

*Préparé par* : Estelle COLIN, Fabrice BERNA  
*Formation* : Troisième année IUP Génie Mathématiques et Informatique  
*Enseignant* : Claude ZURBACH

## Le Protocole IPv6

# Le protocole IPv6 (IPng, ou IP new generation)

## Introduction : pourquoi un nouveau protocole IP ?

Lors de la conception d'IP (Internet Protocole) en 1978, les ingénieurs pensaient que seuls quelques milliers d'ordinateurs seraient concernés répartis sur une douzaine de réseaux. Or tout le monde sait, aujourd'hui que ce n'est pas le cas.

Avec IPv4 (Internet Protocole version 4), l'adressage se fait sur 32 bits, ce qui serait suffisant comme espace, mais, IPv4 est un protocole qui est trop restreint de par son utilisation et qui est donc coûteux en terme d'adresses gaspillées.

Bientôt, étant donné l'expansion de l'Internet, il n'existera plus d'adresse disponible sous Ipv4. Certains spécialistes pronostiquent la pénurie d'adressage sous Ipv4 d'ici 2008-2010.

Par exemple :

\* Les adresses de classe A : elles représentent douze réseaux de 16.7 millions de nœuds. Toutes les adresses de classe A sont déjà toutes épuisées.

\* Les adresses de classe B : elles représentent 16368 réseaux de 65534 nœuds. Ce sont les adresses les plus répandues parmi les industriels et certains fournisseurs d'accès. Elles sont déjà presque toutes utilisées.

\* Les adresses de classe C : elles représentent 2 millions de réseaux de 254 nœuds. Elles sont principalement pour les petites organisations, et, actuellement, elles sont distribuées aux fournisseurs d'accès. Ces adresses sont déjà épuisées.

De plus, aujourd'hui, le nombre de réseaux connectés est devenu très important, les tables de routage ont pris des proportions considérables, donnant ainsi une charge de travail énorme aux administrateurs.

De par la taille des tables de routage, le traitement des paquets est fortement ralenti. Actuellement, les routeurs principaux des infrastructures de l'Internet comptent environ 7000 routes.

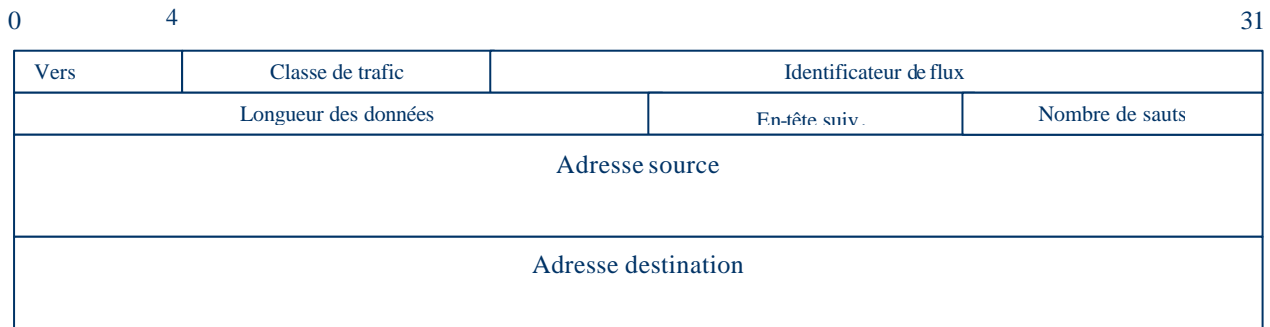
Le nouveau protocole, IPv6, doit permettre un adressage plus grand et un routage plus simple et plus rapide.

## Structure des paquets IPv6

Le protocole IPv6 apporte une simplification de l'en-tête. Les champs y sont désormais moins nombreux, sept champs au lieu de quatorze sous Ipv4. Cet allègement de l'en-tête permet une meilleure efficacité de commutation des équipements de routage qui ont moins de données à dépiler pour effectuer le routage.

On peut remarquer la disparition du « checksum » qui fixait la taille de l'en-tête, ainsi que la disparition des en-têtes optionnels dans l'en-tête lui-même.

## Format du paquet IPv6



**Version :** Seul champ inchangé par rapport à la version 4, contient la version IP du paquet. Seule modification, sur IPv6, sa valeur est 6.

**Classe de trafic :** Nature du trafic. Permet d'offrir un niveau de priorité aux paquets.

**Identificateur de flux :** Ce champ permet la mise en œuvre des fonctions de qualités de service. Il permet d'optimiser le routage par un acheminement plus rapide des données. Par ce champ, on peut donner un identifiant à la communication. Selon sa valeur, les routeurs du chemin reconnaissent la connexion et ne dépilent pas les informations, ils les transmettent directement.

**Longueur des données :** Longueur des paquets sans l'en-tête (en octets).

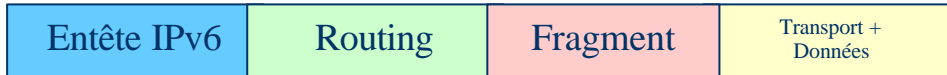
**En-tête suivant :** Ce champ indique le prochain entête dans le datagramme IPv6, c'est-à-dire l'emplacement des en-têtes optionnels si ils existent.

**Nombre de sauts :** Ce champ remplace le champ « TTL » d'IPv4. Sa valeur, sur 8 bits, est décrétementée à chaque traversée d'un routeur. Si sa valeur atteint la valeur 0, le paquet est détruit et un message d'erreur est émis par ICMPv6.

**Adresse de destination :** Peut être une adresse différente de l'adresse destination finale si l'option "Routing Header" est présente.

## Entêtes optionnels

Le paquet IPv6 inclut un champs d'extension pour les fonctionnalités optionnelles (sécurité, source routing, ...). Les options de IPv6 sont placées dans des en-têtes séparés, intercalés entre l'en-tête IPv6 et l'en-tête de la couche transport.



Les différents entêtes optionnels sont :

- *Entête Hop-by-Hop* : Information examinée sur chaque nœud du chemin.
- *Entête End-to-end* : Information examinée par le destinataire uniquement.
- *Entête Routing* : Routage effectué par la source. Liste des nœuds intermédiaires "à visiter", s'ils existent.
- *Entête Fragment* : envoi de paquets plus long que le MTU. La fragmentation réalisée par la source uniquement.
- *Entête authentification et intégrité des données*
- *Entête Privacy* : cryptage des données à protéger. Un des aspects de la sécurité IPv6

## Fragmentation

Alors que dans le cas du protocole IPv4 tous les routeurs pouvaient fragmenter les datagrammes, pour IPv6, ce n'est plus le cas ; Seule la source a le droit de fragmenter et seule la destination celui de défragmenter (fragmentation de bout en bout). S'il est nécessaire de fragmenter, la source insère un petit en-tête d'extension après l'en-tête de base de chaque fragment.

Le but de la fragmentation de bout en bout est de réduire les frais de gestion de la fragmentation dans les routeurs et permettre ainsi à chaque routeur de traiter plus de datagrammes par unité de temps. Une des conséquences est que si un routeur tombe en panne, il est difficile de changer le chemin car cela peut changer la MTU du chemin. Lorsqu'un protocole utilise la fragmentation de bout en bout, la source doit faire une recherche de MTU (cf. chapitre ICMPv6) minimum tout au long du chemin et fragmenter tout datagrammes sortant inférieur au MTU. La fragmentation de bout en bout s'accommode mal des modifications de chemin.

## Adressage

### Adressage IPv6

L'adressage sous IPv6 se fait désormais sur 128 bits (32 bits sur IPv4).

Sous IPv6 on n'a plus de notion de classes, on a seulement un adressage hiérarchique, par préfixe. L'adressage se fait désormais par l'attribution d'une partie d'adresse fixe qui définit le réseau, cette partie est appelée le préfixe.

On a, en fait, une conservation de l'adressage CIDR sous IPv4.

Cet adressage hiérarchique consiste en l'attribution d'un préfixe au premier routeur d'un réseau, sur 10 bits par exemple. Le routeur du sous réseaux aura lui une partie fixe qui sera celle de son père plus un complément de préfixe qui lui sera imposé. Et ainsi de suite l'attribution des adresses se fait de manière hiérarchique.

IPv6 reconnaît trois types d'adressage :

- **Adresse UNICAST** : Le type unicast, est le plus simple. Une adresse de ce type désigne une interface unique. Un paquet envoyé à une telle adresse sera donc remis à l'interface ainsi identifiée.
- **Adresse MULTICAST** : ce sont les successeurs des adresses broadcast (envoi à un ensemble de machines qui se doivent d'appartenir à une même classe). Une adresse de type multicast désigne un groupe d'interfaces appartenant, en général, à des équipements différents pouvant être situés n'importe où dans l'Internet. Lorsqu'un paquet a pour destination une adresse de type multicast, il est acheminé par le réseau à toutes les interfaces membres de ce groupe.
- **Adresse ANYCAST** : Ce type d'adresse est nouveau en IPv6. Comme dans le cas du multicast, une adresse de type anycast désigne un groupe d'interfaces, la différence étant que, lorsqu'un paquet a pour destination une adresse de type anycast, il est routé à un seul des éléments du groupe et non pas à tous. Ce sera, par exemple, le plus proche au sens de la métrique des protocoles de routage. Ce type d'adresse est encore en cours d'expérimentation et est réservé pour le moment aux routeurs. Les adresses anycast ont deux points communs avec les adresses unicast : elles sont allouées dans le même espace d'adressage et ont les mêmes formats.

### Représentation des adresses

Une adresse IPv4 est un mot de 32 bits tandis qu'une adresse IPv6 est un mot de 128 bits. La taille des adresses a donc été quadruplée, ce qui permet d'obtenir un espace adressable en IPv6 nettement plus large que celui en IPv4.

Une adresse sur IPv6 est un ensemble de 8 mots de 2 octets, qui sont en fait, 8 groupes de 4 lettres hexadécimales séparés par « : ». (Ex : FEDC:BA98:7654:3210:FEDC:BA 98:7654:3210).

Dans un champ, il n'est pas nécessaire d'écrire les zéros placés en tête. En outre plusieurs champs nuls consécutifs peuvent être abrégés par «::». Ainsi les deux notations suivantes sont équivalentes :

FEDC:0000:0000:0000:0400:A987:0043:210F

FEDC::400:A987:43:210F

Plus particulièrement, l'adresse formée uniquement par des zéros est représentée comme suit :

Le protocole Ipv6 - Estelle COLIN, Fabrice BERNA

::

Naturellement, pour éviter toute ambiguïté, l'abréviation «::» ne peut apparaître qu'une fois au plus dans une adresse.

La représentation des préfixes IPv6 est similaire à la notation CIDR utilisée pour les préfixes IPv4. Un préfixe IPv6 est donc représenté par la notation :

adresse-ipv6 / longueur-du-préfixe -en-bits

Les formes abrégées avec «::» sont autorisées :

3EDC:BA98:7654:3210:0000:0000:0000:0000/64

3EDC:BA98:7654:3210:0:0:0:0/64

3EDC:BA98:7654:3210::/64

::/0 (défaut)

Enfin on peut combiner l'adresse d'une interface et la longueur du préfixe réseau associé en une seule notation :

3EDC:BA98:7654:3210:945:1321:ABA8:F4E2/64

### **D'autres types d'adresses**

- Adresse indéterminée : l'adresse indéterminée est utilisée comme adresse source par un équipement du réseau pendant son initialisation, avant d'acquérir une adresse. Sa valeur est 0:0:0:0:0:0:0:0 (ou en abrégé ::).
- Adresse de bouclage (loopback address) : L'adresse de bouclage vaut 0:0:0:0:0:0:0:1, soit en abrégé ::1. Il s'agit de l'équivalent de l'adresse 127.0.0.1 d'IPv4. Elle est utilisée par un équipement du réseau pour envoyer un paquet IPv6 à lui-même.

### **Adresse compatible IPv4 :**

Si l'adresse sous IPv4 est 134.157.4.16, elle devient alors :

0:0:0:0:0:0:134.157.4.16

Soit après compression :

::134.157.4.16

## **ICMPv6**

Le protocole de contrôle IP a été revu. Dans IPv4, ICMP (Internet Message Control Protocol) sert à la détection d'erreurs (par exemple : équipement inaccessible, durée de vie expirée...), aux tests (par exemple ping) et à la configuration automatique des équipements (redirection ICMP, découverte des routeurs). Ces trois fonctions sont mieux définies dans IPv6.

### **Champs d'un paquet ICMPv6**

0	8	16	24	31
Type	Code	Checksum		
Données ICMPv6				

*Type* : nature du message (0-127 : erreur, 128-255 : messages d'information, utilisés par exemple pour l'auto configuration)

*Code* : cause du message ICMPv6

*Checksum* : permet de vérifier l'intégrité du paquet

*Données* : peuvent contenir un compte rendu de ce qui a provoqué l'erreur

### **Fonctions intégrées**

#### **MLD**

Grâce au sous-protocole MLD (1), ICMPv6 intègre les fonctions de gestion des groupes de multicast qui sont effectuées par IGMP (2) dans IPv4.

(1) MLD (Multicast Listener Discovery) est identique à IGMP.

(2) IGMP (Internet Group Management Protocol) Protocole de gestion des groupes multicast en réseau IP local.

#### **ARP**

ARP (Address Resolution Protocol) est un protocole de résolution d'adresse IPv4 en une adresse de niveau liaison. Il permet de générer une table des correspondances *adresse physique* ⇔ *adresse logique*.

ICMPv6 reprend les fonctions de ce protocole.

## **Découverte de la MTU**

La MTU (Maximum Transmission Unit) est la taille maximum qu'un paquet peut avoir pour être acheminé sur un réseau, pour des raisons logicielles ou matérielles.

Il s'agit d'une opération qui permet de maintenir la valeur des MTU des différents chemins utilisés par un nœud. Tout au long de sa vie sur le réseau, chaque nœud maintient une base de données de cette information.

Pour détecter la MTU du réseau sur lequel elle se trouve, une machine émet des paquets de demande MTU à tous ses voisins. IPv6 conseille l'utilisation d'une MTU de 1280 octets.

## **Messages d'erreur**

ICMPv6 permet, aux différentes machines, d'émettre des messages d'erreur :

- *Fragmentation* (paquet trop gros) : La fragmentation à la demande des paquets IP augmente les risques de congestion du réseau et ralentit la transmission dans IPv4. Dans le cas de IPv6, si un paquet dépasse la MTU d'un réseau, le paquet est détruit, et un paquet ICMPv6 est envoyé à l'initiateur du paquet, qui va redéfinir la taille de tous les paquets qu'il va envoyer.
- *Destination inaccessible*
- *Temps dépassé*
- *Entête invalide*

## **Messages d'information**

ICMPv6 permet aux différentes machines d'échanger des informations, comme pour l'auto configuration par exemple. Ces messages sont de deux types :

- *Message requête*
- *Message réponse*

## **Auto-configuration**

Le besoin de simplifier le processus de configuration des machines se fait ressentir. Cela inclut les services DHCP comme les interactions avec les voisins. La configuration automatique est un atout principal d'IPv6.

La configuration automatique signifie qu'une machine obtient toutes les informations nécessaires à sa connexion à un réseau local IP sans aucune intervention humaine. Le protocole IPv6 introduit la notion de « Plug & Play » dans les réseaux.

## **Objectifs**

Les objectifs de l'auto configuration sous IPv6 sont

- L'acquisition d'une adresse quand une machine est attachée à un réseau pour la première fois.
- L'obtention d'une nouvelle adresse en cas de renumérotation des machines du site (changement de la partie haute de l'adresse)
- L'obtention d'une nouvelle adresse en cas de déplacement.

## **ID d'interface**

L'ID d'interface est une nouvelle notion introduite avec IPv6. L'ID occupe les 64 bits de poids faible de l'adresse. Dans un réseau local basé sur Ethernet, il est construit grâce aux 48 bits du nombre MAC des cartes réseau dans lesquels on insère par octets des valeurs constantes pour obtenir 64 bits.

*Exemple* : Une carte réseau de numéro MAC 00:E0:4C:39:B2:A9 donnera un ID 02E0:4CFF:FF39:B2A9

## **Méthodes d'auto configuration**

### ***Adresse lien-local :***

Les adresses lien-local sont des adresses dont la portée est restreinte à un site donné. Par exemple, un site qui n'est pas encore connecté à Internet peut utiliser ce type d'adressage, et sera dispensé d'emprunter un préfixe.

L'adresse lien-local est créée en prenant le préfixe FE80::/64 auquel on ajoute les 64 bits d'ID d'interface. L'adresse constituée est encore interdite d'usage. La machine doit encore vérifier l'unicité de cette adresse sur le réseau par le protocole de détection d'adresse dupliquée. Si la machine détermine que sa création d'adresse lien-local a échoué, alors une intervention manuelle est nécessaire. Sinon, l'adresse provisoire devient définitive.

### **Auto configuration sans état**

Elle est utilisée dans un réseau connecté par routeur à un autre réseau (Internet par exemple), et quand la gestion stricte des adresses attribuées n'est pas nécessaire au sein d'un site. Cette méthode décentralisée permet à chaque machine du site de construire sa propre adresse IPv6. Elle ne demande ni une configuration particulière des machines ni de serveur supplémentaire. Elle se sert du protocole ICMPv6. Une machine construit son adresse IPv6 à partir d'informations locales et d'informations fournies par le routeur. Le routeur lui donne le préfixe (par un message d'annonce de routeur), puis elle construit son adresse comme vu précédemment.

### **Auto configuration avec état (DHCPv6)**

La plus complète car permet de configurer l'adresse du client, le nom de domaine, le serveur de nom, etc. Elle est retenue lorsqu'un site demande un contrôle strict de l'attribution des adresses. Ceci signifie que toute attribution d'une adresse IPv6 globale doit passer par un serveur DHCPv6 du site. Le routeur joue alors un rôle important : il dicte à la machine la méthode à retenir et fournit éventuellement les informations nécessaires à sa configuration.

Actuellement, le protocole DHCPv6 n'est pas encore standardisé.

### **Utilisation de routines ICMPv6**

L'auto configuration est effectuée grâce à un ensemble de routines ICMPv6 :

- Découverte des routeurs du réseau.
- Découverte des préfixes imposés par les routeurs.
- Détection des adresses dupliquées.
- Découverte des paramètres (dans le cas d'une auto configuration avec état).

## **Routeage**

### **SPF**

**Rappel** : SPF (Shortest Path First) est une technique de routage basée sur le plus court chemin.

Ce protocole ne subit pas de modifications dans IPv6.

### **OSPFv6**

Le protocole OSPFv6 (Open Shortest Path First) cherche à atteindre plusieurs objectifs dont :

- Routage par type de service : les administrateurs peuvent définir plusieurs routes, de qualité de service différente, vers une destination donnée. Le routeur choisit alors la route de QoS adéquate pour acheminer les paquets.
- Equilibrage des charges : si un administrateur définit plusieurs routes de même QoS vers une destination donnée, OSPF répartit équitablement le trafic sur toutes ces routes.
- OSPF permet à un site de décomposer ses réseaux et routeurs en sous-ensembles appelés *zones*. Chaque zone est autonome et la topologie d'une zone reste invisible pour les autres zones.

### **Spécificités**

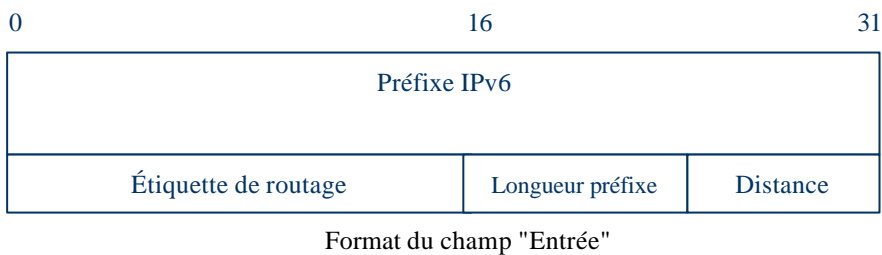
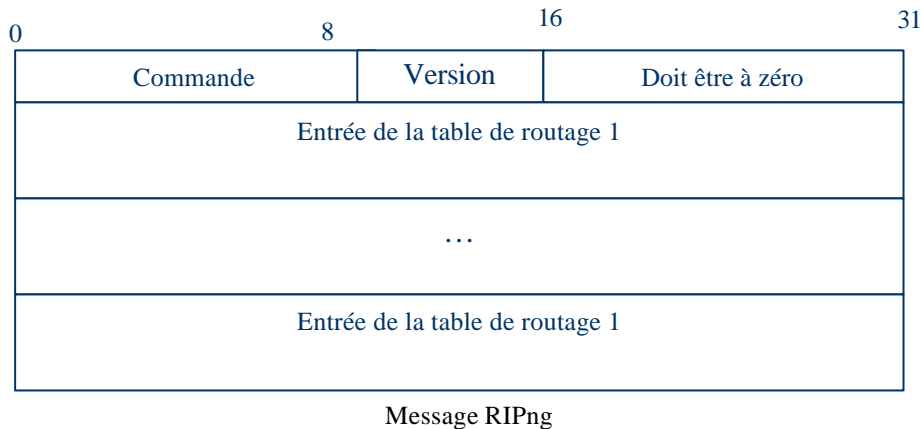
Le routage sous IPv6 inclut les extensions suivantes

- Le routage se fait de manière classique, sur les préfixes (attribution de plages d'adresses)
- Le routage peut se faire intégralement par la source (avec un en-tête optionnel « Routing »)

### **RIPng**

**Rappel** : RIP (Routing Information Protocol) : Chaque routeur propage toutes les routes qu'il connaît vers les autres routeurs. Chaque routeur possède une table de routage qui comporte une entrée pour chaque destination possible

Dans RIPng, un mécanisme de temporisation permet de gérer l'ensemble des événements. Ainsi toutes les 30 secondes, le processus de routage est réveillé afin d'envoyer un message de type *réponse* contenant la table de routage complète. Ce message est envoyé à tous ses voisins.



## Plan de transition de IPv4 vers IPv6

### Plan de transition IPv4 vers IPv6

La transition d'IPv4 vers IPv6 ne se fera pas du jour au lendemain. On prévoit qu'elle s'effectuera d'ici 2010. Elle doit se faire de manière progressive et doit permettre, durant la période de transition, la coexistence des protocoles IPv4 et IPv6. L'objectif principal est de terminer le passage à IPv6 avant l'épuisement total des adresses IPv4.

La transition d'IPv4 vers IPv6 peut se faire en 3 phases

1. Seuls les équipements IPv4 existent. On arrive en fin de cette phase. De nombreux constructeurs vont proposer dans un délai très court les premières versions d'IPv6 pour les postes de travail et les routeurs
2. Phase de coexistence. Phase qui sera très longue. Les machines devront conserver les adresses IPv4 déjà allouées.
3. Phase où seuls subsisteront les équipements IPv6.

### IPv6 techniques de transition

Les machines actuelles et à venir devront être capables de traiter des paquets IPv6 autant que les paquets IPv4. Pour transiter de la version 4 à la version 6 d'IP, trois techniques ont été mises au point : la double pile IP, l'encapsulation de IPv6 dans IPv4 (tunneling), et la traduction des en-têtes IPv6 en en-têtes IPv4 (voire l'inverse).

#### ***Le modèle Dual Stack***

Les équipements ont une adresse dans chacun des plans d'adressage IPv4 et IPv6. Ils acheminent aussi bien les paquets IPv6 qu'IPv4. La majeure partie du code de la pile IPv4 peut être réutilisée pour IPv6. En effet, un seul branchement est nécessaire pour distinguer le bon code, en regardant le premier champ de l'en-tête IP qui donne le numéro de version

#### ***Les tunnels***

L'encapsulation consiste à faire transiter des données d'un protocole donné à l'intérieur d'un autre. A l'heure actuelle, tous les routeurs ne sont pas capable de router des paquets IPv6. On place alors un paquet IPv6 à l'intérieur d'un paquet IPv4 pour le faire passer dans les réseaux anciens, et pouvoir retrouver un paquet IPv6 en sortie. On crée ainsi des tunnels IPv6 à travers une infrastructure IPv4. Cette méthode conserve les problèmes inhérents à IPv4 (adressage, routage, fragmentation) quoiqu'il arrive.

## Conclusion

La normalisation du successeur de l'Internet Protocol que nous utilisons aujourd'hui est déjà bien avancée, même s'il reste encore du " pain sur la planche " .

La France fait partie des premiers pays du monde qui s'est intéressé à la mise en oeuvre et à l'expérimentation du protocole IPv6. Des chercheurs issus de milieux académiques et industriels ont formé un groupe de travail, le G6, et se sont fixés dans un premier temps les deux objectifs suivants :

- déployer un réseau de test d'IPv6 en France, le G6bone, et l'interconnecter au réseau de test mondial, le 6bone, afin d'expérimenter le transport d'IPv6 au-dessus du réseau IPv4 (au moyen de tunnels).
- vulgariser les nouvelles techniques liées à IPv6 (installation, interconnexion, transition, ...) auprès des spécialistes réseau en France.

Les premières expérimentations ont déjà commencé, elles sont encore peu nombreuses.

Néanmoins de nombreuses implantations sont en tests chez les constructeurs tant pour les postes de travail que pour les équipements de routage. Plusieurs pensent pouvoir fournir une version commerciale dans un délai très rapproché.

Dès lors, la question qui émerge est de savoir qui doit migrer vers IPv6 et quand. La réponse est naturellement liée aux priorités de chacun, mais aussi aux possibilités nouvelles offertes par IPv6 et qui pour certaines d'entre elles au moins, vont probablement devenir essentielles aux applications courantes de demain : applications de vidéoconférence ou de temps réel, nécessitant une qualité de service garantie, la configuration automatique des équipements, la sécurité des données transportées...