IPV6

Avec l'introduction d'IPv6(1999), le fonctionnement de la communication en réseau change drastiquement. Grâce à l'augmentation de l'espace d'adressage de 32 à 128 bits, ce nouveau protocole permet non seulement de prévenir le risque croissant de ruptures d'adresses, mais aussi de communiquer de manière claire et sans ambiguïté. Contrairement à IPv4(1981), la version 6 applique formellement l'idée de base des IP, le principe de bout en bout. Nous vous expliquons comment.

Norme RFC_2460 IPV6 1999 EN

IPv6, qu'est-ce que c'est ?

IPv6 signifie « Internet Protocol version 6 ». Il a été introduit par l'IETF (Internet Engineering Task Force) et constitue l'un des processus standardisés de transfert de paquets de données sur les réseaux informatiques. Avec les 500 autres protocoles réseaux de la suite TCP/IP, le successeur direct d'IPv4(1981), à savoir IPv6 (IPv5 n'ayant jamais vu le jour), constitue la base de la communication Internet. Parmi les fonctions centrales de IPv6, on compte l'envoi des éléments réseaux aux adresses IPv6 et l'acheminement de paquets entre sous-réseaux, appelé également routage. Pour ce faire, IPv6 est basé sur la couche réseau (Layer 3) du modèle OSI.

L'attribution des adresses IP se fait à partir du registre Internet régional (le RIR), qui répartit les adresses IP par l'intermédiaire de l'autorité IANA (Internet Assigned Numbers Authority). Le RIR compétent pour l'Europe, le Proche-Orient et l'Asie Centrale est le RIPE NCC (Réseaux IP Européens Network Coordination Centre).

IPv6 versus IPv4

Un simple coup d'œil permet déjà de constater que le format d'adresse de la sixième version d'IP est très différent de la version précédente d'IPv4 :

- Adresse IPv4 : 203.0.120.195
- Adresse IPv6 : 2001:0620:0000:0000:0211:24FF:FE80:C12C

Alors que le protocole Internet de la version 4 est codé sur 32 bits et s'écrit sous forme décimale, son successeur IPv6 permet des adresses de 128 bits, qui sont basées sur une écriture hexadécimale pour des raisons de lisibilité. Cette comparaison permet de comprendre nettement que le problème central de IPv4 a été résolu : avec 128 bits, il est maintenant possible de générer bien plus d'adresses IP uniques qu'avec 32 bits.

- Espace d'adressage de IPv4: 32 bits = 232 adresses ≈ 4,3 milliards d'adresses
- Espace d'adressage de IPv6: 128 bits = 2128 adresses ≈ 340 sextillions d'adresses

Les chiffres permettent de constater clairement l'énorme écart entre les deux protocoles : alors que l'espace d'adressage de IPv4, avec près de 4,3 milliards d'IP, est loin de permettre de fournir une adresse unique à chaque individu sur terre, un système à 128 bits pourrait en théorie permettre

d'attribuer plusieurs adresses à chaque grain de sable de notre planète ! L'introduction d'IPv6 permet ainsi d'investir pour le futur. En effet, des tendances comme celles décrites par l'internet des objets (« Internet of Things », IoT) suggèrent que le nombre d'appareils connectés à Internet et qui doivent être clairement identifiés, augmentera de manière significative dans les prochaines années.

Construction d'une adresse IPv6

Les 128 bits des adresses IPv6 sont répartis sur 8 blocs de 16 bits. Un bloc de 16 bits s'écrit avec 4 caractères sous forme hexadécimale (c'est à dire les 10 nombres entiers et 6 lettres de l'alphabet). Pour séparer ces blocs, on utilise les deux-points comme signe de ponctuation. Voici un exemple :

- 2001:0620:0000:0000:0211:24FF:FE80:C12C

Afin de simplifier une adresse IPv6, il est possible de raccourcir l'écriture de l'adresse en supprimant les zéros qui débutent un bloc. Si un bloc est constitué uniquement de zéro, le dernier zéro doit être conservé.

- 2001:0620:0000:0000:0211:24FF:FE80:C12C
- 2001:620:0:0:211:24FF:FE80:C12C

De plus, sur uniquement une partie d'une adresse IPv6, les blocs de zéros qui se suivent peuvent être supprimés :

- 2001:620:0:0:211:24FF:FE80:C12C
- 2001:620::211:24FF:FE80:C12C

Les deux-points qui se suivent (par deux reprises uniquement) permettent de connaître l'emplacement des zéros supprimés (ci-dessus après le deuxième bloc).

Il faut bien comprendre que dans la pratique, les internautes disposent de moins d'adresses que le format 128 bits ne semble l'indiquer. Ceci est dû au principe même sur lequel est conçu le protocole : contrairement à son prédécesseur, le nouveau standard IPv6 doit permettre une connexion de bout en bout réelle et rendre la correspondance des adresses privées aux adresses publiques par le NAT (Network Address Translation) inutile. En principe, il est également possible d'établir des connexions de bout en bout avec IPv4 ; toutefois, comme l'espace d'adressage IPv4 est trop petit pour assigner une adresse unique à chaque appareil, l'intermédiaire NAT a été développé. Avec le nouveau standard, chaque appareil qui est connecté à un réseau local peut maintenant être traité logiquement via sa propre adresse. Les adresses contiennent par conséquent, outre le préfixe de routage, un identifiant d'interface unique, qui est généré manuellement ou à partir de l'adresse MAC de la carte réseau de l'appareil. Le préfixe de routage et l'identifiant d'interface comprennent chacun 64 bits de l'adresse IPv6.

Construction du préfix de routage

Le préfixe de routage d'une adresse IPv6 est divisé en un préfixe réseau et un préfixe sous-réseau. Ceci est représenté dans la notation CIDR (Classless Inter-Domain Routing), c'est-à-dire le routage inter-domaine sans classe. Ainsi, la longueur du préfixe en bits est définie à l'aide du signe slash (/).

La notation 2001:0820:9511::/48 correspond par exemple à un sous-réseau avec une adresse de 2001:0820:9511:0000:0000:0000:0000:0000 à 2001:0820:9511:FFFF:FFFF:FFFF:FFFF:FFFF.

En règle générale, le réseau /32 est attribué par le RIR aux fournisseurs d'accès à Internet (FAI), qui le divise ensuite en sous-réseaux. Pour les clients, ce sont des réseaux /48 ou /56 qui sont octroyés. Le tableau suivant montre la construction classique d'une adresse unicast globale sous IPv6, (préfixe réseau, préfixe sous-réseau et identifiant d'interface) :

Image: Construction du préfix de routage

<table>
<tr><td colspan="2">Préfixe de routage</td><td>Identifiant d'interface (Interface ID)</td></tr>
<tr><td>2001:0620:0000</td><td>:0000</td><td rowspan="3">:0211:24FF:FE80:C12C</td></tr>
<tr><td>Préfixe de réseau / Topologie publique</td><td>Préfixe sous-réseau / Topologie du site</td></tr>
<tr><td>48 bits</td><td>16 bits</td></tr>
<tr><td colspan="2">64 bits</td><td>64 bits</td></tr>
<tr><td colspan="2">Le préfixe caractérise le réseau ou sous-réseau</td><td>L'ID d'interface caractérise un appareil donné avec une carte réseau au sein d'un réseau.</td></tr>
</table>

Construction de l'identifiant d'interface

L'ID d'interface permet l'identification claire d'un appareil donné connecté à un réseau. Il est généré manuellement ou sur la base de l'adresse MAC de la carte réseau de l'appareil. Le second cas est le plus classique. Il repose sur la conversion du format d'adresse MAC standard au format EUI-64 modifié. Cela se déroule en trois étapes :

- Premièrement, l'adresse MAC, longue de 48 bits, est découpée en deux parties longues de 24 bits. Ces parties constituent alors le début et la fin des 64 bits de l'identifiant d'interface complet.
  - Adresse MAC : 00-11-24-80-C1-2C
  - Adresse MAC découpée : 0011:24:80:C12C
- Deuxièmement, les 16 bits restants sont alloués au milieu par défaut avec la suite 1111 1111 1111 1110 qui correspond au code hexadécimal FFFE.
  - Adresse MAC complète : 0011:24FF:FE80:C12C
  - L'adresse MAC est maintenant au format EUI-64 modifié.
- Enfin, le septième bit, appelé également bit universel ou local, est inversé. Cela indique si une adresse est unique globale ou locale.
  - Suite avant l'inversion : 0000 0000
  - Suite après l'inversion : 0000 0010
- ID d'interface avant l'inversion : 0011:24FF:FE80:C12C
- ID d'interface après l'inversion : 0211:24FF:FE80:C12C

Extension de la confidentialité

Une adresse IPv6 qui repose sur un format EUI-64 modifié pourrait permettre à des tiers de tirer des conclusions sur l'adresse MAC. Ceci pouvant générer quelques craintes de la part des utilisateurs sur la protection de leurs données, des extensions de confidentialités ont été développées, afin de rendre les ID d'interfaces anonymes également avec IPv6. Le lien entre l'adresse MAC et l'identifiant d'interface est alors rompu. A la place, les extensions de confidentialité génèrent des identifiants d'interface temporaires avec des connexions sortantes plus ou moins établies au hasard. Il est ainsi plus difficile d'en déduire des informations sur l'hôte et d'établir des profils de comportement en se basant sur l'IP. Les types d'adresses IPv6

Comme avec IPv4, les différentes zones de l'adresse d'IPv6 présentent des tâches et propriétés spécifiques. Elles sont spécifiées dans la RFC 4291 et RFC 5156 et sont identifiables déjà par les premiers bits d'une adresse IPv6, ce que l'on appelle le préfixe. Parmi les principaux types d'adresse, on compte les adresses unicast, les adresses multicast et les adresses anycast.

Adresses unicast

Les adresses unicast sont utilisées pour faire communiquer un élément réseau à un seul autre élément. Elles se divisent en deux catégories : les adresses lien-local et les adresses unicast globales.

- Les adresses lien-local : les adresses de cette catégorie ne sont valides qu'au sein d'un réseau local. Elles commencent par le préfixe FE80::/10. Les adresses de type lien-local sont utilisées pour traiter des éléments au sein d'un réseau local et servent par exemple à l'auto-configuration. En règle générale, l'adresse de lien-local s'étend jusqu'au routeur suivant, afin que chaque appareil connecté au réseau puisse être en mesure de communiquer avec lui, et générer une adresse IPv6 globale. Ce protocole est nommé Neighbor Discovery.
- Les adresses unicast globales : il s'agit d'adresses uniques au monde dont un appareil réseau a besoin pour établir une connexion à internet. Le préfixe est généralement 2000::/3 et englobe ainsi toutes les adresses qui commencent par 2000 jusqu'à 3FFF. L'adresse unicast globale est « routable » et s'utilise pour traiter un hôte d'un réseau local sur Internet. Les adresses globales unicast qui sont redistribuées par un fournisseur Internet à ses clients, commencent par le bloc hexadécimal 2001.

Les adresses multicast

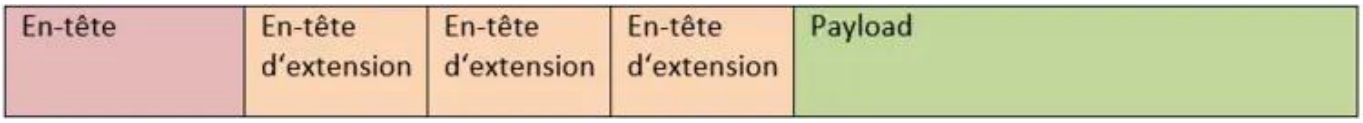
Alors que les adresses unicast servent à établir une communication point à point, les adresses multicast permettent une communication d'un élément vers plusieurs. On parle de diffusion multipoint ou de diffusion de groupe. Les paquets qui sont envoyés à une adresse multicast, sont reçus par l'ensemble des appareils réseau qui font partie du groupe multicast. Un appareil peut appartenir à plusieurs groupes multicast. Si une adresse IPv6 est établie pour un appareil réseau, il devient automatiquement membre d'un groupe multicast donné, ce qui est nécessaire pour la reconnaissance, l'accessibilité mais aussi le préfixe. Des exemples de groupes multicast classiques : « tous les routeurs » ou « tous les hôtes ». En général, le préfixe FF00::/8 est appliqué pour les adresses multicast.

Adresses anycast

Les paquets peuvent également être envoyés à des groupes depuis une adresse anycast. Contrairement aux adresses multicast toutefois, les paquets de données ne sont pas envoyés à tous les membres du groupe anycast mais seulement à l'appareil le plus proche. Les adresses anycast sont principalement utilisées pour permettre une répartition des charges et pour des raisons de sécurité. Format du paquet IPv6

Le protocole Internet IPv6 se distingue d'IPv4 par un format de paquet simplifié. Pour simplifier le traitement des paquets d'IPv6, une longueur standard de 40 bytes (320 bits) a été définie pour l'en-tête. Les informations optionnelles, qui ne sont nécessaires que pour des cas spécifiques, se retrouvent dans ce que l'on nomme les en-têtes d'extension, qui sont insérées entre l'en-tête et le payload. Cela permet d'insérer des options sans avoir à modifier l'en-tête.

Image: Format du paquet IPv6



L'en-tête de paquet IPv6 ne comporte que 8 champs en-têtes. Avec IPv4, il s'agissait de 13 champs. La construction d'un en-tête IPv6 peut être représentée de manière schématique comme ci-dessous :

Image: paquet IPv6

Chaque champ des en-têtes IPv6 comporte des informations précises, qui sont nécessaires au transfert des paquets sur le réseau IP :

Champs	Description
Version	Contient la version du protocole IP selon laquelle le paquet IP a été créé.
Classe de trafic (traffic class)	Définit les priorités (8 bits)
Identificateur de flux (flow label)	Les paquets avec le même identificateur de flux sont traités de la même manière (20 bits)
Longueur des données utiles (payload length)	Donne la longueur du contenu du paquet, y compris les extensions mais sans les données d'en-tête (16 bits)
En-tête suivant (next header)	Indique le protocole de la couche de transport supérieure (8 bits)
Sauts maximum (hop limit)	Indique le nombre de sauts maximal pour les étapes intermédiaires (routeurs), sur lesquelles un paquet peut passer avant d'expirer (8 bits)
Adresse IP source (Source IP address)	Comprend l'adresse de l'expéditeur (128 bits)
Adresse IP destination (destination IP address)	Comprend l'adresse du destinataire (128 bits)

Grâce à l'introduction des en-têtes d'extension, les informations optionnelles des paquets IPv6 peuvent être mise en place de manière bien plus efficace qu'avec IPv4. Comme les routeurs ne vérifient et ne traitent pas les en-têtes d'extension IPv6 à l'envoi d'un paquet, ces dernières ne sont en générale traitées qu'à destination. La performance des routeurs a donc été considérablement améliorée depuis IPv6, car sous IPv4, les informations optionnelles devaient être vérifiées tout au long du chemin. Parmi les informations qui peuvent inclure les en-têtes d'extension IPv6, on trouve les options node-to-node, les options de destination, de routage, de fragmentations, d'authentification et de chiffrement (IPsec).

Les fonctionnalités du protocole Internet version 6

La plupart des internautes sont connectés à IPv6 du fait de son large espace d'adressage. Pourtant, le nouveau standard offre également un certain nombre de fonctions qui permettent de pallier les limites majeures d'IPv4. Il s'agit tout particulièrement de la mise en place du chiffrement de bout en bout, qui rend le détour par NAT superflu et qui simplifie de manière significative l'implémentation des protocoles de sécurité comme IPsec.

De plus, IPv6 permet la configuration automatique d'adresse via Neighbor Discovery ainsi que l'attribution de plusieurs adresses IPv6 uniques par hôte de champs d'application différents, pour rendre compte de différentes topologies de réseau. Par ailleurs, on compte dans ses avantages la simplification des en-têtes de paquet et le transfert des informations optionnelles aux extensions d'en-tête pour l'envoi des paquets pour un routage plus rapide.

Avec QoS (Quality of service), IPv6 dispose d'un mécanisme intégré pour la sécurisation de la qualité des services, qui permet de prioriser les paquets urgents et de gérer avec plus d'efficacité le traitement des paquets de données. Les champs « Classe de trafic » et « Identificateur de flux » ont ainsi été définis selon la méthodologie QoS.

Plus critique par contre : l'attribution d'adresses IP statiques à des appareils réseaux locaux ainsi que la pratique de créer des identifiants d'interface uniques basés sur les adresses MAC. Les extensions de confidentialité offrent certes une alternative au format d'adresse EUI-64 modifié ; toutefois, le préfixe d'une adresse IPv6 étant finalement suffisant pour dresser un profil de comportement d'un internaute, il serait souhaitable d'ajouter aux extensions de confidentialité un préfixe assigné par le FAI pour assurer l'anonymat sur Internet.

Autres Doc IPV6

Doc1 IPV6

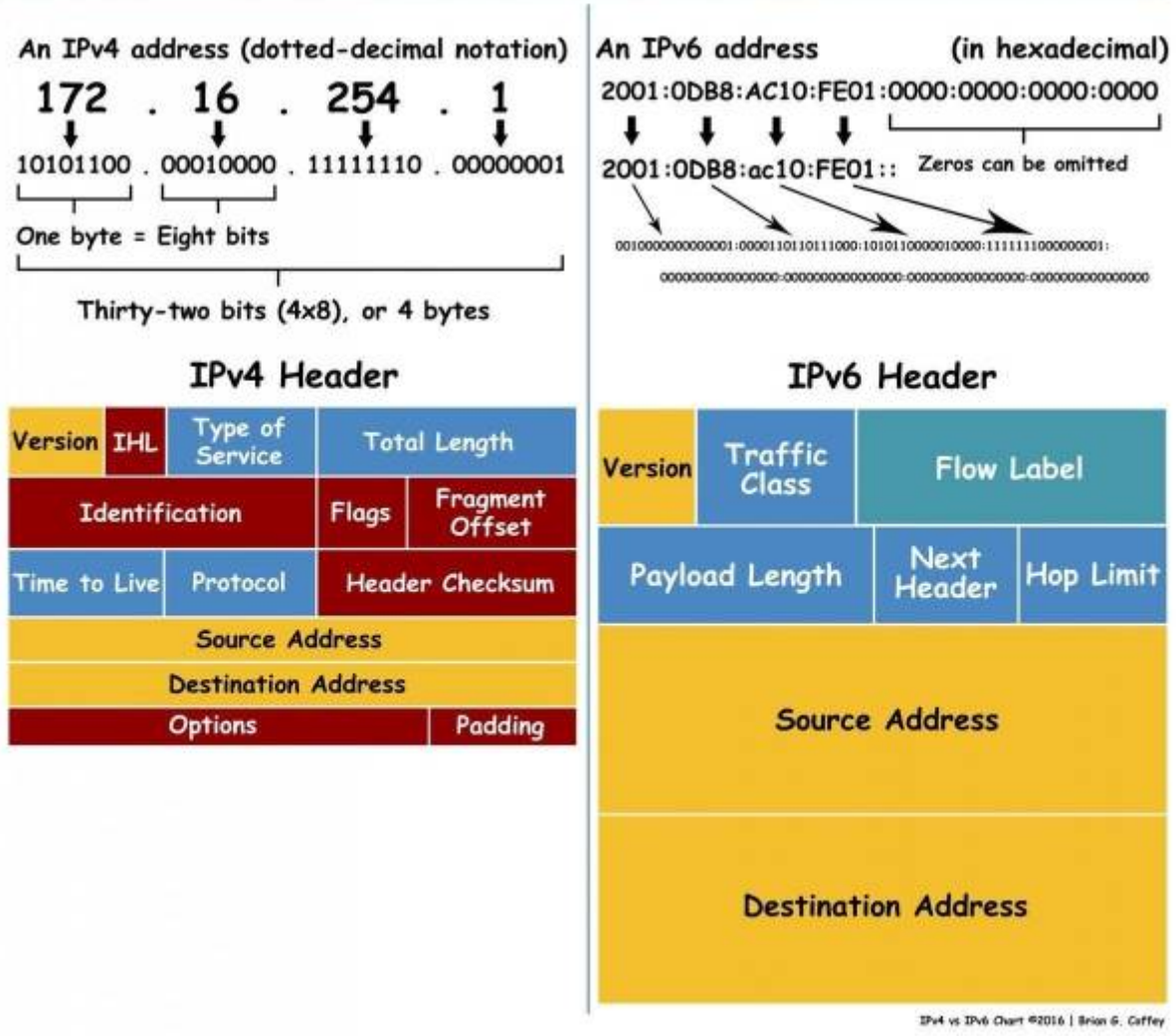
Livre IPV6 G6 FR

Cours IBM : Protocol IPV6 FR

Difference entre IPV4 et IPV6

IPv4 vs IPv6 Chart

	Internet Protocol version 4 (IPv4)	Internet Protocol version 6 (IPv6)
Deployed	1981	1999
Address Size	32-bit number	128-bit number
Address Format	Dotted Decimal Notation: 192.149.252.76	Hexadecimal Notation: 3FFE:F200:0234:AB00: 0123:4567:8901:ABCD
Profix Notation	192.149.0.0./24	3FFE:F200:0234::/48
Number of Addresses	2^{32} = ~4,294,967,296	2^{128} = ~340,282,366, 920,938,463,463,374, 607,431,768,211,456



Convertir une @IP en Binaire et inversement

Convertir un nombre décimal en binaire

Dans les nombres binaires, chaque bit successif d'un groupe représente une puissance de deux et les valeurs augmentent de droite à gauche. Ainsi, le bit le plus à droite représente 2^0, le deuxième bit le plus à droite représente 2^1, et ainsi de suite, comme le montre le tableau ci-dessous. Chaque bit successif à gauche représente le double de la valeur. La valeur de chaque chiffre d'un nombre binaire est déterminée par sa position dans le tableau. La somme de toutes ces valeurs de colonne pour chaque chiffre donne la représentation décimale du nombre binaire.

8e bit	7e bit	6e bit	5e bit	4e bit	3e bit	2e bit	1e bit
2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
128	64	32	16	8	4	2	1

Valeurs de chaque bit dans un octet

En utilisant cette logique, nous pouvons facilement calculer la représentation décimale d'un nombre binaire comme 11100011 par exemple. Il nous suffit d'activer les bits respectifs et de calculer la valeur des valeurs décimales.

8e bit (128)	7e bit (64)	6e bit (32)	5e bit (16)	4e bit (8)	3e bit (4)	2e bit (2)	1e bit (1)
1	1	1	0	0	0	1	1

Nombre binaire 11100011

Le tableau ci-dessus montre que les bits ayant les valeurs 128, 64, 32, 2 et 1 sont tous activés. Comme nous l'avons déjà mentionné, calculer la valeur d'un nombre binaire revient à additionner toutes les valeurs des bits « activés ».

8e bit (128)	7e bit (64)	6e bit (32)	5e bit (16)	4e bit (8)	3e bit (4)	2e bit (2)	1e bit (1)
1	1	1	0	0	1	1	1

Ainsi, pour la valeur binaire du tableau, 11100111, nous additionnons 128+64+32+4+2+1 pour obtenir le nombre 231.

Par exemple :

Binaire	Décomposition	Décimal
1100 0000	128+64+0	192
10101000	128+32+8	168
00000001	0*7+1	1
00110010	32+16+2	50

Convertir un nombre binaire en décimal

Voici comment convertir dans l'autre sens. Nous commençons par le nombre décimal que nous

voulons convertir et recherchons la valeur de colonne la plus élevée qui entre dans la décimale. Ensuite, nous soustrayons la valeur de la colonne du nombre original et nous répétons le processus jusqu'à ce que le nombre original devienne zéro.

A partir de là, on peut convertir chaque décimale d'une adresse IP, masque de sous-réseau ou broadcast en binaire. Ainsi :

- La décimale 192 se convertir en binaire par 11000000
- 168 donne 10101000 en binaire