proxy d'adaptation chaque fois que possible (de nombreuses applications et sites web devront être adaptés pour être accessibles directement en IPv6, sans nécessiter ces adaptations, si elles désirent conserver des performances acceptables pour leurs clients sans accès IPv4 natif).

Bien que certains équipements n'auraient besoin que d'une mise à jour de micrologiciel pour IPv6, il n'est pas certain que leurs fabricants investiront dans cette voie alors que la vente de produits *IPv6 Ready* s'avérerait plus rentable.

Notes et références

1. **(en)** « Internet Protocol, Version 6 (IPv6) Specification (https://tools.ietf.org/html/rfc2460) », Request for Comments n° 2460, décembre 1998.
2. **(en)** « Internet Protocol, Version 6 (IPv6) Specification, Request for Comments 8200 » (https://tools.ietf.org/html/rfc8200) sur *ietf.org*, juillet 2017
3. **(en)** « Reasons to Move the Network Address Translator - Protocol Translator (NAT-PT) to Historic Status (https://tools.ietf.org/html/rfc4966) », Request for Comments n° 4966, juillet 2007.
4. Google teste IPv6 sur son réseau interne (http://www.lemondeinformatique.fr/actualites/lire-google-teste-ipv6-sur-son-reseau-interne-47010-page-1.html) Jean Elyan avec IDG News Service, LeMondeInformatique.fr 12 décembre 2011
5. Google IPv6 statistics (http://www.google.com/intl/en/ipv6/statistics/)
6. « IANA IPv4 Address Space Registry » (http://www.iana.org/assignments/ipv4-address-space/ipv4-address-space.xhtml)
7. **(en)** « Supernetting: an Address Assignment and Aggregation Strategy (https://tools.ietf.org/html/rfc1338) », Request for Comments n° 1338, juin 1992.
8. Free Pool of IPv4 Address Space Depleted (http://www.nro.net/news/ipv4-free-pool-depleted)
9. APNIC IPv4 Address Pool Reaches Final /8 (http://www.apnic.net/publications/news/2011/final-8), APNIC, 15 avril 2011
10. RIPE NCC Begins to Allocate IPv4 Address Space From the Last /8 (http://www.ripe.net/internet-coordination/news/ripe-ncc-begins-to-allocate-ipv4-address-space-from-the-last-8), 14 septembre 2012
11. Exactement 4 294 967 296
12. Exactement 340 282 366 920 938 463 463 374 607 431 768 211 456
13. **(en)** Scott Bradner, A. Mankin, « The Recommendation for the IP Next Generation Protocol (https://tools.ietf.org/html/rfc1752) », Request for Comments n° 1752, janvier 1995.
14. **(en)** Scott Bradner, A. Mankin, « IP: Next Generation (IPng) White Paper Solicitation (https://tools.ietf.org/html/rfc1550) », Request for Comments n° 1550, décembre 1993.
15. **(en)** History of the IPng effort (http://playground.sun.com/ipv6/doc/history.html)
16. **(en)** Robert Hinden, « Simple Internet Protocol Plus White Paper (https://tools.ietf.org/html/rfc1710) », Request for Comments n° 1710, octobre 1994.
17. IANA IP Version Numbers Registry (http://www.iana.org/assignments/version-numbers/version-numbers.xml#version-numbers-1), IANA
18. **(en)** L. Delgrossi et L. Berger, « Internet Stream Protocol Version 2 (ST2) (https://tools.ietf.org/html/rfc1819) », Request for Comments n° 1819, août 1995.
19. **(en)** Robert Hinden, Steve Deering, « Internet Protocol, Version 6 (IPv6) Specification (https://tools.ietf.org/html/rfc1883) », Request for Comments n° 1883, décembre 1995.
20. **(en)** Robert Hinden, Steve Deering, « Internet Protocol, Version 6 (IPv6) Specification (https://tools.ietf.org/html/rfc2460) », Request for Comments n° 2460, décembre 1998.
21. *« 96 More Bits, No Magic. »* Gaurab Upadhaya.
22. **(en)** « Reasons to Move the Network Address Translator - Protocol Translator (NAT-PT) to Historic Status (https://tools.ietf.org/html/rfc2373) », Request for Comments n° 2373, juillet 2007.
23. **(en)** « A Recommendation for IPv6 Address Text Representation (https://tools.ietf.org/html/rfc5952) », Request for Comments n° 5952, août 2010.
24. On note que, en termes d'adressage IPv4, 127.0.0.0/8 forme la plage des adresses possibles de boucle locale. Cela représente 2^{24}-2 adresses potentielles de cette nature en IPv4 contre « une seule » en IPv6.
25. **(en)** « IPv6 Address Prefix Reserved for Documentation (https://tools.ietf.org/html/rfc3849) », Request for Comments n° 3849, juillet 2004.
26. **(en)** R. Hinden, S. Deering, « IP Version 6 Addressing Architecture (https://tools.ietf.org/html/rfc4291) », Request for Comments n° 4291, février 2006.
27. **(en)** M. Kohno, B. Nitzan, R. Bush, Y Matsuzaki, L. Colitti, T Narten, « Using 127-Bit IPv6 Prefixes on Inter-Router Links (https://tools.ietf.org/html/rfc6164) », Request for Comments n° 6164, avril 2011.
28. **(en)** « Analysis of the 64-bit Boundary in IPv6 Addressing (https://tools.ietf.org/html/rfc7421) », Request for Comments n° 7421, janvier 2015.
29. **(en)** « IPv6 Scoped Address Architecture (https://tools.ietf.org/html/rfc4007) », Request for Comments n° 4007, mars 2005.
30. IPv6 Global Unicast Address Assignments (http://www.iana.org/assignments/ipv6-unicast-address-assignments/ipv6-unicast-address-assignments.xml), IANA
31. **(en)** T. Narten, G. Huston, L. Roberts, « IPv6 Address Assignment to End Sites (https://tools.ietf.org/html/rfc6177) », Request for Comments n° 6177, mars 2011.
32. La taille fixe de bloc /48 était autrefois considérée comme standard par la RFC 3177, la politique concernant les tailles des blocs à assigner à l'utilisateur final est désormais laissée à l'appréciation du RIR.
33. **(en)** « INTERNET PROTOCOL (https://tools.ietf.org/html/rfc791) », Request for Comments n° 791, septembre 1981.
34. **(en)** « If unchecked, IPv6 extension headers may affect router performance » (http://searchenterprisewan.techtarget.com/feature/If-unchecked-IPv6-extension-headers-may-affect-router-performance) sur *TechTarget*, août 2011
35. **(en)** « IPv6 Extension Headers Review and Considerations [IP version 6 (IPv6)] » (https://www.cisco.com/en/US/technologies/tk648/tk872/technologies_white_paper0900aecd8054d37d.html), sur *Cisco* (consulté le 12 mars 2018)
36. **(en)** Narten, Thomas et Simpson, William Allen, « Neighbor Discovery for IP version 6 (IPv6) » (https://tools.ietf.org/html/rfc4861) sur *tools.ietf.org* (consulté le 12 mars 2018)
37. **(en)** Mohacsi, Janos et Davies, Elwyn B., « Recommendations for Filtering ICMPv6 Messages in Firewalls » (https://tools.ietf.org/html/rfc4890) sur *tools.ietf.org* (consulté le 12 mars 2018)
38. **(en-US)** « The network nightmare that ate my week », *Occasionally Coherent*, 6 septembre 2014 (lire en ligne (https://blog.bimajority.org/2014/09/05/the-network-nightmare-that-ate-my-week/) consulté le 12 mars 2018)
39. RFC 791, p. 24, la RFC précise qu'un hôte doit être capable de recevoir un paquet réassemblé de 576 octets
40. **(en)** « IPv6 Jumbograms (https://tools.ietf.org/html/rfc2675) », Request for Comments n° 2675, août 1999.
41. **(en)** Request for Comments n° 2460 (https://tools.ietf.org/html/rfc2460)
42. **(en)** Request for Comments n° 2675 (https://tools.ietf.org/html/rfc2675)
43. **(en)** Request for Comments n° 3775 (https://tools.ietf.org/html/rfc3775)
44. **(en)** Request for Comments n° 5095 (https://tools.ietf.org/html/rfc5095)
45. **(en)** Request for Comments n° 4302 (https://tools.ietf.org/html/rfc4302)
46. **(en)** Request for Comments n° 4303 (https://tools.ietf.org/html/rfc4303)
47. **(en)** Assigned Internet Protocol Numbers (http://www.iana.org/assignments/protocol-numbers/protocol-numbers.xhtml)
48. **(en)** Request for Comments n° 4861 (https://tools.ietf.org/html/rfc4861)
49. **(en)** Request for Comments n° 5006 (https://tools.ietf.org/html/rfc5006)
50. **(en)** Request for Comments n° 4862 (https://tools.ietf.org/html/rfc4862)
51. **(en)** Request for Comments n° 4941 (https://tools.ietf.org/html/rfc4941)
52. **(en)** Request for Comments n° 3972 (https://tools.ietf.org/html/rfc3972)
53. **(en)** Request for Comments n° 3315 (https://tools.ietf.org/html/rfc3315)
54. articles 16 et 17 de la directive générale 95/46 *Les risques majeurs de IPv6 pour la protection des données à caractère personnel (http://www.droit-technologie.org/dossier-57/les-risques-majeurs-de-ipv6-pour-la-protection-des-donnees-a-caractere.html)*
55. **(en)** Request for Comments n° 988 (https://tools.ietf.org/html/rfc988)
56. **(en)** Request for Comments n° 3306 (https://tools.ietf.org/html/rfc3306)
57. **(en)** Request for Comments n° 3956 (https://tools.ietf.org/html/rfc3956)
58. **(en)** Request for Comments n° 3596 (https://tools.ietf.org/html/rfc3596)
59. **(en)** Request for Comments n° 2673 (https://tools.ietf.org/html/rfc2673)
60. **(en)** Request for Comments n° 2874 (https://tools.ietf.org/html/rfc2874)
61. **(en)** Request for Comments n° 3363 (https://tools.ietf.org/html/rfc3363)
62. **(en)** Request for Comments n° 6563 (https://tools.ietf.org/html/rfc6563)
63. **(en)** RFC 5902 : IAB Thoughts on IPv6 Network Address Translation
64. **(en)** SixXS (https://www.sixxs.net)
65. **(en)** Hurricane Electric Free IPv6 Tunnel Broker (http://tunnelbroker.net/)
66. **(en)** Request for Comments n° 4213 (https://tools.ietf.org/html/rfc4213)
67. **(en)** AYIYA: Anything In Anything (http://tools.ietf.org/html/draft-massar-v6ops-ayiya-02), Internet Draft, 2004
68. **(en)** Request for Comments n° 5572 (https://tools.ietf.org/html/rfc5572)
69. **(en)** Request for Comments n° 3056 (https://tools.ietf.org/html/rfc3056)
70. **(en)** Request for Comments n° 5569 (https://tools.ietf.org/html/rfc5569)
71. **(en)** Request for Comments n° 2529 (https://tools.ietf.org/html/rfc2529)
72. **(en)** Request for Comments n° 5214 (https://tools.ietf.org/html/rfc5214)
73. **(en)** Request for Comments n° 4380 (https://tools.ietf.org/html/rfc4380)
74. miredo (http://www.remlab.net/miredo/)
75. **(en)** Request for Comments n° 2766 (https://tools.ietf.org/html/rfc2766)
76. **(en)** Request for Comments n° 4966 (https://tools.ietf.org/html/rfc4966)
77. *Provider Independent (PI) IPv6 Assignments for End User Organisations (http://www.ripe.net/ripe/policies/proposals/2006-01.html)* 2009
78. **(en)** Request for Comments n° 5533 (https://tools.ietf.org/html/rfc5533)
79. **(en)** Request for Comments n° 4423 (https://tools.ietf.org/html/rfc4423)
80. **(en)** Request for Comments n° 5102 (https://tools.ietf.org/html/rfc5102)

81. **(en)** GSE - An Alternate Addressing Architecture for IPv6 (http://tools.ietf.org/html/draft-ietf-ipngwg-gseaddr-00) Internet Draft 1997
82. **(en)** Multihoming (http://www.ripe.net/ripe/meetings/ripe-52/presentations/ripe52-multihoming-bof.pdf) présentation RIPE 52 **[PDF]**
83. ocator/ID Separation Protocol (LISP) (http://tools.ietf.org/html/draft-farinacci-lisp-12) Internet Draft, 2009
84. **(en)** Request for Comments n° 6296 (https://tools.ietf.org/html/rfc6296)
85. RRG (http://www.irtf.org/charter?gtype=rg&group=rrg) « Copie archivée » (https://web.archive.org/web/20060812095706/http://www.irtf.org/charter?gtype=rg&group=rrg) (*version du 12 août 2006 sur Internet Archive*)
86. Internet Addressing: Measuring deployment of IPv6 (http://www.oecd.org/dataoecd/48/51/44953210.pdf), OCDE, avril 2010 **[PDF]**
87. **(en)** Next-generation IPv6 Address Added to the Internet's Root DNS Zone (http://www.icann.org/en/announcements/announcement-20jul04.htm) - ICANN, 20 juillet 2004
88. L'ICANN commence à convertir les serveurs DNS à l'IPv6 (http://www.zdnet.fr/actualites/l-icann-commence-a-convertir-les-serveurs-dns-a-l-ipv6-39378221.htm)
89. **(en)** *Hurricane Electric Statistics (http://ipv6.he.net/statistics/)*
90. **(en)** Which DNS Registrars allow me to add AAAA glue for my Domain Name Servers? (http://www.sixxs.net/faq/dns/?faq=ipv6glue) - Sixxs.net
91. **(en)** Request for Comments n° 1035 (https://tools.ietf.org/html/rfc1035)
92. **(en)** Request for Comments n° 2671 (https://tools.ietf.org/html/rfc2671)
93. **(en)** Request for Comments n° 2545 (https://tools.ietf.org/html/rfc2545)
94. **(en)** Request for Comments n° 5340 (https://tools.ietf.org/html/rfc5340)
95. **(en)** Request for Comments n° 5308 (https://tools.ietf.org/html/rfc5308)
96. **(en)** Request for Comments n° 4798 (https://tools.ietf.org/html/rfc4798)
97. **(en)** Request for Comments n° 2464 (https://tools.ietf.org/html/rfc2464)
98. **(en)** DOCSIS 2.0 Interface (http://www.cablemodem.com/specifications/specifications20.html)
99. **(en)** Request for Comments n° 2472 (https://tools.ietf.org/html/rfc2472)
100. **(en)** Request for Comments n° 2767 (https://tools.ietf.org/html/rfc2767)
101. **(en)** Request for Comments n° 3338 (https://tools.ietf.org/html/rfc3338)
102. **(en)** Peter Bieringer & all, « Current Status of IPv6 Support for Networking Applications » (https://www.deepspace6.net/docs/ipv6_status_page_apps.html), 11 février 2017
103. communiqué de presse free (Iliad) (http://www.iliad.fr/presse/2007/CP_IPv6_121207.pdf) **[PDF]**
104. **(en)** IPv6 @ free, native IPv6 to the user (http://ripe58.ripe.net/content/presentations/ipv6-free.pdf) **[PDF]**
105. forum.sfr.fr (http://forum.sfr.fr/c144-2-questions-techniques/f32-materiel/f126-neufbox-de-sfr-et-modem-routeur/t462529-vous-avez-des-questions-sur-l-ipv6-topic-de-centralisation.htm)
106. newsroom.cisco.com (http://newsroom.cisco.com/press-release-content?type=webcontent&articleId=358080)
107. *pcinpact*, Présentation du protocole et des zones qui devrait être couverte d'ici fin 2012 (http://www.pcinpact.com/news/65084-numericable-reseau-fttla-montee-debit.htm,)
108. **(en)** Request for Comments n° 3633 (https://tools.ietf.org/html/rfc3633)
109. http://www.ovh.fr/adsl/fiche_technique_no_tv.xml
110. « Le déploiement de l'IPv6 démarre chez Orange ! » (https://communaute.orange.fr/t5/Orange-et-Vous/Le-d%25C3%25A9ploiement-de-l-IPv6-d%25C3%25A9marre-chez-Orange/ba-p/857401) 4 février 2016 (consulté le 1er juillet 2016)
111. http://abonnez-vous.orange.fr/residentiel/equipements/Livebox.aspx
112. https://lafibre.info/bbox-les-news/ipv6-chez-bouygues/msg382659/#msg382659
113. [1] (https://lafibre.info/bbox-les-news/ipv6-chez-bouygues/msg382679/#msg382679)
114. [2] (https://lafibre.info/bbox-les-news/ipv6-chez-bouygues/msg386216/#msg386216)
115. https://twitter.com/QuanticTelecom/status/310469921143474688
116. Swisscom Labs IPv6 Trial (http://labs.swisscom.ch/fr/node/692/)
117. RIPE 59, Stratégie IPv6 de France Télécom (http://ripe59.ripe.net/presentations/jacquenet-france-telecom-v6.pdf) **[PDF]**
118. **(en)** 6INIT (http://www.ec.ipv6tf.org/index.php?page=news/newsroom&id=23&id_others=64)
119. Plan d'action pour le déploiement d'IPv6 en Europe (http://ec.europa.eu/information_society/newsroom/cf/document.cfm?action=display&doc_id=479)
120. Ghost Route Hunter : IPv6 DFP visibility (http://www.sixxs.net/tools/grh/dfp/)
121. **(en)** IPv6 Ripeness (http://labs.ripe.net/content/ipv6-ripeness) - RIPE
122. IPv6 ripeness country pie charts (http://ipv6ripeness.ripe.net/pies.html)
123. « OECD Communications Outlook 2013 » (https://books.google.fr/books?id=MRQMAAAAQBAJ&pg=PA146&lpg=PA146#v=onepage&q&f=false)
124. **(en)** Request for Comments n° 2471 (https://tools.ietf.org/html/rfc2471)
125. « Liste des pTLA 6bone » (http://www.go6.net/ipv6-6bone/6bone_pTLA_list.html)
126. **(en)** Request for Comments n° 3701 (https://tools.ietf.org/html/rfc3701)
127. **(en)** « Sixy.ch » (http://sixy.ch/)
128. **(en)** « Google over IPv6. » (http://www.google.com/intl/en/ipv6/)
129. **(en)** « Comcast open for IPv6 business, juin 2009 » (http://www.networkworld.com/news/2009/061809-comcast-ipv6.html?hpg1=bn) Networkworld.com
130. **(en)** « LTE devices must support IPv6, says Verizon, *juin 2009* » (http://www.networkworld.com/news/2009/061009-verizon-lte-ipv6.html?fsrc=netflash-rss) *Networkworld.com*
131. **(en)** « U.S. carriers quietly developing IPv6 services, *avril 2008* » (http://www.networkworld.com/news/2008/040208-ipv6-carrier-services.html) *Networkworld.com*
132. **(en)** *NTT Com — IPv6 Global Community — IPv6 Top* (http://www.v6.ntt.net/index_e.html)
133. L'UE encourage l'utilisation du nouveau protocole Internet IPv6 (http://www.french.xinhuanet.com/french/2008-05/28/content_641389.htm) mai 2008
134. Les tests IPv6 de Comcast (http://www.comcast6.net/)
135. http://french.peopledaily.com.cn/Economie/7686884.html
136. http://french.peopledaily.com.cn/Sci-Edu/7688106.html
137. http://www1.cnnic.cn/html/Dir/2012/08/31/6060.htm
138. **(en)** www.personal.psu.edu (http://www.personal.psu.edu/dvm105/blogs/ipv6/2008/04/wikipedias-foray-into-ipv6.html)
139. **(en)** features.techworld.com (http://features.techworld.com/networking/3212045/where-do-web-giants-stand-on-ipv6/)
140. **(en)** www.personal.psu.edu (http://www.personal.psu.edu/dvm105/blogs/ipv6/2008/08/ipv6-going-mainstream-little-b.html)
141. **(en)** http://toolserver.org/~river/pages/projects/ipv6
142. **(en)** http://wikitech.wikimedia.org/view/IPv6_deployment
143. **(en)** meta.wikimedia.org (http://meta.wikimedia.org/wiki/Translation_of_the_week/2012_translations/Archive#en:World_IPv6_Day)
144. http://meta.wikimedia.org/wiki/IPv6_initiative/2012_IPv6_Day_announcement/fr
145. **(en)** http://bugzilla.wikimedia.org/show_bug.cgi?id=35540
146. **(en)** http://blog.wikimedia.org/2012/08/02/engineering-july-2012-report/
147. **(en)** http://www.worldipv6launch.org/participants/?q=1
148. World IPv6 Day (http://isoc.org/wp/worldipv6day)
149. **(en)** World IPv6 day : firing uo engines on the new Internet protocol (http://googleblog.blogspot.com/2011/01/world-ipv6-day-firing-up-engines-on-new.html), Google 21 janvier 2011
150. World IPv6 Day Debrief (http://www.nanog.org/meetings/nanog52/presentations/Monday/Gashinsky-Yahoo_v6d_v5.pdf), Yahoo, NANOG 52, 13 juin 2011 **[PDF]**
151. https://www.legifrance.gouv.fr/affichTexte.do;jsessionid=7E2504406D54E4B63CDEE065E4ABD3A5.tpdila17v_1?cidTexte=JORFTEXT000033202746&categorieLien=id
152. **(en)** IPv6 Transition & Operational Reality (http://www.iepg.org/2007-07-ietf69/070722.v6-op-reality.pdf) - Randy Bush, IEPG / Chicago, juillet 2007 **[PDF]**
153. **(en)** IPv6 dual-stack client loss in Norway (http://fud.no/ipv6/)
154. **(en)** Measuring World IPv6 Day - Some Glitches And Lessons Learned (http://labs.ripe.net/Members/emileaben/measuring-world-ipv6-day-glitches-and-lessons-learned) RIPE NCC, 28 juin 2011
155. **(en)** Peering Disputes Migrate to IPv6 (http://www.datacenterknowledge.com/archives/2009/10/22/peering-disputes-migrate-to-ipv6/) 22 septembre 2009
156. **(en)** A strategy for IPv6 adoption (http://www.ripe.net/ripe/meetings/ripe-57/presentations/Colitti-A_strategy_for_IPv6_adoption.Z8ri.pdf) présentation Google au RIPE 57 **[PDF]**
157. **(en)** IPv6 deployment survey (http://www.ripe.net/ripe/meetings/ripe-59/presentations/botterman-v6-survey.pdf) RIPE 59, juin 2009 **[PDF]**

Exemple

1. Le premier octet de l'adresse 2000::/3 s'écrit en binaire 0010 0000. Le masque /3 implique que seuls les 3 bits de poids forts sont figés. L'adresse haute correspondant à ce préfixe s'écrit ainsi en binaire de la manière suivante : 0011 1111 suivi de 8+7×16 "1" soit 3fff:ffff:ffff:ffff:ffff:ffff:ffff:ffff.

Voir aussi

Articles connexes

- Adresse IP - format des adresses, masques réseaux, CIDR.
- Adresse IPv6 - format d'une adresse IPv6
- Histoire d'IPv6 - l'évolution du protocole
- Transition d'IPv4 vers IPv6 - les technologies permettant à des paquets IPv6 d'être transmis à travers un réseau IPv4

Liens externes

- Association pour la promotion et le développement d'IPv6 (G6)
- Migration IPv6 : enjeux de sécurité - Note d'information du CERTA

Tests et statistiques

- Test de la compatibilité IPv6 d'un site Web
- **(en)** Test de connectivité IPv6
- **(de)** Principaux hôtes disponibles en IPv6 dans le TLD .fr

---