NOTIONS IPV6

Principales caractéristiques d'IPv6
- les adresses IPv6 sont codées sur 128 bits (1 milliard de réseaux).
- le principe des numéros de réseaux et des numéros d'hôtes est maintenu.
- IPv6 est conçu pour interopérer avec les systèmes IPv4 (transition douce prévue sur 20 ans). L'adresse IPv6 peut contenir une adresse IPv4 : on place les 32 bits de IPv4 dans les bits de poids faibles et on ajoute un préfixe de 96 bits (80 bits à 0 suivis de 16 bits à 0 ou 1)
- IPv6 utilise un adressage hiérarchique (identification des différents réseaux de chaque niveau) ce qui permet un routage plus efficace.
- IPv6 est prévu pour les systèmes mobiles : auto-configuration, notion de voisinage (neighbor).
- IPv6 permet l'authentification et le chiffrement dans l'en-tête des paquets, ce qui permet de sécuriser les échanges. En effet IP v.6 intègre IPSec (protocole de création de tunnel IP avec chiffrement), qui garantit un contexte sécurisé par défaut.
- IPv6 intègre la qualité de service : introduction de flux étiquetés (avec des priorités)
- IPv6 prend mieux en charge le trafic en temps réel (garantie sur le délai maximal de transmission de datagrammes sur le réseau).

IPv4

Adresse IPv4 sur 32 bits (4 octets), soit 2^32 adresses, soit 4,3 milliards

2^32 = (1,024 * 2^10) * (1,024 * 2^10) * (1,024 * 2^10) * (2^2) = 1,024^3 * 2^10^3 * 4 = 1,024^3 * 4 2^10^3 = 4,3 * 2^10^3 = 4,3 * 10^3^3 = 4,3 10^9

L'adressage IPv4 ne répond donc plus aux besoins : pas assez au vue du nombre d'humain, pas assez avec l'arrivée des objets connectés.

Cette pénurie d'adresse a été résolue par l'utilisation d'adresses privées et du NAT. Le NAT a été créé pour pallier à cet insuffisance. Le bout en bout, qui était la philosophie d'IPv4 a alors disparu.

IPv6

Adresse IPv6 sur 128 bits (16 octets), soit 2^128 adresses, soit 3,4 10^38 adresses

2^128 = (2^10) ^12 * (2^8) = (2^10) ^12 * (2^10) / 4 = (1,024*10^3)^12 * (1,024*10^3)/4 = 1,024^12 * 10^36 * (1,024*10^2)*10/4 = 1,024^13 * 10^38 * 2,5

= 3,4 10^38

La pénurie d'adresse IPv6 n'est donc pas pour demain. La notion de NAT ne sera plus nécessaire avec IPv6.

Notation des adresses IPv6

Les 128 bits de l'adresse IPv6 sont présentées sous la forme de 8 blocs de 16 bits. Chaque bloc de 16 bits est alors noté sous forme hexadécimal et non décimal comme en IPv4.

Exemple :

En binaire, les 128 bits

00100000 00000001 00001101 10111000 00000000 00000000 00000000 00000000 00000000

00001000 00001000 00000000 00100000 00001100 01000001 01111010

En notation hexadécimal IPv6 :

2001:0db8:0000:0000:0008:0800:200c:417a

En notation compacte :

2001:db8::8:800:200c:417a

Notation des préfixes IPv6

Comme en IPv4, la longueur du préfixe d'une adresse IPv6 permet de connaitre le nombre de bits qui représentent la partie réseau.

Exemple, une adresse IPv6 avec 60 bits pour la partie réseau 2001:db8:24:a1a1:8:800:200C:417a/60

Le réseau correspondant est

2001:db8:24:a1a0::/60

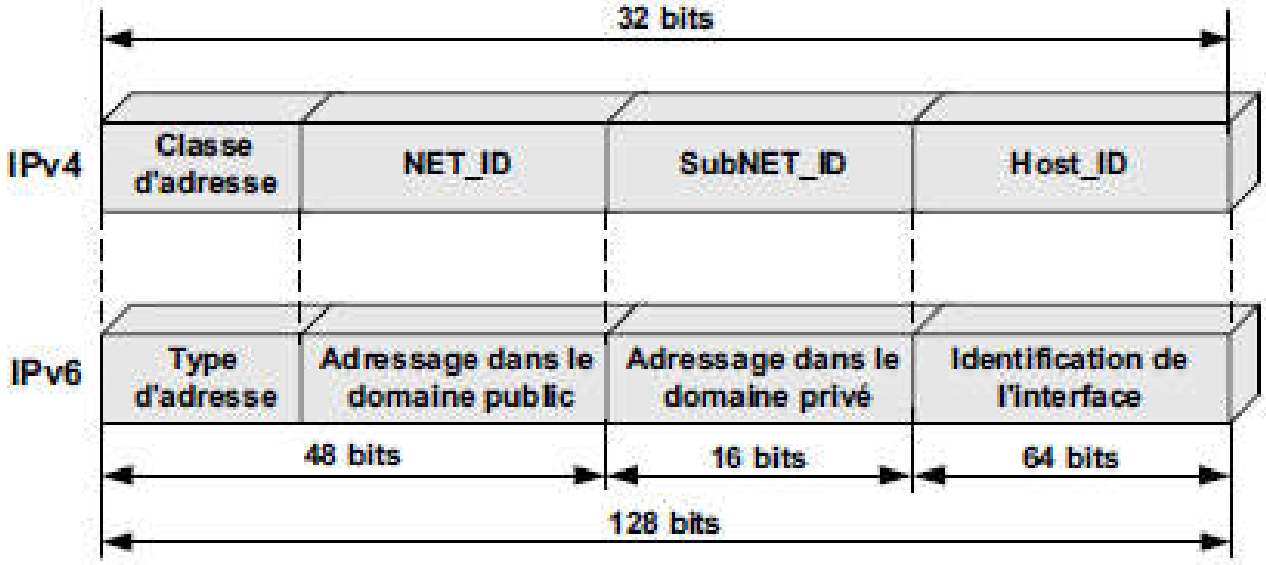
Attention, le dernier 0 de a1a0 ne fait pas partie du réseau, mais il faut le mettre car sinon on pourrait croire que le réseau est 2001:db8:24:0a1a::/60 .

Dans l'exemple, l'adresse IP avait pour ce bit une valeur de 1. On a mis un 0 pour exprimer le réseau d'appartenance de cet IP.

Représentation des Masques de sous-réseaux
Leur notation classique comme en IPV4 est impossible avec 128 bits, c'est donc la notation CIDR, plus simplement appelée notation "slash" qui est utilisée.
Exemple l'adresse fe80::20d:61ff:fe22:3476/64 a un masque de 64 bits , masque par défaut pour une adresse de type lien-local.

Le préfixe de sous-réseau contient toujours 64 bits. Ceux-ci se décomposent en 48 bits pour le préfixe de site et 16 bits pour l'ID de sous-réseau.

Le préfixe de site d'une adresse IPv6 occupe jusqu'à 48 des bits situés complètement à gauche de celle-ci. Par exemple, le préfixe de site de l'adresse IPv6 2001:db8:3c4d:0015:0000:0000:1a2f:1a2b/48 réside dans les 48 bits situés complètement à gauche, soit 2001:db8:3c4d. Vous pouvez représenter ce préfixe de la façon suivante, avec zéros compressés :
2001:db8:3c4d::/48 (48car 16*3 ou [(4*4)*3])



NBD:

Une adresse dont tous les hôtes commencent par
2001:0DB8:BC15:0XXX :XXXX :XXXX :XXXX :XXXX
On part de
2001: 0DB8 :BC15: 0000: 0000: 0000: 0000: 0000
16 16 16 16 16 16 16 16 (8*16 = 128)
4+4+4+4
16+16+16+4 = 52
Il s'agit donc d'un /52

A connaître
• L'adresse de bouclage qui correspond à 127.0.0.1 en IPv4
0000:0000:0000:0000:0000:0000:0000:0001
L'adresse de bouclage ou localhost se note en abrégé :
::1

• L'adresse indéterminée qui correspond à 0.0.0.0 en IPv4.
Elle caractérise l'absence d'adresse. Elle est utilisée lors de certaines phases d'initialisation. C'est une adresse transitoire. Elle se note 0:0:0:0:0:0:0:0 ou ::

Le préfixe 2001:db8::/32 est un préfixe IPv6 spécial utilisé spécifiquement dans les exemples de documentation

Vous pouvez spécifier un préfixe de sous-réseau définissant la topologie interne du réseau vers un routeur.
Le préfixe de sous-réseau de l'exemple d'adresse IPv6 est le suivant.
2001:db8:3c4d:15::/64

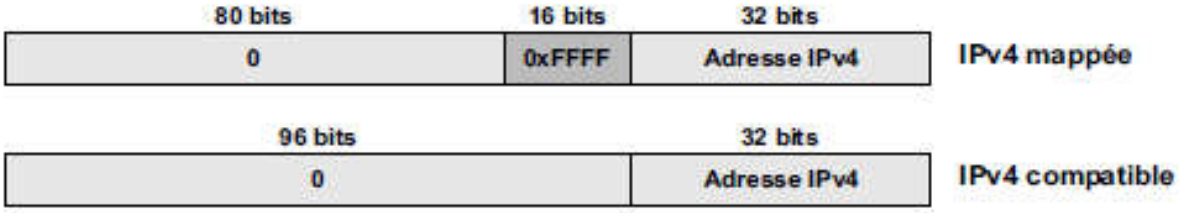
Les préfixes suivants sont réservés à un usage spécial :
2002::/16
Indique qu'un préfixe de routage 6to4 suit.
fe80::/10
Indique qu'une adresse lien-local suit.

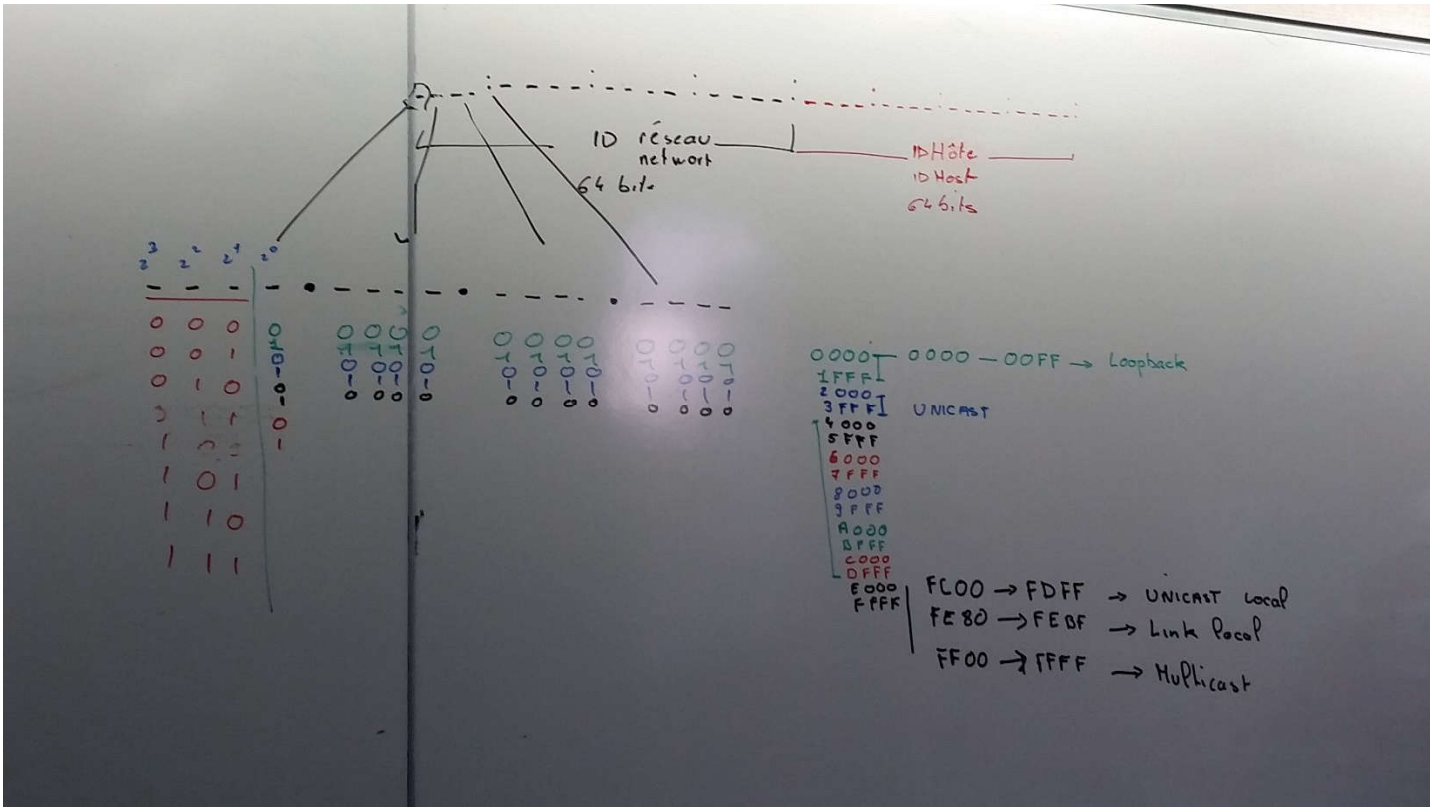
ff00::/8
Indique qu'une adresse multidiffusion suit.

Adresse anicast : type d'adresse au stade expérimental. Comme multicast, désigne un groupe d'adresse, mais la datagramme à destination d'une adresse anycast ne sera pas remis à tous ces membres, mais seulement à un seul.

Toutes ces différents type d'adresse / portée sont identifiables par des préfixes réservés.

Type	Bit de poids forts	Notation hexadécimale	Commentaire
Non spécifié	0...0	::/128	
Adresse de bouclage (loopback)	0...1	::1/128	
Multicast	1111 1111	ff00::/8	
Unique local (ULA)	1111 1101	fd00::/8	Ces adresses ne peuvent sortir sur internet, les fournisseurs d'accès ne doivent pas les router. En principe, c'est fc00::/7 (1111 110). En prenant 1111 1101, on aboutit à fd00::/8 qui est bien un sous ensemble de fc00::/7.
Globale unique (GUA)	001	2000::/3	Comprend donc les adresses commençant par 2 ou 3 : 0011 = 0x3
Adresse 6to4		2002::/16	Adresse utilisée pour des sites IPv6 isolés interconnectés par un réseau IPv4.
Unique lien local (link local address)	1111 1110 10	fe80::/10	





Le type d'adresse IPv6 est indiqué par les premiers bits de l'adresse qui sont appelés le "Préfixe de Format" (Format Prefix). L'allocation initiale de ces préfixes est la suivante :

Allocation	*Préfixe*	*Usage*
Adresses Unicast globales	010	Adresses dont le routage est effectué sans restriction, utilisables sur Internet.
Adresses Unicast expérimentales	001	
Adresses "Lien local"	1111 1110 1000	Adresses d'un même lien physique,obtenues par autoconfiguration
Adresses "Site Local"	1111 1110 1100	Adresses d'un même site
Adresses Multicast	1111 1111	Elles remplacent les adresses "broadcast" d'IPv4

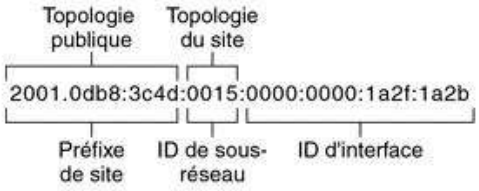
15 % de l'espace d'adressage est actuellement alloué. Les 85% restants sont réservés pour des usages futurs. En réalité sur les 128 bits, seulement 64 sont utilisés pour les hôtes (Interface ID).

• Les adresses unicast :
Elles désignent une et une seule machine.
Elles comportent une partie réseau "préfixe" et une partie hôte "suffixe":
La partie réseau ou préfixe est codée sur 64 bits : les 48 bits publics "Global Routing Prefix" et les 16 bits de site définissant le sous-réseau
La partie hôte ou suffixe est codée aussi sur 64 bits, fabriquée à partir de l'adresse MAC de l'interface, elle permet d'identifier la machine dans un réseau donné.
Prenons par exemple cette adresse fe80::20d:61ff:fe22:3476
fe80:: ,en réalité fe80:0000:0000:0000 correspond au préfixe ou partie réseau
20d:61ff:fe22:3476 correspond au suffixe ou partie hôte

Adresse unicast globale

L'adresse unicast globale est unique au monde sur Internet. L'adresse IPv6 d'exemple figurant à la section Préfixes d'IPv6 constitue une adresse unicast globale. L'illustration suivante représente l'étendue de l'adresse unicast globale, en comparaison avec les parties de l'adresse IPv6.

Figure 3–3 Parties de l'adresse unicast globale



• Les adresses multicast :
Le protocole IPv6 généralise l'utilisation des adresses multicast qui remplacent les adresses de type "broadcast" (diffusion) qui n'existent plus en IPv6. La raison de cette disparition est que l'émission d'un paquet broadcast était très pénalisante pour toutes les machines se trouvant sur un même lien.
Une adresse multicast est une adresse désignant un groupe d'interfaces donné. Une interface est libre de s'abonner à un groupe ou de le quitter à tout moment, c'est donc moins pénalisant qu'en IPv4.
Le format des adresses multicast est le suivant :
ff01 : noeud local, les paquets ne quittent pas l'interface.
ff02 : lien local, les paquets ne quittent pas le lien .
ff05 : site local, les paquets ne quittent pas le site .

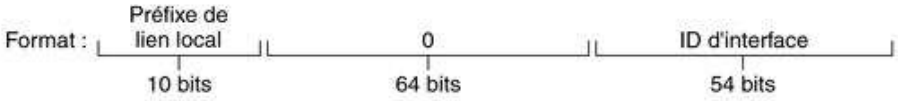
Listes des adresses multicast bien connues

Adresse de multicast	Population concernée
ff01::101	Tous les serveurs NTP de la même interface (c.à.d. le même noeud) que l'émetteur
ff02::101	Tous les serveurs NTP du même lien que l'émetteur
ff05::101	Tous les serveurs NTP du même site que l'émetteur
ff0e::101	Tous les serveurs NTP de l'Internet
ff01::1	Toutes les interfaces du noeud
ff02::1	Toutes les noeuds sur le même lien que l'interface émettrice (correspond au broadcast 255.255.255.225 d'IPv4)
ff01::2	Tous les routeurs du noeud
ff02::2	Tous les routeurs du lien
ff05::2	Tous les routeurs du site
ff02::1:2	Tous les serveurs DHCPv6 et relais DHCPv6

Adresse unicast lien-local

L'adresse unicast lien-local s'utilise exclusivement sur le lien de réseau local. Les adresses lien-local ne sont ni valides ni reconnues en dehors de l'entreprise. L'exemple suivant représente le format de l'adresse lien-local.

Exemple 3–1 Parties de l'adresse unicast lien-local



Exemple : fe80::123e:456d

Le format d'un **préfixe lien-local** est le suivant :

```
fe80:: ID-interface /10
```

L'exemple suivant constitue une adresse lien-local :

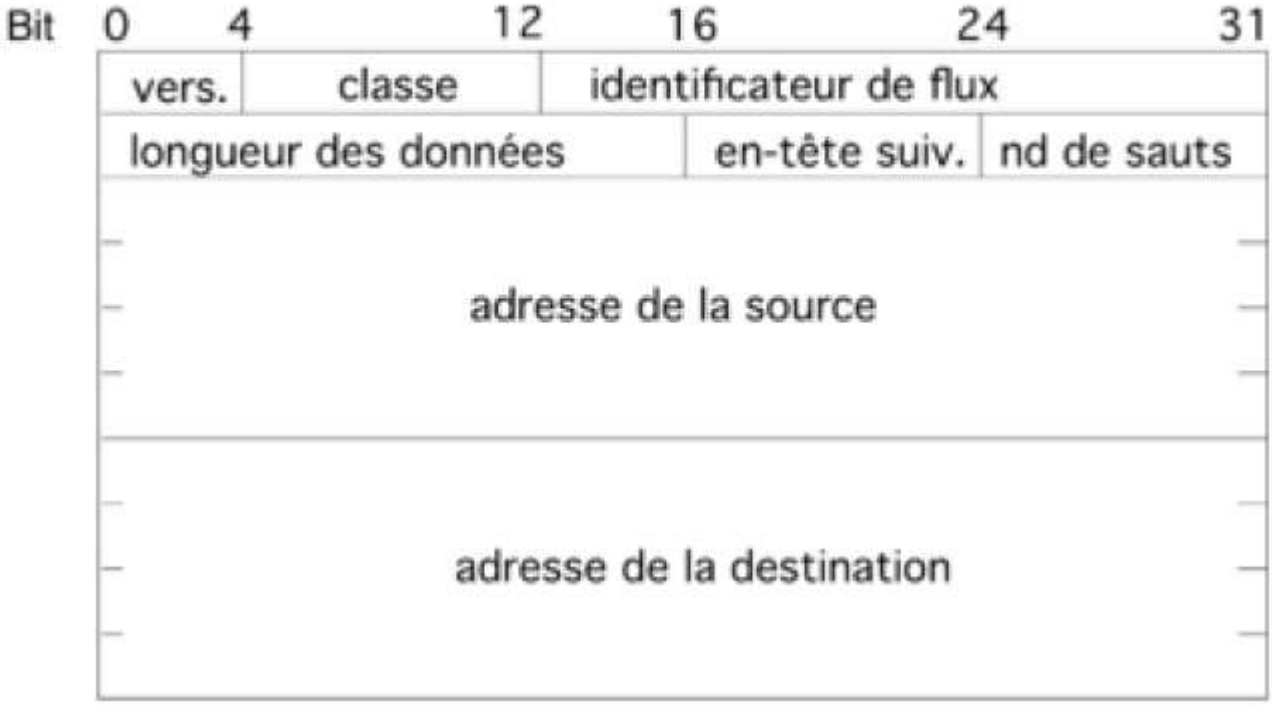
```
fe80::23a1:b152
```

• Les adresses anycast :
Anycast est un nouveau type d'adressage. Il identifie qu'un noeud, parmi un groupe de noeuds, doit recevoir l'information.
Une adresse anycast, comme une adresse multicast, désigne un groupe d'interfaces, à la différence qu'un paquet émis avec comme destinataire une adresse anycast ne sera remis qu'à un seul membre du groupe, par exemple le plus proche au sens de la métrique des protocoles de routage, même si plusieurs interfaces ont répondu au message. L'interface de destination doit spécifiquement être configurée pour savoir qu'elle est anycast.
Pour l'instant, une seule adresse anycast est utilisée, elle est réservée au routeur mais dans l'avenir, d'autres pourraient être définies.

Portée des adresses
La portée ou "scope" des adresses, est une nouvelle notion qui n'existait pas en IPv4.
En fait une interface ne possède pas une seule adresse IPv6 mais peut en avoir plusieurs.
Les quatre portées d'adresses sont :
Noeud-local : il s'agit de l'adresse de loopback . Elle est notée ::1/128.
Lien-local : adressage commun aux machines d'un même lien physique reliées entre elles sans routeur intermédiaire .Ces adresses ont comme préfixe fe80::/64. Seuls les équipements de la couche 2 du modèle OSI peuvent utiliser ces adresses pour communiquer entre eux. Cette adresse est obtenue par autoconfiguration "sans état".
Site-local : adressage commun des machines d'un même site.Par exemple, un site qui n'est pas encore relié à Internet peut utiliser ce type d'adresse. C'est un peu le concept des adresses privées en IPv4 (192.168.x.x ou 10.x.x.x). Une adresse site local a comme préfixe fec0::/48 suivi d'un champ de 16 bits permettant de définir des sous-réseaux.
Globale : ce sont des adresses dont le routage est effectué sans restriction. Leur préfixe est 2000::/3 , ce qui signifie qu'elles commencent par 001 en binaire. Concrètement, on utilise 2xxx ou 3xxx.
Par exemple 2001:7a8:4b09:1bff:feb1:defa est une adresse globale

En-tête IPv6

Ci-dessous la structure de l'en-tête IPv6 :



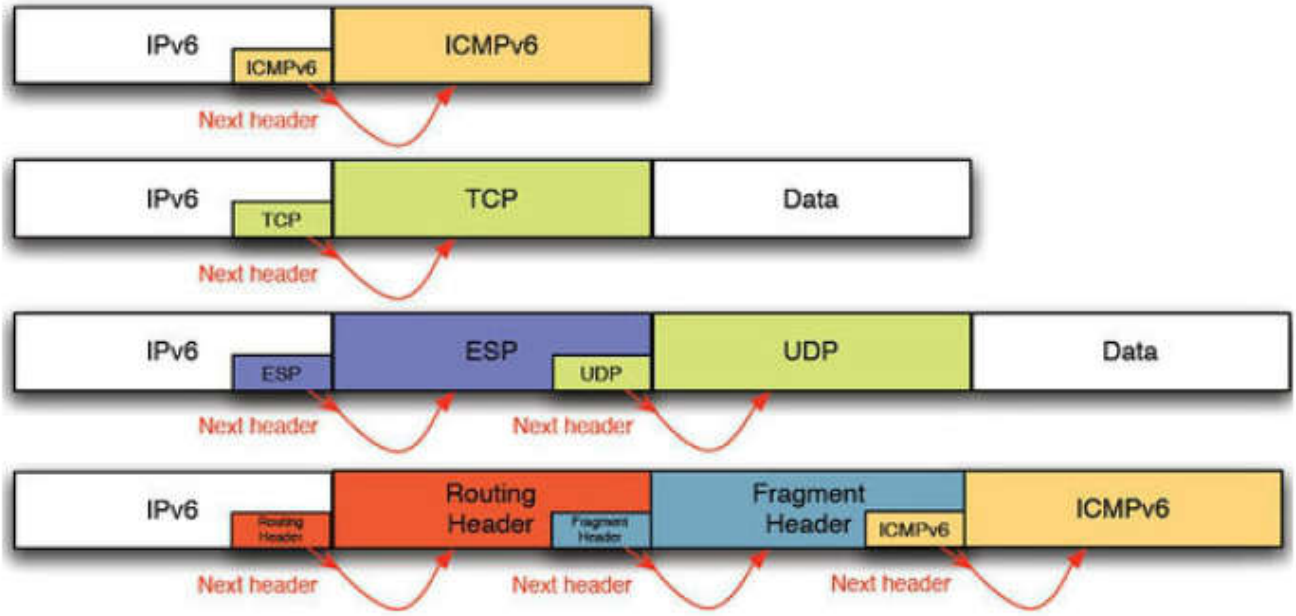
En-tête suivant / Next Header (sur 8 bits) :

permet d'indiquer le contenu du paquet IP : un flux TCP, un flux UDP, ...

Ainsi les valeurs des en-têtes les plus utilisés sont les suivants :

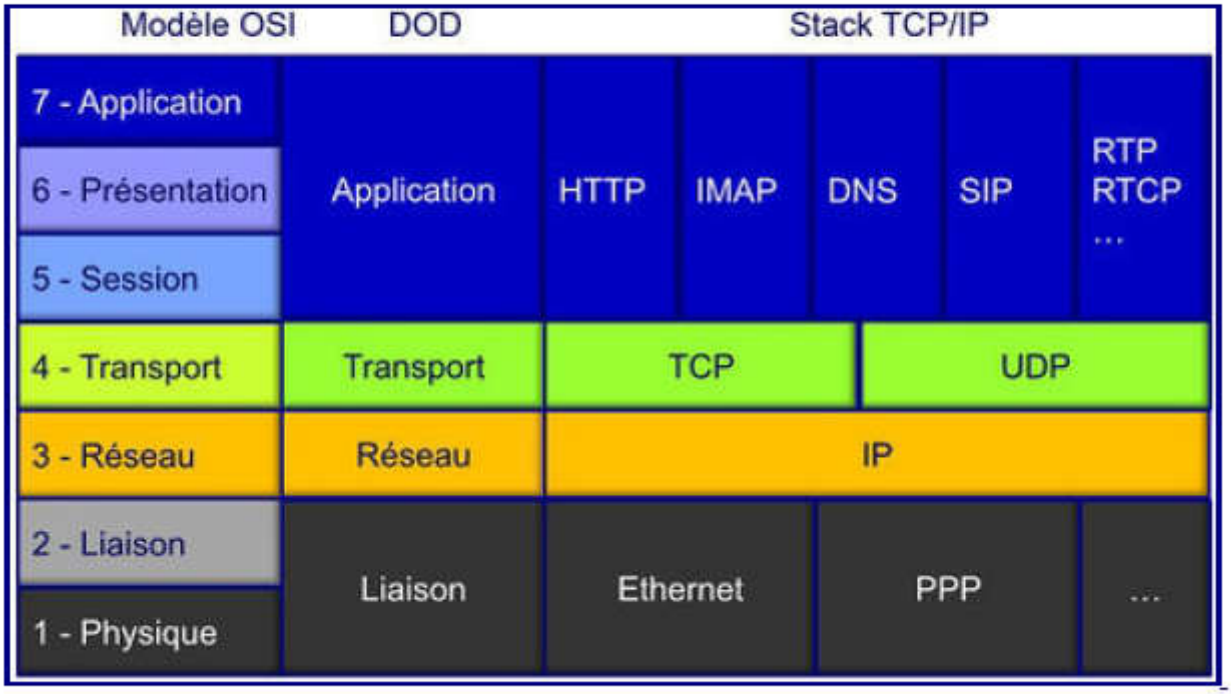
Valeur décimale	Valeur hexadécimale	Protocole
0	0x00	Proche en proche
4	0x04	IPv4
6	0x06	TCP
17	0x11	UDP
41	0x29	IPv6
43	0x2b	Routage
44	0x2c	Fragmentation
50	0x32	Confidentialité
51	0x33	Authentification
58	0x3a	ICMPv6

Ci-dessous divers cas d'extensions IPv6 :



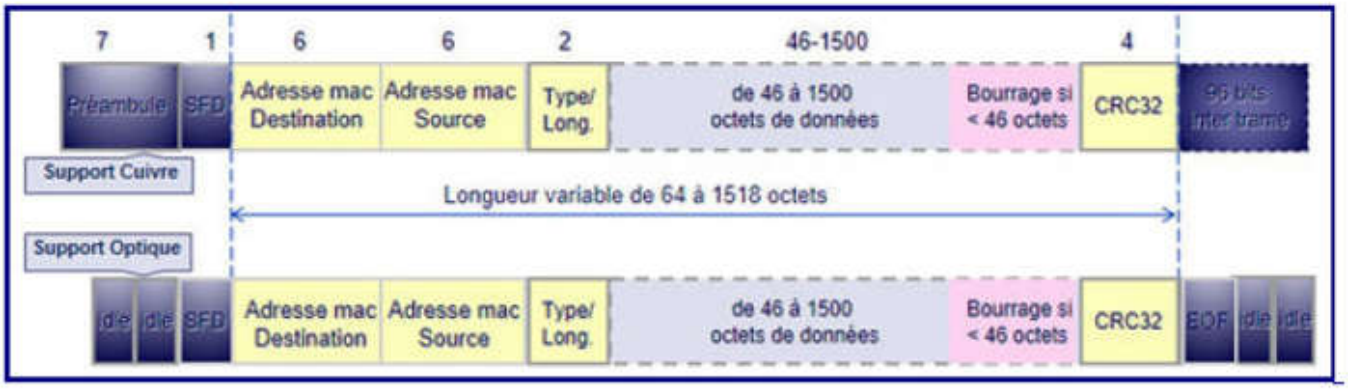
Encapsulation

Ci-dessous un schéma de l'encapsulation :



DOD : Department Of Defense, qui est à l'origine de TCP/IP.

Ci-dessous la trame Ethernet :

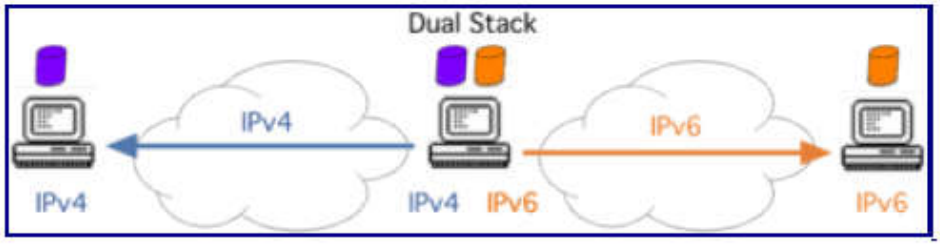


Cette intégration d'IPv6 dans IPv4 nécessite de considérer 6 cas différents :

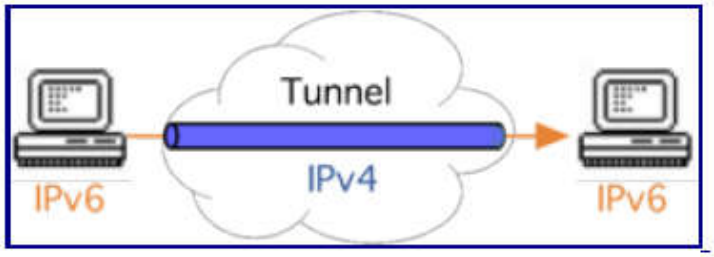
1. Un hôte IPv4 qui communique avec un hôte IPv4 via un réseau IPv4;
2. un hôte IPv6 qui communique avec un hôte IPv6 via un réseau IPv6;
3. un hôte IPv6 qui communique avec un hôte IPv6 via un réseau IPv4;
4. un hôte IPv4 qui communique avec un hôte IPv4 via un réseau IPv6;
5. un client IPv4 qui communique avec un serveur IPv6;
6. un client IPv6 qui communique avec un serveur IPv4.

Le cas 1 est le point de départ IPv4, le cas 2 est le point d'arrivée IPv6.

Pour faire cohabiter le **cas 1 et 2** pour un même hôte travaillant soit en IPv4, soit en IPv6 suivant les applications, cette hôte doit utiliser la **technique de la double pile.**



Pour le cas 3, on utilise la technique du tunnel IPv6 dans IPv4; il faut que ces tunnels traversent le moins de routeurs IPv4 possibles.



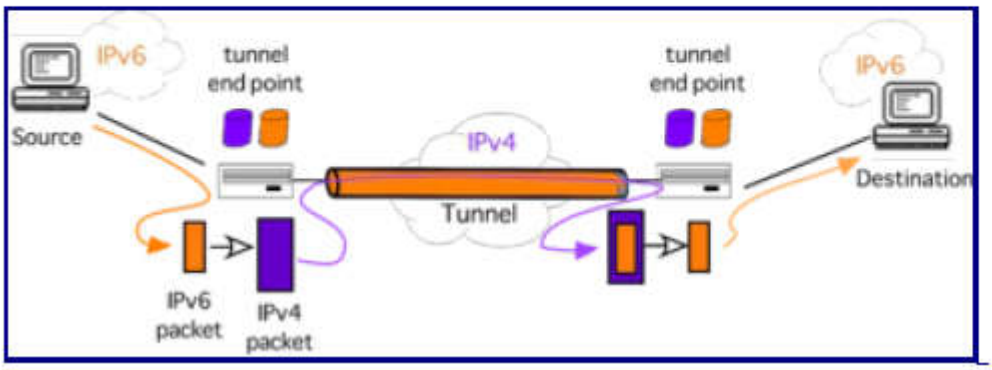
Pour le cas 4, on utilise la technique du tunnel IPv4 dans IPv6.

Pour le cas 5, il faut mettre en place des techniques de traduction.

La démarche de déploiement d'IPv6 est décrite dans la RFC 7381.

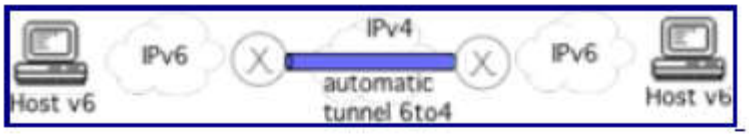
Tunnel IPv6 sur IPv4

Comme le montre le schéma ci-dessous, il faut que le tunnel soit le plus court possible pour obtenir de bonnes performances. Les tunneliers sont, dans cet exemple, des routeurs en double pile.



Tunnel automatique

Des solutions d'automatisation ont été étudiées, qui ont comme principe de contenir l'adresse IPv4 du tunnelier de destination dans l'adresse IPv6. La technique de transition 6to4 décrite par le RFC 3056 suit ce principe. Elle vise à interconnecter entre eux des sites IPv6 isolés en créant des tunnels automatiques IPv6 dans IPv4 en fonction du destinataire des données. La figure ci-dessous montre 2 réseaux IPv6 communiquant entre eux via un tunnel automatique 6to4. Le point fort du mécanisme présenté ici est l'automatisation, où l'intervention de l'administrateur est réduite à une phase de "configuration/initialisation" du service, et non à une phase de configuration des tunnels.



Pour que ce mécanisme soit automatique, il faut que les adresses globales ait un format particulier dit 6to4. Cette adresse contient l'adresse IPv4 du routeur 6to4 permettant d'accéder à l'hôte.

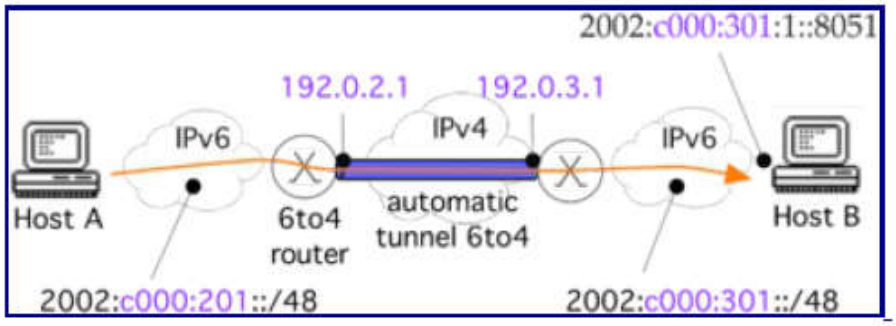
Ainsi, une adresse 6to4 a le format suivant :

Le préfixe est de la forme 2002::/16.

Suit ensuite l'adresse IPv4 du routeur 6to4 qui gère la zone de l'hôte

Ci-dessous l'exemple d'un hôte A IPv6 voulant joindre un hôte B IPv6 via un tunnel IPv4. Ces deux hôtes ont de adresses 6to4, les pattes IPv4 des routeurs 6to4 sont donc connues.

Au niveau du routage, la figure ci-dessous présente l'envoi d'un paquet IPv6 de l'hôte A vers l'hôte B. Il est important de noter ici que A et B sont des hôtes ayant une adresse IPv6 prise dans le plan d'adressage 6to4 . Dans un premier temps, A interroge le DNS pour connaître l'adresse IPv6 de B. Dans notre exemple, la réponse est 2002:c000:301:1::8051 . Dans un second temps, l'hôte A émet le paquet vers cette destination. Ce paquet IPv6, dont l'adresse de destination commence par le préfixe 2002::/16 , doit passer par un tunnel 6to4 . C'est au routeur 6to4 du site de A qu'il revient d'effectuer cette opération. Ainsi, le paquet doit suivre la route IPv6 2002::/16 pour atteindre ce routeur 6to4 . Ce dernier analyse l'adresse IPv6 de destination et trouve l'adresse IPv4 de l'autre extrémité du tunnel (192.0.3.1 dans l'exemple). Il pourra alors effectuer la transmission en encapsulant le paquet IPv6 dans un paquet IPv4. C'est cette encapsulation qui forme le tunnel. Le routeur 6to4 du coté de B désencapsule le paquet Pv6 et le route normalement vers sa destination finale B en utilisant le routage interne.



Cette technique est adaptée à des sites IPv6 isolés non connectés à l'Internet v4.

Cette technique n'est pas adapté si l'adresse IPv6 est prise dans le plan d'adressage globale. De plus, la route aller n'est pas forcément égale à la route retour. Cette technique est déprécié et est remplacé par une technique similaire dite 6rd.

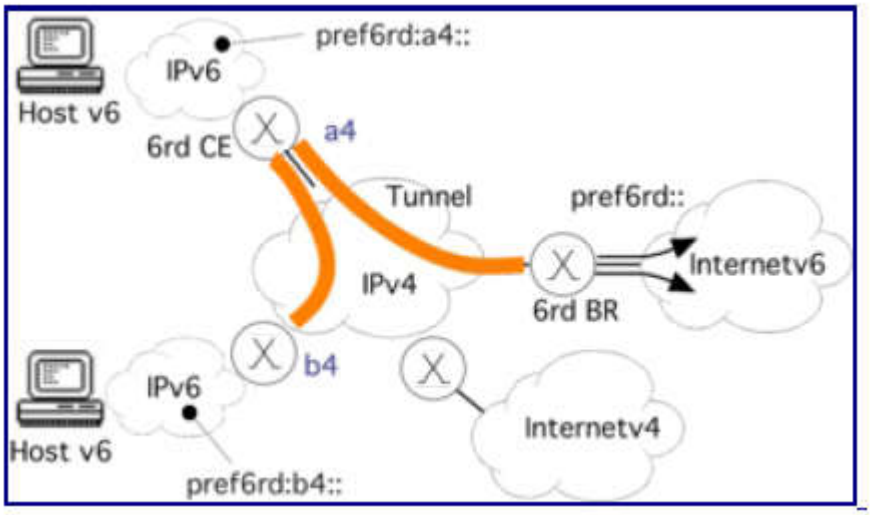
Connectivité d'un site isolé via un tunnel broker

Un intermédiaire, le tunnel broker, crée le tunnel à la demande. Ce mécanisme s'appuie sur un protocole nommé TSP (Tunnel Set Up Protocol).

Tunnel 6rd

Cette solution (imaginée par Free) est destiné à un opérateur pour offrir une connectivité IPv6 alors que son infrastructure repose sur IPv4. Cet opérateur peut être aussi bien public, comme un FAI, ou privé, comme une entreprise ou une administration. Cette solution reprend le principe du 6to4 en ayant supprimé les défauts.

La différence majeure se situe sur l'utilisation du préfixe IPv6 propre à l'opérateur plutôt que le préfixe commun à tous, employé par 6to4 (2002::/16). Il s'ensuit que l'opérateur doit installer ses propres relais pour offrir la connectivité avec l'Internet v6. Le relais est un routeur de bordure équipé en "double pile". Dans la figure 12, qui schématise l'architecture de 6rd , le routeur de bordure est noté, selon la terminologie du RFC 5969 , " 6rd BR"(Border Relays). Le préfixe IPv6 propre à cet opérateur est noté "pref6rd". En contrepartie de l'installation des relais, l'opérateur contrôle les tunnels. Il peut ainsi garantir que la voie "retour" est symétrique à la voie "aller". Autre conséquence, les tunnels sont plus courts: ils servent à passer la section IPv4 de l'opérateur. En contrôlant les tunnels, les principaux défauts du déploiement de 6to4 , comme des délais importants ou l'asymétrie, sont corrigés. Avec 6rd , on se retrouve dans le cas classique où les routeurs internes (dont les relais) traitent le trafic des noeuds internes. Ainsi, ces relais ne servent que les clients de l'opérateur (contrairement à 6to4 où les relais étaient mutualisés et publics).


pref6rd:a4::
IPv6
Host v6
6rd CE
a4
Tunnel
pref6rd::
Internetv6
IPv4
6rd BR
b4
IPv6
Internetv4
Host v6
pref6rd:b4::