ART Autorité de Régulation des Télécommunications

RÉPUBLIQUE FRANÇAISE

La migration vers IPv6

Étude réalisée par l'IDATE et
le cabinet de Pardieu Brocas Maffei & Leygonie

pour
l'Autorité de Régulation des Télécommunications

Juin 2002

Sommaire

Introduction

IPv4, élaboré il y a une vingtaine d'années, est la version du protocole IP utilisée actuellement sur Internet. Sa principale faiblesse réside dans son espace d'adressage puisque dans IPv4, une adresse est définie sur 32 bits seulement. Le succès rapide d'Internet et l'accélération de la consommation d'adresses IP, fait craindre une pénurie d'adresses IP dans les années à venir. Pour l'instant, IPv4 a réussi à repousser les limites de son système d'adressage grâce à des procédés tels que la translation d'adresses (NAT) ou le schéma de routage CIDR qui permet d'agréger des adresses IP.

IPv6, élaboré par l'IETF au milieu des années 90, est la prochaine version du protocole IP. En premier lieu IPv6 améliore les capacités d'adressage d'IPv4 en allouant 128 bits au lieu de 32 aux adresses IP, ce qui ouvre un réservoir quasi infini d'adresses IP.

Ces derniers mois plusieurs évènements se sont enchaînés qui peuvent laisser croire à une migration prochaine vers IPv6 : prises de position d'autorités gouvernementales notamment en Asie, de la Commission Européenne ou de certains industriels.

Dans ce contexte, l'**Autorité de Régulation des Télécommunications** a souhaité réaliser une étude permettant de cerner les problématiques de la migration d'IPv4 vers IPv6 en identifiant notamment les stratégies des différents acteurs couvrant l'ensemble de la chaîne de valeur des services et des équipements de réseaux Internet : équipementiers, opérateurs, ISP, entreprises utilisatrices de technologies IP, fabricants de logiciels,... L'étude s'est attachée en particulier à examiner les problématiques de cette migration sous l'angle réglementaire et concurrentiel et les impacts de celles-ci sur les marchés des réseaux et services de télécommunications utilisant le protocole IP.

IDATE
Roland MONTAGNE
Sébastien VIDAL
Vincent POULBERE

Cabinet de Pardieu Brocas Maffei & Leygonie
Martine GEORGES-NAÏM
Clotilde FOREST

Partie 1 : Synthèse générale

1 IPv6 : un protocole adapté à la diffusion massive d'Internet

1.1 IPv4 : certaines limites perceptibles - IPv6 : des atouts pour un relais de croissance

- **IPv4 : un espace d'adressage restreint avec une répartition géographique inégale**

Le protocole IPv4, finalisé en 1983 s'adressait alors à une communauté restreinte. Ainsi, l'adressage d'IPv4 est-il prévu sur 32 bits, ce qui permet de disposer d'un « stock » de 4,3 milliards d'adresses IP environ. À cette époque et avec la vision qu'avaient alors les responsables, à savoir un réseau destiné aux militaires et scientifiques (donc assez éloignée de ce qu'allait devenir l'Internet que nous connaissons aujourd'hui), le stock paraissait plus que suffisant.

Aujourd'hui, ce stock d'adresses IPv4 est très entamé et si près de 47% des adresses ne sont pas attribuées (parmi le stock total d'adresses), la répartition géographique en est très inégale. Les adresses allouées (destinées à être utilisées par un registre régional ou par des organisations pré-RIR) représentent la majorité du stock et sont destinées essentiellement à la zone américaine aux dépens de l'Asie qui présente pourtant un important potentiel de développement (Chine, Inde). Il est également à noter, que parmi le total des adresses IPv4 disponibles, 53% ont été attribuées directement à des organisations (américaines pour la plupart), avant l'apparition des RIR qui ne les contrôlent donc pas.

Ainsi, en tenant compte de ces organisations pré-RIR, on peut estimer, fin 2001, que 74% des adresses allouées le sont pour l'Amérique du Nord, 17% pour l'Europe et 9% pour l'Asie.

- **IPv4 est face à une explosion des besoins**

Outre la croissance organique encore forte d'Internet dans le monde entier (et particulièrement en Asie où le potentiel de croissance est très élevé et les ressources en adresses très faibles), bon nombre d'applications nouvelles, consommatrices d'adresses IP devraient se développer :

- l'arrivée des services mobiles autour du GPRS d'abord puis de l'UMTS,
- les accès haut débit et le mode « always on »,
- l'électronique connectée et les véhicules communicants,
- les applications domotiques et réseaux de capteurs.

- **IPv4 : un protocole non pensé pour un usage commercial d'Internet**

Prévu à l'origine pour des usages non commerciaux, IPv4 n'a pas été conçu pour assurer les fonctions de QoS attendues aujourd'hui, ni pour assurer les fonctions d'auto configuration ou Multicast, ou encore la sécurité, essentielles dans l'Internet commercial moderne. Des solutions ont été trouvées pour assurer ces fonctions, alourdissant le protocole de couches supplémentaires, ou pour doper artificiellement la durée de vie du stock d'adresses (NAT), faisant notamment exploser la complexité des tables de routage.

- **Nous sommes dès à présent dans une période de gestion de la pénurie d'adresses IP**

Cette gestion de la pénurie d'adresses se traduit par des politiques drastiques d'attribution d'adresses IPv4 pratiquées par les RIR. De plus, l'emploi généralisé des NAT permet de retarder la pénurie, mais cela alourdit la gestion des réseaux et constitue un frein au développement d'applications temps réel et P2P.

Ainsi, toutes choses égales par ailleurs, on peut estimer un épuisement du stock d'adresses IPv4 d'ici 2010.

- **L'immense capacité d'adressage d'IPv6 justifie à elle seule, le passage au nouveau protocole**

Malgré les divers avantages techniques d'IPv6 décrits ci-après, l'essentiel, de l'avis général des experts, reste l'espace d'adressage large, qui permettra de faire face aux besoins engendrés par le développement des nouvelles applications « always on » et de rétablir l'usage du mode end-to-end qui est le principal apport d'IPv6 au niveau des applicatifs. Les autres avantages techniques, bien que réels, ne présentent pour l'heure que des potentiels intéressants, mais ne sont pas l'atout premier d'IPv6 :

- Adressage hiérarchique pour optimiser le routage,
- Auto configuration,
- IPSec natif,
- Multicast,
- Mobile IPv6.

IPv6 présente également plusieurs avantages permettant de mieux gérer la QoS mais qui ne sont pas encore significatifs. De manière générale, on considère que dans un premier temps, la QoS sera gérée de la même façon sous IPv6 que ce que l'on connaît aujourd'hui sous IPv4.

1.2 La normalisation IPv6 est stable

- **Le cœur d'IPv6 est aujourd'hui stable et permet des déploiements commerciaux**

À ce jour, le cœur d'IPv6, essentiel pour son fonctionnement, est considéré comme stable par la plupart des spécialistes. Considérant qu'IPv4 a commencé à être utilisé alors que l'ensemble de ses spécifications n'était pas totalement stable, on peut considérer qu'IPv6 est en mesure, dès maintenant, d'être utilisé « commercialement ». Qui plus est, les « chantiers » encore existants concernent essentiellement des spécificités d'IPv6, des nouveautés par rapport à IPv4 :

- Gestion du DNS mondial sous IPv6,
- Mobile IPv6,
- Auto configuration,
- Champ Flow Label.

Au final, les chantiers encore en cours sous IPv6 n'ont pas d'effet négatif sur le développement de celui-ci, le protocole étant suffisamment abouti pour fonctionner sur un mode commercial aussi bien qu'IPv4, et les nouveautés inachevées ne nuisant pas à ce fonctionnement.

2 Certains acteurs déjà en ordre de marche

- **Les équipementiers et éditeurs informatiques détiennent un rôle clé**

Les équipementiers télécoms fournissent les matériels qui permettent l'acheminement des données sur les réseaux IP : il s'agit principalement des routeurs. Ces routeurs sont actuellement conçus pour acheminer les paquets de données en utilisant le protocole IPv4. L'utilisation d'IPv6, donc d'un format de paquets différent, nécessite en premier lieu une mise à niveau de ces infrastructures de routage. Ces mêmes équipementiers télécoms fournissent également des équipements d'accès à Internet : CPE et terminaux mobiles notamment.

Sur le marché de l'informatique grand public, c'est d'abord le système d'exploitation (OS) qui rend possible l'utilisation d'IPv6. Les produits Microsoft, leader absolu du marché des OS pour terminaux sont sur le point d'être prêts pour IPv6 : Windows XP est déjà prêt et présentera, d'ici fin 2002, IPv6 par défaut (pour le moment, il est disponible mais doit être activé), et les autres produits Windows seront prêts avant la fin 2002. Le fait que le leader du marché aille vers IPv6 est un élément essentiel : si l'OS majoritaire est compatible IPv6, l'un des principaux points de blocage à la transition est levé.

- **Un goulet d'étranglement dans une seconde phase : les opérateurs de backbone ?**

Les opérateurs de backbone peuvent constituer un goulet d'étranglement dans la transition vers IPv6 : s'ils n'assurent pas le transit des données en IPv6, les autres opérateurs et ISP sont contraints d'avoir recours à des techniques d'encapsulation dans IPv4 pour faire transiter les données entre des nœuds distants. Ces techniques peuvent suffire pour un premier stade de déploiement d'IPv6. Cependant, la gestion à grande échelle de tunnels ne sera pas viable ; les opérateurs de backbone devront migrer leurs routeurs de cœur de réseau sous IPv6 quand la demande le justifiera.

- **Mobilité et nomadisme : IPv6 incontournable à terme**

En Europe, les équipementiers leaders spécialisés dans la mobilité et notamment les réseaux cellulaires sont actifs dans le domaine d'IPv6. Ainsi, Ericsson (par ailleurs propriétaire de Telebit, pionnier en matière de routeur IPv6) et Nokia proposent des gammes de routeurs compatibles pour IPv6. Ces acteurs considèrent que l'Internet mobile sera un moteur de croissance d'IP et qu'IPv6 sera nécessaire pour développer des services attrayants. L'horizon de la 3G est clairement évoqué par ces derniers comme une réelle opportunité pour IPv6. De plus, le saut technologique IPv6 a été identifié par le 3GPP à partir du release 5 de la norme UMTS.

Le marché des WLAN connaît un développement sensible à la fois dans le domaine des réseaux d'entreprises et, plus récemment, dans le domaine des réseaux d'accès public. Les WLAN permettent la connexion à la fois des assistants personnels et des ordinateurs. Toutefois, la prolifération attendue du nombre de terminaux connectés par ces technologies est bien moindre que celle attendue de la téléphonie mobile. Ainsi, le développement des WLAN n'aura pas un effet majeur dans un premier temps, comparé à la téléphonie mobile. Cependant, aujourd'hui, de plus en plus de demandes se font sentir quant à l'utilisation des technologies WLAN sur des réseaux publics. Si une telle utilisation tend à se généraliser, l'arrivée de Mobile IPv6 pourrait s'accélérer de manière notable ; l'attitude des autorités réglementaires sera déterminante dans les prochains mois quant à l'utilisation des technologies WLAN sur des réseaux publics.

- **IPv6 : un relais de croissance**

Les équipementiers télécoms ont clairement identifié IPv6 en tant que relais de croissance : IPv6 va accélérer le renouvellement des parcs (terminaux et réseaux d'accès). De plus, IPv6 sera pour les différents équipementiers un moyen d'atteindre de nouveaux marchés :

- via l'électronique connectée : équipementiers grand public,
- de par l'intrusion d'IP dans d'autres secteurs que l'informatique et les télécommunications : équipementiers IP.

Dans le cadre du développement des connexions permanentes des terminaux (développement des hauts débits notamment, 3G), les opérateurs peuvent trouver, dans IPv6, un réservoir d'adresses qui leur permettra d'offrir un service de qualité à leurs clients, sans souci de gestion complexe (NAT). La gestion du réseau est globalement simplifiée, notamment grâce à l'adressage hiérarchique et aux fonctions d'auto configuration. En offrant un meilleur service, on peut imaginer que l'opérateur puisse augmenter ses tarifs sur certaines parties de son offre. La gestion du réseau étant moins onéreuse, certains équipementiers estiment ainsi que des opérateurs peuvent accroître leurs marges.

- **Des coûts maîtrisables mais des modèles économiques à inventer**
- **Des modèles économiques à inventer sous IPv6 pour des ISP tirant leurs revenus exclusivement de services IPv4**

Les coûts engendrés par le passage à IPv6 pour les ISP sont marginaux, du moins dans le domaine matériel : la mise à jour software des routeurs est souvent gratuite. En revanche, si l'ISP gère les deux versions d'IP sur un même réseau, la lourdeur de gestion peut être ressentie, le surcoût des équipements restant marginal. Les principaux coûts identifiés par les fournisseurs d'accès sont les coûts humains : les personnels maîtrisent la technologie IPv4. IPv6 présente de nouvelles particularités et les techniciens doivent donc s'adapter. Ils devront, en outre, être capables de gérer les deux versions d'IP simultanément pendant une longue période.

L'architecture MPLS ou Dual Stack semble bien adaptée pour les ISP car elle leur permet dans un premier temps d'être assez flexibles face à la demande de leurs clients en accès IPv6 : possibilité d'ouvrir des accès IPv6 au cas par cas sans avoir à migrer tout le réseau.

Aujourd'hui, le principal souci des ISP, sur un marché particulièrement concurrentiel en phase de concentration, est de stabiliser leur position et de trouver le meilleur modèle qui leur permettra d'atteindre l'équilibre sous IPv4. Leur souci majeur n'est donc pas de tenter de nouvelles aventures en proposant IPv6, pour lequel la demande n'est pas encore identifiée. Le développement des accès haut débit via ADSL notamment, peut être un facteur déclencheur pour la fourniture d'accès IPv6 pour les ISP. Au Japon, c'est à travers des accès ADSL via IPv6 que les ISP (IIJ, NTT) proposent leurs premiers accès commerciaux IPv6.

- **Vers un environnement plus concurrentiel pour les ISP ?**

Comme nous venons de l'évoquer, l'abondance d'adresses IPv6 est une opportunité qui permet à de nombreux ISP de se repositionner sur un marché plus ouvert, de proposer de nouveaux services, d'améliorer ou de simplifier des services existants ou de gérer plus simplement leurs réseaux.

Ainsi, la fourniture de services d'accès à Internet sous IPv6 va permettre de fluidifier la concurrence entre les ISP dès lors, par exemple, que le système d'auto configuration permettra aux entreprises de changer de fournisseur à moindre coût, la renumérotation d'un réseau devenant automatique, mais est aussi susceptible de réduire, dans cette mesure, l'étendue de leurs services.

- **Entreprises et IPv6 : l'engouement se fait attendre**

Il faut distinguer deux types d'entreprises de technologie IP : les entreprises qui utilisent le protocole pour leurs communications et leurs réseaux (Intranet, Extranet), et les entreprises qui, bien qu'étant hors du champ des acteurs du marché « traditionnel » d'Internet, peuvent trouver des opportunités pour utiliser IPv6 dans de nouvelles applications, ou en substitution d'applications existantes.

Ces deux aspects peuvent se manifester au sein d'une même entreprise, avec des attitudes différentes par rapport à IPv6 selon le contexte.

Les premières, utilisatrices de réseaux d'entreprises IP, ne ressentent pas nécessairement le besoin de passer à IPv6. Bien que les avantages potentiels d'IPv6 soient perçus, les responsables informatiques estiment, dans leur ensemble, qu'il n'y a ni urgence, ni priorité. Dans le contexte actuel, la priorité est à la pérennisation des investissements déjà réalisés sous IPv4. C'est le cas d'une majorité de grandes entreprises qui estiment pour l'instant que rien n'est possible sous IPv6 qui ne soit faisable sous IPv4.

Parallèlement, certaines entreprises non utilisatrices d'IP, ou non orientées à l'origine vers les TIC, voient dans IPv6 une opportunité. Ainsi, dans le secteur de l'Aéronautique, on étudie attentivement le nouveau protocole IPv6. Les acteurs y voient une possibilité de passer à IP. Qui plus est, l'abondance d'adresses peut permettre d'imaginer le développement de nouvelles applications : suivi des sous-ensembles des aéronefs, maintenance, Internet embarqué. Les constructeurs automobiles, qui, s'ils estiment que leurs réseaux internes peuvent demeurer en IPv4, voient avec IPv6, allié aux technologies cellulaires, la possibilité de nouvelles applications autour de la voiture connectée. Les constructeurs d'électroménager imaginent également des applications domotiques.

Il y a donc face à IPv6 une attitude relativement neutre des grandes entreprises, voire indifférente de la part des directions informatiques, alors que les directions de R&D y voient un certain nombre d'opportunités dans le domaine des objets communicants. Dans tous les cas, il y a une volonté de se tenir informé, même si l'information semble parfois faire défaut.

3 Les facteurs déclencheurs du passage à IPv6

3.1 Au-delà de la pénurie d'adresses IPv4, d'autres facteurs déclencheurs de 1er rang : services mobiles (GPRS et 3G) et nomades (WLAN)

Outre la pénurie d'adresses IPv4, premier facteur déclencheur du passage à IPv6 et qui s'annonce pour les prochaines années (cf. ci-dessus), d'autres facteurs déclencheurs de 1er rang se sont dégagés de cette étude :

- **IPv6 est considéré par les acteurs du secteur comme une évolution à terme incontournable des réseaux mobiles**

L'émergence des services de données mobiles, au Japon notamment avec l'i-mode de DoCoMo et les autres services des opérateurs concurrents, et en Europe avec le succès des SMS, conduit à s'interroger sur l'influence de ce marché sur l'introduction d'IPv6. Par ailleurs, l'arrivée de nouvelles générations de technologies réseaux devrait conduire à la prolifération des terminaux mobiles connectés : le GPRS tout d'abord, dont les premiers services commerciaux à destination des entreprises sont à présent offerts par la plupart des opérateurs GSM d'Europe de l'Ouest, puis la 3G (UMTS et CDMA 2000) qui fait l'objet d'investissements colossaux en Europe et dont le premier service commercial a été ouvert au Japon par DoCoMo en octobre 2001.

Même si dans un premier temps, les systèmes mobiles GPRS et UMTS exploitent IPv4, la version IPv6 apparaît comme un enjeu important pour les opérateurs de réseau mobile, car il permettra d'allouer une adresse IP permanente à chaque terminal mobile connecté. En effet, le GPRS introduit le concept de « always-on », c'est-à-dire de connexion permanente au réseau de données en IP, même lorsque l'utilisateur est inactif. À terme, IPv6 est considéré par les acteurs du secteur comme une évolution incontournable des réseaux mobiles.

- **L'utilisation des technologies WLAN sur des réseaux publics pourrait accélérer l'arrivée de Mobile IPv6 ; l'attitude des autorités de réglementation sera déterminante à ce niveau**

Aujourd'hui, de plus en plus de demandes se font sentir quant à l'utilisation des technologies WLAN sur des réseaux publics. Si une telle utilisation tend à se généraliser, l'arrivée de Mobile IPv6 pourrait s'accélérer de manière notable ; l'attitude des autorités réglementaires sera déterminante dans les prochains mois quant à l'utilisation des technologies WLAN sur des réseaux publics.

La gestion native de la mobilité par IPv6 et ses solutions simples permettant une simplification de la gestion de la mobilité d'un terminal dans un réseau (auto configuration, renumérotation automatique) constituent des avantages évidents pour ce type de technologies et font d'IPv6 une solution particulièrement séduisante pour la gestion de la mobilité dans des réseaux hétérogènes. On pense notamment aux terminaux mobiles au travers d'un WLAN, puis sur les réseaux 3G : mobilité totale et transparente pour l'utilisateur.

3.2 La dynamique de l'accès haut débit, de l'électronique connectée et des réseaux de capteurs : facteurs déclencheurs de 2ème rang

Derrière ces facteurs déclencheurs de 1er rang, apparaissent d'autres moteurs de la migration vers IPv6 :

- **Les accès hauts débit consommateurs d'adresses permanentes**

Le marché des hauts débits en devenir pourrait accélérer la pénurie d'adresses sous IPv4. En effet, la plupart des accès haut débit se font en always-on, c'est-à-dire que le terminal reste connecté en permanence et nécessite donc une adresse IP fixe. En pratique, les fournisseurs d'accès haut débit via ADSL par exemple, continuent à proposer un adressage dynamique. Cependant, les usages qui se développent autour de ces connexions permanentes font que ces ISP ne peuvent appliquer les mêmes taux modem/abonnés que sous connexion RTC ; ces taux peuvent ainsi passer de 1/10 ou 1/20 sous accès commuté à 1/2 ou 1/4 sous accès ADSL. Cela accélère donc la consommation d'adresses IP. De plus, si l'on examine la situation au Japon, on observe que les premiers déploiements IPv6 ne se font pas du côté des services mobiles comme on aurait pu s'y attendre mais à travers des accès ADSL sous IPv6 (IIJ, NTT).

- **L'électronique connectée : un levier de développement pour IPv6 unanimement reconnu**

Le développement des objets électroniques connectés est unanimement reconnu comme un levier potentiel pour IPv6. Les produits de l'électronique grand public et de l'électroménager (de type TV, appareils photos, etc.) devraient de plus en plus fréquemment être connectés à Internet : ceux-ci pourraient se comporter comme des terminaux (écrans de télévision pour surfer sur Internet, …) ou comme des serveurs (appareils électroménagers dans le cadre du développement de la domotique). En outre, les terminaux portables de type PDA devraient se multiplier à l'avenir et être également connectés. Le besoin en adresses IP généré par les développements annoncés devrait rendre impératif le passage des réseaux à IPv6, du moins pour les réseaux concernés par ces applications.

À ce jour, les développements ont commencé, notamment au Japon, où les produits électroménagers connectés devraient apparaître courant 2003 et les jeux en réseaux, moteurs de la croissance du marché des consoles de jeux connectés, devraient exploser en Asie en 2002.

- **L'adressage global d'un réseau de capteurs : une source de consommation en adresses IP**

La mise en réseau et la connexion de capteurs via IP est une technique émergente sur laquelle des expérimentations sont menées (au Japon notamment). De nombreux acteurs l'identifient comme un levier de croissance du besoin en adresses IP : adressage global de « méga réseaux de capteurs », pour la météorologie, développement des réseaux de capteurs embarqués dans l'automobile, ou l'aéronautique. Les fournisseurs d'applications militaires ont également intérêt à passer à IPv6 : qu'il s'agisse de systèmes de communications « traditionnels » ou de nouveaux systèmes de contrôle du matériel ou de suivi des soldats, IPv6 peut apporter de réels avantages. Si ces techniques prennent effectivement un essor important, elles constitueront une source de croissance du besoin en adresses IP et donc un facteur influençant le passage vers IPv6.

4 IPv4 – IPv6 : une cohabitation longue et incontournable

4.1 Un risque limité de morcellement de l'Internet

- **Des risques limités de morcellements technologiques de par la longue cohabitation inévitable entre les deux protocoles**

Même si IPv6 a été conçu dans la continuité d'esprit d'IPv4, sans réelle rupture technologique, le nouveau protocole n'en reste pas moins différent et l'interopérabilité entre les deux IP n'est pas naturelle. Il apparaît plus judicieux de parler de transition et de déploiement que de migration : on ne se situe pas dans un cas de figure du type an 2000 avec une bascule subite, mais dans celui d'une transition douce et progressive des réseaux. Ceci signifie que les deux standards seront amenés à cohabiter pendant plusieurs années et donc à inter opérer. Les scenarii de transition sont multiples et les outils qui les appuieront ont été largement envisagés par l'IETF, ainsi que leurs usages dans les différentes phases de la transition.

Ainsi, la cohabitation entre les deux standards risque d'être relativement longue. On peut estimer qu'à partir des premiers déploiements IPv6, il faudra au moins une dizaine d'années pour qu'IPv6 devienne majoritaire. Qui plus est, il n'y a pas uniformité dans ce domaine : il est probable que les ISP migrent bien avant les entreprises qui cherchent d'abord à rentabiliser les applicatifs développés sous IPv4 avant d'investir dans de nouvelles techniques.

- **L'Asie avec le Japon et la Corée devrait connaître un décollage significatif du marché IPv6 d'ici 2003**

D'un point de vue géographique, le rythme d'entrée dans IPv6 des différentes régions du monde sera assez différent. Toutefois, le morcellement géographique (barrière des langues, habitudes d'utilisation) existe déjà de fait, et les conséquences techniques de la cohabitation de différents standards en différentes zones devraient donc être minimes.

4.2 Une opportunité pour remettre à plat la répartition des DNS racines

- **L'arrivée d'IPv6 peut être l'occasion de remettre en cause l'hégémonie des USA dans la gestion du DNS mondial**

Le serveur DNS est l'outil qui permet de faire correspondre un nom de domaine « en clair » à une adresse IP. Actuellement, les serveurs DNS fonctionnent en IPv4. Si quelques problèmes se posent encore pour le fonctionnement en IPv6, au Japon et en France, des serveurs DNS IPv6 fonctionnent néanmoins. La principale difficulté sera donc d'assurer l'interopérabilité IPv4/IPv6 pour cette fonction, de façon transparente notamment lors du procédé de résolution de noms de domaine.

Actuellement, les serveurs DNS sont hébergés par des organismes associés à la gouvernance de l'Internet. Ainsi, en France, c'est Renater qui administre le premier serveur DNS IPv6. Selon les experts, le principal problème ne sera pas technique et ne concernera pas les serveurs DNS « nationaux » : l'organisation du DNS est hiérarchique, et ce qui manque aujourd'hui est une capacité de gérer le DNS au sommet de cette hiérarchie : les serveurs racines (root) ne sont pas prêts. Il s'agirait là d'une cause « politique » plus que technique : blocages de l'IANA et de l'ICANN.

Une prise de position des autorités internationales de l'Internet s'impose à présent. En effet, c'est en partie en décidant de la hiérarchie du DNS IPv6 mondial que l'on construira l'Internet de demain. En l'absence de décision, on pourrait assister à un morcellement du DNS mondial : serveur DNS racine en Asie, serveur DNS racine en Europe. Ainsi l'arrivée d'IPv6 peut être l'occasion de remettre en cause l'hégémonie des USA dans la gestion actuelle du DNS mondial.

5 Les enjeux pour la régulation

- **Intensification de la concurrence mais risque de nouveaux goulets d'étranglement**

L'arrivée d'IPv6 pourra conduire à **intensifier la concurrence sur des marchés existants liés à l'accès à Internet** : la suppression de la rareté des ressources en adresses IP et une baisse des coûts de gestion des réseaux par les ISP pourraient abaisser les barrières à l'entrée ; le système d'auto-configuration et le modèle de communication poste à poste pourraient contribuer à fluidifier la concurrence entre ISP. De nouveaux marchés sont susceptibles d'apparaître essentiellement sur les services (solutions de transition, accès par de nouveaux terminaux d'accès à Internet, fonctionnalités spécifiques offertes par IPv6 pour les services de jeux distribués ou de visioconférence).

A l'inverse, IPv6 peut également faire apparaître **de nouveaux goulets d'étranglement** : en l'absence d'assouplissement du mécanisme actuel restrictif d'allocation des adresses, en l'absence de disponibilité d'une offre de transit sous IPv6, en cas de retard ou de limitation dans la disponibilité de systèmes d'exploitation compatibles. Des positions dominantes pourraient se créer ou se renforcer sur des marchés de produits (routeurs et systèmes d'exploitation) ou de services, au profit des opérateurs de backbone IPv6, ou de certains équipementiers.

- **Déploiement d'IPv6 dans un cadre réglementaire rénové**

Le déploiement d'IPv6 interviendra en grande partie dans un cadre réglementaire rénové, au plus tard à la mi 2003, marqué notamment par l'harmonisation du régime applicable aux différents réseaux et services de communications électroniques.

À la suite des travaux de l'IPv6 Task Force, la Commission Européenne a publié le 21 mars 2002, une communication sur l'Internet nouvelle génération, proposant **des priorités d'actions dans la migration vers le nouveau protocole IPv6.**

L'utilisation de ce protocole par les opérateurs n'est pas susceptible de modifier la qualification juridique de réseaux et services, ni leur régime, mais un suivi du déploiement pourra être effectué sur la base des informations qui leur seraient demandées.

- **IPv6 et la réforme des instances de gouvernance de l'Internet**

Le passage à IPv6 s'effectue dans le contexte plus global de la réforme des instances de l'Internet. Une certaine opacité entoure les règles d'attribution des adresses IPv6 en raison de l'absence de visibilité sur le calendrier d'adoption et du nombre d'intervenants dans le processus, mais les futures règles d'allocation tentent de limiter les risques d'atteinte à l'égalité des conditions de concurrence.

On peut relever qu'à l'occasion de la définition des nouvelles politiques d'allocation IPv6, un effort de clarification du rôle respectif des différents organismes d'autorégulation est effectué, qui témoigne d'un souci de plus grande transparence dans les processus d'adoption. Ainsi, selon le projet d'accord au 9 avril 2002 entre l'ICANN et les RIR, les RIR sont responsables pour l'allocation des adresses et le développement des politiques relatives à leur région. L'ICANN est responsable de la coordination globale et de la gestion des ressources. L'accord reconnaît la validité de la révision au sein de l'ASO des politiques actuelles d'adressage et l'ICANN comme l'organisme responsable de l'allocation des adresses aux RIR, mettant ainsi fin à la persistante incohérence de l'IANA dans la description des processus d'allocation. Mais les régulateurs n'ont pas de compétence en la matière et les gouvernements interviennent en bout de chaîne à titre consultatif.

- **Une nouvelle politique d'adressage**

Les nouvelles politiques d'adressage IPv6, tout en réaffirmant les principes de gestion des adresses IP, conduisent à donner une plus grande importance à l'objectif d'agrégation qu'à celui de « conservation » des adresses et ont introduit un nouveau principe d'équité et d'impartialité des pratiques et politiques. La publication des adresses attribuées par les RIR, l'absence de droit de propriété sur les adresses IP attribuées et le contrôle des différents transferts entre les registres des adresses attribuées tentent de répondre à l'objectif d'une meilleure gestion des adresses IPv6.

Les conditions prévues par la politique actuelle (définie à titre intérimaire en 1999) sont favorables aux grands acteurs et à ceux positionnés tôt sur des réseaux expérimentaux, mais la nouvelle politique témoigne d'un rééquilibrage au profit des acteurs IPv4 tout en n'évitant pas tout risque de discrimination à l'égard des nouveaux acteurs « tout IPv6 ». Les discussions du projet « IPv6 Address Allocation and Assignement Policy » diffusé en décembre 2001 ont conduit à assouplir des conditions d'accès aux adresses IPv6 et à prendre en compte les bases de clients IPv4 des demandeurs.

La reprise des adresses non utilisées ne semble pas être un moyen déterminant pour retarder la pénurie des adresses IPv4 : **les mécanismes juridiques de reprise des adresses existent en théorie mais ne semblent pas utilisés par le RIPE**. Une politique restrictive d'allocation et d'attribution des adresses IPv4 pourrait retarder la pénurie des adresses IPv4. Une telle politique est prévue par le RFC 2050 et par le document RIPE 185 qui limite l'allocation et l'attribution des adresses aux besoins précis du demandeur d'adresses.

- **Interopérabilité : pas de difficultés majeures en vue**

Le nouveau protocole devra conduire à s'assurer que les ISP disposent, à terme, d'une offre d'accès non-discriminatoire aux réseaux sous IPv6. L'interopérabilité des services semble assurée par l'existence de solutions de transition et la disponibilité de routeurs et terminaux compatibles IPv4/IPv6. En cas de besoin, non avéré à ce jour, une possibilité théorique d'intervention de l'ETSI existe. La continuité de la qualité des services mobiles multimédia pourrait conduire à intervenir sur les accords d'itinérance.

- **Le choix de l'utilisateur**

Du côté des utilisateurs, IPv6 n'a pas d'incidence sur le choix, par l'internaute, de son opérateur d'accès ni de son ISP, sauf dans l'hypothèse où s'installerait une pratique de pré installation dans les terminaux des adresses d'ISP. Quant à la liberté d'accès aux sites et aux contenus, c'est l'ISP qui détient les moyens de la garantir, en proposant aux fournisseurs de contenus des accès IPv6, c'est-à-dire en pratique en s'équipant en serveurs à double pile pouvant être utilisés indifféremment par tous les fournisseurs. Néanmoins, la capacité d'auto-configuration facilite la pré-installation des adresses : selon les accords conclus entre le fournisseur du terminal (également ISP) avec les tiers, l'accès à des plates-formes de services pourrait être limité.

- **L'adresse IP et données personnelles**

La Commission européenne a rappelé dans sa communication du 21 février 2002 que **l'adresse IP pouvait être une donnée personnelle** au sens du cadre juridique communautaire. Les données de trafic, telles que l'adresse IP, doivent, en principe, être effacées ou rendues anonymes dès l'achèvement de la transmission, sauf exceptions. Le nouvel article L. 32-3-1 du Code des postes et télécommunications pose le principe de l'effacement immédiat ou de l'anonymat des données de communication, cette obligation s'imposant notamment aux ISP. Le respect du cadre communautaire relatif à la protection de la vie privée devrait également s'imposer au RIPE s'agissant de ses bases de données.

6 Conclusion

Plusieurs facteurs annoncent une transition prochaine vers **IPv6** :

- **l'immense capacité d'adressage** offerte par IPv6 permettra de sortir de la période de gestion de la pénurie d'adresses IP que nous vivons actuellement ;
- plusieurs facteurs déclencheurs du passage à IPv6 s'annoncent dès à présent autour notamment des **applicatifs « always on »** :
    - l'émergence des **services de données mobiles** autour du GPRS et UMTS. Toutefois, cette affirmation est à modérer. Le GPRS et l'UMTS se déploient dans leur première version avec l'IPv4,
    - les **accès haut débit (fixes et nomades du type WLAN)** consommateurs d'adresses permanentes,
    - **l'électronique connectée** qui constitue un levier potentiel de développement pour IPv6.
- Enfin, la **normalisation IPv6 est à présent suffisamment stable** pour commencer des déploiements commerciaux mais des chantiers importants restent ouverts.

Face à cette arrivée annoncée d'IPv6 on trouve **des acteurs en ordre de marche dispersé** :

- **les plus engagés sont les équipementiers télécoms** qui ont clairement identifié en IPv6 un relais de croissance,
- concernant les **opérateurs mobiles,** si le saut technologique IPv6 a bien été identifié par les instances de normalisation (notamment le 3GPP), les premiers déploiements GPRS et UMTS se font pour l'instant sous IPv4,
- les **opérateurs de backbone**, la plupart, sont attentistes et ne voient pas une forte demande IPv6 ; quelques exceptions sont à noter comme NTT ou Telia,
- concernant les **ISP**, la priorité semble aujourd'hui à la stabilisation de leurs modèles économiques sous IPv4 ; de plus, l'arrivée d'IPv6 suscite certaines craintes concernant principalement un contexte concurrentiel,
- enfin, **les entreprises** utilisatrices de technologies IP ne se sentent pas encore vraiment concernées par l'arrivée d'IPv6, d'autant plus que le retour sur investissement n'est pas évalué.

Le positionnement de ces différentes catégories d'acteurs est à moduler selon les zones géographiques, **les acteurs asiatiques étant globalement précurseurs** face au passage à IPv6.

La cohabitation entre IPv4 et IPv6 sera longue et inévitable, il est ainsi plus opportun de parler de déploiement d'IPv6 plutôt que de migration.

Par ailleurs, l'arrivée d'IPv6 peut remettre **en cause l'hégémonie américaine dans la gestion du DNS mondial**. À ce titre, les décisions à venir concernant la mise en place de DNS racine IPv6 seront cruciales. Disposant de serveurs DNS à un niveau national, l'Asie et l'Europe doivent de se positionner dès à présent sur ces questions.

Plusieurs enjeux pour la régulation ont été mis en évidence lors de cette étude :

- l'arrivée d'IPv6 pourrait conduire à intensifier la concurrence sur les marchés existants liés à l'accès Internet mais également à l'apparition de goulets d'étranglement notamment via les systèmes d'exploitation ou, en fin de déploiement, au niveau des backbones IP ;

- le passage à IPv6 s'effectue dans un contexte plus global de réforme des instances de l'Internet et de rééquilibrage des instances de gouvernance ;

- les procédures d'allocations d'adresses IP se distinguent des procédures d'attribution des numéros par l'absence de mise en œuvre du principe de séparation des fonctions de réglementation et d'exploitation qui permet, en pratique, de garantir réellement l'application des principes d'objectivité et de non-discrimination ;

- les nouvelles règles d'attribution d'adresses IPv6 proposées au printemps 2002 paraissent plus équitables mais une vigilance s'impose toutefois dans cette période de transition ;

- l'IPv6 n'a pas d'incidence sur le choix, par l'internaute, de son opérateur ni de son ISP, sous réserve d'une pré-installation dans les terminaux des adresses IP ; l'interopérabilité ne semble pas soulever de problématiques insolubles. L'existence de solutions de transition et la disponibilité de routeurs et terminaux compatibles IPv4/IPv6 permettront vraisemblablement d'assurer l'interopérabilité des deux protocoles.

Ainsi, si nécessaire, des lignes directrices relatives au calendrier des offres de transit sous IPv6 proposées par les opérateurs de backbones ou aux principes à respecter par les opérateurs et les ISP en vue de permettre le libre accès des utilisateurs aux services et contenus sont susceptibles d'apporter la visibilité souhaitée par le marché. Cependant, au stade actuel, les attentes des acteurs interrogés relèvent plus d'un environnement industriel favorable que d'interventions spécifiques de type réglementaire ou du régulateur.

Partie 2 : Notes de synthèse

1 Catégories d'acteurs et IPv6

1.1 Équipementiers télécoms, grand public et informatique

1.1.1 Rôle des équipementiers dans la migration vers IPv6

- **Les équipementiers télécoms ont adopté différentes stratégies, plus ou moins dynamiques, face à l'arrivée d'IPv6.**

Les équipementiers télécoms fournissent les matériels qui permettent l'acheminement des données sur les réseaux IP : il s'agit principalement des routeurs. Ces routeurs sont actuellement conçus pour acheminer les paquets de données en utilisant le protocole IPv4. L'utilisation d'IPv6, donc d'un format de paquets différent, nécessite une mise à niveau de ces infrastructures de routage. Ces mêmes équipementiers télécoms fournissent également des équipements d'accès à Internet : CPE et terminaux mobiles notamment.

- **IPv6 est un élément qui doit être pris en compte par les équipementiers grand public dans leurs réflexions sur l'avenir de l'électronique grand public connectée.**

Les équipementiers grand public fournissent des terminaux qui, à terme, devraient être connectés aux réseaux. Ces terminaux sont aussi bien des PDA, des consoles de jeux, que des mini-ordinateurs, des téléviseurs ou autres appareils domestiques (électroménager).

- **Les équipementiers et éditeurs informatiques ont un rôle majeur dans la migration vers IPv6.**

Les équipementiers informatiques quant à eux, fournissent les ordinateurs qui, actuellement, sont les principaux terminaux permettant d'accéder à Internet, mais surtout les serveurs, qui permettent d'héberger les sites Web, de distribuer les données et les mails, et constituent, sous IPv4, les principaux nœuds du réseau. Ils fournissent en outre les systèmes d'exploitation (OS) de ces terminaux et serveurs.

Tous ces équipementiers, peuvent, avec l'ouverture de nouveaux marchés et de nouveaux débouchés pour IP en dehors du monde informatique originel (on pense notamment aux secteurs de l'automobile, ou de l'aéronautique), se positionner comme de nouveaux entrants, capables d'apporter une expertise nouvelle et de proposer des solutions ad-hoc en complément des équipementiers traditionnels de ces secteurs.

1.1.2 Évolution du positionnement des équipementiers avec l'arrivée d'IPv6

1.1.2.1 Réseaux fixes

Équipementiers télécoms

- **Les leaders américains du marché des routeurs rattrapent leur retard face aux équipementiers japonais**

Les leaders américains du marché ont depuis le début participé aux travaux de l'IETF sur la définition des spécifications d'IPv6. Cependant, le travail de mise à niveau de leur matériel a semblé se faire attendre. Ainsi, les acteurs asiatiques (notamment HITACHI) ou européens (notamment Ericsson Telebit) ont pris une certaine avance dans la préparation de produits commerciaux. Aujourd'hui, les leaders comme Cisco ou Juniper ont, semble-t-il, rattrapé leur retard et la majorité des acteurs propose déjà (ou va proposer sous peu) des gammes de routeurs capables d'acheminer des trafics IPv6 : Cisco et Juniper proposent déjà des offres commerciales, Alcatel annonce des produits pour 2003, Hitachi fournit d'ores et déjà des routeurs aux quelques réseaux qui opèrent en IPv6.

- **Les leaders des équipements IP ne font pas une forte promotion d'IPv6 et se tiennent prêts.**
- **IPv6 est identifié par les équipementiers comme un relais de croissance en devenir.**

Bien qu'IPv6 ne soit pas encore largement déployé, il semble que les équipementiers télécoms aient pris la résolution de se tenir prêts à la transition en proposant des produits compatibles. Même s'ils interviennent dans les manifestations de promotion d'IPv6 en se déclarant prêts et en encourageant la transition, on ne décèle pas chez eux une tendance forte à pousser vers IPv6 autre que la volonté de voir s'accroître par ce biais le marché du renouvellement des matériels. Ainsi, même si certains équipementiers identifient IPv6 comme un relais de croissance, il est avant tout, pour le moment, un argument marketing.

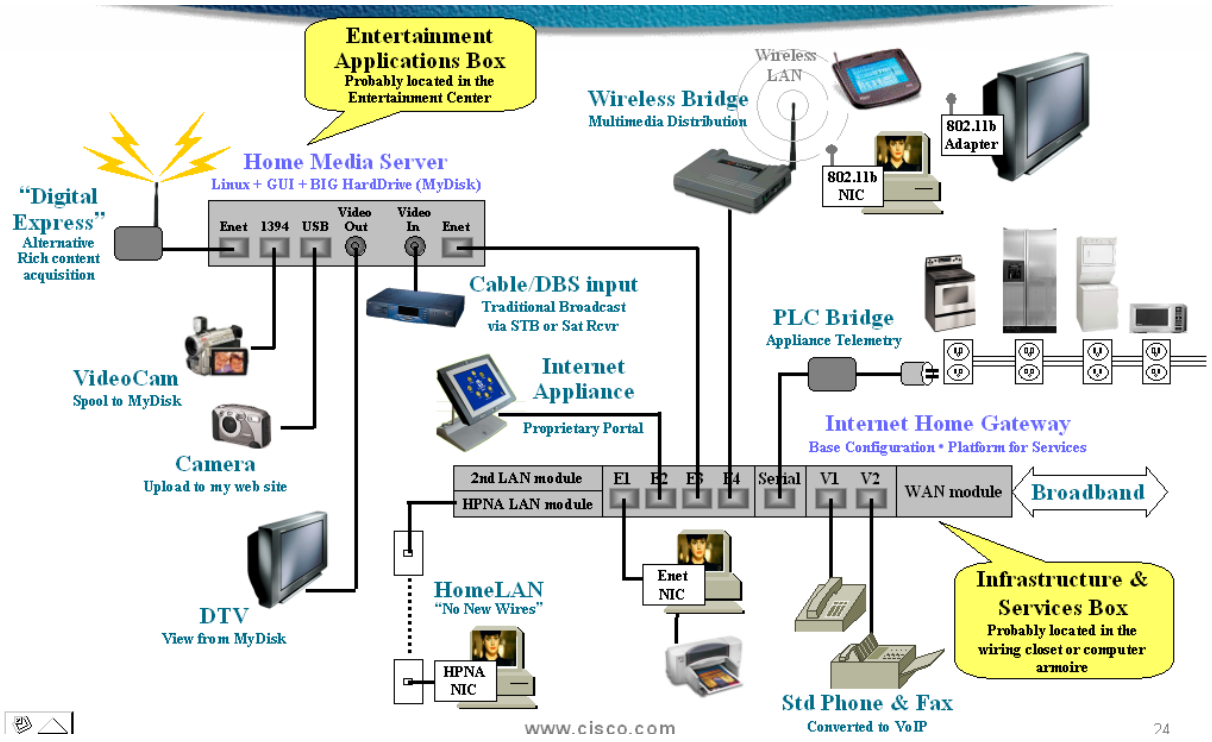
Équipementiers grand public

- **Le développement de l'électronique grand public connectée apparaît comme un enjeu d'avenir crucial pour Internet.**

Dans ce cadre, IPv6 apparaît pour beaucoup comme incontournable, notamment du fait de la quantité d'adresses qu'il est capable de fournir (nécessaire en cas d'accroissement des besoins), ainsi que les nouvelles fonctionnalités (gestion de la mobilité améliorée, auto configuration,...) qui sont de nature à améliorer la facilité d'utilisation d'IP pour le grand public et la prolifération du protocole IP en dehors du milieu informatique originel.

Aujourd'hui Thomson produit déjà des téléviseurs connectés à Internet (système TAK) en IPv4 (Thomson estime cependant que l'on a pas fait le tour de toutes les possibilités offertes par IPv4), alors que Sony doit présenter une console de jeux PS2 compatible IPv6 et que Panasonic propose déjà des produits de VoIP ou de fax sous IPv6. Philips déclare se positionner en observateur actif et participe aux discussions de l'IETF.

Figure 1 : Exemple d'application domotique : la maison connectée selon Cisco



Source : Cisco

Tableau 1 : Marché des terminaux numériques : Europe, Japon et USA

	2001	2002	2003	2004	2005	2006
Marché des STB[1] en volume (millions) – Europe	3,02	10,34	12,03	13,26	14,43	14,62
Marché des IDTV[2] en volume (millions) – Europe	0,11	0,16	0,36	0,78	1,11	1,51
Marché des STB en volume (millions) – Japon	3,51	3,85	4,40	4,77	5,48	4,95
Marché des IDTV en volume (millions) – Japon	0,16	0,29	0,46	0,56	0,70	1,23
Marché des STB en volume (millions) – USA	8,92	12,12	11,46	12,43	13,41	14,42
Marché des IDTV en volume (millions) – USA	0,07	0,08	0,14	0,20	0,29	0,44
Marché total des STB (millions)	**15,45**	**26,31**	**27,89**	**30,46**	**33,32**	**33,99**
Marché total des IDTV (millions)	**0,34**	**0,53**	**0,96**	**1,54**	**2,1**	**3,18**

Source : IDATE

- **Une claire avance des équipementiers grand public japonais : SONY, Panasonic.**
- **Une échéance encore lointaine pour les équipementiers grand public européens.**

Globalement, les équipementiers grand public japonais sont particulièrement dynamiques (IPv6 s'est imposé au Japon comme une « cause nationale ») alors que les Européens, même s'ils se tiennent prêts, adoptent une position moins motrice. IP constitue une opportunité pour ce type d'acteurs, notamment IPv6, mais le positionnement varie selon les zones géographiques, de moteur (Japon) à « suiveur actif » (Europe).

[1] STB : Set Top Box.
[2] IDTV : Integrated Digital TeleVision ; TV numérique intégrant la fonction STB.

Équipementiers informatiques – Grands éditeurs

- **La compatibilité IPv6 des OS est un élément clé dans le processus de migration vers IPv6.**
- **L'adaptation des OS est une condition nécessaire à la compatibilité IPv6 non seulement des terminaux d'accès et des serveurs mais aussi au développement d'applicatifs software sous IPv6.**

Les fabricants de serveurs, comme Compaq ou SUN, se déclarent aujourd'hui prêts pour IPv6. Le point crucial sur ce type de produits est l'Operating System (OS) qui permet d'exploiter les possibilités de la machine. La plupart des serveurs fonctionnent sous Unix avec des systèmes propriétaires. À ce jour, l'ensemble des constructeurs de serveurs proposent des systèmes Unix compatibles avec IPv6.

- **D'ici la fin 2002, la quasi-totalité des produits Microsoft et notamment les OS seront compatibles IPv6 par défaut (à partir de la version 2000).**
- **Windows XP est déjà compatible IPv6 mais pas par défaut.**
- **Les ordinateurs s'appuyant sur les Windows 95 et Windows 98 (majorité du parc PC aujourd'hui installé) ne seront jamais compatibles IPv6.**

Sur le marché de l'informatique grand public, la problématique est la même : c'est l'OS qui rend possible l'utilisation d'IPv6. Les produits Microsoft, leader absolu du marché des OS pour terminaux sont sur le point d'être prêts pour IPv6 : Windows XP est déjà prêt et présentera d'ici fin 2002, IPv6 par défaut (pour le moment, il est disponible mais doit être activé), et les autres produits Windows seront prêts avant la fin 2002. Le fait que le leader du marché aille vers IPv6 est un élément essentiel : si l'OS majoritaire est compatible IPv6, l'un des principaux points de blocage à la transition est levé.

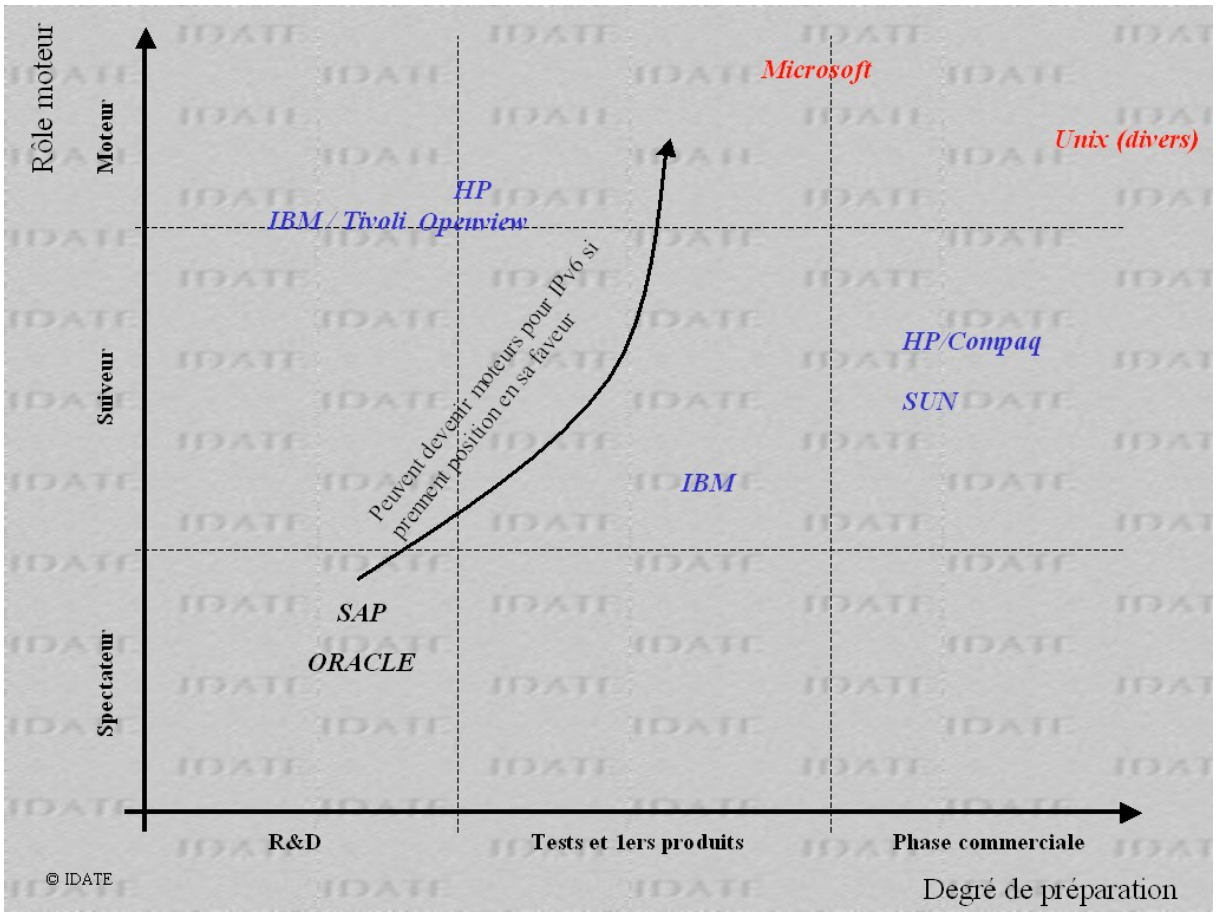
Il reste tout de même le problème du parc installé de PC dont la majorité possède encore comme OS des versions de Windows antérieures à Windows XP : Windows 2000 Windows NT et surtout Windows 98 et Windows 95. S'il existe des kits de mise à niveau IPv6 pour Windows NT et Windows 2000 par contre rien n'est disponible pour Windows 98 et Windows 95.

- **Les principaux fournisseurs d'applicatifs ne se prononcent pas face à IPv6 : SAP, Oracle.**
- **Aujourd'hui, ces fournisseurs d'applicatifs n'ont pas de demandes claires de la part des entreprises pour des produits compatibles IPv6.**
- **Il n'existe pas aujourd'hui d'outils de gestion de réseaux IP compatibles IPv6 : HP Openview, Tivoli**

Les principaux fournisseurs d'applicatifs ne sont pas prêts aujourd'hui face à l'arrivée d'IPv6. Le déblocage venant des OS peut changer rapidement la situation, tout comme une prise de position d'éditeurs comme Oracle ou SAP sur le sujet.

Il n'existe, en outre, pas d'applicatifs de gestion des réseaux IPv6, à l'exception d'une version bêta de HP Openview destinée au Japon uniquement. Pour l'instant, tous les réseaux expérimentant IPv6 s'appuient sur des outils de gestion sous IPv4 ; la situation pourrait devenir préoccupante si cette incompatibilité IPv6 des outils de gestion réseau perdure.

Figure 2 : Positionnement des acteurs (éditeurs)



Source : IDATE

1.1.2.2 Réseaux mobiles

Mobilité dans IPv6 et Mobile IPv6

- **Il faut bien distinguer IPv6 et les avantages inhérents au protocole (espace d'adressage notamment), de Mobile IPv6, protocole distinct d'IPv6.**
- **Mobile IPv6, protocole issu du monde informatique, est bien adapté pour une gestion de la mobilité au sein ou entre réseaux locaux.**

Un certain nombre d'améliorations fonctionnelles d'IPv6 par rapport à IPv4 permettent de mieux gérer la mobilité dans les réseaux au sens large : parmi celles-ci on trouve les fonctions d'auto configuration qui permettent à un terminal de trouver sa place dans un réseau visité, secondées par des fonctions de type « neighbour discovery », etc…, qui remplacent avantageusement des fonctions « rajoutées » à IPv4, ou encore le format des en-têtes qui permet d'optimiser le routage et de le simplifier dans les cas de mobilité (mise à jour du chemin avec chaque paquet, …)[3].

[3] On pourra se reporter à l'étude documentaire pour plus de précision.

Parallèlement, une version v6 du protocole Mobile IP a été développée. Elle a pour but, notamment, de remplacer Mobile IPv4 et d'améliorer des points comme le routage (suppression du routage triangulaire, etc.). Mobile IP version 4 n'est aujourd'hui pas utilisé dans les réseaux cellulaires (c'est GTP qui est utilisé) et l'importance de l'évolution de v4 vers v6 dans ce domaine est donc toute relative. Mobile IP n'est qu'un outil permettant de gérer la mobilité, mais pas le seul. Il apparaît en revanche comme très utile pour la gestion de la mobilité dans les réseaux hétérogènes.

Le développement d'une solution particulière pour gérer la mobilité dans les réseaux cellulaires (GTP) s'explique par le fait que Mobile IP n'est pas adapté à la gestion de la mobilité dans ce contexte : Mobile IP est en fait une solution issue du monde informatique, dont le but est la gestion de la mobilité entre ou à l'intérieur de réseaux locaux en IP en s'appuyant typiquement sur des technologies de type WLAN (802.11).

Équipementiers de cœur de réseaux

- **Les équipementiers européens leaders dans la mobilité comme Ericsson ou Nokia sont actifs dans le domaine d'IPv6.**
- **Ces mêmes équipementiers identifient IPv6 comme un relais de croissance.**
- **Ces équipementiers identifient les services mobiles s'appuyant sur des réseaux GPRS tout d'abord puis 3G, comme une réelle opportunité pour IPv6.**
- **C'est essentiellement par l'apport de son espace d'adressage permettant des accès permanents qu'IPv6 permettra de développer des services mobiles attrayants.**

En Europe, les équipementiers spécialisés dans la mobilité et notamment les réseaux cellulaires sont actifs dans le domaine d'IPv6 qu'ils identifient comme un relais de croissance. Ainsi, Ericsson (par ailleurs propriétaire de Telebit, pionnier en matière de routeur IPv6) et Nokia proposent des gammes de routeurs compatibles pour IPv6. Ces acteurs considèrent que l'Internet mobile sera un moteur de croissance d'IP et qu'IPv6 sera nécessaire pour développer des services attrayants. L'horizon de la 3G est clairement évoqué par ces derniers comme une réelle opportunité pour IPv6.

Terminaux

- **Ericsson et Nokia livreront à partir de 2003 des terminaux GPRS puis UMTS avec une double pile v4/v6.**
- **L'ampleur du relais de croissance IPv6 identifié par les équipementiers mobiles dépendra fortement du succès des services mobiles sur GPRS.**

Pour le moment, les premiers terminaux cellulaires « IP » sont les terminaux GPRS en Europe, qui fonctionnent en utilisant IPv4. Ericsson insiste néanmoins sur le fait que ses terminaux haut de gamme intègrent une double pile v4/v6 et Nokia affirme que ses terminaux seront livrés en 2003 avec une double pile v4/v6. Au Japon, l'i-mode de DoCoMo, ainsi que les premiers réseaux 3G FOMA fonctionnent encore sous IPv4, tout comme les terminaux utilisés.

Pour la plupart des constructeurs de terminaux cellulaires, IPv6 apparaît comme incontournable dans un scénario de développement fort de l'Internet mobile, du fait du nombre d'adresses offertes, et même si IPv6 ne sera obligatoire que pour certaines applications (multimédia) qu'à partir d'UMTS Release 5, dont les spécifications devraient s'achever courant 2002.

- **OS mobile : Symbian a une forte demande de ses clients pour une compatibilité IPv6 de son OS.**

Concernant les produits nomades type PDA, ordinateurs portables, etc..., la compatibilité v6 passe par les OS mobiles : Symbian dit avoir une forte demande de ses clients pour une compatibilité IPv6 et Windows CE est en cours de mise à jour.

Nouvelles applications

- **Mobile IPv6 représente une opportunité pour les équipementiers positionnés sur les technologies de type WLAN**

Hors des réseaux cellulaires, nous l'avons vu, les ordinateurs portables, les PDA, les outils nomades en général sont mobiles. La mobilité au sein de réseaux hétérogènes, le développement des technologies de type WLAN comme 802.11b ou encore Bluetooth peut être un facteur de croissance important du besoin en adresses. Dès lors, IPv6 et surtout Mobile IPv6 se présente comme une solution confortable pour les équipementiers positionnés sur ces technologies.

Plusieurs secteurs sont intéressés par la mobilité et la connectivité mobile : entre autre l'aéronautique avec la possibilité d'utiliser IP plutôt que ses protocoles propriétaires, avec en outre l'opportunité de développer nombre d'applications embarquées, assez proches de ce que peuvent aujourd'hui imaginer les constructeurs automobiles avec la voiture connectée.

Néanmoins, les standards supportant la mobilité 3G/WLAN ne sont pas encore développés : il est donc probable que la mobilité entre réseaux hétérogènes ne soit envisageable qu'au-delà de 2005.

1.1.3 Impacts techniques

1.1.3.1 Évolution des équipements IP

- **Dans l'évolution des équipements IP vers IPv6, il faut distinguer les étapes Software et Hardware.**
- **La compatibilité IPv6 Software est une première étape qui précède l'implémentation Hardware d'IPv6 pour des performances accrues.**

Dans le domaine des équipements, les évolutions peuvent être logicielles ou hardware. Les évolutions logicielles correspondent principalement à des mises à niveaux des logiciels qui permettent aux équipements de fonctionner (OS). Ces mises à niveaux correspondent à un nouveau code introduit dans la machine et que celle-ci interprète afin de prendre en compte de nouvelles fonctionnalités ou modes de procédure. Les produits hardware correspondent à un stade plus abouti du matériel : lorsque les évolutions sont stabilisées, les « programmes » passent alors d'un ensemble de « lignes de codes » exploitées par un processeur à une implémentation sous forme de processeur dédié, plus rapide et plus fiable.

1.1.3.1.1 Hardware

- **Une claire avance des équipementiers japonais sur les routeurs IPv6 Hardware.**

Dans le domaine des équipements de réseau (routeurs), on trouve peu de produits hardware pour le moment. Hormis quelques petites sociétés européennes, ce sont les équipementiers japonais qui sont le plus avancés dans ce domaine. Hitachi notamment, propose des routeurs hardware prêts pour IPv6. Matsushita également propose un routeur IPv6, tout comme Fujitsu. Dans le domaine des équipements grand public, comme nous l'avons vu, des produits sont présentés chez Sony et Panasonic. Côté Amérique du Nord, Nortel Networks propose un produit hardware, mais si celui-ci était techniquement prêt, il n'était pas encore commercialisé fin 2001.

1.1.3.1.2 Software

- **Les équipementiers IP leaders disposent de routeurs compatibles IPv6 en Software**

L'ensemble de la gamme de Cisco peut subir un upgrade logiciel afin de bénéficier de la double pile v4/v6. Un service commercial complet est attaché à cette possibilité. Juniper propose également des produits IPv6, tout comme Nortel. JUNOS, le système d'exploitation des routeurs Juniper est déjà prêt pour IPv6 et l'équipementier prépare une offre IPv6 Hardware.

En Europe, Alcatel propose des upgrades logiciels sur les produits de sa gamme et pense commercialiser des versions Hardware d'ici 2003.

Sur le plan des matériels informatiques, nous l'avons vu, la plupart des OS sont à niveau, y compris sur le marché grand public, et Symbian travaille sur le sujet concernant les produits mobiles (demande de ses clients).

1.1.3.2 Techniques d'interopérabilité

- **Il existe à présent plusieurs techniques permettant d'inter opérer des réseaux IPv6 et IPv4 ; ces techniques sont des outils Software.**
- **Il manque à présent, parmi ces différents mécanismes, une grille d'utilisation précise et des déploiements hors des laboratoires pour tester leur efficacité.**

Les équipements d'interopérabilité sont conçus pour permettre le fonctionnement des réseaux IPv4 et IPv6 sans rupture : un nœud IPv4 doit pouvoir adresser un nœud IPv6, et vice versa. Ces équipements sont principalement des logiciels et s'apparentent ainsi plus à des techniques qu'à des matériels.

Les routeurs peuvent présenter une double pile IPv4/IPv6 qui leur permet d'acheminer indifféremment des paquets IPv4 ou IPv6. En effet, si certains réseaux sont 100% IPv6, il est à prévoir que la majorité des acheminements de données IPv6 se fasse sur les réseaux IPv4 existants (cf. scenarii de transition).

La plupart des constructeurs déjà cités proposent des doubles piles. De la même manière, sur les terminaux, les téléphones portables (notamment Ericsson) proposent des doubles piles v4/v6.

Pour les terminaux dont l'exploitation se fait au travers d'un OS purement logiciel (ordinateurs, serveurs), les OS présentent aussi, dans leur quasi-totalité, cette double pile.

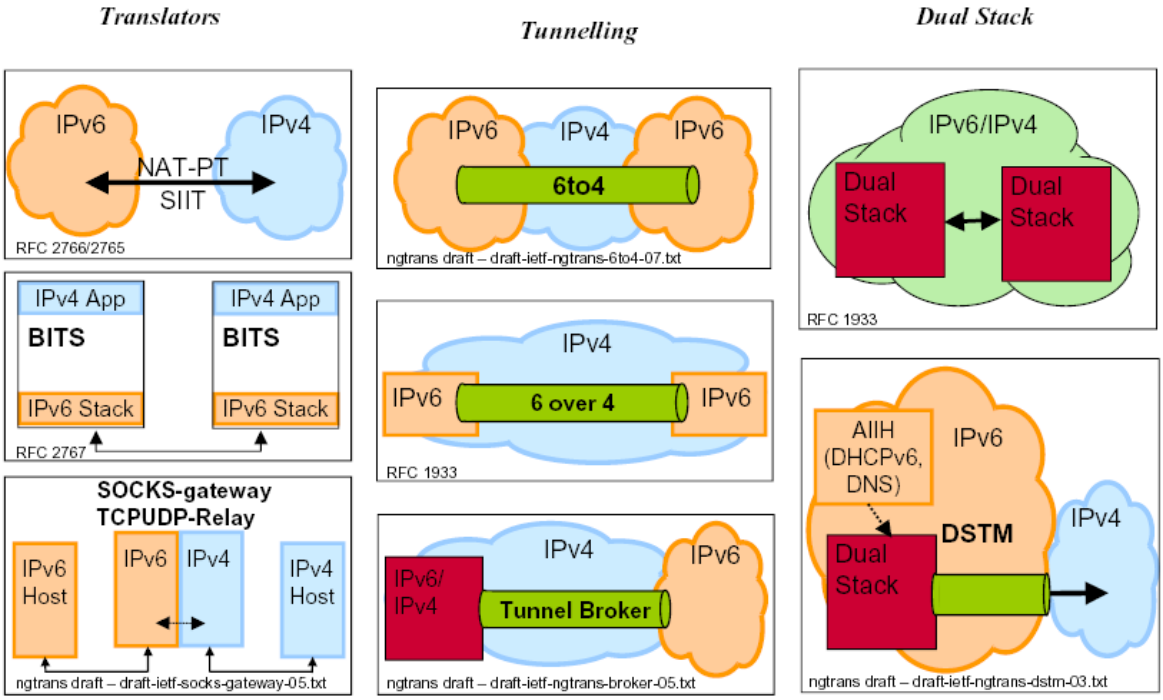
Plusieurs outils d'interopérabilité existent :

- les tunnels, permettent l'encapsulation de paquets v6 dans des paquets v4 (technique 6to4) : on peut ainsi opérer en v6 au travers des réseaux v4 existants. Les premiers ISP à proposer des services v6, faute d'infrastructures v6 natives, ont recours à ces techniques ;
- les translations d'adresse sont également utilisées pour assurer l'interopérabilité (NAT-PT).

Nombre de techniques, globalement basées sur ces principes existent, et sont préconisées par l'IETF dans le cadre de la transition ; elles doivent permettre d'assurer cette transition avec un minimum de heurts. C'est l'épreuve du « terrain » qui seule pourra révéler la valeur de ces solutions qui fonctionnent sur les bancs d'essais. Il manque aujourd'hui une certaine visibilité au niveau de ces mécanismes : il faut à présent déterminer une « grille d'utilisation » des mécanismes : quel mécanisme, dans quel cas, à quel endroit, à quel moment ?

Aujourd'hui, certains acteurs se positionnent sur le marché comme fournisseur de ces solutions de transition et d'interopérabilité : on retiendra notamment l'exemple de Free6net au Canada qui fournit des solutions tunnels.

Figure 3 : Mécanismes de transition d'IPv4 vers IPv6 selon l'IETF



Source : BT

1.1.4 Les étapes de transition vers IPv6

- **Plusieurs scénarios de transition ont été élaborés par l'IETF.**
- **Les équipementiers s'accordent pour définir 5 phases dans le processus de migration vers IPv6 allant de la domination totale d'IPv4 (situation actuelle) à la domination totale d'IPv6 (situation future a priori lointaine).**

Tableau 2 : Les 5 phases de transition vers IPv6

Phase	Situation	Outils
1	IPv4 = Internet	Les outils connus et hérités de l'Internet actuel.
2	Quelques îlots v6 dans un océan de v4	Tunneling, 6to4, -over4, NAT-PT, etc. permettent de faire passer IPv6 dans les réseaux v4.
3	Des grands réseaux IPv4 et IPv6 cohabitent.	Chaque réseau a ses propres outils et la communication se fait grâce à des outils comme NAT-PT, des socks-Gateway, …
4	IPv6 domine et quelques îlots IPv4 subsistent.	Les outils « inverses » de ceux de la phase 2 permettent à IPv4 de traverser l'Internet v6 : DSTM, NAT-PT, 4to6, …
5	Internet = IPv6	Les outils sont ceux d'IPv6. Les derniers îlots d'IPv4 sont anecdotiques et utilisent les outils de la phase 4.

Source : IDATE

En parallèle, les équipementiers envisagent plusieurs **stratégies de transition** pour les fournisseurs d'accès, on en dénombre essentiellement 4 se déclinant sur une échelle de coûts et temporelle :

- **IPv6 sur IPv4 : à base de tunnel** ; c'est le réseau 6 Bone :

Sur ce scénario il y a une pléthore de méthodes définies par l'IETF. C'est par ce scénario que commence l'arrivée d'IPv6 : ça ne coûte rien (upgrade gratuit) et il n'existe pas de risques techniques. Des produits d'équipementiers permettent de faire du v6 sur v4 depuis 5 à 6 ans.

Ce scénario a une vocation pédagogique ; dès que l'on arrive à 100 ou 200 sites à gérer via des tunnels cela devient vite ingérable.

- **IPv6 natif sur des liens dédiés** :

Ce sont des opérateurs/ISP qui ont un réseau IPv4 sous ATM, Frame Relay,… Le but est de séparer le trafic IPv4 du trafic IPv6 et de construire des liens dédiés sous IPv6. Ainsi les opérateurs ne prennent pas de risques en séparant le réseau IPv4 qui est aujourd'hui leur seule source de revenus. La gestion du réseau continue à se faire sous IPv4.

Le coût de ce scénario se limite aux liens dédiés plus quelques routeurs IPv6.

IIJ (Japon), NTT Verio ou Telia ont opté pour ce scénario.

- **Construire un réseau mixte IPv4 et IPv6** : 2 solutions sont alors possibles :
  - construire un réseau IPv4 et un réseau IPv6 gérés en **Dual Stack,**
  - solution **MPLS**.

Ce scénario est plus compliqué à mettre en œuvre ; cette fois-ci ont à un réseau à la fois IPv4 et IPv6.

On peut, sur ce scénario, ouvrir des accès IPv6 à des clients en déployant des routeurs v6 uniquement sur le bord de réseau (Edge). Ce scénario n'implique pas de changer tout le hardware mais seulement une partie et un upgrade logiciel sur tout le réseau suffit.

Dans ce scénario, il y a un coût homme non négligeable puisqu'il faut mettre à jour tout le réseau en software et conduire les tests nécessaires.

La solution MPLS permet de disposer d'une certaine flexibilité : on peut mettre à jour en IPv6 les équipements de bord de réseau en fonction de la demande.

- **Construire un réseau « IPv6 only »**

Il y a très peu d'opérateurs qui veulent aujourd'hui remettre en cause toute leur infrastructure IPv4. Dans ce scénario, l'opérateur doit changer tout le Hardware. Des équipementiers leaders ont quelques demandes de la part de start-ups « Je dois créer un nouveau réseau, pourquoi ne pas le faire directement en IPv6 ? ».

Aujourd'hui, la technologie n'est pas assez mature pour ce scénario. De plus, il est difficile de justifier un déploiement « IPv6 only » alors que l'Internet est IPv4 aujourd'hui : on fera donc que du tunnelling IPv4 dans IPv6 !

De plus, on ne trouve pas aujourd'hui d'outil de gestion de réseaux sous IPv6 (à nuancer avec l'apparition de HP Openview en version bêta au Japon), ni de provisionning sous IPv6.

1.1.5 Impacts économiques : IPv6, quels avantages pour les équipementiers ?

1.1.5.1 Équipementiers leaders

- **IPv6 va accélérer le renouvellement des parcs (terminaux et routeurs d'accès) mais sans imposer un surcoût d'équipement pour les utilisateurs finaux.**
- **La compatibilité IPv6 des routeurs d'accès se fera d'abord à travers une mise à jour Software puis par un renouvellement des équipements d'accès.**
- **En cœur de réseau, à coût égal, de par la taille plus importante des en-têtes IPv6, les performances (vitesse) des routeurs sous IPv6 seront moindres comparées à celles des routeurs sous IPv4.**
- **Globalement, on doit quand même s'attendre, à coût égal, à une dégradation des performances en cœur de réseau (vitesse) avec le passage à IPv6 : les en-têtes IPv6 sont plus lourdes à traiter que les en-têtes IPv4 et le temps calcul est donc plus important.**

Les coûts induits pour les équipementiers informatiques sont, a priori, assez faibles : en effet, Compaq déclare avoir dépensé moins de $1 million sur 5 ans pour mettre à niveau ses produits, et globalement, les travaux de mise à niveau ne présentent pas de difficultés majeures. L'impact économique sur les différents équipementiers (constructeurs de routeurs, de serveurs, fournisseurs d'OS,…) est donc plutôt positif, avec l'opportunité de voir un renouvellement du matériel, pour un coût de mise à niveau relativement faible.

Pour les équipementiers, les impacts techniques sont plutôt positifs également : tables de routage allégées compensant l'accroissement de la taille des en-têtes, qui par ailleurs ne sont plus traitées par chaque routeur, grâce à une fonction de « saut ». Il faut cependant nuancer cette avancée par le fait que tous les paquets ne seront pas traités de la sorte et on ignore quelle sera la proportion de ceux bénéficiant de cette fonction de saut, ou devant au contraire être examinés par le routeur.

Tableau 3 : Coût de la transition IPv6, à performances égales

Faible	Moyen	Fort
Fabricants de PC	OS et serveurs CPE	Routeurs cœur de réseau

- **Les équipementiers IP leaders n'ont pas tous les éléments aujourd'hui pour construire en direction de leurs clients ISP et entreprises le « Business case IPv6 ».**

Si la plupart des équipementiers IP s'accordent pour identifier l'arrivée d'IPv6 comme un levier de croissance, ils ne peuvent pour l'instant disposer de tous les éléments leur permettant de démontrer l'intérêt économique de la migration vers IPv6 chez leurs clients. La difficulté étant d'identifier précisément les surcoûts d'exploitation de solutions IPv4 en face des avantages offerts par IPv6 : techniques et applicatifs.

- **IPv6 est utile pour atteindre de nouveaux marchés pour les différents équipementiers :**
  - **via l'électronique connectée : équipementiers grand public,**
  - **l'intrusion d'IP dans d'autres secteurs que l'Informatique et les télécommunications : équipementiers IP.**

De nouveaux marchés s'ouvrent pour les équipementiers grand public, qui voient la possibilité d'adresser le marché de l'électronique communicante. Pour les équipementiers IP et informatique, s'ouvrent de nouvelles opportunités, grâce à l'apparition des nouvelles applications connectées, motrices pour IPv6.

Dans tous les cas, si de nouveaux marchés ne s'ouvrent pas, l'apparition d'IPv6 est un encouragement à la mise à niveau des produits chez les clients et devrait donc jouer un rôle positif sur les équipementiers de tout ordre, dynamisant le marché.

1.1.6 Calendrier

1.1.6.1 Équipementiers leaders

Les leaders du marché ont l'opportunité de se positionner comme des spécialistes de la nouvelle technique et d'encourager leurs clients à renouveler le matériel. Comme un fabricant de processeur communique sur la présence de ses produits dans les ordinateurs, on peut imaginer que les équipementiers leaders n'hésiteront pas à communiquer, si ce n'est en disant « IPv6 inside », du moins en clamant « IPv6 enable ».

- **Selon Cisco, le gros du marché IPv6 pour ces produits devrait apparaître vers 2004.**

On note toutefois une certaine prudence chez les leaders, qui semblent considérer que l'échéance reste encore lointaine. Selon Cisco, le gros du marché IPv6 pour ces produits devrait apparaître vers 2004 et le leader des équipements IP ne conduit pas aujourd'hui de campagne agressive de promotion d'IPv6 envers ses clients.

1.1.6.2 Start ups

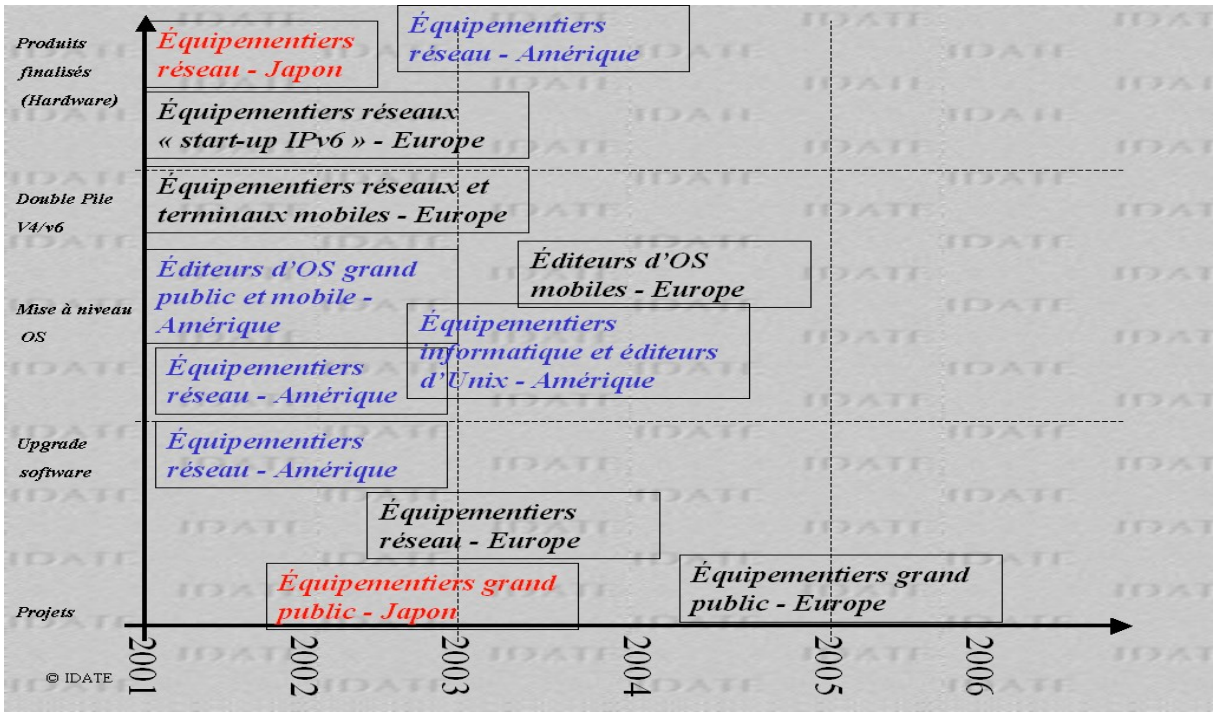
- **Des start ups comme 6WIND en France sont particulièrement dynamiques face à IPv6 et parient sur l'avènement prochain du nouveau protocole.**

Des sociétés, comme 6Wind en France, parient sur l'avènement d'IPv6 et fondent leur savoir-faire et leur communication sur la nouvelle version d'IP. Si le positionnement est correct, les bénéfices en termes d'image et donc de marchés peuvent être positifs. L'inconnue reste la date à laquelle les déploiements IPv6 deviendront massifs. Le risque est donc de devancer la fenêtre stratégique, comme l'a fait l'opérateur américain Zama, parti trop tôt, et/ou, de sous-estimer l'importance du nouveau marché. La tranquillité des leaders du marché enfin, est peut être due à une estimation du marché encore lointaine, mais aussi à une volonté de retarder ce marché afin d'être prêt à faire face à des demandes pointues : les nouveaux entrants auront alors perdu l'avantage de la précocité. De nombreuses incertitudes pèsent donc sur les réels avantages de ce choix stratégique.

On trouve des start-ups en Europe, aux USA. En Asie, le marché IPv6 plus dynamique a été largement occupé par des géants industriels réunis au sein du consortium WIDE (projet de coopération industrielle entre les principaux industriels des secteurs électronique/ informatique/ télécoms au Japon, dans le but de promouvoir IPv6).

1.1.6.3 Roadmap IPv6

Figure 4 : Roadmap IPv6



Source : IDATE

Dès 2001, les principaux équipementiers réseaux ont commencé à proposer des upgrades logiciels et des mises à jour des OS de leurs routeurs pour les rendre compatibles avec IPv6. Les équipementiers Japonais sont quant à eux déjà prêts pour IPv6 avec des produits Hardware finalisés, alors que de tels produits Hardware n'arriveront dans les gammes des leaders du marché qu'aux alentours de 2003, à l'exception d'Alcatel qui adopte un rythme plus lent.

Les OS Unix des fabricants de serveurs sont déjà prêts pour IPv6 alors que Microsoft devrait avoir procédé à la mise à jour de l'ensemble de son offre d'ici la fin de l'année 2002. Parallèlement, Symbian pense qu'IPv6 devrait être rapidement intégré dans ses produits, sous la demande de ses clients (au plus tard 2004). Les outils de gestion de réseaux sous IPv6 n'existent pas encore, mais des annonces laissent espérer une arrivée de produits (au moins en version beta) pour 2003.

Sur le plan de l'électronique grand public, les firmes Japonaises semblent en avance et proposent déjà des produits pour certaines (Matsushita) ou sont sur le point de le faire (Sony) : les Européens, quant à eux, adoptent dans ce domaine une position de suiveurs et ne devraient pas, en l'état actuel des choses, réagir avant 2005.

1.1.7 Synthèse

Télécommunications

- **Réseaux fixes**
  - **Après avoir pris du retard, les leaders américains s'adaptent à IPv6 pour l'instant en se limitant au Software.**
  - **Ces leaders ont encore du mal à convaincre leurs clients ISP et entreprises (ROI).**
  - **Les équipementiers japonais ont sorti des routeurs Hardware IPv6 et ont une politique visant à être les premiers sur le marché.**
- **Réseaux mobiles**
  - **Le saut technologique IPv6 a été identifié par le 3GPP (Release 5).**
  - **Les équipementiers leaders européens (Nokia, Ericsson) sont actifs afin de se positionner sur IPv6.**

Informatique

- **Les acteurs des serveurs et des OS sont prêts ou sur le point de l'être face à l'arrivée d'IPv6**
- **D'ici la fin 2002, la quasi-totalité des produits Microsoft et notamment les OS seront compatibles IPv6 par défaut (à partir de la version 2000).**
- **Les ordinateurs s'appuyant sur les Windows 95 et Windows 98 (majorité du parc PC aujourd'hui installé) ne seront jamais compatibles IPv6.**
- **Les fournisseurs d'applicatifs ne se prononcent pas face à IPv6 (SAP, Oracle) car pas de demandes claires de la part des entreprises.**

Électronique Grand Public

- **Une claire avance des Japonais (SONY, Panasonic) avec une vision optimiste du développement de leur marché domestique : domotique, jeux en ligne**
- **Les européen ne perçoivent pas de marché dans l'immédiat.**

1.2 Opérateurs : fixe et mobile

1.2.1 Rôle des opérateurs de backbone dans la migration vers IPv6

- **L'attitude « Wait & See » des opérateurs de backbone leaders en place et de la plupart des opérateurs historiques :**
    - **ils expérimentent et se tiennent prêts,**
    - **pas de demandes significatives de leurs clients ISP ou entreprises.**

Les opérateurs de backbone peuvent constituer un goulet d'étranglement dans la transition vers IPv6 : s'ils n'assurent pas le transit des données en IPv6, les autres opérateurs et ISP sont contraints d'avoir recours à des techniques d'encapsulation dans IPv4 pour faire transiter les données entre des nœuds distants. Ces techniques peuvent suffire pour un premier stade de déploiement d'IPv6.

Ainsi, le préalable au développement généralisé d'IPv6 est la possibilité de disposer de backbones capables d'assurer le trafic en IPv6.

À ce jour, les opérateurs de backbone semblent plutôt attentistes. Ils se tiennent prêts, maîtrisent la technologie, notamment en participant à des tests, ou en opérant localement des réseaux IPv6 expérimentaux, mais attendent qu'une demande significative apparaisse.

Un acteur comme UUNET WorldCom est précisément dans ce cas : la technique est maîtrisée (opération de réseaux universitaires aux USA), la réponse à la demande sera réelle (politique commerciale), des points de peering existent (à Londres), mais pour l'heure, il n'y a pas (du moins en Europe) d'offre commerciale.

De la même manière, la majorité des opérateurs historiques européens, qui disposent d'infrastructures à grande échelle, sont en attente d'une demande avant de se lancer sur une offre de transport IPv6 : pour autant, ces opérateurs mènent des programmes de recherche poussés, et se tiennent prêts à réagir rapidement (c'est notamment le cas pour BT et France Telecom). Les réseaux de recherche (VTHD en France par exemple), sont opérés en double pile, mais l'offre et les efforts commerciaux, ne viendront que quand la demande sera réellement perçue : selon ces mêmes acteurs, pas avant 2 ou 3 ans.

- **Certains opérateurs de backbone saisissent l'opportunité IPv6 pour conforter leur position sur le marché du transit IP : NTT, Telia.**

Parallèlement, certains opérateurs majeurs développent des réseaux IPv6 commerciaux. Au Japon en premier lieu, où NTT opère un réseau commercial (à faible capacité toutefois), ou en Europe, où Telia s'est lancé dans le déploiement d'un réseau IPv6 sur liens dédiés, en pariant sur l'avènement rapide du standard.

1.2.2 Évolution du positionnement des opérateurs mobiles avec l'arrivée d'IPv6 [4]

1.2.2.1 La situation au Japon

- **Aujourd'hui, NTT DoCoMo n'est pas moteur face à IPv6 :**
  - **L'opérateur gère ses 31 millions d'abonnés i-mode en IP de bout-en-bout sous IPv4 en utilisant la translation d'adresses (NAT),**
  - **Les premiers services 3G de NTT DoCoMo (FOMA) s'appuient également sur une architecture IPv4 + NAT.**
- **Le succès des services mobiles, le volontarisme du gouvernement et de l'Industrie nipponne face à IPv6, peut être un indicateur d'un passage à IPv6 sur les réseaux cellulaires plus précoce qu'en Europe. Mais, au stade actuel, elle n'est pas perceptible aux initiatives dans les réseaux fixes.**

À ce jour, les réseaux cellulaires utilisent IPv4 pour le trafic Internet. Mobile IP n'est même pas utilisé au profit de GTP. Même DoCoMo au Japon utilise IPv4 pour gérer, de bout-en-bout, les 31 millions d'abonnés à son service i-mode. Ses premiers services 3G (FOMA) utilisent IPv4.

Au Japon, IPv6 ne semble donc pas à l'ordre du jour dans les réseaux mobiles, et même s'il est rendu obligatoire dans UMTS Release 5 pour le traitement des données multimédia, cette version ne sera pas utilisée avant 2004 : les spécifications 3GPP s'achevant courant 2002, c'est pour le moment IPv4 qui est utilisé (Release 99).

Une croissance forte des besoins en adresses due à un décollage de la 2,5 et 3G, et surtout des services interactifs offerts, pourrait amener un opérateur à utiliser IPv6 plus rapidement qu'on ne l'imagine pour son réseau 3G. Cependant, les opérateurs semblent prisonniers du temps d'implémentation des spécifications 3GPP (Release 5).

Le fait que les opérateurs fixes au Japon, et notamment NTT exploitent déjà des réseaux IPv6 commerciaux, qu'IPv6 y soit une « cause nationale », et qu'IP soit déjà utilisé sur les réseaux cellulaires jusque dans les terminaux, peut être un indicateur d'un passage à IPv6 plus précoce qu'en Europe.

1.2.2.2 GPRS : un démarrage avec IPv4

- **Le démarrage du GPRS se fait aujourd'hui sous IPv4+NAT, avec une utilisation de GTP et non de mobile IP.**
- **L'arrivée d'IPv6 pour le GPRS est conditionnée au succès des services interactifs nécessitant une connectivité de bout-en-bout.**
- **Des équipements GPRS compatibles IPv6 ont été annoncés avec des premiers produits expérimentaux en 2002.**

Aujourd'hui, tous les premiers services GPRS démarrent en se basant sur le protocole IPv4. Les nouveaux services qui pourraient trouver une opportunité à utiliser IPv6 sont encore à venir. L'enjeu est aujourd'hui sur le potentiel de développement pour des applicatifs utilisant IP : il existe un réel potentiel, et si aujourd'hui on estime qu'il n'existe pas (encore) d'applications spécifiques à IPv6, il est certain que la plate-forme IPv6 sera plus favorable au développement de certaines applications que ne l'est IPv4.

On pense notamment aux applications « temps réel », de type streaming video, visioconférences sur IP, VoIP, et toutes les applications multimédia. L'intérêt est de disposer d'IP de bout-en-bout. Le mode always-on n'est pas encore pleinement utilisé et le besoin en adresses permanentes peu important. On assiste donc à un démarrage du GPRS en IPv4+NAT, avec une utilisation de GTP et non de mobile IP.

[4] On se reportera également à la note de synthèse Facteurs déclencheurs / Mobilité.

1.2.2.3 La troisième génération mobile (3G) : IPv6 dans un second temps

- **La tendance aujourd'hui est clairement en faveur d'un démarrage de la 3G sous IPv4 avec le Release 99 du standard UMTS comme l'a fait NTT DoCoMo avec son service FOMA.**
- **IPv6 n'est rendu obligatoire que pour certaines parties de la version 5 d'UMTS (Multimedia Subsystem), qui ne devrait pas être utilisée avant 2004.**
- **La gestion de l'itinérance ne sera pas impactée par le passage d'IPv4 à IPv6.**

Le démarrage de la 3G devrait a priori se faire en IPv4, même si la philosophie de la 3G, orientée vers le always-on, va plutôt vers IPv6 et ses nombreuses adresses, ainsi que sa gestion améliorée de la mobilité, etc. Comme nous l'avons vu, IPv6 n'est rendu obligatoire que pour certaines parties de la version 5 de l'UMTS (qui préconise toutefois son emploi généralisé sans le rendre obligatoire), qui ne devrait pas être utilisée avant 2004. Cependant, selon les experts du secteur (3GPP notamment), si le besoin d'utiliser IPv6 se fait sentir (besoin d'adresses en particulier), des opérateurs pourraient utiliser directement de l'IPv6 natif dans leurs réseaux cellulaires 3G (au Japon entre autre ou sur des segments de marché particuliers : véhicule communicant, etc.), sous réserve de disponibilité d'équipements de réseau compatibles (rappelons que le « standard » de la Release 99 d'UMTS est IPv4 et non IPv6, prévu uniquement à partir de la release 5 en cours de finalisation).

Les problématiques d'applications sont dans le prolongement de celles du GPRS (c'est justement pour les applications multimédia qu'IPv6 est obligatoire dans la Release 5 d'UMTS).

Sur ce point, les incertitudes demeurent. On se demande notamment s'il est opportun de démarrer en IPv4 puis de migrer vers IPv6 ou s'il faut démarrer directement en IPv6, au risque de s'isoler provisoirement et partiellement des autres réseaux. La tendance aujourd'hui est clairement en faveur d'un démarrage de la 3G sous IPv4 avec le Release 99 du standard UMTS.

1.2.2.4 Réseaux hétérogènes

- **Un protocole (GTP), utilisé en cœur de réseau GPRS et UMTS au-dessus de la couche IP pour gérer la mobilité s'impose (Release 99 et Release 4) mais il est spécifique aux réseaux cellulaires.**
- **Au contraire, Mobile IPv6 est bien adapté à la mobilité entre réseaux hétérogènes ; son succès sera conditionné à celui des technologies 802.11.**

La distinction entre IPv6 et ses éléments permettant une meilleure gestion de la mobilité et Mobile IPv6 ayant été faite, et une fois précisé le fait que c'est GTP qui est, et sera, du moins dans un premier temps pour la 3G, utilisé pour gérer la mobilité dans le monde cellulaire, on peut s'interroger sur l'utilité réelle de mobile IPv6.

GTP est utilisé en cœur de réseau GPRS et UMTS au-dessus de la couche IP pour gérer la mobilité. GTP est spécifique aux réseaux cellulaires, mais la mobilité entre réseaux de technologies différentes (WLAN, etc.), requiert une certaine unité et Mobile IP s'impose donc logiquement comme le protocole idéal. Son succès sera certainement conditionné à celui des technologies 802.11.

1.2.3 Impacts techniques

1.2.3.1 Cœur de réseau

- **Les opérateurs de backbone devront gérer en cœur de réseau une longue cohabitation entre IPv4 et IPv6 : routeurs double pile IPv4/IPv6.**
- **Pas d'outils de gestion de réseaux IP sous IPv6 disponibles aujourd'hui.**

Le principal impact pour les opérateurs est la mise à niveau des infrastructures notamment les routeurs, dans l'optique d'un transit des deux versions sur les mêmes réseaux : il faut disposer de routeurs double pile, afin de pouvoir gérer les deux flux. Dans le cas de déploiement de réseaux IPv6 sur liens dédiés (Telia) de simples routeurs IPv6 suffisent sur quelques liens. La mise à niveau peut se faire dans le cadre du renouvellement des matériels, ou au travers des « updates » logiciels proposés par les équipementiers. Cependant, en cœur de réseau ce sont plus des renouvellements de matériels qui s'imposeront (ou un passage à une architecture MPLS), les mises à jour logicielles étant plus adaptées pour des routeurs d'accès.

En termes de gestion du réseau, il n'existe pas pour le moment d'outil spécifique IPv6 (à l'exception d'une version bêta de HP Openview au Japon prévue pour fin 2002). Les outils IPv4 devraient donc être encore utilisés.

Les opérateurs de backbone devront gérer en cœur de réseau une longue période de cohabitation IPv4 / IPv6.

1.2.3.2 Gestion de la Mobilité

- **IPv6 permet de disposer d'adresses permanentes afin de développer des applicatifs « always on » mobiles ; cela devrait remettre en cause les architectures IPv4 +NAT.**
- **La prochaine disponibilité de terminaux mobiles double pile IPv4/IPv6 rassure les opérateurs mobiles.**

Si IPv6 contient des fonctions permettant de gérer de façon plus simple la mobilité d'un terminal, il se différencie pourtant de mobile IPv6 (cf. supra). Mobile IP (version 4) n'est pas utilisé dans les réseaux cellulaires et ne devrait pas l'être dans l'immédiat.

En revanche, IPv6 pourrait, lui, être utilisé rapidement. La possibilité de disposer d'adresses permanentes et globalement routables pour les terminaux peut constituer une remise en cause des modèles « réseaux privés » utilisés actuellement par les opérateurs en IPv4 : la gestion de grandes quantités d'abonnés au travers de NAT (comme c'est le cas pour i-mode ou FOMA au Japon) présente, même avec une grande maîtrise technique, des inconvénients évidents de lourdeur et des freins en termes de développement des applications temps réel.

La prochaine disponibilité de terminaux mobiles double pile IPv4/IPv6 est rassurante pour les opérateurs mobiles ; leur parc d'abonnés sera ainsi immédiatement compatible aux éventuelles nouvelles applications IPv6.

1.2.4 Impacts économiques

1.2.4.1 IPv6 : quels avantages pour les opérateurs ?

- **IPv6 pour offrir un meilleur service temps réel et accroître les marges.**

Dans le cadre du développement des connexions permanentes des terminaux (développement des hauts débits notamment, 3G, etc.), les opérateurs peuvent trouver, dans IPv6, un réservoir d'adresses qui leur permettra d'offrir un service de qualité à leurs clients, sans souci de gestion complexe (plus de NAT, etc.). La gestion du réseau est globalement simplifiée, notamment grâce à l'adressage hiérarchique, aux fonctions d'auto configuration, etc. Évidemment, ceci reste conditionné à la présence sur le marché d'outils d'administration spécifiques sous IPv6.

En offrant un meilleur service, on peut imaginer que l'opérateur puisse augmenter ses tarifs sur certaines parties de son offre. La gestion du réseau étant moins onéreuse, certains équipementiers estiment que des opérateurs peuvent accroître leurs marges de l'ordre de 60% ! Ces mêmes équipementiers pensent que certaines fonctionnalités d'IPv6 (notamment le flow label, dont l'usage n'est pas encore défini par l'IETF) peuvent être utilisées pour faire de la tarification sur mesure…

1.2.4.2 Coûts associés à la transition vers IPv6 et à la cohabitation IPv4 et V6

- **Les coûts matériels ne seront pas les plus importants et pourront être maîtrisés car le déploiement d'IPv6 sera progressif.**
- **Les coûts seront principalement dus à la formation des personnels techniques.**
- **Un coût induit : la gestion simultanée des deux protocoles.**

Les coûts associés au passage à IPv6 pour les opérateurs sont directement liés aux impacts techniques. La mise à niveau des matériels devrait engendrer des coûts marginaux : on ne se situe pas dans une optique de basculement, mais de déploiement progressif : le renouvellement des anciens matériel, les upgrades logiciels des matériels en place ne devraient pas engendrer de surcoûts élevés dus à IPv6 (mais cela au prix d'une dégradation des performances en cœur de réseau : à performances égales, le coût pourrait être beaucoup plus élevé ; cf. paragraphe équipementiers). Pour de grands réseaux IP, les coûts matériels de mise à niveau pour IPv6 seront proportionnels au nombre de routeurs impliqués. Toutefois, les équipementiers admettent aujourd'hui ne pas être capable de fournir à leurs clients un calcul du retour sur investissement (ROI) qui reste un élément essentiel à la décision des opérateurs.

Un élément essentiel est la formation des personnels techniques aux nouvelles implications liées à IPv6. Les coûts sont principalement concentrés sur ce poste.

Parallèlement à ces dépenses, on doit identifier d'autres coûts. Même si l'administration d'un réseau IPv6 est théoriquement plus simple que celle d'un réseau IPv4 ; la cohabitation des deux IP sur deux mêmes réseaux risque d'engendrer des complications et des lourdeurs de gestion (on ne sait pas, tant que le déploiement n'a pas eu lieu à grande échelle, quelles seront les interférences opérationnelles entre les deux IP).

1.2.4.3 Des modèles économiques à inventer

- **IPv6 peut remettre en cause le modèle client-serveur ; chaque nœud, chaque terminal devient un serveur potentiel.**

Les opérateurs, comme les ISP sont concernés par le rétablissement du fonctionnement « end-to-end » qu'interdisent les NAT de plus en plus présents avec IPv4. Ce retour du « end-to-end », la présence d'adresses globalement routables permanentes permet d'envisager une remise en question du mode client-serveur, chaque nœud, chaque terminal, devenant potentiellement serveur, remet en cause les modèles économiques développés sous IPv4.

Les opérateurs ne sont plus, caricaturalement, que des fournisseurs de capacité et doivent alors trouver de nouveaux modèles adaptés, mais ils peuvent aussi exploiter leur savoir-faire et proposer de nouveaux services. Les réflexions sur ces sujets s'engagent à peine et les solutions d'apport de valeur, ainsi que les modèles associés sont encore à définir.

1.2.5 Synthèse

Opérateurs de backbone

- **La plupart sont attentistes et ne voient pas une forte demande IPv6**
  - **L'arrivée d'IPv6 est annoncée par le bord du réseau, les opérateurs de backbone se tiennent prêts**
  - **Les historiques expérimentent à grande échelle ; ce sont eux qui ont mené la R&D en Europe**
  - **Certains lancent des services pré-commerciaux : Telia, UUNET WorldCom**
- **La gestion à grande échelle de tunnels ne sera pas viable ; les opérateurs de backbone devront migrer leurs routeurs de cœur de réseau sous IPv6 quand la demande le justifiera**
- **IPv6 : une fenêtre d'opportunité pour se repositionner pour certains (NTT)**
- **Les premières offres se développent en Asie ; le marché naissant de l'accès IPv6 devrait constituer une base pour le marché du transit IPv6**

Opérateurs mobiles

- **NTT DoCoMo n'est pas moteur pour l'instant face à IPv6**
  - **FOMA (3G), i-mode et ses plus de 31 millions d'abonnés s'appuient sur une architecture IPv4 + NAT**
- **Tous les réseaux GPRS utilisent aujourd'hui IPv4 + NAT ; certains opérateurs pourraient déployer IPv6 afin de développer des applicatifs « always on » mobiles**
- **Les premiers déploiements 3G se feront sous IPv4 + NAT ; plus de déploiements optionnels d'IPv6 attendus si des applicatifs le justifient**
- **Le Release 5 (3GPP) instaurant IPv6 pour les applications Multimédia pas implémenté avant 2004**
- **Des opérateurs mobiles japonais pourraient partir sur IPv6 avant le Release 5 si des applicatifs le justifient**

1.3 ISP : accès et services

1.3.1 Le rôle moteur des ISP dans la migration vers IPv6

1.3.1.1 Accès

- **IPv6, accès et services : le problème de la poule et de l'œuf**

Les différents acteurs s'accordent sur l'idée que la demande en accès IPv6 ne sera pas nécessairement une demande consciente : c'est plutôt la demande de services nécessitant IPv6 qui sera motrice, l'utilisateur ne se souciant pas du protocole sous-jacent. Cependant, les services et applications s'appuyant sur IPv6 ne seront rendus possibles que si des accès IPv6 existent pour les utilisateurs.

Le fameux problème de la poule et de l'œuf est dans ce cas particulièrement significatif. Au Japon et en Corée, la solution apportée est de faire précéder la demande par l'offre : culturellement, ces marchés ont tendance à adopter quasi spontanément une offre novatrice. Dès lors, les opérateurs et ISP proposent de l'accès IPv6, la demande venant se « greffer » naturellement.

1.3.1.2 Incertitudes sur les services

- **Pas de visibilité claire sur des applications nécessitant impérativement IPv6**
- **Le rôle moteur des ISP dans la diffusion d'IPv6 ; eux seuls peuvent faire sauter le verrou de l'accès IPv6**

Comme nous venons de l'évoquer, ce sont les nouveaux services qui reposeront sur IPv6 qui seront moteurs pour la demande en accès IPv6. La difficulté est aujourd'hui d'identifier ces applications : globalement, les applications que nous connaissons aujourd'hui fonctionnent (plus ou moins bien), sous IPv4, et pour le moment, l'identification d'applications pour lesquelles IPv6 est indispensable s'avère bien difficile.

Les applications temps réel, de type VoIP, VoD, visio conférences, pourraient trouver un réel intérêt dans IPv6, du fait de son nombre d'adresses qui permet d'éviter d'avoir recours au NAT qui nuisent à ce type de services, mais aussi grâce à son potentiel de QoS. Des applications comme les jeux en réseaux peuvent trouver de nombreux avantages à l'utilisation d'IPv6. Le développement de ces services pourrait donc inciter les ISP à offrir des accès IPv6.

Pourtant, les applications nouvelles qui reposeront totalement sur IPv6 sont loin d'être clairement identifiées, et n'apparaîtrons que lorsque les accès seront disponibles. Il semble donc essentiel que les ISP proposent la possibilité de disposer d'accès IPv6 comme préalable au développement du marché. Eux seuls peuvent faire sauter le verrou.

1.3.2 Évolution du positionnement des ISP avec l'arrivée d'IPv6

- **De nouveaux services, à inventer, avec le retour du « end-to-end »**
- **IPv6 et l'abondance d'adresses associée ; une opportunité pour les « petits » ISP**

Avec l'avènement d'IPv6, le positionnement des ISP est bouleversé. En effet, l'abondance d'adresses leur permet de proposer à leurs clients des adresses globalement routables, en grand nombre, et permanentes (utile dans le cadre du développement des accès « always-on »).

En outre, le rétablissement du mode bout-en-bout permet de proposer de nouveaux services (restant pour la plupart à imaginer, cf. supra).

La possibilité de disposer d'un grand nombre d'adresses (notamment avec la refonte et la simplification en cours du mode d'attribution des adresses IPv6 par les registres régionaux) peut permettre à de « petits » entrants de se positionner sur des marchés de niche, voire de bousculer les « gros » ISP déjà en place en offrant une offre alternative et abondante.

Le principal avantage d'IPv6 est donc, pour un ISP, la simplification de la gestion de son parc d'adresses (renumérotations automatiques, disparition des NAT, etc.), l'abondance d'adresses, mais surtout le fait que cette abondance permette une réouverture d'un marché qui a tendance actuellement à se concentrer autour de quelques ISP majeurs.

1.3.3 Impacts économiques

1.3.3.1 IPv6 : quels avantages et inconvénients pour les ISP ?

- **L'arrivée d'IPv6 peut dynamiser le marché de l'accès et permettre d'offrir de nouveaux services ou de simplifier les services existants**
- **Mais des craintes existent face à l'arrivée d'IPv6 :**
  - **Des clients moins captifs de leurs ISP**
  - **L'intelligence quitte l'ISP pour aller vers le réseau**
  - **L'arrivée de concurrents venant de l'électronique grand public**

Comme nous venons de l'évoquer, l'abondance d'adresses IPv6 est une opportunité qui permet à de nombreux ISP de se repositionner sur un marché plus ouvert, de proposer de nouveaux services, d'améliorer ou de simplifier des services existants, de gérer plus simplement leurs réseaux, etc.

Cependant, ces avantages présentent également des risques. Notamment, la complexité des plans d'adressage en IPv4 et la complexité de gestion des réseaux constituaient un frein au départ d'un client (grand compte) vers un autre ISP. Avec IPv6, l'abondance d'adresses et la concurrence accrue permettent non seulement aux clients de disposer d'une offre plus large, mais également de pouvoir changer d'ISP avec plus de facilité : avec les systèmes d'auto configuration, la renumérotation d'un réseau devient automatique, et le client n'est plus « prisonnier » de son ISP.

Qui plus est, tous les services à valeur ajoutée (on pense notamment à ceux offerts autour des VPN, ou des services de hosting, etc.) sont menacés : l'intelligence quitte l'ISP pour aller dans le réseau lui-même, via le protocole. Le mode end-to-end couplé au always-on permet à tout un chacun d'héberger des données. L'ISP n'étant plus qu'un fournisseur de bande passante et perdant sa valeur ajoutée. D'autre part le développement de l'électronique connectée souvent associée à l'arrivée d'IPv6 fait craindre à certains ISP l'arrivée de nouveaux concurrents venant de l'électronique grand public.

Certes, ces idées sont à nuancer, l'inertie du marché doit permettre aux ISP de réagir, néanmoins, ces menaces sont très souvent évoquées par les acteurs. Aux ISP de saisir ces opportunités pour créer de nouveaux services à valeur ajoutée, en utilisant les simplifications du protocole pour économiser sur la gestion du réseau, etc.

1.3.3.2 Coûts associés à la migration vers IPv6

1.3.3.2.1 Équipements

- **Des coûts matériels associés au passage à IPv6 assez peu élevés**
- **L'architecture MPLS ou Dual Stack semble bien adaptée car flexible pour les ISP**

Les coûts engendrés par le passage à IPv6 pour les ISP sont marginaux, du moins dans le domaine matériel : la mise à jour des routeurs est souvent gratuite. En revanche, si l'ISP gère les deux versions d'IP sur un même réseau, la lourdeur de gestion peut être ressentie, le surcoût des équipements restant marginal.

L'architecture MPLS ou Dual Stack semble bien adaptée pour les ISP car elle leur permet d'être assez flexible face à la demande de leurs clients en accès IPv6 : possibilité d'ouvrir des accès IPv6 au cas par cas sans avoir à migrer tout le réseau.

1.3.3.2.2 Formation

- **Les coûts liés à la formation des équipes techniques seront les plus importants**

Les principaux coûts identifiés par les acteurs interrogés sont les coûts humains : les personnels maîtrisent la technologie IPv4. IPv6 présente de nouvelles particularités et les techniciens doivent donc s'adapter. Ils devront, en outre, être capables de gérer les deux versions d'IP simultanément pendant une longue période, ainsi que les outils d'interopérabilité. Les coûts de formation sont donc significatifs.

1.3.3.3 Des modèles économiques à inventer

- **Des modèles économiques à inventer sous IPv6 pour des ISP tirant leurs revenus exclusivement de services IPv4**
- **Une entrée des accès IPv6 via l'ADSL au Japon**
- **Face à l'arrivée d'IPv6, pas de visibilité claire sur le ROI**

Aujourd'hui, le principal souci des ISP, sur un marché particulièrement concurrentiel en phase de concentration, est de stabiliser leur position et de trouver le meilleur modèle qui leur permettra d'atteindre l'équilibre sous IPv4.

Leur souci majeur n'est donc pas de tenter de nouvelles aventures en proposant IPv6, pour lequel la demande n'est pas encore identifiée : on n'est pas en phase de conquête mais de consolidation.

Le développement des accès haut débit via ADSL notamment, peut être un facteur déclencheur pour la fourniture d'accès IPv6. Au Japon, c'est à travers des accès ADSL via IPv6 que les ISP (IIJ, NTT) proposent leurs premiers accès commerciaux IPv6.

Les nouveaux modes de fonctionnement évoqués plus haut, notamment le bout-en-bout, et le fait que le mode client-serveur disparaisse en partie, chaque nœud du réseau, disposant d'une adresse globalement routable devenant potentiellement un serveur, remet en cause les modèles économiques appliqués jusqu'ici. En forçant le trait, alors que les opérateurs se borneront à fournir de la bande passante, les ISP se contenteront de fournir de l'accès. De nouveaux modèles sont à inventer, de nouvelles sources de valeur sont donc à trouver afin de parvenir, face aux risques identifiés, à un équilibre économique.

La problématique du calcul du ROI face à l'arrivée d'IPv6 est ici similaire à celle des opérateurs de backbone.

1.3.4 Synthèse

- **Le rôle déterminant des ISP face à l'arrivée d'IPv6 : ils détiennent le verrou de l'accès**
- **En Asie, un marché IPv6 perçu comme proche par les ISP : les accès haut débit (ADSL) et le succès de certains applicatifs comme les jeux en réseau motivent les ISP**
- **Aux USA et en Europe : des ISP frileux vis-à-vis d'IPv6**
  - **Pas de visibilité claire sur les applicatifs « IPv6 only »**
  - **Visibilité sur le ROI ?**
  - **La priorité est la stabilisation de leurs modèles économiques sous IPv4**
  - **L'arrivée d'IPv6 suscite certaines craintes :**
    - Perte de la maîtrise des services à valeur ajoutée
    - Des clients moins captifs
    - Arrivée de nouveaux concurrents : EGP

1.4 Entreprises utilisatrices de technologies IP

1.4.1 Attitude des entreprises face à l'arrivée d'IPv6

- **Une certaine dualité au sein des grandes entreprises :**
    - **Neutralité voire indifférence des DSI**
        - **Pérennisation des investissements déjà réalisés sous IPv4**
        - **Pas de besoins IPv6 ressentis**
    - **Des opportunités perçues par les équipes R&D autour de l'électronique connectée et de l'électronique embarquée**

Il faut distinguer deux types d'entreprises de technologie IP : les entreprises qui utilisent le protocole pour leurs communications, leurs réseaux (Intranet, Extranet, etc.), et les entreprises qui, bien qu'étant hors du champ des acteurs du marché « traditionnel » d'Internet, peuvent trouver des opportunités pour utiliser IPv6 dans de nouvelles applications, ou en substitution d'applications existantes.

Ces deux aspects peuvent se manifester au sein d'une même entreprise, avec des attitudes différentes par rapport à IPv6 selon le contexte.

Les premières, utilisatrices de réseaux d'entreprises IP, ne ressentent pas nécessairement le besoin de passer à IPv6. Bien que les avantages potentiels d'IPv6 soient perçus, les responsables informatiques estiment, dans leur ensemble, qu'il n'y a ni urgence, ni priorité. Dans le contexte actuel, la priorité est à la pérennisation des investissements déjà réalisés sous IPv4 : modernisation des interfaces, amortissement des investissements, réponses à des besoins exprimés réalisables sans avoir à remettre en cause l'architecture IP générale (donc en maintenant IPv4). C'est le cas d'une majorité de grandes entreprises qui estiment que rien n'est possible sous IPv6 qui ne soit faisable sous IPv4, les priorités sont ailleurs.

Parallèlement, certaines entreprises non utilisatrices d'IP, ou non orientées à l'origine vers les TIC, voient dans IPv6 une opportunité.

Ainsi, dans le secteur de l'Aéronautique, on étudie attentivement le nouveau protocole IPv6. Les acteurs y voient une possibilité de passer à IP. Pour le moment, les protocoles utilisés sont propriétaires, le nombre d'adresses d'IPv4 étant insuffisant pour les besoins de l'aéronautique. IPv6 comble ce défaut et pourrait permettre au secteur, en utilisant des produits standardisés, de réaliser de substantielles économies. Qui plus est, l'abondance d'adresses peut permettre d'imaginer le développement de nouvelles applications : suivi des sous-ensembles des aéronefs, maintenance, Internet embarqué (la différenciation par le service tenant à cœur aux compagnies aériennes, etc.). Les constructeurs automobiles, qui, s'ils estiment que leurs réseaux internes peuvent demeurer en IPv4, voient avec IPv6, allié aux technologies cellulaires, la possibilité de nouvelles applications autour de la voiture connectée. Les constructeurs d'électroménager peuvent imaginer des applications domotiques, etc.

Il y a donc face à IPv6 une attitude des grandes entreprises relativement neutre, voire indifférente de la part des directions informatiques, alors que les directions de R&D y voient un certain nombre d'opportunités dans le domaine des objets communicants. Dans tous les cas, il y a une volonté de se tenir informé, même si l'information semble parfois faire défaut et même dans certains cas (équipementiers de l'électronique grand public) de s'impliquer plus avant dans IPv6 (participation à l'IETF, etc.).

1.4.2 Impacts techniques

1.4.2.1 Terminaux

- **Vu les taux de renouvellement des OS et des PC : il faudra encore 3 ou 4 ans avant que les parcs de PC soient massivement compatibles IPv6.**

La plupart des terminaux utilisés par les entreprises (mais aussi les particuliers !) sont des ordinateurs, dont la compatibilité avec IPv6 passe par la compatibilité de l'OS. La base majoritaire dans le parc informatique des entreprises (et plus encore des particuliers) est aujourd'hui Microsoft Windows. Les produits seront mis à jour et présenteront IPv6 par défaut d'ici fin 2002 avec Windows XP. Sachant que peu d'utilisateurs installeront les kits de mise à niveau de leurs OS, il faut compter avec le taux de renouvellement des OS et des PC pour que la majorité de la base soit compatible IPv6. Il faudra donc encore 3 ou 4 années avant que les parcs de PC soient massivement compatibles IPv6.

1.4.2.2 Réseaux d'entreprises

- **Des routeurs d'accès compatibles IPv6 en software sont aujourd'hui disponibles**

Globalement, grâce aux fonctions « plug and play » développées pour IPv6, les réseaux d'entreprises devraient être plus légers à gérer : renumérotation simple et automatique, plan d'adressage automatisé, facilité pour insérer un nouveau terminal (il trouve seul sa place dans le réseau).

Toutefois, les matériels fournis par les équipementiers (routeurs d'accès) ne sont pas encore prêts, du moins en Hardware. Mais un premier déploiement devrait être possible avec des mises à jour logicielles. Ce retard de préparation des produits est à nuancer par nos propos précédents : il faudra plusieurs années avant que les réseaux d'entreprises aient des terminaux massivement compatibles.

1.4.2.3 IPv4 séduit encore

- **Les NAT vus comme un rempart sécuritaire supplémentaire**
- **La pénurie d'adresses IP ne se fait pas encore sentir dans les entreprises**
- **Des applications de type machine/machine tournent très bien sous IPv4**

Malgré les lourdeurs associées à la gestion de plus en plus complexe d'architectures s'appuyant sur IPv4 + NAT, IPv4 séduit encore bon nombre de DSI. En effet, les NAT installés en entrée des réseaux d'entreprises sont jugés à tort ou à raison comme des remparts sécuritaires. De plus, la pénurie d'adresses ne se faisant pas encore sentir parmi les entreprises, l'utilité d'un passage imminent à IPv6 est difficile à percevoir. Enfin, les applicatifs machine/machine fonctionnant aujourd'hui sous IPv4 subsisteront encore longtemps sur les réseaux d'entreprises.

1.4.3 Impacts économiques

1.4.3.1 IPv6 : quels avantages pour les entreprises ?

- **Une gestion des réseaux plus allégée et moins onéreuse**
- **Une entreprise moins captive de son fournisseur d'accès**
- **Une arrivée progressive d'IPv6 via des applicatifs trop complexes à implémenter sous IPv4 + NAT**

Comme nous venons de le voir, l'ensemble de fonctionnalités « plug and play » prévues pour IPv6 doivent permettre de simplifier et d'alléger la gestion des réseaux. En outre, ces capacités permettent aux entreprises de ne plus être captives des prestataires (ISP notamment) qui maîtrisent leurs plans d'adressage : la renumérotation est simplifiée, la concurrence peut jouer, la « volatilité » de l'entreprise par rapport à ses prestataires plus grande (d'où possibilité de réduire les coûts). Globalement, les entreprises devraient réaliser des économies avec l'utilisation d'IPv6, une fois toutes les fonctionnalités opérationnelles mises en place. En effet, la gestion des réseaux devenant plus légère, elles ont recours à moins de personnel et consacrent moins de temps à cette gestion. Les prestataires ne maîtrisant plus seuls les plans d'adressage, l'entreprise peut faire pleinement jouer la concurrence.

L'arrivée d'IPv6 dans l'entreprise pourrait se faire progressivement via des applicatifs trop complexes à implémenter sous IPv4 + NAT : applicatifs sécuritaires de bout-en-bout, applications temps réels.

1.4.3.2 Coûts associés à la migration vers IPv6

1.4.3.2.1 Équipements

- **Les coûts de mise à niveau des routeurs d'accès ne seront pas importants et noyés dans les coûts normaux de renouvellement du matériel**
- **Des craintes existent quant à la communication entre équipements IPv4 et IPv6**
- **Des applicatifs IPv4 et IPv6 cohabiteront longtemps sur les réseaux d'entreprises**

Les routeurs de réseaux d'entreprises devront être mis à niveau ou changés : à l'heure actuelle, il n'existe pas encore d'offre complète dans ce domaine (des versions software sont disponibles). Toutefois, les coûts engendrés ne devraient pas être importants, car noyés dans les coûts normaux de renouvellement du matériel.

Certains utilisateurs craignent cependant que des matériels hétérogènes aient du mal à communiquer entre eux ; le renouvellement des parcs étant progressif, il sera donc nécessaire sur des parcs existants d'avoir recours à la double pile IPv4/IPv6.

En effet, IPv4 subsistera encore longtemps dans le monde de l'entreprise dans lequel les investissements prioritaires ne vont pas vers IPv6, mais plutôt vers la pérennisation d'applications IPv4. De plus, des applications de communication machines à machines sous IPv4 qui fonctionnent de façon très satisfaisante perdureront longtemps dans certaines entreprises.

1.4.3.2.2 Formation

- **Les coûts de formation sont identifiés comme les plus importants face à l'arrivée d'IPv6**

Sans pouvoir chiffrer les coûts de formation des personnels, les DSI estiment que ceux-ci risquent d'être élevés et de représenter une part importante des coûts de transition vers IPv6. Toutefois, les besoins en personnel pour l'entretien des réseaux IPv6 étant moindres et la possibilité de réduire les coûts d'intervention de prestataires externes (cf. supra) étant à prévoir, on peut considérer qu'un certain équilibre est à attendre, avant de passer rapidement à une phase de coûts réduits, une fois le personnel formé. La phase la plus critique sera celle de la cohabitation des deux IP.

1.4.3.3 Des applicatifs à inventer

- **Les applicatifs d'entreprises « IPv6 only » non identifiés**
- **Des applicatifs temps réels (VOIP, visioconférences) gênés dans leur développement par des architectures IPv4 + NAT**
- **Pas d'outils de gestion et d'administration de réseaux sous IPv6 disponibles aujourd'hui**

À ce jour, les nouvelles applications d'entreprises qui s'appuieront sur IPv6 exclusivement, et qui donc tireront les entreprises vers son adoption ne sont pas encore identifiées. Il est d'ailleurs probable qu'elles n'apparaissent qu'une fois l'infrastructure IPv6 prête, et qu'elle ne constitue pas au final un rôle moteur dans le déploiement en entreprises.

Qui plus est, les outils de gestion et d'administration des réseaux, type HP Openview ou Tivoli ne sont pas prêts pour IPv6 (cf. supra) : dans un premier temps, ce sont des outils IPv4 qui seront utilisés.

On peut tout de même estimer que le développement d'applications temps réel, comme la voix sur IP (VoIP), les visioconférences, actuellement gênées dans leur fonctionnement par les NAT sous IPv4, puissent trouver en v6 une réponse efficace, qui incite les entreprises à utiliser la nouvelle version.

1.4.4 Le manque d'information

- **Un manque évident d'informations concernant IPv6 :**
  - **enjeux techniques et économiques**
  - **avantages et inconvénients d'IPv6**
  - **coûts engendrés par le passage à IPv6**

Un des éléments marquants dans les propos des entreprises utilisatrices est le manque d'informations au sujet d'IPv6. Certes, les responsables informatiques sont sensibilisés au sujet, mais ils estiment souvent manquer d'informations synthétiques sur les avantages, les inconvénients et les différences par rapport à IPv4. Les seules sources documentaires identifiées, lorsqu'il y en a, sont souvent les RFC, dont l'abord est peu pratique. Il y a une attente de vulgarisation, même de la part de personnes impliquées dans le domaine d'IP, afin de pouvoir plus rapidement identifier les éléments clefs et les enjeux techniques d'IPv6.

Par ailleurs, on note une attente en termes d'information sur les coûts engendrés par le passage à IPv6 ; même les équipementiers communiquent assez peu sur le sujet. Il y a aussi une attente d'information sur les enjeux, le degré de maturité des produits, le niveau de stabilité d'IPv6.

C'est cette demande d'information, simple d'accès et permettant d'identifier les points clefs sur le plan technique et économique, qui revient le plus souvent comme une attente vis-à-vis des pouvoirs publics.

1.4.5 Synthèse

- **Une neutralité globale des entreprises en tant qu'utilisatrices d'IP**

- **Des avantages potentiels**
  - **IPv6 permet de simplifier la gestion des réseaux et de libérer les entreprises de l'emprise de leurs prestataires**
  - **Le protocole permet plus de souplesse et de sécurité (auto configuration, renumérotation, IPSec de bout-en-bout, suppression des NAT)**

- **Mais pas d'urgence perçue par les entreprises pour le passage à IPv6**
  - **Pas de visibilité sur les applicatifs spécifiques IPv6 face aux coûts qu'implique une migration**
  - **Le retour sur investissement n'est pas évalué**
  - **Les entreprises ont d'autres priorités actuellement : pérennisation de l'existant IPv4**
  - **Un grand manque d'information sur le sujet est ressenti**

1.5 Synthèse générale acteurs

	Éléments moteurs pour la transition vers IPv6	Freins pour la transition vers IPv6
Équipementiers télécoms	• IPv6 est identifier comme un relais de croissance en devenir. • IPv6 va accélérer le renouvellement des parcs (terminaux et routeurs d'accès). • Les équipementiers IP leaders disposent de routeurs compatibles IPv6 en Software. • IPv6 pourra permettre l'intrusion d'IP dans d'autres secteurs que l'informatique et les télécommunications.	• Les équipementiers IP leaders n'ont pas tous les éléments aujourd'hui pour construire en direction de leurs clients ISP et entreprises le « Business case IPv6 ».
Équipementiers grand public	• Le développement de l'électronique grand public apparaît comme un enjeu d'avenir crucial pour Internet. • IPv6 pourra permettre via l'électronique connectée d'atteindre de nouveaux marchés.	• Les équipementiers européens ne perçoivent pas de marché dans l'immédiat.
Équipementiers Informatique – Grands éditeurs	• D'ici la fin 2002, la quasi-totalité des produits Microsoft et notamment les OS seront compatibles IPv6 par défaut (à partir de la version 2000).	• Les ordinateurs s'appuyant sur les Windows 95 et 98 (majorité du parc PC aujourd'hui installé) ne seront jamais compatibles IPv6. • Les principaux fournisseurs d'applicatifs ne se prononcent pas face à IPv6 : SAP, Oracle. • Ces fournisseurs d'applicatifs n'ont pas aujourd'hui de demandes claires de la part des entreprises.
Opérateurs de backbone	• Certains opérateurs saisissent l'opportunité IPv6 pour conforter leur position sur le marché du transit IP.	• En cœur de réseau, à coût égal, de par la taille plus importante des en-têtes IPv6, les performances des routeurs sous IPv6 seront moindres comparées à celles des routeurs sous IPv4. • Pas de demandes significatives de leurs clients ISP ou entreprises
Opérateurs mobiles	• Ericsson et Nokia livreront à partir de 2003 des terminaux GPRS puis UMTS avec une double pile v4/v6. • Symbian (OS mobile) a une forte demande de ses clients pour une compatibilité IPv6 de son OS. • IPv6 permet de disposer d'adresses permanentes afin de développer des applicatifs « always on » mobiles.	• L'ampleur du relais de croissance IPv6 identifié par les équipementiers mobiles dépendra fortement du succès des services mobiles sur GPRS. • Le démarrage du GPRS puis celui de la 3G se font sous IPv4 + NAT.
ISP	• L'arrivée d'IPv6 peut dynamiser le marché de l'accès et permettre d'offrir de nouveaux services ou de simplifier les services existants.	• Il n'existe pas aujourd'hui d'outils de gestion de réseaux IP compatibles IPv6 : HP Openview, Tivoli. • IPv6 peut remettre en cause le modèle client serveur • Des craintes existent face à l'arrivée d'IPv6 • Pas de visibilité claire sur le ROI et des applications nécessitant impérativement IPv6

	Éléments moteurs pour la transition vers IPv6	Freins pour la transition vers IPv6
Entreprises	• Des routeurs d'accès compatibles IPv6 en software sont aujourd'hui compatibles. • Des applicatifs temps réels (VOIP, visioconférence) gênés dans leur développement par des architectures IPv4 + NAT.	• Vu les taux de renouvellement des OS et des PC, il faudra encore 3 ou 4 ans avant que les parcs de PC soient massivement compatibles IPv6. • La pénurie d'adresses IP ne se fait pas encore sentir dans les entreprises. • Les applicatifs d'entreprises « IPv6 only » non identifiés.

2 Facteurs déclencheurs du passage à IPv6

2.1 Les facteurs déclencheurs de premier rang

2.1.1 La pénurie d'adresses IPv4

2.1.1.1 IPv4 : un espace d'adressage restreint

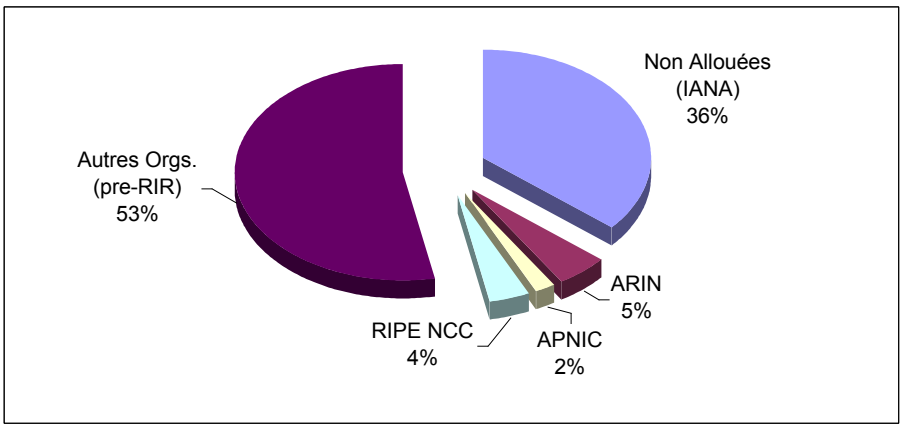
- **IPv4 : un espace d'adressage restreint avec une répartition géographique inégale**
  - **L'Asie représente un fort potentiel de croissance**
  - **53% des adresses IPv4 ont été attribuées avant l'apparition des RIR à des organisations américaines pour la plupart**
  - **Fin 2001, 74% des adresses allouées pour les USA, 17% pour l'Europe et 9% pour l'Asie**

Le peu d'adresses disponibles sous IPv4 commence à constituer un réel problème. En effet, le stock est aujourd'hui très entamé, et si près de 47% des adresses sont non attribuées (parmi le stock total d'adresses), la répartition géographique en est très inégale. Les adresses allouées (destinées à être utilisées par un registre régional ou par des organisations pré-RIR) représentent la majorité du stock et sont destinées essentiellement à la zone américaine au dépend de l'Asie qui présente pourtant un important potentiel de développement.

Il est également à noter, que parmi le total des adresses IPv4 disponibles, 53% ont été attribuées directement à des organisations (américaines pour la plupart), avant l'apparition des RIR et ces adresses ne sont donc pas aujourd'hui sous le contrôle de ces derniers.

Ainsi, en tenant compte de ces organisations pré-RIR, on peut estimer fin 2001 que 74% des adresses allouées le sont pour l'Amérique du Nord, 17% pour l'Europe et 9% pour l'Asie.

Figure 5 : Allocations des adresses IPv4 (11/01)



Source : RIPE NCC

2.1.1.2 Nous sommes aujourd'hui dans une période de gestion de la pénurie d'adresses

- **Toutes choses égales par ailleurs, on peut estimer un épuisement du stock d'adresses IPv4 d'ici 2010**
- **Nous sommes déjà dans une période de gestion de la pénurie d'adresses**
  - **Politiques drastiques d'attribution d'adresses IPv4 pratiquées par les RIR**
  - **Emploi généralisé des NAT :**
    - **Alourdit la gestion des réseaux et entraîne un surcoût**
    - **Un frein au développement des applications temps réel et P2P**
- **Le stock d'adresses IPv4 tendra vers 0 de manière asymptotique**

L'emploi généralisé du NAT permet de retarder la pénurie, tout comme les politiques drastiques d'attribution pratiquées par les RIR, mais les estimations permettent d'envisager un épuisement du stock avant la fin de la décennie (cf. étude documentaire). Les zones les moins favorisées par les allocations d'adresses IPv4 seront par ailleurs vraisemblablement les premières concernées par la pénurie, car elles sont en outre les plus dynamiques en termes de croissance de l'Internet.

Le développement de nouvelles applications consommatrices d'adresses (électronique connectée, Internet mobile, etc. cf. infra) devrait en outre agir comme un levier sur la croissance du besoin et accélérer la pénurie. Même si celle-ci ne devrait pas se matérialiser subitement : on tendra vers un stock nul de manière asymptotique.

Afin de pallier ce problème, l'utilisation des NAT s'est généralisée, complexifiant et alourdissant la gestion des réseaux (à dire d'expert : 30 à 35% de surcoût). Les tables de routages sont aujourd'hui surchargées et en croissance exponentielle : les temps de traitement des routeurs de cœur de réseau s'allongent, la QoS se dégrade, etc.

En outre, ces mêmes NAT nuisent au développement d'applications fonctionnant mieux en bout-en-bout, et ralentissent le développement des applications temps réel. Même si elles peuvent exister dans un environnement de NAT, des applications comme la VoIP sont freinées par la complexité qu'elles doivent affronter.

Signalons que l'espace d'adressage d'IPv6 constitue son principal atout, et que de l'avis général, c'est cette caractéristique à elle seule qui justifiera un basculement ; les autres avantages d'IPv6, bien qu'intéressants, n'étant perçus que comme secondaires.

2.1.2 L'émergence des services de données mobiles (i-mode, GPRS, 3G)

- **IPv6 est considéré par les acteurs du secteur comme une évolution incontournable des réseaux mobiles :**
  - **La forte croissance attendue du nombre de terminaux mobiles utilisés pour des services non-voix nécessitera de plus en plus d'adresses IP**
  - **La connexion « always on » et certains services (push par exemple) nécessiteront une adresse IP unique et permanente**
  - **IPv6 est rendu obligatoire par les standards (à partir des fonctionnalités IP Multimédia d'UMTS Release 5)**

L'émergence des services de données mobiles, au Japon notamment avec l'i-mode de DoCoMo et les autres services des opérateurs concurrents, et en Europe avec le succès des SMS, conduit à s'interroger sur l'influence de ce marché sur l'introduction d'IPv6.

Par ailleurs, l'arrivée de nouvelles générations de technologies réseaux devrait conduire à la prolifération des terminaux mobiles connectés : le GPRS tout d'abord, dont les premiers services commerciaux à destination des entreprises sont à présent offerts par la plupart des opérateurs GSM d'Europe de l'Ouest, puis la 3G (UMTS et CDMA 2000) qui fait l'objet d'investissements colossaux en Europe et dont le premier service commercial a été ouvert au Japon par DoCoMo en octobre 2001.

IPv6 est un enjeu important pour les opérateurs de réseau mobile, car il permettra d'allouer une adresse IP permanente à chaque terminal mobile connecté. En effet, le GPRS introduit le concept de « always-on », c'est-à-dire de connexion permanente au réseau de données en IP, même lorsque l'utilisateur est inactif. À terme, IPv6 est considéré par les acteurs du secteur comme une évolution incontournable des réseaux mobiles.

- **Néanmoins, le marché de la téléphonie mobile ne sera probablement pas le marché précurseur pour l'introduction d'IPv6 :**
  - **Investissements et déploiements actuels dans les solutions IPv4 + NAT pour le GPRS et l'UMTS (Release 99 et 4)**
  - **Introduction dans les réseaux 3G avec IP Multimédia, à partir de 2004/2005**

Plusieurs éléments montrent que le marché de la téléphonie mobile ne sera probablement pas le marché précurseur pour l'introduction d'IPv6. Les solutions reposant sur l'utilisation d'IPv4 et de la translation d'adresse (NAT) seront utilisées dans un premier temps :

- NTT DoCoMo gère ses quelques 31 millions de clients i-mode au Japon, avec IPv4 et NAT. En fait l'opérateur ne maintient pas la connexion permanente des utilisateurs, qui doivent ré-initier la connexion après une période d'inactivité.
- Standardisé en 1997, le cœur de réseau GPRS utilise également IPv4 et NAT. Par ailleurs, la connexion permanente pourrait ne pas être maintenue en pratique par les opérateurs. Ainsi, les utilisateurs restés inactifs trop longtemps pourraient être déconnectés, ce qui permettrait de relâcher les adresses IPv4 inutilisées.
- Le standard UMTS n'introduit IPv6 de bout-en-bout qu'à partir de la release 5. Les premiers déploiements auront lieu avec la Release 99 qui utilise quasiment le même cœur de réseau que le GPRS. La Release 5 sera standardisée courant 2002 par 3GPP, ce qui place la disponibilité d'équipements compatibles à partir de 2003 et les réels déploiements commerciaux au-delà.

Tableau 4 : IPv6 et standards mobiles

Phase	Cœur de réseau (SGSN, GGSN, …)	Terminaux et services	Éléments de réseaux pour le multimédia IP
GPRS Release 98	IPv4	IPv4 ou IPv6 En pratique, ce sera IPv4 ; IPv6 optionnel	-
UMTS Release 99 et 4	IPv4, IPv6 optionnel	IPv4 ou IPv6 En pratique, ce sera IPv4 ; IPv6 optionnel	-
UMTS Release 5	Non décidé A priori, identique à la Release 99	IPv4 et IPv6 (IPv6 exclusivement pour IP Multimedia)	IPv6 exclusivement

Ainsi, les déploiements commerciaux d'IPv6 dans les réseaux mobiles auront vraisemblablement lieu à partir de 2004/2005 en Europe, ce qui place l'introduction d'IPv6 dans les réseaux mobiles après l'introduction dans les réseaux fixes.

Au Japon, NTT DoCoMo souhaite, de la même façon, attendre une pénétration suffisamment importante d'IPv6 dans les réseaux fixes avant de faire migrer son infrastructure mobile.

- **Le succès du lancement du GPRS est un facteur clé pour l'introduction d'IPv6 par les opérateurs mobiles.**
- **Des terminaux doubles pile disponibles dès 2003.**
- **IPv6 d'abord intégré dans les terminaux mobiles et les applications avant d'être introduit dans le cœur des réseaux mobiles pour fournir une connectivité en IPv6 de bout-en-bout.**

Les standards ne déterminent toutefois pas à eux seuls le calendrier et la rapidité des déploiements IPv6. Les conditions du marché des services de données mobiles détermineront l'empressement des opérateurs à faire évoluer leurs infrastructures. Ces facteurs clés sont les suivants :

- une large pénétration des terminaux GPRS/UMTS sur le marché de la téléphonie mobile,
- une large part de ces terminaux sont utilisés en connexion permanente,
- un large usage quotidien de services "push".

Un engouement important du grand public pour les services GPRS aurait pour conséquence d'accélérer l'arrivée d'IPv6.

Enfin, la migration d'IPv4 vers IPv6 dans les réseaux mobiles nécessitera des terminaux double-pile IPv4/IPv6. Ceux-ci pourraient être prêts dès 2003 par les constructeurs majeurs du secteur. Ainsi, pourrait-on se diriger vers un scénario où IPv6 serait d'abord intégré dans les terminaux mobiles et les applications avant d'être introduit dans le cœur des réseaux mobiles pour fournir une connectivité en IPv6 de bout-en-bout.

Rappelons, par soucis de clarté, qu'il faut distinguer deux niveaux de signalisation utilisant le protocole IP dans les réseaux mobiles :

- l' « in-band signaling » : la signalisation au niveau des applications, pour interagir avec le monde Internet (mettant en jeu les terminaux et les plates-formes applicatives) ;
- l' « out-band signaling » : la signalisation pour le transport des données à l'intérieur des réseaux cellulaires.

En guise de conclusion, l'enjeu de l'introduction d'IPv6 porte sur les deux niveaux de signalisation mais les conditions d'introduction sont différentes :

- IPv6 dans l'in-band signaling peut apparaître très tôt (possiblement avec le GPRS) à condition que IPv6 soit intégré (en plus d'IPv4) dans les terminaux et au niveau des applications ;
- En revanche, IPv6 dans l'out-band signaling, donc dans la signalisation du réseau cellulaire, ne peut probablement intervenir qu'à partir des déploiements d'équipements UMTS Release 5.

2.1.3 Mobile IP et les technologies WLAN

La mobilité au sens large devrait être mieux prise en compte par IPv6. D'une part, Mobile IPv6 qui apporte un certain nombre d'améliorations par rapport à Mobile IPv4 (cf. infra), a été conçu parallèlement à IPv6, et est pris en compte de façon native par le protocole. En outre, des fonctions comme l'auto configuration permettent aux terminaux de prendre une adresse dans un réseau visité de façon simple ou des fonctions comme le neighbor discovery permettent de simplifier la gestion de la mobilité.

Mobile IP

- **Mobile IP : un protocole bien adapté à la mobilité au sein de réseaux locaux**

Rappelons que Mobile IP est un protocole élaboré par l'IETF, qui permet à des terminaux mobiles de se déplacer dans différents réseaux tout en gardant valide son adresse IP et donc en évitant toute reconfiguration de la part de l'utilisateur final. Mobile IP a été d'abord conçu dans le contexte de la micro-informatique et des réseaux locaux (LAN). Mais dans la perspective du développement des réseaux mobiles et des réseaux locaux sans-fil (WLAN), l'utilisation de Mobile IP est envisagée également pour la gestion de la mobilité en temps réel pour des terminaux mobiles (téléphone et PDA).

Il est probable que dans ce dernier cas, ce soit GTP, déjà utilisé aujourd'hui, qui continue d'être utilisé dans les réseaux cellulaires. Les démarrages se font en IPv4 avec GTP pour la gestion de la mobilité en cœur de réseau. Mobile IPv6 devrait se rendre incontournable pour la gestion de la mobilité d'un terminal IP entre réseaux hétérogènes.

Tableau 5 : Tableau récapitulatif des différences entre Mobile IPv4 et Mobile IPv6

	Mobile IPv4	Mobile IPv6
Mécanisme général	Mécanisme d'encapsulation des paquets IP et de transfert vers l'adresse IP temporaire dans le réseau visité	Suppression du foreign agent, devenu inutile grâce aux fonctionnalités de gestion de la mobilité intégrées dans IPv6
Routage	Routage triangulaire lors de la réception des paquets par le terminal mobile L'optimisation du routage est développée et disponible comme une option	Support intégré de l'optimisation du routage (« Route Opimisation »)
Adressage	Seule l'adresse IP du réseau d'origine est connue du correspondant ; le foreign agent assure la correspondance entre l'adresse IP d'origine et celle dans le réseau visité	Les 2 adresses IP (dans le réseau d'origine et dans le réseau visité) sont codées dans l'adresse IPv6, permettant à l'équipement distant de connaître directement l'adresse de destination et d'éviter l'encapsulation

Il faut néanmoins rappeler qu'IP et Mobile IP relèvent du domaine de « l'informatique » (donc de l'échange de données) et ne gèrent la mobilité du terminal dans les réseaux qu'à ce niveau, sans se soucier du « sous-jacent » (réseau cellulaire, WLAN, etc.). Dans le cas de la téléphonie, ce sont des protocoles spécifiques qui gèrent la mobilité des terminaux technique dans le réseau cellulaire au niveau télécoms (handover, roaming, …).

Technologies WLAN

- **Sur le court terme : une technologie destinée aux LAN privés**
- **Comparées au cellulaire, les technologies WLAN n'ont aujourd'hui qu'un impact de 2ème ordre sur l'introduction d'IPv6 mais …..**
- **L'utilisation des technologies WLAN sur des réseaux publics pourrait accélérer l'arrivée de Mobile IPv6 ; l'attitude des autorités de réglementation sera déterminante à ce niveau**

Le marché des WLAN connaît un développement important à la fois dans le domaine des réseaux d'entreprise et, plus récemment, dans le domaine des réseaux d'accès public (d'abord dans les aéroports et certains hôtels). Les WLAN permettent la connexion à la fois des assistants personnels et des ordinateurs. Toutefois, la prolifération attendue du nombre de terminaux connectés par ces technologies est bien moindre que celle attendue dans le téléphone mobile.

Ainsi, le développement des WLAN n'auront pas un effet majeur dans un premier temps, comparé à la téléphonie mobile (le marché cible des WLAN est avant tout un marché entreprise). En fait, il vaut mieux les assimiler à l'Internet fixe pour le moment (connexions d'ordinateurs sur des LAN d'entreprises ou via des ISP, en général) plutôt qu'à la téléphonie mobile. L'interconnexion des réseaux WLAN publics avec les réseaux mobiles est envisagée avec prudence par les grands opérateurs (par exemple : Orange). Par conséquent, il s'agit plus d'une perspective à moyen terme.

Cependant, aujourd'hui de plus en plus de demandes se font sentir quant à l'utilisation des technologies WLAN sur des réseaux publics. Si une telle utilisation tend à se généraliser, l'arrivée de Mobile IPv6 pourrait s'accélérer de manière notable ; l'attitude des autorités réglementaires sera déterminante dans les prochains mois quant à l'utilisation des technologies WLAN sur des réseaux publics.

La gestion native de la mobilité par IPv6 et ses solutions simples permettant une simplification de la gestion de la mobilité d'un terminal dans un réseau (auto configuration, renumérotation automatique, ...) constituent des avantages évidents pour ce type de technologies et font d'IPv6 une solution particulièrement séduisante pour la gestion de la mobilité dans des réseaux hétérogènes (on pense notamment aux terminaux mobiles au travers d'un WLAN, puis sur les réseaux 3G, etc... : mobilité totale et transparente pour l'utilisateur).

Le développement de ces technologies pourra effectivement constituer un facteur de croissance en adresses IP, mais le terme semble encore éloigné.

Il est clair que le développement de tels réseaux aurait des conséquences sur l'ensemble de la chaîne de valeur des réseaux informatiques, et en particulier chez les équipementiers réseaux et constructeurs informatiques (monde de l'entreprise) et les équipementiers grands publics qui pourraient y voir un débouché pour les terminaux connectés (applications dans la sphère privée) mais dans une moindre mesure (cf. supra : le marché principal est celui des entreprises).

2.2 Les facteurs déclencheurs de deuxième rang

2.2.1 Développement du « always-on »

- **Les accès hauts débit consommateurs d'adresses permanentes**
- **Au Japon, les premiers services d'accès ADSL sous IPv6 ont été commercialisés**

Le marché des hauts débits en devenir pourrait accélérer la pénurie d'adresses sous IPv4. En effet, la plupart des accès haut débit se font en always-on, c'est-à-dire que le terminal reste connecté en permanence et nécessite donc une adresse IP fixe. En pratique, les fournisseurs d'accès haut débit via ADSL par exemple, continuent à proposer un adressage dynamique (donc temporaire). Cependant, les usages qui se développent autour de ces connexions permanentes font que ces ISP ne peuvent appliquer les mêmes taux modem/abonnés que sous connexion RTC ; ces taux peuvent ainsi passer de 1/10 ou 1/20 sous accès commuté à 1/2 ou 1/4 sous accès ADSL. Cela accélère donc la consommation d'adresses IP. Illustrant cette nécessité de disposer d'une adresse IP fixe, Windows XP propose 4 adresses IP par connexion IPv6 : 1 fixe pour le mode serveur et 3 aléatoires pour le fonctionnement en terminal. Dans ce cadre, la pénurie d'adresses IPv4 devrait rapidement devenir critique, rendant nécessaire le passage à IPv6 afin de bénéficier de son espace d'adressage. Il est à noter que cette problématique se retrouve dans le cas de la téléphonie mobile de nouvelle génération (cf. infra).

Si l'on examine la situation au Japon, on observe que les premiers déploiements IPv6 ne se font pas du côté des services mobiles comme on aurait pu s'y attendre mais à travers des accès ADSL sous IPv6 (IIJ, NTT).

2.2.2 Électronique grand public

- **L'électronique connectée : un levier de développement pour IPv6 unanimement reconnu**
- **Les premiers produits électroménagers connectés apparaîtront au Japon courant 2003**

Le développement des objets connectés est unanimement reconnu comme un levier potentiel pour IPv6. Les produits de l'électronique grand public et de l'électroménager (de type TV, appareils photos, etc.) devraient de plus en plus fréquemment être connectés à Internet : ceux-ci pourraient se comporter comme des terminaux (écrans de télévision pour surfer sur Internet, …) ou comme des serveurs (appareils électroménagers dans le cadre du développement de la domotique, etc.).

En outre, les terminaux portables de type PDA devraient se multiplier à l'avenir et être également connectés. Le besoin en adresses IP généré par les développements annoncés devrait rendre impératif le passage des réseaux à IPv6, du moins pour les réseaux concernés par ces applications.

À ce jour, les développements ont commencé, notamment au Japon, où les produits électroménagers connectés devraient apparaître courant 2003 et les jeux en réseaux, moteurs de la croissance du marché des consoles de jeux connectés, représentent déjà un marché important et devraient exploser en 2002. En Europe, des sociétés comme Thomson commercialisent déjà des produits connectés (notamment le système TAK, de TV connectée à Internet), mais ont commencé leurs développements sous IPv4 : IPv6 pourrait être adopté en cas d'explosion du marché donc d'accroissement du besoin en adresses.

2.2.3 Réseaux de capteurs et applications militaires

2.2.3.1 Réseaux de capteurs

- **L'adressage global d'un réseau de capteurs : une source de consommation en adresses IP**

La mise en réseau et la connexion de capteurs via IP est une technique émergente sur laquelle des expérimentations sont menées (au Japon notamment). De nombreux acteurs l'identifient comme un levier de croissance du besoin en adresses IP : adressage global de « méga réseaux de capteurs », pour la météorologie, etc. Développement des réseaux de capteurs embarqués dans l'automobile, l'aéronautique, etc.

Si cette technique prend effectivement un essor important, elle constituera une source de croissance du besoin en adresses IP et donc un facteur influençant le passage vers IPv6.

2.2.3.2 Applications militaires

- **Applications militaires : un intérêt certain pour IPv6 mais peu de communication sur les projets en cours**

Déjà à l'origine de l'utilisation d'IPv4, les militaires américains jouent ouvertement un rôle actif dans le domaine d'IPv6. Ils sont particulièrement intéressés par les solutions de sécurité, les développements sur les réseaux de capteurs. La possibilité, du fait du grand nombre d'adresses, de disposer du mode end-to-end (et donc d'applications de type VoIP qui fonctionnent mieux ainsi) et de rendre plus difficile le « traçage » d'une adresse, sont également autant de points attractifs pour les communications militaires.

Il est à noter que les préoccupations des militaires rejoignent souvent celles des milieux aéronautiques civils.

Les fournisseurs d'applications militaires ont donc intérêt à passer à IPv6 : qu'il s'agisse de systèmes de communications « traditionnels » ou de nouveaux systèmes de contrôle du matériel (ex. des mines connectées pour faciliter le déminage) ou de suivi des soldats (réseaux de capteurs, mobile router), IPv6 peut apporter de réels avantages.

Le transfert de technologie entre les applications militaires et les applications civiles (cryptage, réseaux de capteurs, etc.), dans ce champ d'activité peut constituer un réel levier pour IPv6 ; en outre, les sociétés qui développent les applications militaires ayant tout intérêt, pour leurs applications civiles, à se baser sur les mêmes technologies, il est probable que le secteur soit un relais fort pour le développement d'IPv6.

2.3 Synthèse

Les facteurs déclencheurs de premier rang

- La pénurie d'adresses IP se profilant d'ici la fin de la décennie
- Les services mobiles « always on » : conditionnés au succès du GPRS et de la première version de la 3G lancés sou IPv4

  Mobile IP et les technologies WLAN : l'utilisation des technologies WLAN sur des réseaux publics pourrait accélérer l'arrivée de Mobile IPv6 ; l'attitude des autorités de réglementation sera déterminante à ce niveau

Les facteurs déclencheurs de deuxième rang

- Les accès permanents haut débit
- L'EGP : l'émergence se fera d'abord au Japon
- Réseaux de capteurs et militaires

3 Risques et conséquences soulevés par la migration vers IPv6

3.1 Procédures d'allocation d'adresses sous IPv6 et DNS

- **La première procédure d'allocation (TLA/NLA) a laissé place à un modèle qui devrait s'apparenter aux procédures aujourd'hui connues sous IPv4**
- **Cette nouvelle procédure est en cours d'adoption par les RIR en concertation avec l'IETF**
- **L'ICANN est pour l'instant absente des débats**

3.1.1 Phase de démarrage : TLA, NLA et SLA

Lors du démarrage d'IPv6, une procédure différente mais non moins stricte de celle utilisée sous IPv4, a été mise en place pour gérer l'attribution des adresses (cf. étude documentaire).

Cette procédure mise en place en fonction des recommandations de la RFC 2374 de l'IETF, avait pour objectif de faire cohabiter considérations techniques et « politiques », en s'appuyant sur la structure de l'adressage hiérarchique d'IPv6.

Les registres régionaux ont aujourd'hui décidé de réformer cette procédure afin de s'adapter aux réalités commerciales : l'idée originale de l'IETF était de limiter la taille des tables de routage à 8 000 entrées. Début 2001, les RIR ont jugé que ce nombre n'était pas réaliste et que la conservation de cette structure n'était plus possible. Ainsi, l'IETF a décidé d'abandonner cette procédure durant l'été 2001 (RFC 2373 et 2374).

3.1.2 La nouvelle procédure d'allocation

Depuis l'été 2001, les discussions sont engagées entre les RIR et l'IETF pour que l'ancienne structure d'attribution (TLA / NLA) cède la place à une nouvelle, plus proche de l'ancienne structure IPv4, avec des règles moins restrictives quant au choix des entités se voyant attribuer des adresses. Ainsi, de par cette nouvelle procédure d'allocation, l'accès aux blocs d'adresses IPv6 pour les ISP est plus équitable et ne se fait pas uniquement via un acteur tiers majeur comme dans le cas du schéma TLA / NLA.

La concertation se poursuit aujourd'hui entre le RIPE NCC, l'APNIC et l'ARIN afin de déterminer quelles seront les modalités exactes de l'attribution d'adresses IPv6. On peut regretter que l'ICANN ne participe pas pour l'instant à ces discussions. Toutefois, le récent contrat signé le 2 avril 2002 entre les RIR et l'ICANN amènera peut être l'organisation à participer aux débats.

3.2 Les serveurs DNS

- **Des problèmes techniques se posent encore quant à l'interopérabilité IPv4/IPv6 dans le procédé de résolution de noms de domaine**
- **Des DNS régionaux existent en Asie et en Europe mais il manque aujourd'hui des serveurs racines au sommet de cette hiérarchie**
- **Rôle capital de l'ICANN et de l'IANA :**
  - **Des blocages subsistent aujourd'hui**
  - **C'est la structuration de l'Internet de demain qui se décide aujourd'hui : risque de morcellement du DNS mondial**
  - **L'arrivée d'IPv6 peut être l'occasion de remettre en cause l'hégémonie des USA dans la gestion du DNS mondial**

Le serveur DNS est l'outil qui permet de faire correspondre un nom de domaine « en clair » à une adresse IP. Actuellement, les serveurs DNS fonctionnent en IPv4. Si quelques problèmes se posent encore pour le fonctionnement en IPv6, au Japon et en France, des serveurs DNS IPv6 fonctionnent néanmoins. La principale difficulté sera donc d'assurer l'interopérabilité IPv4/IPv6 pour cette fonction, de façon transparente notamment lors du procédé de résolution de noms de domaine.

Actuellement, les serveurs DNS sont hébergés par des organismes associés à la gouvernance de l'Internet, équivalents des LIR (ou TLA registries dans l'ancien vocabulaire IPv6). Ainsi, en France, c'est Renater qui administre le premier serveur DNS IPv6. Selon les experts, le principal problème ne sera pas technique et ne concernera pas les serveurs DNS « nationaux » : l'organisation du DNS est hiérarchique, et ce qui manque aujourd'hui est une capacité de gérer le DNS au sommet de cette hiérarchie : les serveurs racines (root) ne sont pas prêts. Il s'agirait là d'une cause « politique » plus que technique : blocages de l'IANA et de l'ICANN.

Une prise de position des autorités internationales de l'Internet s'impose à présent. En effet, c'est en partie en décidant de la hiérarchie du DNS IPv6 mondial que l'on construira l'Internet de demain. En l'absence de décision, on pourrait assister à un morcellement du DNS mondial : serveur DNS racine en Asie, serveur DNS racine en Europe. Ainsi l'arrivée d'IPv6 peut être l'occasion de remettre en cause l'hégémonie des USA dans la gestion actuelle du DNS mondial.

3.3 IPv6 : un risque de morcellement de l'Internet

3.3.1 Morcellement géographique

Outre le risque de morcellement au niveau de noms de domaines que nous venons d'évoquer, examinons à présent ce qu'il en est quant à la distribution d'adresses IP à travers le monde.

- **Un rythme d'entrée dans IPv6 différent selon les régions**
  - **Moins d'adresses IPv6 attribuées pour l'Amérique du Nord**
  - **Un apparent équilibre Asie-Europe mais :**
    - **Principalement des réseaux de recherches en Europe, peu d'ISP**
    - **Principalement des ISP et des opérateurs en Asie**

Tableau 6 : Adresses IPv6 attribuées au 29/01/02

RIR	Nombre de /35 attribuées	Remarques
ARIN (Amérique du Nord)	24	Réseaux de recherche Équipementiers Apparition d'opérateurs
RIPE (Europe)	51	Au moins une dizaine d'opérateurs et ISP Réseaux de recherche
APNIC (Asie)	50	28 pour le Japon, 9 pour la Corée Principalement des ISP et opérateurs Équipementiers grand public (Sony)
TOTAL	**125**	**-**

Source : IDATE d'après RIPE NCC

Le rythme d'entrée dans IPv6 des différentes régions du monde sera assez différent. Toutefois, le morcellement géographique (barrière des langues, habitudes d'utilisation, etc.) existe déjà de fait, et les conséquences techniques (cf. infra) de la cohabitation de différents standards en différentes zones devraient donc être minimes.

Asie

- **L'Asie avec le Japon et la Corée devrait connaître un décollage significatif du marché IPv6 d'ici 2003**

L'Asie et notamment le Japon est actuellement en avance sur le reste du monde. En effet, suite à une politique gouvernementale poussant vers IPv6, les industriels Japonais (suivis par les Coréens) sont aujourd'hui en mesure de proposer des gammes de produits dans le domaine des équipements de réseau, mais aussi dans le domaine des produits grand public (produits électroménagers connectés et IPv6 prévus pour fin 2002). En outre, les réseaux IPv6 commerciaux commencent à prendre de l'envergure, notamment au travers des accès ADSL.

Le marché de l'Internet mobile et de la 3G n'est donc pas celui qui permettra à IPv6 de démarrer au Japon (pour le moment le fonctionnement se fait en IPv4, mais les besoins futurs imposeront le passage à IPv6).

La fin de l'année 2002 devrait correspondre à un décollage significatif du marché d'IPv6 au Japon et en Corée.

Le marché asiatique, mal pourvu en adresses IPv4 sera le premier à ressentir la pénurie, notamment dans des pays à fort potentiel de développement comme la Chine ou l'Inde. Le Japon se positionne en précurseur sur son marché domestique.

Europe

- **L'Europe affirme pour l'instant sa maîtrise technique d'IPv6 mais des déploiements significatifs d'IPv6 ne devraient pas apparaître avant 2004 ou 2005**
- **L'attitude volontariste de la Commission Européenne avec l'IPv6 Task Force**

L'Europe affirme sa position en termes de maîtrise technique d'IPv6 : les réseaux de recherche sont très avancés dans le domaine, les opérateurs d'envergure se tiennent prêts pour lancer des offres (Telia a même commencé à développer un réseau IPv6 natif), mais l'attitude reste prudente : les acteurs ont actuellement comme priorité de stabiliser leur situation économique et ne se lanceront dans une phase commerciale d'IPv6 que si la demande est identifiée. Les équipementiers nordiques proposent déjà des matériels pour réseaux mobiles prêts pour IPv6 et les terminaux haut de gamme ont déjà une double pile IPv4/IPv6. Les équipementiers spécialisés dans les réseaux fixes (à l'exception de précurseurs comme Telebit ou de spécialistes d'IPv6 comme 6Wind) devraient être prêts à répondre à la demande en 2003.

Le démarrage en Europe pourrait bien être dû au développement des applications mobiles, mais on ne prévoit pas de développement d'envergure avant 2004 ou 2005.

La commission Européenne, au travers de l'IPv6 Task force, recommande aujourd'hui une action plus volontaire des pouvoirs publics en faveur du développement d'IPv6, afin que l'Europe ne soit pas distancée par le Japon.

Amérique du Nord

- **Les acteurs nord-américains se préparent à IPv6 : les équipementiers leaders et quelques grands ISP se positionnent**

Longtemps assoupie sur le sujet d'IPv6, l'Amérique et notamment les États-Unis semblent aujourd'hui plus réactifs. Les équipementiers leaders du marché proposent des gammes de produits mis à jour grâce à des logiciels et devraient proposer des produits hardware d'ici 2003. Les opérateurs et ISP qui disposaient d'un grand nombre d'adresses IPv4 commencent à prendre conscience de la pénurie qui se profile et semblent porter un intérêt à IPv6. Certains opérateurs majeurs, s'ils ne proposent pas d'offre IPv6 packagée, sont néanmoins capables d'offrir un service IPv6 à la demande (UNNET WorldCom), et des opérateurs majeurs disposent maintenant d'adresses IPv6, signe d'un intérêt croissant pour le sujet. Le réveil de l'Amérique, bien que tardif, ne semble pas arriver trop tard par rapport à la lenteur de décollage du marché. Les développements IPv6 des réseaux aux États-Unis ne sont pas prévisibles à ce jour, mais des dates similaires aux dates Européennes semblent plausibles.

Les pouvoirs publics américains ne sont officiellement pas engagés dans le processus de déploiement d'IPv6 (principe de non intervention auprès du secteur privé, qui ne présagent en rien des travaux menés par les agences de sécurité de type NSA, par exemple), toutefois, l'Armée Américaine ne cache pas son intérêt pour IPv6.

3.3.2 Morcellement technologique

- **Des risques limités de morcellement technologiques de par la longue cohabitation inévitable entre les deux protocoles**
- **De nombreux mécanismes de transition ont déjà été définis par l'IETF**
- **Le passage à IPv6 sera une transition progressive et lente**

Même si IPv6 a été conçu dans la continuité d'esprit d'IPv4, sans réelle rupture technologique, le nouveau protocole n'en reste pas moins différent et l'interopérabilité entre les deux IP n'est pas naturelle.

Or, il apparaît plus judicieux de parler de transition et de déploiement que de migration : on ne se situe pas dans un cas de figure du type an 2000 avec une bascule subite, mais dans celui d'une transition douce et progressive des réseaux. Ceci signifie que les deux standards seront amenés à cohabiter et donc à inter opérer.

Les scenarii de transition sont multiples et les outils qui les appuieront ont été largement envisagés par l'IETF, ainsi que leur usage dans les phases de la transition progressive (cf. infra).

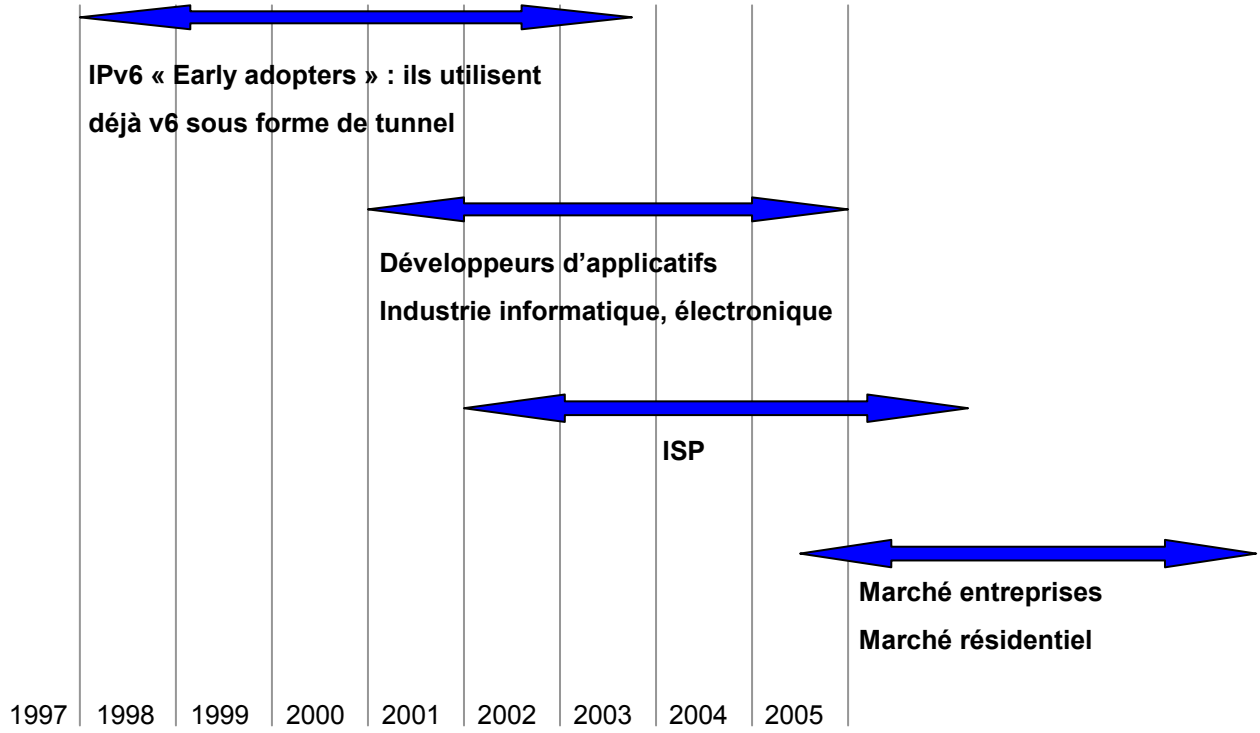
Ainsi, la cohabitation entre les deux standards risque d'être relativement longue. On peut estimer qu'à partir des premiers déploiements IPv6, il faudra au moins une dizaine d'années pour qu'IPv6 devienne majoritaire. Qui plus est, il n'y a pas uniformité dans ce domaine : il est probable que les ISP migrent bien avant les entreprises (qui cherchent d'abord à rentabiliser les applicatifs développés sous IPv4 avant d'investir dans de nouvelles techniques).

- **Les cœurs de backbone pourraient devenir des goulets d'étranglement prisonniers du protocole IPv4**

Le passage à IPv6 des opérateurs de backbone, s'il n'est pas critique aujourd'hui, pourrait le devenir lorsque les applicatifs IPv6 se généraliseront. Étant donné les performances moindres annoncées des routeurs de cœur de réseau sous IPv6, il y a ici un risque que la migration se fasse rapidement en bord de réseau avec des cœurs de backbone qui restent trop longtemps sous IPv4. L'absence d'outil de gestion et de provisioning sous IPv6 ne fait qu'accentuer cette crainte.

On peut établir la chronologie suivante pour le démarrage de l'utilisation d'IPv6. Gardons à l'esprit que la rentabilisation des outils IPv4 devrait permettre à l'ancien protocole de subsister encore plusieurs dizaines d'années (jusqu'à 20 ans).

Figure 6 : Chronologie de passage à IPv6 (à pondérer selon les zones géographiques)



Source : IDATE

3.3.3 Dichotomie fixe/mobile

- **L'introduction d'IPv6 ne se fera pas de façon uniforme sur les réseaux fixes et mobiles**
- **Les premiers accès fixes ADSL sous IPv6 ouverts au Japon**
- **Des services mobiles IPv6 commerciaux devraient suivre à l'horizon 2004/2005 mais des incertitudes demeurent :**
  - **Dans le Release 5, IPv6 sera uniquement utilisé dans le IP Multimédia Subsystem, son utilisation en cœur de réseau n'a pas encore été décidée**
  - **La Release 5 n'étant pas encore achevée, un risque de dérapage temporel existe, le 3GPP n'étant pas maître du calendrier**

Les premiers accès commerciaux IPv6 ADSL ouverts par des ISP japonais laissent penser que l'arrivée d'IPv6 se fera d'abord par des accès fixes et notamment haut débit.

En ce qui concerne les réseaux cellulaires de type 2,5G et 3G, il est difficile de se prononcer sur un calendrier et des incertitudes demeurent : IPv6 deviendra obligatoire pour certains types d'applications à partir de la version 5 d'UMTS, qui ne devrait pas être implémentée avant 2004. De plus, cette Release 5 n'est pas encore terminée et le 3GPP n'est pas maître du calendrier. Cependant, pour des raisons techniques, les opérateurs pourraient voir un intérêt à une utilisation plus précoce d'IPv6. Il y a peut-être pour eux une opportunité de démarrer sous ce standard, le morcellement de fait existant entre réseaux fixes et mobiles (pas de contraintes fortes en termes d'interopérabilité).

Ceux-ci éviteraient également de devoir investir dans une « migration » ultérieure. Aujourd'hui, les opérateurs, mais surtout les industriels voyant dans leurs services un support mobile (véhicule connecté, ...) se posent cette question.

L'incertitude règne sur le sujet et même le marché Japonais, habituellement étalon dans le domaine n'apporte pas de réponse définitive : aujourd'hui, DoCoMo administre le i-mode et FOMA (son réseau 3G) en IPv4+NAT : cela représente plus de 31 millions d'abonnés. Toutefois, l'utilisation d'IPv6 pourrait leur permettre de développer plus simplement de nouvelles applications (cf. supra) et d'alléger (donc de fiabiliser) la gestion des leurs réseaux.

Côté applications mobiles d'entreprises, il est possible qu'IPv6 soit tiré par le développement de technologies comme les WLAN (802.11b) et les applications mobiles connectées (accroissement du besoin en adresses). Mobile IPv6 devrait permettre notamment une meilleure gestion de la mobilité entre réseaux hétérogènes.

Il semble donc plausible qu'IPv6 démarre à moyen terme dans le monde de la mobilité (au sens large, pas uniquement au sein des réseaux cellulaires), pour permettre le développement des nouvelles applications ayant besoin des apports d'IPv6 (adresses permanentes, fin du NAT...). Les opérateurs ne se prononcent cependant pas sur un calendrier précis ou sur un démarrage des nouveaux services en IPv6.

3.4 IPv6 ne résout pas tous les problèmes actuels de l'Internet

- **L'immense espace d'adressage d'IPv6 justifie à lui tout seul le nécessaire passage à IPv6**

Le principal apport d'IPv6 est son espace d'adressage. Bien que réelles, les autres améliorations d'IPv6 ne seront pas nécessairement utiles immédiatement et il est important de se garder de tout optimisme technologique : si IPv6 apporte des avantages, il n'est pas non plus la solution miracle à l'ensemble des problèmes de l'Internet.

3.4.1 Qualité de service

- **En l'état actuel de la normalisation, les outils de Qualité de Service sous IPv6 seront identiques à ceux que l'on connaît aujourd'hui sous IPv4**
- **Une performance des routeurs de cœur de réseau dégradée sous IPv6, dans un premier temps**

Les spécificités d'IPv6 qui doivent permettre un meilleur support de la gestion de la Qualité de Service (QoS) permettent au nouveau protocole de disposer d'un bon potentiel. Toutefois, ceci suppose qu'il existe des outils qui s'appuient sur ces caractéristiques. Or, en l'état actuel des choses, ces outils n'existent pas, et les premiers temps d'IPv6 devraient voir une gestion de la QoS s'appuyant sur les mêmes outils qu'en IPv4 : ceux-ci n'utilisent évidemment pas les spécificités d'IPv6.

En outre, en cœur de réseau, l'en-tête IPv6 étant plus volumineuse que l'en-tête IPv4, les temps de calcul devraient être allongés pour les routeurs (à matériel égal, donc à coût nul…), et de fait, la performance globale du réseau et la QoS légèrement dégradées.

Les inconnues sont dès lors le temps que durera la vie des outils de gestion de QoS non spécifiques, et le temps nécessaire pour que les routeurs de cœur de réseau aient des performances accrues : la migration d'IPv6 sera probablement un « effet de bord » dans un premier temps, ce qui permettra de laisser le temps aux matériels de cœur de réseaux pour être mis à niveau.

3.4.2 Multihoming

- **Le Multi-homing va perdurer sous IPv6**

La multiplication des fournisseurs d'accès Internet pour les entreprises (sites distants, réseaux hétérogènes, ...) est une tendance actuelle. Ainsi, pour un même accès du point de vue de l'utilisateur, ce sont plusieurs prestataires qui peuvent intervenir (un pour l'Internet mobile, un pour l'accès sur un site A, un autre sur un site B, ...). Cette tendance pourrait même s'accroître et s'étendre aux particuliers avec le développement des applications mobiles connectées (mobilité entre réseaux hétérogènes : un individu veut pouvoir se connecter de façon transparente chez lui, dans sa voiture, dans son bureau, ...). Le routage est rendu extrêmement complexe par ces pratiques.

Le problème est déjà apparu sous IPv4 : IPv6 ne prévoit pas de solution spécifique à ce problème. L'adressage hiérarchique devrait permettre d'apporter des solutions plus simples, mais à ce jour, il n'y a pas de solution « miracle ».

3.4.3 Sécurité

- **L'utilisation d'IPSec de bout-en-bout est impossible à travers des NAT**
- **Comme sous IPv4, l'absence de distribution de clés publiques (PKI) rend impossible une utilisation optimale d'IPSec**

IPSec est, nous l'avons vu, prévu en mode natif dans IPv6. Cependant, son utilisation n'est pas obligatoire. Mais le principal point faible d'IPSec sous IPv4 se retrouve sous IPv6, du moins lors de la phase de transition : le NAT. En effet, IPSec traverse mal les NAT, ce qui nuit à la sécurisation de bout-en-bout. Dans les premiers temps de migration, afin de faire inter opérer les deux mondes, IPv4 et IPv6, le recours à une nouvelle forme de NAT devrait être nécessaire (le NAT-PT). Dès lors, l'avantage apporté par IPv6, sans être annulé, serait néanmoins repoussé dans sa pleine expression.

Enfin, un autre problème, déjà connu sous IPv4 n'est pas encore résolu sous IPv6 : l'absence de distribution de clés publiques (PKI) pour l'utilisation d'IPSec : sans solution, c'est l'utilisation même d'IPSec qui est fortement limitée.

3.5 Enjeux industriels

Le développement des applications et objets connectés devrait être un moteur de croissance des besoins en adresses IP et donc un accélérateur de passage à IPv6. Cependant, le réalisme technologique oblige à préciser qu'il est inconcevable d'offrir une adresse fixe à tous les objets connectés : le routage ne le supporterait pas ! IPv6 pourrait également permettre l'émergence (durable ?) de nouveaux acteurs et de nouveaux modèles économiques : on est, dans ce domaine, au stade de la prospective et il serait prématuré de prévoir les effets réels de ces spéculations. Toutefois, le fait que les différents acteurs réfléchissent à ces sujets, ou s'engagent dans des recherches, voire créent des entreprises dédiées, est une preuve suffisante de l'intérêt de la question.

3.5.1 IPv6 vecteur de diffusion de l'Internet

- **L'arrivée d'IPv6 va permettre au protocole IP de sortir de sa sphère d'origine pour migrer vers d'autres secteurs industriels**

IPv6 peut constituer une opportunité pour de nouvelles applications de se développer en utilisant la technologie IP et du fait des avantages d'IPv6, ces technologies IP peuvent se diffuser dans des secteurs économiques en dehors des secteurs informatique et télécoms et jusqu'ici non utilisateurs.

3.5.1.1 Électronique grand public

- **L'une des évolutions annoncées pour les 10 années à venir est le développement des applications connectées, mobiles ou fixes**

Les téléviseurs, les appareils de prise de vue, etc. deviennent communicants. D'ores et déjà, on peut utiliser son téléviseur comme un terminal Internet. La multiplication de ces objets devrait constituer un levier pour le besoin d'adresses IP, accélérant ainsi le besoin de passage vers IPv6. En outre, les fonctions d'auto configuration qui rendent la connexion de ces terminaux au réseau plus simple participent elles aussi à l'intérêt d'une utilisation d'IPv6 pour ce type d'applications.

Une fois de plus dans ce domaine, ce sont les industriels nippons qui nous montrent la voie pour l'instant.

3.5.1.2 Domotique

- **Les possibilités d'auto configuration et d'adressage hiérarchique associées à IPv6 ouvrent la porte à bon nombre d'applications domotiques**
- **Au Japon, les premiers « produits blancs » connectés sont annoncés pour 2003, preuve d'une émergence de ce marché**

En liaison avec l'électronique grand public et en particulier avec les appareils électroménagers, on voit l'émergence de la domotique comme un facteur de croissance des besoins en adresses IP. En outre, l'adressage hiérarchique, la possibilité d'affecter un « préfixe » permettant de structurer un réseau en aval, l'auto configuration, sont autant d'arguments plaidants en faveur d'une utilisation d'IPv6.

Plusieurs visions coexistent cependant :

- adressage direct des appareils (très consommateur d'adresses IP),
- pas d'adressage global de ces « nœuds » du réseau domestique, mais adressage du réseau domestique comme un nœud et adressage privé en dessous.

Le principal avantage attendu d'IPv6 dans ce domaine est en fait l'auto configuration qui permet au terminal de prendre seul sa place dans un réseau, ce qui est indispensable dans le cas d'utilisateurs a priori non spécialistes.

En outre, quelle que soit la vision qui l'emporte (a priori la seconde : si tous les objets étaient connectés, on aboutirait vite à une saturation des routeurs), le besoin d'adresses IP sera accru par le développement de ces nouvelles applications : même si le foyer est le seul à disposer d'une adresse globalement routable, le nombre de foyers potentiellement connectés est très important. Il faut donc un stock suffisant d'adresses pour faire face à de tels besoins.

Dans ce domaine, nous voyons qu'encore une fois, le principal atout d'IPv6 réside dans son stock d'adresses et donc son espace d'adressage.

Au Japon, les premiers « produits blancs » connectés sont annoncés pour 2003, preuve d'une émergence de ce marché.

3.5.1.3 Automobile

- **Le secteur automobile : un potentiel important de développement pour IPv6 mais une attitude encore réservée des industriels du secteur**
- **Deux tendances se dégagent pour des services mobiles :**
  - **Partir en IPv4 + NAT**
  - **Partir directement sous IPv6**

Le développement du véhicule communicant, des applications multimédia embarquées (même si pour le moment, le coût du MO transmis plaide plus pour un téléchargement en poste fixe et une utilisation off line…) sont une tendance d'avenir de l'automobile. Les constructeurs étudient aujourd'hui la possibilité d'appuyer leurs services sur des réseaux 3G : le fait qu'IPv6 soit obligatoire dans les applications 3G multimédia dès la version 5 d'UMTS devrait constituer un levier de développement d'IPv6 : l'automobile peut donc être un moteur de son expansion.

Il faut néanmoins nuancer cette tendance par le fait que pour le moment, les principales applications de télémétrie automobile peuvent reposer sur l'emploi du SMS.

Cependant, dans le cas d'un développement de l'Internet ou des applications connectées automobiles, on peut estimer, au vu du nombre de véhicules produits chaque année, que le besoin en adresses risque de devenir très fort dans les 10 années à venir.

On trouve deux tendances dans l'industrie automobile : certains préfèrent partir sur une architecture IPv4 + NAT, d'autres plus innovants se positionnent plutôt pour un départ de certains de leurs services embarqués sous IPv6.

3.5.1.4 Aéronautique

- **L'industrie Aéronautique examine de près IPv6 :**
  - **Pour des applications de maintenance et de traçabilité**
  - **Pour des applications multimédia dans les avions**

Aujourd'hui, IP n'est pas ou peu utilisé dans le monde de l'aéronautique, principalement du fait du manque d'adresses et du fait que l'utilisation du NAT nuit au fonctionnement des applications temps réel, qui sont les principales utilisées dans ce domaine. Le développement d'IPv6 et de produits fiables, pourrait constituer une opportunité pour ce secteur, pour passer à IP et ainsi utiliser des produits « industriels » (donc moins chers) en lieu et place des protocoles propriétaires utilisés actuellement.

Les applications de maintenance des matériels (cruciales dans ce domaine) et de suivi et traçabilité, pourraient s'appuyer sur des outils développés sur IPv6. En outre, les applications « multimédia » à destination des passagers (comparable à la problématique automobile) pourraient également s'appuyer sur IPv6.

L'arrivée de ce nouvel utilisateur dans le jeu IP pourrait donc constituer, à moyen terme, un levier de croissance pour IPv6.

3.5.1.5 Acteurs du contenu

- **Des applications temps réels rendues difficiles sous IPv4 + NAT se développeront facilement sous IPv6 : des acteurs se positionnent notamment au Japon (jeux vidéo)**

L'emploi d'IPv4 ne favorise pas les applications temps réel, et notamment la diffusion de contenu de type musical ou vidéo (en outre, la sécurité nécessaire pâtit de l'emploi des NAT). La possibilité d'alléger la gestion des joueurs pour les jeux en réseau (annoncés comme un secteur d'avenir) constitue, du point de vue des éditeurs, un réel avantage et la gestion des NAT des réseaux constitués par les communautés de joueurs devraient disparaître en v6. Le Japon, réceptif à ce dernier marché, se prépare déjà à offrir des services IPv6 spécifiques.

Les fonctions multicast, ou anycast, disponibles en natif de façon simple, peuvent permettre le développement de nouvelles applications, ou tout du moins aux applications existantes, mais peu répandues (VoD, streaming, etc.) de prendre un plus grand essor. Il est donc probable que ce type d'applications soit à la fois favorisées et favorisent également IPv6.

3.5.1.6 Autres secteurs

- **IPv6 et les réseaux de capteurs**
- **Un intérêt certain des militaires pour IPv6**

Une des applications identifiées comme forte consommatrice d'adresses IP est le réseau de capteur. Il semble que de nombreux usages se développent, dans l'industrie, l'automobile, l'aéronautique, pour des réseaux de capteurs capables de communiquer simplement.

Ce type de réseaux intéresse également les militaires, qui voient aussi dans l'espace d'adressage d'IPv6 et dans ses fonctions de sécurité (notamment), des avantages sérieux pour le développement d'applications propres.

Le transfert de technologie de l'environnement militaire vers l'environnement civil (principalement en provenance des prestataires, soucieux de rentabiliser le savoir-faire acquis pour développer les applications militaires) devrait constituer un levier fort pour le développement d'IPv6.

3.5.2 IPv6 porteur de nouveaux services

3.5.2.1 Possibilité d'émergence de nouveaux modèles économiques

- **IPv6 ouvre la porte à de nouveaux modèles économiques qui restent à inventer afin de lever les incertitudes sur les scenarii de passage à IPv6.**

Actuellement, les différents acteurs (opérateurs et ISP notamment) cherchent à valider les modèles économiques utilisés avec IPv4.

IPv6 amène la restauration du mode bout-en-bout et la possibilité pour chaque nœud de devenir un serveur (adresses fixes globales). De nouveaux modèles économiques doivent se mettre en place : la nature des services fournis par les ISP et opérateurs change (l'intelligence quitte le prestataire et est contenue dans le protocole, l'hébergement de serveurs perd de son intérêt, ...), la nature et le niveau des coûts de maintenance du réseau également.

Actuellement, la demande des opérateurs et ISP est forte pour que les équipementiers fournissent des modèles qui permettraient de justifier l'investissement nécessaire au passage à IPv6. Ces modèles ne sont pas encore établis, d'où l'incertitude sur les scenarii de passage à IPv6.

3.5.2.2 L'amélioration des services temps réels

- **IPv6, de par la suppression des NAT permettra une meilleure diffusion des services temps réels**

Comme il a été dit précédemment, les applications reposant sur le mode bout-en-bout sont potentiellement améliorées par l'emploi d'IPv6. Le potentiel d'accroissement de la QoS constitue également un moteur pour l'emploi d'IPv6 dans ce domaine.

Ces applications peuvent donc s'appuyer sur IPv6 et de fait, constituer un levier pour sa diffusion.

3.5.2.3 L'avènement du peer-to-peer et fin du modèle client-serveur ?

- **IPv6 peut permettre l'avènement du modèle P2P au dépend du modèle client serveur**
- **Une crainte des ISP : le P2P représente un réel danger pour leurs revenus actuels**

Comme il y a été fait allusion, la restauration d'adresses globalement routables (suppression des NAT) permet de transformer tout nœud du réseau en serveur potentiel. Les applications peer-to-peer n'ayant plus à traverser de serveurs, peuvent se développer de façon plus certaine qu'en IPv4.

La question, pour ce type d'applications, qui trouvent un intérêt à l'utilisation d'IPv6 est de savoir si elles seront réellement motrices pour IPv6 ou le contraire. À ce jour, la demande n'est pas identifiée, et il est plus probable qu'elles accéléreront le déploiement d'IPv6 une fois que celui-ci aura commencé, mais ne constitueront pas l'application « amorce » de la transition.

De plus, cet éventuel avènement du modèle P2P au dépend du modèle client/serveur ne séduit pas vraiment les fournisseurs d'accès qui y voient un réel danger pour leurs revenus actuels.

3.5.3 Perspectives de nouveaux entrants

- **Des opportunités pour de nouveaux entrants spécialisés sur IPv6**
- **IPv6 offre la possibilité à des acteurs traditionnels de l'informatique d'étendre leur marché adressable**

Le déploiement d'IPv6 est l'occasion pour de nouveaux acteurs de se positionner sur un marché IP en mutation. Ainsi voit-on apparaître des équipementiers entièrement tournés vers IPv6, des fournisseurs de services de transition, d'interopérabilité, opérateurs dédiés, ISP, ...

L'opportunité existe également, nous l'avons vu, tant pour des acteurs actuellement absents du domaine IP comme les constructeurs automobiles, mais aussi pour des spécialistes de l'IP de devenir des fournisseurs de ces acteurs : demain IBM sera-t-il équipementier automobile ? Microsoft fournira-t-il les fabricants d'électroménager ? La question n'est finalement pas absurde.

À ce jour, ce domaine reste mal défriché et les différents acteurs en sont au stade de l'exploration et du questionnement, mais les potentiels présentés restent néanmoins importants, et la convergence des technologies apparaît ici comme un moteur réel d'IPv6.

3.6 Synthèse

- **Une procédure définitive d'allocation des adresses IPv6 non encore finalisée avec l'ICANN absente des débats**

- **DNS**
  - **Des DNS sous IPv6 régionaux mais pas de DNS racine**
  - **Une prise de position de l'ICANN est urgente**
  - **IPv6 : une opportunité pour remettre en cause l'hégémonie américaine**

- **Un rythme d'entrée dans IPv6 différent selon les régions**
  - **Un apparent équilibre Asie-Europe au niveau des allocations d'adresses IPv6 mais :**
    - Principalement des réseaux de recherches en Europe, peu d'ISP
    - Principalement des ISP et des opérateurs en Asie

- **Le passage à IPv6 sera une transition progressive et lente**

- **Des risques limités de morcellement technologiques de par la longue cohabitation inévitable entre les deux protocoles**
  - **De nombreux mécanismes de transition ont déjà été définis par l'IETF**

- **L'introduction d'IPv6 ne se fera pas de façon uniforme sur les réseaux fixes et mobiles**

- **IPv6 ne résout pas tous les problèmes actuels de l'Internet**
  - **QoS, Multihoming, Sécurité**

- **IPv6 et les enjeux industriels associés : de nouveaux modèles économiques qui restent à inventer**
  - **Des opportunités pour de nouveaux entrants spécialisés sur IPv6**
  - **IPv6 offre la possibilité à des acteurs traditionnels de l'informatique d'étendre leur marché adressable**

Partie 3 : les enjeux pour la régulation

1 Enjeux concurrentiels de la transition de IPv4 à IPv6

Si l'arrivée d'IPv6 contribue au progrès technique et, à ce titre, est un facteur de développement de la concurrence sur les marchés liés à Internet, la période de transition du monde IP de v4 vers v6 peut constituer un frein au maintien et/ou au développement de la concurrence sur certains marchés. À cet égard, la Commission européenne a pu rappeler, dans la nouvelle directive « Cadre », que le progrès technique pouvait conduire à l'apparition de nouveaux goulets d'étranglement.

1.1 L'arrivée d'IPv6, facteur de développement de la concurrence

1.1.1 Par l'intensification de la concurrence sur des marchés existants liés à l'accès à Internet

Les acteurs de la fourniture des services d'accès à Internet ne bénéficient pas d'une qualification claire : fournisseurs d'accès à Internet (IAP), ils cumulent également souvent la qualité de fournisseurs de services Internet (ISP). Dans les développements qui suivent, il sera fait uniquement référence aux ISP, exerçant cumulativement ou alternativement des fonctions (i) d'accès (fourniture des adresses IP et de la connectivité à Internet) et/ou (ii) de services (hébergement de données). On notera à cet égard que, selon la Commission européenne, un ISP est un fournisseur de services Internet comprenant essentiellement l'accès au réseau[5].

L'intensification de la concurrence du fait de l'arrivée d'IPv6 peut être anticipée au niveau de l'accès à Internet en raison de la modification prévisible tant des conditions de l'offre d'accès à Internet que des conditions de la demande des services d'accès.

1.1.1.1 Au niveau de l'offre : abaissement des barrières à l'entrée

L'arrivée d'IPv6 devrait se traduire, et c'est l'un de ses principaux objectifs, par un abaissement des barrières à l'entrée sur le marché de la fourniture des services d'accès à Internet. Ainsi, **la suppression de la rareté des ressources en adresses IP** devrait en principe permettre un accès plus large à ces ressources par les entreprises désireuses de fournir des prestations d'accès, sous réserve néanmoins que les mécanismes d'allocation des adresses pendant la transition vers IPv6 ne soulèvent pas de problèmes de concurrence (cf. *infra* 2.1). Dans sa communication du 21 février 2002, la Commission européenne a ainsi relevé que la disponibilité de l'espace d'adressage devrait conduire à une baisse du prix des adresses Internet[6].

L'abaissement des barrières à l'entrée pour les entreprises désireuses de fournir des services d'accès à Internet devrait également résulter d'une **baisse des coûts pour les ISP** dès lors que les

[5] Communication de la Commission au Conseil et au Parlement européen, L'Internet nouvelle génération : priorités d'actions dans la migration vers le nouveau protocole Internet IPv6, Bruxelles, le 21.2.2002, Glossaire.

[6] Communication précitée, p. 8. On notera cependant que le document du RIPE relatif aux demandes d'allocation d'adresses IP indique que l'allocation d'adresses est gratuite et que par conséquent les entités membres n'ont pas à acheter de telles adresses.

fonctionnalités offertes par IPv6, conduisant en particulier à la simplification des tables de routage, permettra de simplifier la gestion de leurs réseaux par les ISP.

Ainsi, l'arrivée d'IPv6 est de nature à favoriser l'entrée de nouveaux acteurs sur le marché de l'accès à Internet.

1.1.1.2 Au niveau de la demande : plus grande transparence

L'une des différences notables d'IPv6 par rapport à IPv4 est l'auto-configuration des réseaux. Cette nouvelle fonctionnalité est susceptible de se traduire par une plus grande possibilité de choix pour les demandeurs de services d'accès à Internet, tant pour les utilisateurs entreprises que résidentiels.

S'agissant des utilisateurs entreprises, IPv4 n'offrant pas de fonctionnalité d'auto-configuration, tout changement de fournisseur d'accès à Internet implique des coûts liés à la nécessité de renuméroter / reconfigurer le réseau. Il en résulte que, en l'état, les entreprises sont largement captives de leur ISP, ce qui n'est pas un facteur de concurrence entre les ISP. Ainsi, la fourniture de services d'accès à Internet sous IPv6 va permettre de **fluidifier la concurrence entre les ISP dès lors que le système d'auto-configuration permettra aux entreprises de changer de fournisseur à moindre coûts**, la renumérotation d'un réseau devenant automatique mais est aussi susceptible de réduire, dans cette mesure, l'étendue de leurs services.

Cette fluidité du marché de l'accès à Internet est susceptible d'être accrue grâce au modèle de communication directe entre utilisateurs (communications de poste à poste) auquel IPv6 va conduire. Dans cette configuration, les utilisateurs pourront héberger leurs propres données, et seront par conséquent moins « dépendant » des services d'hébergement offerts par leur ISP. À cet égard, on notera que **le modèle de communication de poste à poste est susceptible de modifier le modèle économique des ISP** dans la mesure où il pourrait conduire à la limitation de l'activité d'externalisation de l'hébergement des données auprès des ISP.

En ce qui concerne les utilisateurs résidentiels, sous IPv4, en raison de la rareté des adresses IP et de la nécessité de configurer les adresses pour chaque service d'accès, certains acteurs, et en particulier les opérateurs de réseaux mobiles fournissant un service d'accès à Internet *via* les terminaux mobiles, ont été tenté et/ou ont effectivement préconfiguré l'accès à Internet de sorte que celui-ci se fasse *via* leur propre portail. Une telle pratique, qui a été jugée contraire aux règles de concurrence[7], semble possible techniquement sous v6. En effet, la capacité d'auto-configuration facilite la pré-installation des adresses dans les terminaux tels que les stations de jeux ou des matériels électroménagers. Dans ces conditions, les fournisseurs desdits équipements, qui pourront être également ISP, pourraient être tentés de limiter l'accès à leurs propres plates-formes de services (e.g. service après-vente). Néanmoins, il est probable que les utilisateurs disposeront d'un autre moyen d'accès à Internet, l'accès via des terminaux tel qu'un réfrigérateur pouvant, du fait des propriétés du terminal (et indépendamment de la pratique du fournisseur), limiter par nature son utilisation pour accéder à des contenus divers sur Internet.

[7] TC Paris, 30 mai 2000, affaire WAPUP.

1.1.2 Par la création de marchés nouveaux

La création de marchés nouveaux suppose que l'arrivée d'IPv6 conduise à la fourniture de produits et/ou de services nouveaux, c'est-à-dire, au sens du droit de la concurrence, non substituables à ceux actuellement disponibles, cette substituabilité devant s'apprécier essentiellement du côté de la demande[8]. À cet effet, dans le Projet de Lignes Directrices, la Commission a rappelé les éléments importants en vue d'apprécier la substituabilité du côté de la demande dans le secteur des communications électroniques[9] :

(i) les caractéristiques objectives des produits ou services,

(ii) le type d'utilisation des produits ou services,

(iii) le modèle de détermination des prix (qui permettent notamment de distinguer des marchés distincts pour les abonnés d'affaires et les abonnés résidentiels) et,

(iv) l'existence de coûts d'adaptation pouvant restreindre la possibilité pour les utilisateurs de remplacer le produit ou service par un autre (e.g. investissements, liens avec les fournisseurs par un contrat de longue durée).

S'agissant de la dimension géographique du marché, la Commission européenne a indiqué que dans le secteur des communications électroniques, elle devait s'apprécier en fonction notamment de l'étendue du réseau tout en pouvant être limitée à certaines routes[10].

Enfin, tout en rappelant que dans un secteur caractérisé par l'innovation constante et une convergence technologique rapide, **toute définition de marché actuellement en vigueur risque de devenir inexacte ou désuète dans un proche avenir**, la Commission européenne a rappelé qu'il existait deux types de marchés : (i) les marchés amont d'accès aux infrastructures nécessaires pour fournir des services et (ii) les marchés aval des services fournis aux utilisateurs finals[11].

Il résulte de ce qui précède et de la pratique décisionnelle des autorités de concurrence communautaires dans le secteur des communications électroniques que des marchés nouveaux sont susceptibles d'être créés du fait de l'arrivée d'IPv6.

1.1.2.1 Marchés amont

La fourniture de services sous IPv6 requiert l'accès à des infrastructures de transmission et à des matériels assurant que les communications atteignent leurs destinataires (essentiellement les routeurs et les systèmes d'exploitation).

S'agissant des services, les solutions de transitions qui sont proposées par des acteurs tels que Free6net comme le « tunneling » en phase initiale de la cohabitation sont susceptibles de constituer un marché distinct dès lors qu'ils correspondent à une demande spécifique de pouvoir transmettre des données sous v6 dans des paquets sous v4.

Certains accès aux ressources sont également susceptibles de conduire à la définition de nouveaux marchés. Il s'agit essentiellement de l'accès aux capacités de transmission qui seront offertes par les opérateurs GRX dans le cadre du GPRS qui permettent l'accès aux réseaux mobiles via des plates-formes.

---

8 Communication de la Commission sur la définition du marché en cause aux fins du droit communautaire de la concurrence du 9 décembre 1997, point 13, document de travail de la Commission sur la proposition de nouveau cadre réglementaire pour les réseaux et les services de communications électroniques : Projet de Lignes Directrices sur l'analyse du marché et le calcul de la puissance sur le marché , Bruxelles, le 28 mars 2001 (« Projet de Lignes Directrices »).

9 Projet de Lignes Directrices, points 35-42.

10 Projet de Lignes Directrices, points 50-52. Dans le cadre de la présente étude, la dimension géographique des marchés nouveaux pouvant résulter de l'arrivée d'IPv6 ne sera néanmoins pas abordée.

11 Projet de Lignes Directrices, points 54-55.

En ce qui concerne les matériels en revanche, la définition de marchés nouveaux ne se dégage pas dans la mesure où les matériels en cause – routeurs et systèmes d'exploitation essentiellement – (i) ne semblent pas correspondre à une utilisation nouvelle, mais se limitent à assurer la compatibilité entre v4 et v6 et, (ii) selon chaque gamme, leur prix ne variera pas. Néanmoins, s'agissant des routeurs v6, il n'est pas exclu que le fait qu'ils induisent des performances moindres en cœur du réseau par rapport à v4 puisse conduire à considérer qu'ils ne sont pas substituables aux routeurs actuels.

Par ailleurs, il ne semble pas que l'accès aux adresses IP puisse constituer un marché distinct dès lors que leur allocation ne fait pas l'objet, dans ce cadre, d'une offre marchande[12].

1.1.2.2 Marchés aval

La caractérisation de nouveaux marchés de services aux utilisateurs finals dépend essentiellement des caractères de la demande qui sont aujourd'hui difficilement identifiables. Néanmoins, compte tenu de certaines fonctionnalités propres à IPv6 et au vu de la pratique décisionnelle de la Commission européenne, il semble que certains marchés distincts de services pourraient être identifiés selon deux critères principaux :

- **le terminal d'accès à Internet, PC, télévision ou terminal mobile** ; ainsi la Commission européenne a considéré que la fourniture de services numériques interactifs par la télévision et par des ordinateurs personnels (« PC ») constituaient des marchés distincts notamment compte tenu du prix plus élevé de l'accès à de tels services sur ordinateurs (modems) et de la différence de pénétration des téléviseurs et des ordinateurs[13]. Elle a également indiqué que la fourniture de services d'accès à Internet par un terminal mobile et par un ordinateur pouvait constituer des marchés distincts en raison des différences de taille des écrans et du format des contenus auxquels l'utilisateur peut avoir accès par ces supports[14] ;
- **les fonctionnalités offertes par le protocole IPv6 (connectivité permanente et communications de poste à poste)** ; la Commission n'a pas exclu que les services de téléphonie sur les réseaux UMTS puissent constituer un marché distinct des services mobiles fournis sur les réseaux GSM en raison notamment des fonctionnalités propres à l'UMTS et à la différence de prix prévisible des services[15]. **Ainsi, les services de jeux distribués ou de visioconférence offerts sous v6 mobile pourraient être considérés comme des marchés distincts.**

S'agissant des nouveaux produits permettant l'accès à Internet, c'est-à-dire les produits grand public intégrant d'origine l'accès à Internet tels que les voitures communicantes, l'électronique grand public (caméras web), les décodeurs de télévision, les consoles de jeux ou les appareils domestiques, ils seront susceptibles de constituer des marchés distincts dans la mesure où notamment (i) leur utilisation par les utilisateurs finals diffèrera de celle des produits n'intégrant pas une telle fonctionnalité et/ou (ii) leur prix, selon les gammes, sera différent.

[12] Voir supra 1.1.1.1.1, note 6.
[13] Décision de la Commission B Sky B / Kirch pat TV du 21 mars 2000, COM/JV.37, point 36.
[14] Décision de la Commission Telia / Oracle / Druit du 11 septembre 2000, COMP/M.1982, points 16 et 17.
[15] Décision de la Commission Belgacom / Teledanmark / T-mobile international / Ben nederland holding du 25 septembre 2000, COMP/M.2130, point 14.

1.2 La transition vers IPv6, frein au maintien / développement de la concurrence

Dès lors que l'accès à certaines ressources ou infrastructures est nécessaire pour la fourniture des services sous v6 aux utilisateurs finals, on ne peut exclure l'apparition de goulets d'étranglement du fait de la transition vers IPv6. Or, si ces ressources ou infrastructures sont contrôlées par des acteurs dominants ou également présents sur les marchés aval de la fourniture de services sous v6, la relation de dépendance dans laquelle se trouveraient leurs concurrents sur les marchés avals serait de nature à conduire à des pratiques anticoncurrentielles.

Il convient donc d'identifier l'existence de tels goulets avant d'apprécier l'existence ou la possibilité de création ou de renforcement de position dominante des acteurs qui contrôlent ces goulets.

1.2.1 Identification des goulets d'étranglement

L'analyse des mécanismes d'allocation et d'attribution d'adresses ainsi que les entretiens permettent d'anticiper trois goulets d'étranglement dans le cadre de transition d'IPv4 vers IPv6.

1.2.1.1 Mécanisme « restrictif » d'allocation d'adresses IP

Le maintien en vigueur du mécanisme actuel d'allocation des adresses IP risque d'affecter la capacité des petits ISP de concurrencer les gros ISP pour la fourniture d'adresses IP[16].

En effet, en application des règles en vigueur, les gros ISP sont favorisés dès lors que l'allocation d'adresses IP est subordonnée à la conclusion de trois accords de peering[17].

Ce retard que pourrait prendre les petits ISP, en raison de l'impossibilité d'obtenir des ressources en adresses suffisantes, est accentué par l'incertitude dans laquelle ils se trouvent quant au calendrier d'adoption des nouvelles règles plus ouvertes.

Or, l'adoption desdites règles au sein des RIR est soumise à un processus décisionnel dans lequel les droits de votes sont pondérés en fonction de la taille des entreprises et des ISP (KWNQwest, AT&T et Telefónica ayant plus de droits que Worldcom et France Telecom)[18].

1.2.1.2 L'accès des ISP à certains services de connectivité Internet

En fin de déploiement d'IPv6, la fourniture par les ISP de services sous v6 nécessitera l'accès à des services de connectivité Internet, généralement sous la forme d'accords de transit avec les opérateurs de backbone en v6. Les ISP ne disposant pas de telles ressources seront donc dépendant de la disponibilité d'une offre de transit en v6 émanant des opérateurs de backbone.

[16] La distinction entre gros et petits ISP est fondée sur le nombre d'allocations d'adresses obtenues, par les IR, qui pondère le nombre de leurs voix au sein du RIPE (RIPE 213).

[17] Il s'agit des règles en vigueur pendant la phase de démarrage, voir Annexe 1.9.

[18] Ainsi, s'agissant des noms de domaine, le Conseil de la concurrence n'a pas exclu qu'une délibération de l'AFNIC refusant l'attribution d'un nom de domaine puisse être qualifiée d'entente anticoncurrentielle : « Considérant en effet que si la délibération litigieuse – à laquelle ont pu participer des opérateurs évoluant sur les mêmes marchés que la société Concurrence – est susceptible de constituer une entente, le caractère illicite de cette entente doit, en vertu du texte susvisé résulter d'un objet, d'un effet ou d'une potentialité d'effet anticoncurrentiel qui lui serait attaché… ». (Décision n° 00-D-32 du Conseil de la concurrence en date du 9 juin 2000 relative à une saisine au fond et une demande de mesures conservatoires présentées par la société Concurrence).

Or, de tels opérateurs de transit n'auront pas nécessairement intérêt à offrir un tel service, ce d'autant qu'ils sont susceptibles d'être en situation de concurrence avec les ISP sur les marchés aval de la fourniture de services Internet aux utilisateurs finals. Dès lors, selon la position que les opérateurs de backbone occupent sur le marché, ils risquent de limiter ou retarder l'offre de services de transit en v6, et partant de certains services Internet en v6 aux utilisateurs finals.

1.2.1.3 La disponibilité de systèmes d'exploitation compatibles v6

L'existence de systèmes d'exploitation compatibles constitue un passage obligé pour que les applications nouvelles se développent. Dès lors, la limitation ou le retard dans la mise à disposition des systèmes d'exploitation compatibles v6, pour les ordinateurs ou les terminaux mobiles (y compris les PDA) serait de nature à retarder ou limiter le développement d'applications et notamment des outils de gestion des réseaux, et partant, la concurrence sur les marchés aval de la fourniture de tels produits ou services.

1.2.2 Risques de création ou de renforcement de position dominantes

Afin de pouvoir déterminer si la transition vers IPv6 est susceptible de conduire à la création ou au renforcement de positons dominantes, il convient d'identifier les marchés affectés par les goulets d'étranglement avant d'examiner la position qu'occupent les acteurs sur ces marchés.

1.2.2.1 Marchés affectés

(i) Marchés amont

S'agissant des **produits**, il s'agit essentiellement des routeurs et des systèmes d'exploitation fixes (UNIX et Windows) ou mobiles. Lors de la création de l'entreprise commune entre Ericsson et Nokia pour l'acquisition de Psion Software, rebaptisée Symbian, et dans laquelle Motorola est devenue par la suite actionnaire, la Commission européenne a considéré qu'il existait **un marché distinct des systèmes d'exploitation pour équipements informatiques et de communication sans fil**[19].

En ce qui concerne les **services**, deux types d'accès sont visés : (i) l'accès au cœur de réseau et (ii) l'accès au réseau local, ce dernier marché étant de dimension géographique nationale et pouvant se subdiviser en accès via le réseau public commuté ou via une liaison dédiée[20].

L'accès aux infrastructures de cœur de réseau peut également se subdiviser en deux sous marchés :

- **l'accès à la connectivité « universelle »** qui est un marché de dimension géographique mondiale où les offreurs sont les « top-level » ISP ; en 2000, la Commission européenne en a identifié 17 parmi lesquels les cinq principaux sont MCI-WorldCom (32-36%), Sprint (5-15%), AT&T (5-15%), Cable & Wireless (0-10%) et GTE (0-10%)[21] ;
- **l'accès à la connectivité par l'intermédiaire de « second-tier » ISP**, offreurs de services de transit.

[19] IP/98/762 du 13 août 1998 et IP/99/65 du 2 février 1999.
[20] Décision AOL/Time Warner du 11 octobre 2000, COMP.1845, points 33-34.
[21] Décision WorldCom/Sprint du 28 juin 2000, COMP/M.1741-MCI (les parts de marché relevées sont celles résultant des volumes de trafic).

(ii) Marchés aval

En ce qui concerne les **terminaux**, il s'agit, pour les **terminaux fixes**, **du marché de dimension au moins européenne des ordinateurs personnels pouvant éventuellement se subdiviser en deux sous marchés des PC à usage privé et des PC à usage professionnel**. A l'occasion de la fusion HP/Compac, la Commission européenne a récemment considéré que sur ce marché les parts de marché étaient les suivantes22 :

HP/Compac :	20/25%
Fujitsu-Siemens :	10/15%
Dell :	10/15%
IBM :	5/10%

Pour les **terminaux mobiles**, il semble que **chaque type de terminal constitue un marché distinct (PDA, micro-ordinateurs, téléphones mobiles) ou au moins pour certains d'entre eux**. Tel est le cas en particulier pour les PDA où, à l'occasion de la fusion HP/Compac, la Commission européenne a estimé que les PDA constituaient un marché distinct des PC pouvant se subdiviser en fonction du système d'exploitation qu'ils utilisent (en l'occurrence Microsoft Pocket par opposition au Palm OS).

Les parts de marché identifiées sur ce marché sont les suivantes[23] :

Compac (iPaq):	60/65%
HP (Jornada):	30/35%
Casio :	5/10%

En ce qui concerne les **services**, les marchés affectés par la transition vers IPv6 et qui ont été identifiés comme marchés distincts sont les suivants[24] :

(i) **le service d'accès à Internet de dimension géographique nationale**, se subdivisant en marché de **l'accès à Internet à haut débit** ; **En France, la part de marché de Wanadoo** est de 60%, et de 90% pour l'accès à Internet haut débit par l'ADSL[25] ; en 1999, l**es parts de marché en France des fournisseurs d'accès à Internet** étaient les suivantes : Wanadoo : 40,6%, AOL : 27,4% et Club Internet : 18,5%[26]

(ii) **les services de contenus payants à haut débit** ;

(iii) **le service de musique en ligne** ;

(iv) **le stockage de données**.

Comme indiqué ci-dessus, les applications développées par des acteurs tels qu'Oracle sont également susceptibles d'être affecté par la transition vers IPv6.

22 Décision HP/Compac du 31 janvier 2002, COMP/M.2609, 30.
23 Décision HP/Compac, précitée, point 38.
24 Décision AOL/Time Warner, précitée, points 17-41.
25 Décision du Conseil de la concurrence n°02-MC-03 du 27 février 2002 relative à la saisine et à la demande de mesures conservatoires présentées par la société T-Online France.
26 Avis n°2000-A-04 du Conseil de la concurrence du 29 février 2000 relatif à l'acquisition par la société Vivendi de la participation de 15% détenue par le groupe Richemont dans la société Canal +.

1.2.2.2 Appréciation de la puissance des acteurs sur ces marchés

À titre liminaire, il résulte du Projet de Lignes Directrices ainsi que de la pratique décisionnelle de la Commission européenne dans le secteur des communications électroniques que les critères pour apprécier l'existence d'une position dominante détenue, seule ou conjointement, par des entreprises sont de deux ordres. S'agissant de la possibilité pour plusieurs acteurs de détenir conjointement une position dominante sur un marché, il convient de noter que la Commission européenne a estimé que le marché de l'accès à Internet ne s'y prêtait pas dès lors que (i) le marché n'est pas stable et double tous les six mois, (ii) les produits Internet ne sont pas homogènes et (iii) le marché est caractérisé par l'évolution technologique[27].

Il s'agit en premier lieu de **la part de marché détenue par l'entreprise**, qui doit se calculer en fonction du volume des ventes pour les produits, et en fonction du volume de trafic et/ou des revenus pour les services amont et aval liés à l'accès à Internet[28]. Ainsi, selon la Commission européenne, à partir de 40% de part de marché une position dominante est à craindre alors que, sauf circonstances exceptionnelles, dès lors qu'une entreprise détient une part de marché supérieure à 50%, elle jouit d'une position dominante sur ce marché[29].

En second lieu, d'autres facteurs peuvent servir à apprécier la puissance de marché d'une entreprise :

- la taille globale de l'entreprise qui lui permet notamment de pouvoir supporter des coûts d'investissement importants ;
- le contrôle d'une infrastructure qu'il n'est pas facile de dupliquer ;
- l'intégration verticale ;
- la détention d'informations concernant les protocoles d'accès ou les interfaces nécessaires pour assurer l'interopérabilité du logiciel et du matériel[30] ;
- l'intégration horizontale ; en effet, une entreprise détenant une position dominante sur un marché peut être considérée comme détenant également une position dominante sur d'autres marchés distincts mais connexes dès lors que les liens entre les marchés sont tels qu'ils permettent d'utiliser sur un des deux marchés, par effet de levier, la puissance détenue sur l'autre marché, ce qui renforce la puissance de l'entreprise[31].

Au vu de ce qui précède, il existe un risque que la transition vers IPv6 constitue un facteur de création ou de renforcement de la position dominante de certains acteurs sur les marchés affectés par les goulets d'étranglement : il s'agit principalement des opérateurs de backbone et des fournisseurs de systèmes d'exploitation.

Risque de création de position dominante au profit des opérateurs de backbone v6

Dans l'immédiat, il ne semble pas qu'il existe un risque de création de nouvelle position dominante. En revanche, si la pratique des opérateurs de backbone diffère par rapport à celle qu'ils ont indiquée lors des entretiens (i.e. position attentiste), ce risque pourrait apparaître en fin de déploiement.

27 Décision BT/ESAT, COMP/M.1838.
28 Décision WorldCom/MCI,
29 Projet de Lignes Directrices, point 67.
30 Lignes Directrices concernant l'application des règles de concurrence de la Communauté au secteur des télécommunications du 6 septembre 1991, points 81-82.
31 Projet de Lignes Directrices, précité, point 74-76.

En effet, dans une telle hypothèse, ils seraient en mesure d'empêcher ou de limiter la concurrence sur les marchés aval de fourniture de services sous IPv6 soit en ne faisant pas d'offre de transit sous IPv6 soit en accordant l'accès à la connectivité Internet dans des conditions discriminatoires par rapport à l'accès qu'ils offrent pour la fourniture de leurs propres services aux utilisateurs finals[32].

À cet égard, la Commission européenne a relevé à plusieurs reprises **le risque de création de position dominante au profit des « top level » ISP** :

- en 1997, dans l'affaire BT/MCI, elle a indiqué que l'absence de capacités suffisantes d'accès aux infrastructures de cœur de réseau pouvait conduire à la création d'une position dominante au profit des opérateurs disposant de telles infrastructures ;
- en 2000, dans l'affaire WorldCom/Sprint, elle a relevé l'importance des barrières à l'entrée sur le marché des « top level » ISP dès lors que les nouveaux acteurs Cables & Wireless et AT&T avaient acquis ce statut au moyen d'acquisition d'activités internet déjà existantes, le premier celle de MCI suite à la fusion avec WorldCom, le second celle de IBM Global Network. En outre, la Commission Européenne a indiqué que la position de Worldcom sur le marché de l'accès à la connectivité universelle était proche de la domination ;
- or, à l'occasion de la fusion entre WorldCom et MCI, la Commission Européenne avait indiqué que compte tenu de l'effet de réseau, la position de MCI WorldCom pourrait difficilement être remise en cause lorsque celle-ci serait dominante. Elle avait ajouté à cette occasion que si tel était le cas (en l'occurrence du fait de la fusion), le réseau de MCI/WorldCom pourrait constituer –immédiatement ou à terme– une infrastructure essentielle à laquelle les autres ISP seraient obligés de demander l'accès afin de pouvoir proposer une offre d'accès à Internet crédible. C'est la raison pour laquelle la fusion des deux opérateurs a nécessité un engagement de céder l'activité Internet de MCI.

Il résulte de ce qui précède que si les opérateurs de backbone v6 sont des « top-level » ISP, il existe, en fin de déploiement de la transition, un risque que ces acteurs soient dans une position dominante pouvant conduire à deux types d'abus : refus d'accès aux infrastructures de transit et/ou accès à de telles infrastructures dans des conditions discriminatoires.

Risque de renforcement de position dominante existante

Le risque de renforcement de positions dominantes résulte principalement du fait que **certains acteurs, déjà dominants, sont soit intégrés verticalement ou horizontalement, soit disposent des ressources leur permettant de pénétrer facilement les marchés nouveaux**. Dès lors, compte tenu des liens étroits entre les différents marchés liés à Internet, ils risquent d'utiliser leur position initiale comme effet de levier pour renforcer cette position, et le cas échéant, l'étendre à des marchés connexes.

(i) Renforcement de la position de certains équipementiers

La Commission européenne a estimé que le fait pour des entreprises de détenir des droits de propriété intellectuelle et d'en refuser ou d'en limiter l'accès (non communication de l'information ou dans des conditions discriminatoires) pour assurer l'interconnexion des ressources informatiques par d'autres entreprises pouvait constituer un abus de position dominante[33].

Ce risque de renforcement de position en raison de la détention de droits dont l'accès est nécessaire pour assurer l'interconnexion des ressources informatiques est susceptible d'apparaître à deux niveaux.

[32] Voir notamment la décision WorldCom/Sprint.

[33] Lignes Directrices concernant l'application des règles de concurrence de la Communauté au secteur des télécommunications, précitée, point 113.

Au niveau des **systèmes d'exploitation**, dès lors que la disponibilité de systèmes d'exploitation compatibles v6 conditionne le développement de services aval, **les fournisseurs desdits systèmes, peuvent être tentés d'en limiter l'accès aux tiers** et ce afin de renforcer leur position sur ce marché ou de l'étendre sur des marchés connexes. Ainsi, lors de l'appréciation de l'entrée de Motorola dans le capital de Symbian, la Commission a relevé comme élément important le fait que les actionnaires de Symbian se soient engagés à concéder à des tiers des licences sur le systèmes d'exploitation développés par la société en respectant les principes d'ouverture et de non-discrimination.

S'agissant plus particulièrement de **Microsoft**, bien que la Commission européenne ne se soit pas encore prononcée de façon formelle sur la position qu'elle occupe sur le marché des systèmes d'exploitation, il semble peu contestable que celle-ci détienne, au moins sur le marché des systèmes d'exploitation pour les PC personnels, une position dominante.

Dès lors, à l'image des pratiques qui ont été constatées à l'encontre de Microsoft aux États-Unis et qui ont consisté notamment à lier la vente de son système d'exploitation au service de navigation Microsoft Explorer, Microsoft pourrait être tenté d'utiliser sa position actuelle comme levier pour l'étendre sur d'autres marchés connexes soit horizontaux tels que les systèmes d'exploitation pour équipements informatiques et de communication sans fil, soit aval d'accès à Internet ou de contenus et ce notamment **au moyen d'un couplage des services entre eux.**

Au niveau des **routeurs**, les acteurs disposant d'une position importante sur le marché des routeurs compatibles v6 pourraient également être tentés d'utiliser leur position sur ce marché comme levier pour l'étendre sur d'autres marchés connexes tels que les services d'administration des réseaux.

(ii) Avantage concurrentiel des ISP intégrés verticalement

S'agissant des ISP importants, généralement intégrés verticalement à un opérateur de réseau, **il leur est plus facile de supporter les coûts de formation et de R&D liés à la transition vers IPv6 que les ISP indépendants**. Dès lors, l'avantage concurrentiel qu'ils pourraient avoir du fait de la possibilité de pouvoir offrir, les premiers, des services nouveaux sous v6 risque de les amener à (i) renforcer leur position sur le marché de l'accès à Internet et (ii) d'étendre cette position aux marchés nouveaux qui seraient considérés comme distincts mais connexes, notamment au moyen de couplage de ces services.

Cet avantage concurrentiel du fait de leur intégration verticale **pourrait être amplifié du fait de la situation actuelle concernant l'allocation des adresses** (poids des ISP dans la définition des règles et leur calendrier d'adoption ; l'accès aux informations de tests d'interopérabilité menés par les opérateurs de réseau…) et pourrait accentuer le retard des autres ISP.

2 Problématiques réglementaires

Contexte

Le nouveau « paquet » réglementaire concernant les « communications électroniques » a été publié en mars 2002. Les directives correspondantes devront être transposées à la mi 2003. Le déploiement d'IPv6 interviendra donc en grande partie dans un cadre rénové, marqué notamment par l'harmonisation du régime applicable aux différents réseaux et services de communications électroniques.

À la suite des travaux de l'IPv6 Task Force, la Commission Européenne a publié le 21 mars 2002, une communication sur l'Internet nouvelle génération, proposant des priorités d'actions dans la migration vers le nouveau protocole IPv6.

Le Conseil européen de Barcelone des 15 et 16 mars 2002 « accorde une priorité à la mise en place et à l'utilisation généralisée dans l'Union, d'ici 2005, de réseaux à large bande, ainsi qu'au développement du protocole Internet IPv6 » (point 40 des conclusions de la présidence).

- Les problématiques réglementaires affectées par l'introduction du protocole IPv6 devront être, pour l'essentiel, traitées dans un cadre réglementaire rénové.
- L'intervention du régulateur pourra s'appuyer sur les recommandations de la Commission concernant IPv6.

2.1 Incidence sur le régime des licences

- Pas d'obligation d'utiliser IPv6.
- Un suivi du déploiement d'IPv6 pourra être établi.

2.1.1 L'utilisation de ce protocole par les opérateurs n'est pas susceptible de modifier la qualification juridique de réseaux et services, ni leur régime

La fourniture de réseaux de communications électroniques et la fourniture de services de communications électroniques relèvent, en application de l'article 3 de la directive « autorisation »[34], du régime de libre fourniture, sous réserve d'une simple notification. Cette harmonisation du régime applicable à l'ensemble des supports et des services couverts par la directive « cadre »[35], concerne ceux utilisant le protocole IP, quelle que soit sa version.

- On rappellera pour mémoire que l'utilisation du protocole IPv6 (ni même la fourniture d'une information à ce sujet) ne pourra être un préalable à l'obtention d'une licence.

[34] Directive du Parlement européen et du Conseil relative à l'autorisation de réseaux et de services de communications électroniques, ci -après désignée « directive autorisation ».

[35] Directive du Parlement européen et du Conseil relative à un cadre réglementaire commun pour les réseaux et services de communications électroniques, ci-après désignée « directive cadre ».

C'est également le cas des licences dont le nombre est limité. S'agissant plus spécifiquement des opérateurs mobiles de 3 G, le choix de la norme UMTS n'implique pas pour l'opérateur d'obligation d'utiliser le protocole IPv6 pour l'ensemble de son réseau. L'obligation d'utiliser à l'avenir ce protocole est subordonné à l'adoption de la version 5 de la norme UMTS et limitée aux applications fournies grâce au « IP Multimédia Subsystem ». Cette version ne semble pas devoir être mise en œuvre dans les équipements 3G avant 2004 / 2005. Elle ne peut être imposée par le biais des licences.

- L'utilisation du nouveau protocole pourrait rendre les services de voix sur IP de meilleure qualité et contribuer à leur généralisation. Mais ce point sera sans incidence sur la qualification du service téléphonique, lequel ne relèvera en outre pas d'un régime spécifique de licence.
- L'utilisation du nouveau protocole par les fournisseurs d'accès à Internet est également sans incidence sur le régime de libre fourniture des services d'accès, qui relèvent aujourd'hui de l'article L34-2 du code.
- Les fournisseurs de réseaux ou de services de communication électronique pourraient être tenus de **fournir une information sur l'utilisation de la version du protocole IP utilisée**, conformément à l'article 11 de la directive « autorisation », dans la mesure où cette information est raisonnablement nécessaire pour vérifier le respect des conditions des autorisations générales. S'agissant également de suivre les progrès du déploiement d'IPv6, et en cohérence avec la recommandation formulée par la commission dans sa communication du 21 février 2002[36], cette information peut être demandée aux fournisseurs de réseaux et de services en vue de la poursuite d'un objectif statistique, conformément au point 1.e) de l'article 11 précité.

2.1.2 L'utilisation du protocole a un impact sur les conditions de fourniture des services

Le nouveau protocole modifiera certaines conditions de la fourniture des services.

- Les conditions attachées aux autorisations générales -que l'annexe de la directive « autorisation » fixe de manière limitative- pourraient permettre de traiter certains impacts.

- Une possible différenciation des flux en fonction de la nature des données transmises ne devra pas porter atteinte aux principes de **neutralité de l'opérateur** au regard du contenu des messages transmis et de non-discrimination des utilisateurs. Les cahiers des charges aujourd'hui annexés aux licences d'opérateurs de réseaux et de fourniture de service téléphonique rappellent les obligations des opérateurs au regard de ces principes. Les conditions attachées aux autorisations permettront de s'assurer que les fournisseurs n'utilisent pas les nouvelles fonctionnalités pour établir des priorités en fonction du contenu du message transmis ou de l'identité de l'utilisateur, mais seulement pour différencier les flux selon des critères objectifs (type de trafic : voix ; données; images etc…).

  L'utilisation des adresses IP devra respecter les règles de **protection des données personnelles** et de la vie privée, qui pourront être reprises comme conditions attachées aux licences.

  Le **respect des normes et spécifications** nécessaires pourra être imposé par les conditions générales, dans la mesure nécessaire pour assurer l'interopérabilité des services et la liberté de choix des utilisateurs. Mais la mise en œuvre des spécifications établies par l'IETF pour le protocole IP ne peut être rendue, en tant que telle, obligatoire, sauf dans l'hypothèse où les organismes de normalisation européens (CEN, CENELEC, ETSI) les auraient reprises préalablement à leur compte, suite à un mandat de la Commission.

- En revanche, certains impacts ne pourront être traités par le biais des licences.
  Des améliorations de la **qualité de service** ne semblent pas devoir être actées dans l'immédiat. En tout état de cause, l'obligation d'assurer un niveau donné de qualité de service ne pourrait intervenir

[36] La commission recommande aux Etats membres d'assurer… »7.a l'évaluation, au niveau national ou régional, des développements actuels et du degré d'adoption de l'IPv6 ».
Le rapport du CSTI concernant les infrastructures et services à haut débit recommande également « la création d'un observatoire ayant pour mission d'encourager la migration vers IPv6 et de suivre la progression de son déploiement en France ».

comme condition attachée aux licences générales.

Les conditions attachées aux licences visent également à permettre d'assurer aux utilisateurs finals l'**accessibilité des numéros** du plan national de numérotation.

Toutefois, malgré le développement d'un protocole dit ENUM, qui établit une correspondance entre un numéro de téléphone et un nom de domaine ENUM, on ne peut considérer que le numéro lui-même donne accès à une adresse IPv6.

Ce protocole ENUM peut donner à des services fournis sous IPv6 une plus grande accessibilité grâce à l'utilisation pour les utilisateurs d'un numéro de téléphone comme clef d'accès à divers services fournis sous IP, mais il n'a pas pour effet de répercuter sur les adresses IP les règles applicables à l'utilisation ou à la gestion du plan de numérotation.

- La réglementation française permet également de prévoir, lorsque des garanties sont nécessaires pour assurer le bon fonctionnement de la concurrence, des conditions particulières dans les cahiers des charges de certains opérateurs de réseaux ou fournisseurs de services téléphoniques.
  Ces dispositions pourraient permettre de préciser les conditions de transparence et de non-discrimination nécessaires pour qu'un opérateur ayant eu accès à un grand nombre d'adresses IPv6 et ayant une fonction de NIR redistribue ces ressources dans des conditions objectives, transparentes et non discriminatoires.

2.2 Les ressources rares

Dans le cadre réglementaire des télécommunications, l'accès aux ressources de numérotation a toujours été considéré comme essentiel à la concurrence dans le secteur.

D'une part, les procédures d'attribution de cette ressource doivent être **objectives, transparentes et non-discriminatoires**, ce qui implique également la publication des plans de numérotation, et assurer **l'égalité de traitement** de tous les fournisseurs de services. D'autre part, la gestion et l'attribution de ces ressources relèvent des autorités réglementaires nationales lesquelles, en application du principe de **séparation des fonctions**, sont indépendantes des opérateurs et fournisseurs de services. Ces principes, réaffirmés par la nouvelle directive cadre (article 10), figurent en France sous les articles L.34-10 et L.36-7.6° du Code. Enfin, pour qu'une **bonne utilisation** de ces ressources puisse être assurée, elles ne peuvent pas être protégées par un droit de propriété industrielle ou intellectuelle : elles sont **incessibles** et ne peuvent être transférées qu'après accord de l'Autorité de Régulation des Télécommunications.

De ce point de vue, les politiques d'adressage IP qui seront décrites ci-après présentent, incontestablement, **plusieurs similitudes** : cohérence des allocations et attributions avec les objectifs de **bonne gestion des ressources** (agrégation, bonne utilisation, enregistrement), **publication des adresses attribuées par les registres, absence de droit de propriété sur les adresses IP attribuées, contrôle des transferts** entre différents registres des adresses attribuées[37], même si l'on peut relever des différences quant à la politique des différents RIR en la matière[38]. En outre, le **principe d'équité** sera reconnu comme nouvel objectif dans la future politique d'adressage IPv6.

Au-delà de ces similitudes, il reste une différence radicale entre les procédures liées à la numérotation et celles liées aux adresses IP : l'absence de mise en œuvre du **principe de séparation des fonctions de réglementation et d'exploitation**, qui permet, en pratique, de garantir réellement l'application des principes d'objectivité et de non-discrimination.

[37] Aucun RIR n'admet la vente ou le transfert des adresses mais tant l'ARIN que l'APNIC et le RIPE admettent le transfert des activités d'un RIR, et donc des adresses, sous réserve d'un nouvel agrément. Le RIPE peut exiger également les documents qui attestent d'une modification de la situation juridique du registre et de l'utilisation des ressources transférées.

[38] A titre d'exemple, les adresses sont allouées sans limitation de durée par l'ARIN et le RIPE alors que l'APNIC alloue les adresses sur une base d'un droit d'utilisation d'un an renouvelable. Pour les adresses IPv6, c'est ce dernier critère qui devrait être mis en œuvre.

2.2.1 Allocation des adresses IPv6 : un nouveau projet est en cours de discussion

- Le passage à IPv6 s'effectue dans le contexte plus global de la réforme des instances de l'Internet.
- Une certaine opacité entoure les règles d'attribution des adresses IPv6 en raison de l'absence de visibilité sur le calendrier d'adoption et du nombre d'intervenant dans le processus.
- Les futures règles d'allocation tentent de limiter les risques d'atteinte à l'égalité des conditions de concurrence.
- Des règles d'allocation d'adresses IPv6 existent depuis 1999 et ont fait l'objet de discussions au sein de la communauté. Dans un premier temps, le fait de privilégier de grands acteurs de l'IPv4 ont pu créer des obstacles artificiels pour les déploiements par d'autres acteurs d'IPv6.

Les discussions continues, relatives à l'adressage IPv6, qui ont lieu au sein des différents organismes (essentiellement les RIR), ne permettent pas de fixer à l'avance la date d'adoption des règles définitives.

Ces règles sont en constante évolution et l'expérience acquise par les différents opérateurs modifie leur contenu. C'est la raison pour laquelle un nouveau projet appelé « IPv6 Address Allocation and Assignment Global Policy » a été élaboré et diffusé le 22 décembre 2001[39] en vue de se substituer au « Provisional IPv6 and Allocation Policy Document » établi en 1999.

Une nouvelle version d'IPv6 « Adress Allocation and Assignment global policy » (du 25 avril 2002) a été mise en ligne le 23 mai 2002 pour les trois RIR.

Dans ces conditions, il est difficile de prévoir la date d'adoption des règles définitives[40]. Ce constat est partagé par les RIR qui, conscients du fait que les discussions sur les politiques d'IPv6 peuvent durer longtemps, ont décidé de résumer le résultat de ces discussions au sein des documents de politique intérimaires.[41]

2.2.1.1 Les instances chargées de la définition des règles de gestion[42] : les représentants privés de la communauté d'Internet

- Intervention de plusieurs organismes d'autorégulation
- Formalisation progressive du rôle respectif des divers organismes
- Intervention consultative des gouvernements en bout de chaîne

La gestion de l'Internet se fait par le biais d'une autorégulation privée. Par conséquent, l'élaboration, l'adoption et la gestion de la politique IPv6 font intervenir divers organismes privés principalement constitués par les membres de la communauté d'Internet destinataires des politiques élaborées.

La mise en place et la détermination des missions de tels organismes privés ne s'est pas fait selon un processus prédéterminé. La communauté d'Internet, en fonction de ses besoins, a constitué progressivement différents organismes qui ont élaboré et adopté la politique provisoire d'IPv6 telle que définie dans le « Provisional IPv6 Assignment and Allocation Policy Document ».

39 http://www.ripe.net/ripe/mail-archives/ipv6-wg/20020101-20020401/msg00007.html.
40 Au sens d'une nouvelle politique IPv6 qui remplacera la politique provisionnelle du 20 juillet 1999
41 Point 1.2 du IPv6 Address Allocation and Assignment Global Policy.
42 Pour la composition et les missions des différents intervenants, voir l'annexe au présent document.

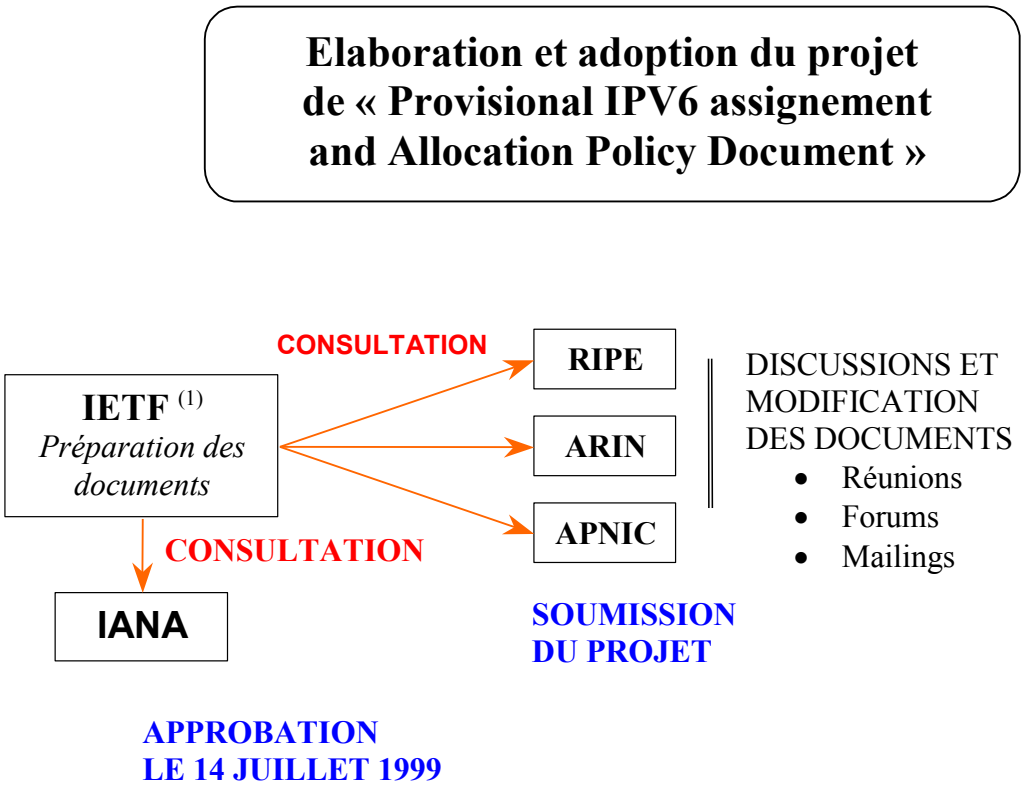
La création de l'ICANN[43] en 1998 et les missions qui lui ont été confiées témoignent de la volonté de la communauté d'Internet de mettre en place un organisme qui coordonne l'élaboration et l'adoption des politiques d'adressage. Le nouvel organisme commence à jouer un rôle central dans le processus d'élaboration et d'adoption de la nouvelle politique IPv6.

L'ICANN est aujourd'hui l'organisme responsable de la mise en place des politiques d'adressage[44]. Dès l'adoption du projet d'accord entre les RIR et l'ICANN, diffusé le 9 avril 2002, l'ICANN remplacera l'IANA et deviendra l'organisme de plus haut niveau pour l'allocation et la gestion des adresses IPv6.

La figure 7 résume les organismes intervenus dans le processus d'adoption des politiques IPv6 intérimaires.

La figure 8 résume les organismes responsables de l'élaboration et de l'adoption des futures politiques IPv6.

Figure 7 : Les organismes intervenus dans le processus d'adoption des politiques IPv6 intérimaires

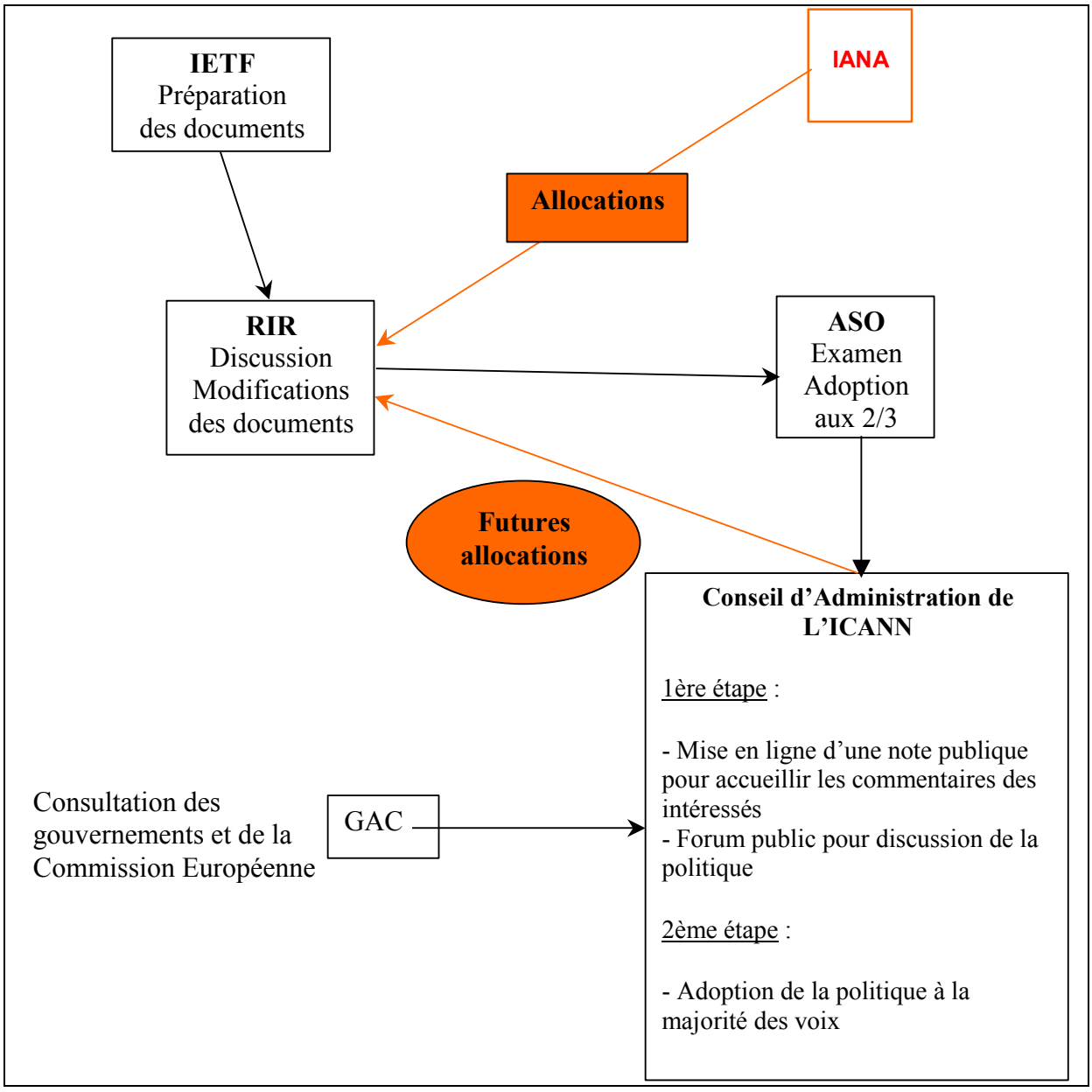


(1) Préparation des protocoles IPv6 : « IETF Draft Standard » du 10 août 1998

(2) Document RIPE NCC 196

43 The Internet Corporation for Assigned Names and Numbers
44 Selon les statuts de l'ICANN

Figure 8 : Les organismes responsables de l'élaboration et de l'adoption des futures politiques IPv6



2.2.1.2 Le processus d'adoption des politiques IPv6[45]

- Pas de calendrier prédéterminé pour l'adoption de la nouvelle politique dépendant des travaux de réflexion (RIR/ASO)
- Décision au sein de RIPE est fonction de la taille des entreprises
- Adoption finale par l'ICANN

Il n'existe pas un document unique qui formalise le processus d'élaboration et d'adoption des politiques IPv6 : nous rappellerons les principales étapes de l'adoption de la politique actuelle résumée dans le la figure 1.

Un nouveau projet de politique est en cours de discussion. « IPv6 Address Allocation and Assignment Global Policy » sera adopté selon un nouveau processus dont les étapes chronologiques et théoriques sont exposées dans l'Annexe 1.8 et que résume la figure 8.

2.2.1.3 Les régulateurs n'ont pas de compétence en la matière

La directive « cadre »[46] précise expressément n'attribuer aucune nouvelle compétence aux autorités de régulation en ce qui concerne le nommage et l'adressage Internet.

Il appartient aux États membres de faire valoir leur point de vue auprès de l'ICANN :

> *« Lorsque cela est approprié afin d'assurer l'interopérabilité globale des services, les États membres coordonnent leurs positions au sein des organisations et des instances internationales où sont prises des décisions concernant des problèmes en matière de numérotation, de nommage et d'adressage des réseaux et des services de communications électroniques »*[47]

La représentation au sein du GAC placé auprès de l'ICANN n'a pas pour effet de conférer aux États une quelconque compétence décisionnelle dans le processus d'adoption de la politique IPv6.

2.2.1.4 Les objectifs relatifs à la gestion des adresses et les principes de la politique IPv6 : vers une meilleure gestion des allocations IPv6

2.2.1.4.1 De nouvelles priorités pour les mêmes objectifs de gestion

Ces objectifs de la gestion des adresses IPv6 ont été déterminés par la communauté d'Internet et sont essentiellement les mêmes que ceux déterminés pour les adresses IPv4. Toutefois, la priorité accordée à certains objectifs n'est pas la même sous IPv6.

Selon le document RIPE 196 *du 20 juillet 1999, chaque Internet Registry doit s'assurer que les allocations et les attributions d'adresses IPv6 sont cohérentes avec les objectifs suivants :*

- Unicité : chaque unité d'adresse IPv6 doit être unique. Une telle unicité garantit l'identification de chaque internaute.
- Enregistrement : chaque allocation et attribution d'adresse Internet doit être enregistrée dans une base d'information publique accessible à tous les membres de la communauté d'Internet.

[45] Pour une présentation détaillée du processus d'adoption, voir l'annexe n°2
[46] Directive cadre, considérant 20.
[47] Directive cadre, article 10.5.

- Agrégation : les adresses doivent être distribuées d'une façon hiérarchique permettant l'agrégation de l'information d'acheminement et la limitation des tables d'acheminement d'Internet. En effet, la spécification d'IPv6 donnera lieu à la création d'un très grand nombre d'adresses et le nombre de visiteurs sous le contrôle d'acheminement interne d'un AS (Autonomous System) va augmenter d'une manière beaucoup plus importante que sous IPv4.
- Conservation des adresses IPv6 : pour une gestion optimale des adresses IPv6, les IR doivent éviter les allocations et les attributions qui ne répondent pas à un besoin spécifique.

Le protocole d'IPv6 conduit à donner une plus grande importance à l'objectif d'agrégation qu'à celui d'une bonne utilisation (conservation) d'adresses.

Le nouveau document « IPv6 Adress Allocation and Assignment Global Policy », diffusé sous forme de projet le 22 décembre 2001, prévoit deux autres objectifs :

- Équité : L'ensemble des pratiques et des politiques relatives à l'utilisation des adresses publiques doivent être appliquées équitablement à tous les membres existants et potentiels de la communauté d'Internet, sans considération de leur nationalité, de leur situation géographique,… ;
- Minimisation des formalités pour obtenir des adresses supplémentaires.

2.2.1.4.2 Les principes de la politique d'IPv6 : la responsabilisation des allocataires

En vue d'atteindre les objectifs décrits ci-dessus, la politique d'IPv6 est fondée sur les principes suivants[48] :

- Les adresses ne doivent pas être considérées comme une propriété. L'allocation d'adresse fait l'objet d'une « lease-licence »[49] sans redevance spécifique[50], d'une durée d'un an et renouvelable automatiquement lorsque les conditions initiales du droit d'usage sont toujours réunies et que les exigences d'enregistrement dans la base de données sont respectées à la date du renouvellement[51].
- Les IR ne sont pas responsables de l'acheminement. Ils doivent toutefois s'assurer que les allocations qu'ils effectuent ne vont pas donner lieu à des adresses excessivement fragmentées donc à une perte d'acheminement.
- Le projet propose une « allocation minimale » des adresses : dans un premier temps, un minimum d'adresses (/32) va être fourni aux divers IR qui peuvent en obtenir plus sur justification de leurs besoins.
- La prise en compte de l'infrastructure IPv4 : lorsqu'un fournisseur actuel d'IPv4 requiert une plage d'adresses en vue d'une éventuelle transition de ses services à IPv6, le nombre actuel de clients IPv4 peut être pris en compte pour l'allocation d'une plage d'adresses plus large.

48 Les trois derniers principes sont prévus par le projet du 22 décembre 2001.
49 Droit d'usage.
50 autre que le paiement de cotisations de membre aux RIR
51 Le nouveau projet de politique IPv6 du 25 avril 2002, mis en ligne le 23 mai 2002 prévoit que l'allocation d'adresse fait l'objet de licence renouvelable périodiquement.

2.2.2 Les règles en cours de révision

Les règles prévues par le document RIPE 196 n'ont pas un caractère définitif : en effet, dès l'origine, il avait été prévu que ces règles seraient révisées.[52.]

Par application de ces dispositions et suite aux réunions de l'APNIC en août 2001, de l'ARIN et du RIPE en octobre 2001, un nouveau document « IPv6 Address Allocation and Assignment Global Policy » a été élaboré pour définir la politique IPv6.

Cette nouvelle politique, diffusée sous forme de projet le 22 décembre 2001, est destinée à remplacer les procédures d'allocation et d'attribution prévues par « The Provisional IPv6 Policy Document ».

Le projet susvisé prévoit une politique globale qui doit être suivie par chaque RIR. Toutefois, l'adoption de ce projet n'aura pas pour conséquence d'empêcher les variations locales de la politique au sein de ces RIR.

Le RIPE 196 sera obsolète dès l'adoption du projet du 22 décembre 2001 actuellement en discussion au sein des trois RIR[53].

Lors de la réunion du RIPE 42 (mai 2002), le groupe de travail a fait état d'un consensus des 3 RIR sur le processus de révision.

2.2.2.1 Les règles relatives aux allocations : entités allocatrices, entités éligibles et taille des allocations.

2.2.2.1.1 Les entités allocatrices :

- ICANN substitué à IANA : organisme allocataire de plus haut niveau.
- RIR : un rôle central formalisé par le projet de « ICANN and RIR Relationship Agreement » du 9 avril 2002[54]

- Le projet du 22 décembre 2001 réintroduit un schéma plus « classique » pour les **délégations successives** des allocations et des attributions d'adresses.

  L'allocation d'adresse consiste en la distribution des adresses IP aux différents IR (Internet Registry / RIR[55]-NIR[56]-LIR[57]). Dans la structure hiérarchique, les plages d'adresses IP sont, en premier lieu, allouées par l'IANA aux RIR qui vont, à leur tour, les allouer aux NIR ou LIR de leurs régions respectives. Chaque NIR alloue les plages d'adresses aux LIR de son pays. Lorsqu'un RIR ou un NIR alloue les plages d'adresses à un LIR, il délègue aux LIR l'autorité pour attribuer ces adresses.

52 L'article 1er du document RIPE 196 : « *Ces politiques et indications seront modifiées en fonction de l'expérience opérationnelle et des innovations techniques qui constituent la meilleure politique d'Internet*. »

53 « IPv6 Adress Allocation and Assignement Global Policy », point1.1.

54 http://www.ripe.net/ripencc/about/regional/icanndraft-announce20020409.html.

55 Les « Regional Internet Registry » sont mis en place et autorisés par les communautés régionales respectives. Ils sont reconnus l'IANA pour desservir et représenter des grandes régions géographiques. La mission première des RIR consiste en la gestion et distribution des adresses publiques d'Internet dans leurs régions.

56 Les « National Internet Registry » allouent les adresses à leurs membres, les LIR. Les membres des NIR sont souvent des fournisseurs nationaux de services Internet (ISP). Toutefois, les NIR ne fonctionnent pas comme les ISP et sont neutres à l'égard des intérêts des ISP de leur champ d'intervention.

57 Les « Local Internet Registry » attribuent les adresses aux utilisateurs du réseau qu'ils fournissent. Les LIR sont généralement des ISP dont les clients sont essentiellement des usagers finaux et parfois des autres ISP.

L'attribution d'adresse consiste en la désignation des plages d'adresses IP que les IR distribuent entièrement ou partiellement aux usagers finaux qui en ont besoin pour leurs propres réseaux. Une adresse est également considérée comme attribuée lorsque l'IR l'utilise pour les besoins d'adressage de ses réseaux.

Les attributions d'adresses ne peuvent intervenir que pour les besoins précis justifiés par les IR. Les adresses attribuées ne peuvent pas faire l'objet d'une sous-allocation ou d'une sous-attribution.

L'adoption de ce nouveau schéma supprimera le sérieux risque concurrentiel qui résulte du schéma prévu par le document de 1999, avec des TLA et conférant une fonction d'allocation aux gros opérateurs ou ISP (Renater et France Télécom), avec la question de discrimination à l'égard des ISP concurrents.

- Les trois RIR et l'ICANN ont diffusé, le 9 avril 2002, un projet d'accord en vue de formaliser leurs relations quant à l'allocation des adresses IPv6. Il tend à clarifier les responsabilités de ces entités et les oblige à appliquer les politiques globales d'adressage.

Les RIR sont responsables pour l'allocation des adresses et le développement des politiques relatives à leur région. L'ICANN est responsable de la coordination globale et de la gestion des ressources en numérotation. L'accord reconnaît la validité de la révision au sein de l'ASO des politiques actuelles d'adressage.

Surtout, il reconnaît l'**ICANN comme l'organisme responsable** de l'allocation des adresses aux RIR, mettant ainsi fin à la persistance incohérente de l'IANA dans la description des processus d'allocation.

2.2.2.1.2 Les conditions requises pour accéder aux adresses IPv6[58]

- Les conditions prévues par la politique actuelle sont favorables aux grands acteurs et à ceux positionnés tôt sur des réseaux expérimentaux.
- Avec la nouvelle politique : rééquilibrage au profit des acteurs IPv4 ; risque de discrimination à l'égard des nouveaux acteurs « tout IPv6 ».

Ces conditions diffèrent selon qu'il s'agit de la période d'amorçage ou de la période de croisière. Les conditions et les règles d'attribution applicables pendant la période d'amorçage, qui semble presque terminée, sont déterminées par le Provisional IPv6 Assignment and Allocation Policy Document.

En ce qui concerne la période de croisière, le projet de « IPv6 Adress Allocation and Assignement Policy » prévoit des nouvelles conditions d'allocation et d'attribution.

[58] Pour une étude détaillée de ces conditions voir l'annexe n° 3

	Provisional IPv6 Assignment and Allocation Policy Document -1999 **Période d'amorçage**	**Provisional IPv6 Assignment and Allocation Policy Document – 1999** **Période de croisière**	**Projet de « IPv6 Adress Allocation and Assignment Policy » – 2001**	**Discussions relatives au projet de 2001**[59]
ÉLIGIBILITÉ	♦ Accords de peering avec au moins trois systèmes autonomes ET ♦ Projet de service IPv6 dans les 12 mois ET Être un fournisseur d'IPv4 avec 40 clients qui peuvent remplir le critère pour une attribution d'a /48 Ou Participation d'au moins 6 mois au projet 6bone dont 3 mois d'exploitation d'un pseudo TLA.	♦ Accords de peering avec au moins trois autres IR ayant bénéficié d'un Sub-TLA. ET ♦ Le demandeur doit avoir attribué des adresses IPv6 à au moins 40 usagers finaux de SLA Ou Intention claire de fournir un service IPv6 dans les 12 mois suivants la réception des adresses allouées.	Demandeur doit démontrer qu'il aura, dans les trois mois, une demande pour au moins un préfixe /36 (776 usagers finaux, dont utilisateurs IPv4).	Sur le seuil de /36 comme point de départ : Trop exigeant ? Sur la durée de trois mois : Trop courte ?
TAILLE DE L'ALLOCATION	Slow Start Mecanism - Allocation aux IR des ID de 13 bits - /35 pour les TLA registries [60]	IDEM	Allocation aux LIR d'un bloc d'adresses de / 32. Attribution aux utilisateurs finaux de /48, sauf exception.	/48 oblige à revenir trop souvent devant le LIR
ALLOCATION ADDITIONNELLE		<u>Critère</u> Utilisation de 80 % des adresses initialement allouées <u>Taille</u> Un préfix d'au moins d'un bit plus court	<u>Critère</u> Utilisation (calculée selon le Ratio – HD) de 80 % des adresses initialement allouées. <u>Taille</u> Un préfix d'au moins 1 bit plus court Lorsqu'un ISP ou un LIR a besoin de plus d'adresses, il doit justifier de son besoin pour les deux années suivantes.	Ce seuil de 80 % pourrait être porté à 85 %.

[59] Un nouveau projet de politique (du 25 avril 2002) mis en ligne le 23 mai 2002 prévoit les critères suivants :
- éligibilité : être un LIR et avoir un plan pour un déploiement de deux cents utilisateurs/48 dans les deux ans ;
- taille d'allocation : confirmation du / 32 ;
- allocation additionnelle : critère confirmé HD ratio = 0.8, taille = doublement du préfixe.

[60] ETNO demande allocations de /29 au sub TLA

Ces critères temporaires du RIPE 196 sont appliqués jusqu'à ce que IPv6 ait une diffusion suffisante soit lorsque plus de 100 entités auront reçu une allocation d'adresse IPv6, dont moins de 60 dans la même région. La procédure temporaire cesse de s'appliquer progressivement, région par région, quand 60 entités ont été désignées dans une région donnée.

On peut considérer que la phase d'amorçage a pratiquement pris fin en Europe. Sur un total de 137 préfixes de /35 alloués aux trois RIR[61], au 9 avril 2002 :

- APNIC : 55 ;
- ARIN : 26 ;
- RIPE : 56.

2.2.2.1.3 La taille des allocations

2.2.2.1.3.1 Les allocations minimales initiales :

Leur caractère suffisant reste discuté

- En vertu **du RIPE 196** (point 4.2.4), les RIR devront adopter un « slowstart mecanism » pour les allocations initiales de sub-TLA : allocation des NLA ID d'une valeur de 13 bits à être utilisé par les IR à moins que l'IR demandeur justifie d'une exception fondée sur des raisons topologiques.

  Les raisons évoquées, par le document RIPE 196, pour l'adoption du mécanisme susvisé sont les suivantes :
  - Ce mécanisme permet aux RIR d'être équitable envers tous les demandeurs de sub-TLA en leur allouant la même quantité limitée d'adresses et en basant les futures allocations sur le nombre d'adresses enregistrées ;
  - Ce mécanisme va avoir pour effet de créer des préfixes de longueur différente, qui, dans l'hypothèse où la table d'acheminement le requiert, va permettre à l'industrie ISP de prendre des décisions rationnelles sur les routes à filtrer ;
  - Ce mécanisme va permettre aux RIR de maintenir le contact avec les TLA Registries pendant leur développement et donc d'assurer une mise en place effective des politiques et des pratiques d'IPv6.

- Selon le nouveau projet, l'allocation est prévue par blocs d'adresses de /32. La contribution de l'ETNO qui réunit 45 opérateurs et LIR la juge insuffisante et souhaite des allocations par blocs de /29 aux sub-TLA (selon le rapport du groupe de travail de l'IPv6 Task Force).

[61] www.ripe.net/cgi-bin/IPv6allocs.

2.2.2.1.3.2 Les allocations additionnelles

- Solution de continuité avec la politique intérimaire
- Règles spécifiques pour les IXP

- Le document RIPE 196 prévoit des allocations additionnelles après 80% d'utilisation[62] des adresses initialement allouées.

- Selon le projet en discussion, ce seuil d'utilisation (calculé selon le Ratio-HD et sur la base du nombre des usagers finaux des unités de /48) pourrait ultérieurement être porté à 85%.

  Les LIR et ISP qui satisfont à ce critère peuvent recevoir un préfixe d'au moins un bit plus court. S'ils en ont besoin de plus, ils doivent justifier de leur besoin pour les deux années suivantes.

  - Le document RIPE 196 prévoit des règles spécifiques pour les Internet Exchange Points (IXP : réseau physique d'infrastructure exploité par une seule entité pour faciliter l'échange de trafic entre les ISP) pour répondre aux hypothèses où il n'est pas souhaitable pour un IXP d'obtenir son espace d'adressage de l'un des ISP qui s'y connecte. Il peut demander directement une adresse au LIR, à condition de (i) connecter au moins trois ISP (II) d'avoir une politique claire d'ouverture aux autres ISP.
    Le projet ne modifie pas ces règles mais indique toutefois que ce cas spécial est en cours de discussion au sein des RIR.

  - **Les détenteurs actuels des adresses IPv6 (en vertu du document RIPE 196) seront immédiatement éligibles** pour une allocation étendue à un bloc d'adresses de a /32. Le bloc d'adresses déjà alloué va être pris en compte comme celui réservé par le RIR pour les besoins d'une **allocation additionnelle**. Une telle disposition est destinée à conserver l'équité (entre les détenteurs actuels d'adresses IPv6 et les prochains détenteurs de telles adresses) quant au nombre d'adresses allouées. En effet, les détenteurs actuels ne pourront pas disposer d'un nombre plus important d'adresses. Les adresses qui leur ont été alloués dans la phase d'amorçage vont être prises en compte pour le calcul du nombre d'adresses lors d'une allocation additionnelle.

2.2.2.2 Les règles d'attribution des adresses aux usagers finaux

- **Le document RIPE 196** prévoit :
  - l'attribution d'un minimum de a /48 (80 bits d'adresses) aux usagers finaux qui ont besoin de créer des sous-réseaux.
    Les demandes d'attributions additionnelles doivent démontrer l'utilisation intégrale de SLA initiale et être accompagnées d'un plan d'architecture justifiant le besoin d'adresses additionnelles.
  - **Le projet du 22 décembre 2001** maintient la règle d'attribution de /48 (sauf pour les grands souscripteurs). Toutefois, les LIR/ISP peuvent attribuer des adresses de :
    - 64/ lorsqu'un seul sous-réseau est nécessaire à l'usager final ;
    - 128/ lorsqu'une seule unité se connecte.

Les RIR et les NIR ne sont pas concernés par la taille des adresses attribuées par les LIR et les ISP.

Une règle spécifique d'attribution est prévue pour les opérateurs de service IPv6 : de tels opérateurs peuvent avoir un /48 par PoP, quel que soit le nombre d'utilisateurs du PoP.

[62] Allocation et attribution des adresses par le TLA Registry à son infrastructure ou ses clients.

Le projet prévoit également :

- une obligation d'enregistrement, dans une base publique d'information, des informations relatives à l'attribution des adresses (au niveau des RIR). Un tel enregistrement permettra aux RIR et aux NIR de calculer le Ratio-HD pour examiner les demandes additionnelles d'allocation et de vérifier les modifications intervenues dans les attributions.
- une délégation (par les RIR/NIR aux LIR/ISP) de l'obligation de surveillance de la zone qui correspond à l'allocation et l'attribution d'adresses.

2.2.3 Les RIR peuvent-ils retarder la butée de la pénurie des adresses IPv4 ?

- La reprise des adresses non utilisées ne semble pas être un moyen déterminant pour retarder la pénurie des adresses IPv4 : les mécanismes juridiques de reprise des adresses existent en théorie mais ne semblent pas utilisés par le RIPE.
- Une politique restrictive d'allocation et d'attribution des adresses IPv4 pourrait retarder la pénurie des adresses IPv4. Une telle politique est prévue par le RFC 2050 et par le document RIPE 185[63]qui limite l'allocation et l'attribution des adresses aux besoins précis du demandeur d'adresse.

2.2.3.1 Les mécanismes juridiques de reprise d'adresses

La question se pose particulièrement **pour les adresses qui ne sont pas utilisées**.

En premier lieu, il convient de préciser que **les mécanismes de reprise des adresses allouées à un RIR ne sont pas connus**.

En second lieu et d'une manière plus générale pour tous les RIR**,** la RFC 2050[64] prévoit que les ISP ont consigne d'utiliser l'espace d'adressage de manière optimisée. Ils doivent donc **justifier chaque attribution d'adresse**. En cas de défaut de justification, les attributions futures pourraient être compromises, et **dans le cas extrême, les acquis pourraient être reconsidérés.**

Toutefois, le RFC 2050 ne précise pas les mécanismes de reprise des adresses IPv4.

S'agissant plus précisément du **RIPE NCC**, the « European Internet Registry Policies and Procedures » du 26 octobre 1998 prévoit deux cas de reprise :

1) La cessation volontaire d'activité :

Lorsqu'un LIR cesse ses activités de LIR, il doit fournir au RIPE NCC la liste des adresses qui lui ont été allouées mais qu'il n'a pas attribuées. De telles adresses sont retournées par le LIR au RIPE.

Par ailleurs, lorsqu'un LIR cesse également de fournir la connexion Internet, il doit procéder à la reprise des adresses qu'il avait attribué à ses clients. Bien que le « European Internet Registry Policies and Procedures » ne prévoie rien, il est logique de penser que de telles adresses reprises par le LIR sont par la suite retournées au RIPE NCC.

2) La fermeture du LIR par RIPE NCC :

Le RIPE NCC peut décider de la fermeture d'un LIR lorsque le LIR ne paye plus ses factures, lorsque le RIPE ne peut plus le contacter pendant une durée significative ou lorsque le LIR viole les politiques mises en place par l'IANA ou le RIPE (une telle violation de la politique peut consister en un défaut d'utilisation des adresses allouées aux LIR).

Dans cette hypothèse, le LIR devra transmettre au RIPE les documents justifiant de ses attributions d'adresses. En l'absence de tels documents, le RIPE décidera de la reprise des adresses attribuées.

63 http://www.ripe.net/docs/ripe-185.html#toc19.
64 Document du Novembre 1996 qui inventorie les meilleures politiques d'attribution des adresses aux ISP.

Ces deux cas de reprise **ne nous semblent pas être suffisants** pour que RIPE puisse mener une politique globale véritablement restrictive de nature à retarder la butée de la pénurie d'adresses IPv4. **Nous n'avons d'ailleurs pas pu relever de cas d'utilisation pratique de tels mécanismes.**

Par ailleurs, 50% des adresses utilisées aujourd'hui sont des adresses dites « libres » qui peuvent être imputées à une zone géographique dépendant d'un RIR mais qui ne sont pas directement administrées par les RIR [adresses attribuées par l'IANA aux grands ISP avant la prise en charge de telles adresses par les RIR]

Dans ces conditions, il semble difficile d'affirmer qu'une politique restrictive des RIR, quant à la reprise des adresses non utilisées, puisse avoir un effet véritablement déterminant sur la butée de la pénurie des adresses IPv4.

2.2.3.2 Une politique d'allocation restrictive des adresses par un RIR

Selon le RFC 2050, l'attribution des adresses IP aux ISP se fait selon une procédure progressive : l'allocation initiale doit répondre aux besoins immédiats des ISP. Les blocs alloués peuvent ensuite être augmentés en fonction des constations du RIR et doivent permettre aux ISP de disposer d'une autonomie de trois mois. Les attributions ne doivent pas se faire sur des éléments prospectifs, mais sur un constat factuel.

Les RIR peuvent plafonner les attributions et/ou soumettre le dépassement d'un plafond à un examen approfondi.

En application de ces « principes de bonne conduite » relatifs à l'allocation des adresses, **les RIR pourraient en théorie retarder la butée de la pénurie des adresses IPv4**.

En conclusion, on peut relever qu'à l'occasion de la définition des nouvelles politiques IPv6, un effort de clarification du rôle respectif des différents organismes d'autorégulation est effectué, qui témoigne d'un souci de plus grande transparence dans les processus d'adoption. Les nouvelles politiques d'adressage IPv6 tout en réaffirmant les principes de gestion des adresses IP conduisent à donner une plus grande importance à l'objectif d'agrégation qu'à celui de « conservation » des adresses et ont introduit un nouveau principe d'équité et d'impartialité des pratiques et politiques.

Les discussions du projet « IPv6 Adress Allocation and assignement Policy » diffusé en décembre 2001 ont conduit à assouplir des conditions d'accès aux adresses IPv6 et à prendre en compte les bases de clients IPv4 des demandeurs.

La publication des adresses attribuées par les RIR, l'absence de droit de propriété sur les adresses IP attribuées et le contrôle des différents transferts entre les registres des adresses attribuées tentent de répondre à l'objectif d'une meilleure gestion des adresses IPv6.

2.3 Incidence sur le régime de l'accès et de l'interopérabilité

Le nouveau protocole ne semble pas avoir d'incidence directe sur le régime de l'interconnexion entre les opérateurs de réseaux.

2.3.1 Accès des ISP aux réseaux de communications électroniques

- Offre de transport sous IPv6
- Accès à des éléments spécifiques

2.3.1.1 Offre de transport sous IPv6 par les opérateurs de backbones

Les ISP devront disposer d'une offre de transport des services sous IPv6.

Dans un premier temps, cette demande pourra être satisfaite par une offre alternative de transit de données sous IPv4, moyennant la mise en œuvre des techniques transitoires (encapsulation).

Dans un second temps, une offre de transit sous IPv6 pourrait être imposée s'il est établi à terme que la poursuite des solutions temporaires fait, in fine, obstacle à l'interopérabilité des services et au développement de la concurrence.

- La **disponibilité** de l'offre devra être assurée. La disponibilité grâce au protocole IPv6 d'un très grand nombre d'adresses peut conduire à ce que les ISP soient plus disséminés et il peut en résulter une plus grande capillarité dans les accès demandés par les ISP.
  L'architecture et le nombre de points d'accès nécessaires aux ISP pourront également être traités par le biais des conditions techniques dans le cadre de l'offre demandée aux opérateurs.
- Il conviendra également de s'assurer du caractère **non-discriminatoire** de l'offre entre les différents ISP, dont certains sont intégrés aux opérateurs de backbone.
  Cette obligation de non-discrimination dans l'offre pourra être imposée sur la base de l'article 10 de la directive « Accès » aux opérateurs disposant d'une puissance significative sur le marché et qui auront été désignés en tant que tels.
- La disponibilité d'une offre d'accès pour les ISP aux fins de transporter des services sous IPv6 pourra avoir une influence sur l'attractivité respective des différentes routes pour l'acheminement du trafic. Elle aura également une incidence sur la localisation des nœuds permettant l'échange de trafic des ISP. L'équipement des nœuds d'échange pour leur disponibilité aux fournisseurs de services en IPv6 passe d'abord par une mise à jour des logiciels puis la modification des interfaces d'échanges de trafic entre ISP. Comme pour les points d'accès, la multiplication des ISP peut également susciter l'émergence de nœuds d'échange de niveau régional plus dispersés.

2.3.1.2 Accès à des éléments spécifiques

Les ISP pourront également demander l'accès à des éléments de réseau spécifiques et à des ressources associées si elles sont nécessaires à la fourniture de leurs services sous IPv6. Ces conditions pourraient être imposées si elles permettent l'émergence d'un marché de détail concurrentiel sur les nouvelles applications développées à partir d'IPv6.

Ce type d'accès pourra être demandé sur la base de l'article 12 de la directive « Accès », qui permet de faire obligation *« … e) d'accorder un accès ouvert aux interfaces techniques, protocoles ou autres technologies clés qui revêtent une importance essentielle pour l'interopérabilité des services ou des services de réseaux virtuels » ou… « g) de fournir les services spécifiques nécessaires pour garantir aux utilisateurs l'interopérabilité des services de bout en bout, notamment en ce qui concerne les ressources destinées aux services de réseaux intelligents ou permettant l'itinérance sur les réseaux mobiles »*

Dans ce cadre, les demandes des ISP pourraient porter sur des interfaces ou systèmes assurant la continuité des services fournis sous IPv6 : **a priori, aucun élément de ce type n'a été identifié**[65].

En revanche, les adresses IPv6 elles-mêmes doivent être demandées aux organismes allocataires (RIR ou LIR : voir supra). L'espace d'adressage offert par IPv6 ne permet pas de faire valoir leur rareté intrinsèque : la restriction de concurrence qui résulterait du caractère restrictif des critères d'éligibilité aux adresses IPv6 faisant obstacle au développement de nouvelles applications ou services devrait être critiquée plutôt sous l'angle des accords restrictifs de concurrence entre entreprises ou associations d'entreprises (Traité de Rome, Article 81)[66].

2.3.2 Interopérabilité des services

Pour qu'un acteur ayant adopté le nouveau protocole IPv6 ne rencontre pas de difficulté à développer ses activités, il convient qu'il dispose : d'équipements compatibles, de solutions permettant d'assurer la continuité des services, des solutions permettant d'assurer la qualité des services fournis.

2.3.2.1 La compatibilité des équipements

- Existence de solutions de transition

Un certain nombre de mécanismes permettant d'assurer la coexistence de services IPv4/IPv6 résultent de solutions logicielles qui sont actuellement disponibles. Des mécanismes ont également été établis par l'IETF qui permettent à des acteurs IPv6 de débuter leur activité dans l'ancien environnement. En outre, les matériels eux-mêmes sont conçus comme étant largement compatibles et on note la disponibilité d'un côté de **routeurs**, de l'autre de **terminaux** mobiles permettant de fonctionner indifféremment sur les deux protocoles.

Il résulte de l'enquête que la plupart des équipements comportent des serveurs dits « double pile v4/v6 ». La Commission elle-même relève que l'IETF a conçu un large éventail de techniques de transition et d'intégration qui permettent aux fournisseurs de choisir les méthodes qui leur conviennent.

2.3.2.2 Les spécifications d'interopérabilité

- en cas de besoin, possibilité théorique d'intervention de l'ETSI
- a priori, pas de besoin avéré

L'interopérabilité des services peut également être assurée en s'appuyant sur des normes ou spécifications relatives à la fourniture de services, d'interfaces techniques ou de fonctionnalités des réseaux.

[65] Les ISP mettant à niveau, de leur côté, leurs points de présence grâce aux systèmes de transition (DSTM, NAT-PT).
[66] Voir Décision du Conseil de la concurrence n° 00-D-32, 9 juin 2000, citée en 1.1.2.1.1.

Le nouveau cadre réglementaire qui s'applique indifféremment à tous réseaux de communications électroniques permet en théorie à la Commission de mandater l'ETSI ou d'autres organismes européens de normalisation pour définir des spécifications favorisant l'interopérabilité de services de communication électronique. La directive cadre en précise la procédure d'adoption. La directive « Accès » permet de fixer des conditions techniques conformes aux normes et spécifications ainsi établies.

À ce jour, l'ETSI n'a pas été mandaté expressément. En revanche, sont favorisés et encouragés les tests pratiques d'interopérabilité au sein de l'ETSI. La communication de la Commission invite les entreprises à soutenir et participer pleinement aux différentes journées d'interopérabilité organisées notamment au sein de l'ETSI.

2.3.2.3 La qualité de service

- intervention éventuelle sur les accords d'itinérance

Une question spécifique a été soulevée : elle concerne les services mobiles multimédia fournis à partir des « multimédias subsystems » qui seront mis en place au sein des réseaux de troisième génération. Les applications développées à partir de ces systèmes fonctionnant sous IPv6[67] (service de vidéo-conférence par exemple) devraient avoir une qualité substantiellement supérieure aux applications identiques fournies à partir des réseaux de deuxième génération ou de troisième génération n'ayant pas introduit IPv6 sur cet élément de réseau. S'il est possible d'établir une relation directe entre la dégradation de qualité de service constatée et l'absence de mise en place dans un réseau mobile d'un multimédia subsystem utilisant le protocole IPv6, la mise en place de solutions permettant d'éviter cette dégradation pourrait être demandée, par exemple dans le cadre d'un accord d'itinérance.

2.4 Protection du consommateur : libre choix des services et contenus et protection des données personnelles

2.4.1 Incidence sur la liberté de choix des internautes

La liberté de choix de l'internaute doit être examinée à trois stades : choix de l'opérateur d'accès, choix de l'ISP, choix des sites et contenus.

- Choix par l'internaute, de son opérateur d'accès :
  Le choix, par l'internaute, de l'opérateur d'accès ne paraît pas impacté par la mise en œuvre du protocole IPv6.
  Les terminaux mobiles (double pile IPv4/IPv6) permettront d'accéder à d'éventuelles applications IPv6.
  IPv6 semble également neutre au regard des diverses technologies d'accès (UMTS, réseaux locaux sans fil, ADSL…).

- Choix, par l'internaute, de son ISP :
  Les clients professionnels devraient être en mesure de changer d'ISP sans la contrainte de renumérotation de leur réseau, grâce à l'auto-configuration permise par le nouveau protocole.

  Pour les clients résidentiels, l'auto configuration se traduit par la possibilité de préinstaller dans les

[67] Obligatoirement avec la version 5 de la norme UMTS.

terminaux des adresses d'un ISP donné. Cette possibilité technique limite en théorie le choix de l'ISP, mais en pratique la multiplication des terminaux d'accès spécifiques est susceptible de conduire à des services d'accès spécifiques. Dans ce cadre, il ne s'agit plus véritablement de choisir un ISP mais un fournisseur d'équipement donnant accès à un service spécifique (exemple du réfrigérateur et de son service après-vente).
Cette pratique ne semble pas être envisagée aujourd'hui par les ISP, sauf au Japon où Sony (à la fois équipementiers et ISP) y a procédé.

- Choix des sites et contenus :
  La liberté de choix des utilisateurs ne doit pas être restreinte par le choix technique fait par son ISP quant au protocole mis en œuvre et l'accessibilité à tous les fournisseurs de contenus doit être favorisée.
  À cet égard, c'est l'ISP qui détient les moyens de garantir cette accessibilité, en proposant aux fournisseurs de contenus des accès IPv6, c'est-à-dire en pratique en s'équipant en serveurs à double pile pouvant être utilisés indifféremment par tous les fournisseurs.
  Par ailleurs, la Commission considère, dans sa communication, qu'avec IPv6, les utilisateurs « ne seront pas limités par la gamme restreinte de services réseau à valeur ajoutée que proposent les opérateurs sur leurs propres portails ».
  On notera néanmoins que la capacité d'auto-configuration facilite la pré-installation des adresses dans les terminaux. Dès lors, selon les accords conclus entre le fournisseur du terminal (également ISP) avec les tiers, l'accès à des contenus autres que ceux de la plate-forme de services dudit fournisseur pourrait être limité.

2.4.2 Protection des données

Une des spécifications d'IPv6 est de permettre d'utiliser **l'adresse MAC** (« Medium Access Control »), qui est, selon certains auteurs, **un numéro unique au monde gravé dans l'électronique de la carte réseau de type Ethernet pouvant être utilisé comme identifiant unique. S'il s'agit d'une solution très pratique** en particulier dans les réseaux d'entreprises car elle permet **l'auto-configuration**, en revanche, **à l'égard des particuliers, elle soulève la question de la protection de la vie privée**.[68]

En effet, avec l'adresse MAC, chaque internaute transmettrait, selon certains auteurs, le plus souvent à son insu et sans qu'il puisse s'y opposer, un numéro de série unique au monde et stable dans le temps (le numéro de série MAC restant toujours une partie de l'adresse IP quel que soit le fournisseur d'accès).

À ce jour, deux techniques semblent néanmoins susceptibles de limiter les risques en termes d'atteinte à la vie privée des internautes :

- le potentiel de sécurité offert par Ipsec (e.g. cryptologie) ;
- la possibilité que les adresses pour l'émission de communications électroniques soient attribuées à l'internaute par son ISP, lors de chaque connexion, de manière automatique et aléatoire ou même choisi et communiqué par l'utilisateur[69].

[68] Jean Marc Dinant (Droit-technologie-org)
[69] Cette possibilité est expressément prévue dans le RFC 3041 « Privacy Extensions for Stateless Address Autoconfiguration in IPv6 ».

D'un point de vue juridique, la Commission européenne a rappelé dans sa communication du 21 février 2002 que l'adresse IP pouvait être une donnée personnelle au sens du cadre juridique communautaire[70]. Il en résulte que **la collecte et le traitement des adresses IP des utilisateurs personnes physiques sont soumis au respect dudit cadre réglementaire et, en France, aux dispositions de la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés**[71]. Il s'agit en particulier (i) de l'obligation d'information lors de la collecte, (ii) de l'obligation de traitement conforme à la finalité déclarée et (iii) du droit d'accès et d'opposition au profit des utilisateurs.

Dans le cadre des télécommunications et, prochainement des communications électroniques, il est précisé que **les données de trafic, telles que l'adresse IP, doivent, en principe, être effacées ou rendues anonymes dès l'achèvement de la transmission, sauf dans trois cas particuliers** (données nécessaires à la facturation, commercialisation de ses propres services par l'opérateur avec le consentement de l'abonné et pour les besoins de la sécurité publique, de la défense et de la sûreté de l'État)[72].

(i) Respect de la vie privée par les RIR

S'agissant de la **conservation des données par les organismes et en particulier les RIR**, il est intéressant de relever que la Commission européenne a indiqué dans sa communication d'avril 2000 relative à l'organisation et à la gestion d'Internet que [certes s'agissant des données d'enregistrement des noms de domaine] qu'elle déterminerait si les exigences définies dans le domaine de la protection de la vie privée par les directives 95/44/CE et 97/66/CE sont respectées par les registres.

Il semble dès lors que **le respect du cadre communautaire relatif à la protection de la vie privée devrait également s'imposer au RIPE s'agissant de ses bases de données**[73]. À cet égard, on relèvera que la Commission a indiqué dans sa communication du 21 février 2002 qu'il était essentiel que la question de la vie privée dans le développement futur de l'Internet soit examinée afin que la confiance des utilisateurs de l'Internet dans l'ensemble du système soit assurée. Elle a ajouté que le groupe de travail de l'article 29 de la directive 95/44/CE et le groupe de travail international sur la protection des données dans les télécommunications (« groupe de Berlin ») envisageaient d'examiner en particulier IPv6.

[70] Directive 95/46/CE du Parlement européen et du Conseil du 4 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données et directive 97/66/CE du Parlement européen et du Conseil du 15 décembre 1997 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des télécommunications ; voir également le proposition de directive relative au traitement des données personnelles et à la protection de la vie privée dans le domaine des communications électroniques.

[71] Un projet de modification de cette loi a été déposé à l'Assemblée Nationale et vise notamment à finaliser la transposition de la directive 95/44/CE précitée.

[72] Articles 1.3 et 6 de la directive 97/66/CE et articles 1.3 et 6 de la proposition de directive.

[73] Le RIPE a établi une procédure d'accès et de rectification aux données concernant les bénéficiaires d'adresses (RIPE 238: article 3. Data protection).

(ii) Respect de la vie privée par les ISP

En ce qui concerne la **conservation des données par les ISP**, on notera que l'article 29 de la loi n°2001-1062 du 15 novembre 2001 relative à la sécurité quotidienne (« LSQ ») précise les obligations applicables aux opérateurs de télécommunications, comprenant notamment les fournisseurs d'accès à Internet. **Le nouvel article L. 32-3-1 du Code des Postes et Télécommunications pose le principe de l'effacement immédiat ou de l'anonymat des données de communication, cette obligation s'imposant notamment aux ISP**. En effet, il met à la charge des opérateurs de télécommunications au sens de l'article L. 32.15 du Code des Postes et Télécommunications une obligation *« d'effacer ou de rendre anonyme toute donnée relative à une communication dès que celle-ci est achevée »*. Ce principe est toutefois assorti de trois dérogations :

(i) conservation de certaines données (concernant l'identification des personnes utilisatrices) pendant une durée maximale de un an, pour les besoins de la recherche, de la constatation et de la poursuite des infractions pénales ;

(ii) conservation des données pour les besoins de la facturation et du paiement des prestations de télécommunications et ce, jusqu'à la période au cours de laquelle la facture peut être légalement contestée c'est-à-dire un an ;

(iii) conservation des données pour la commercialisation par l'opérateur de ses propres services de télécommunications, si ces usagers y consentent (la durée ne peut dépasser la durée des relations contractuelles avec ledit utilisateur).

Le protocole IPv6 semble a priori relativement neutre sur le choix par l'internaute de son opérateur d'accès, de son ISP, des sites et contenus.

L'adresse IP peut être une donnée personnelle et l'examen spécifique d'IPv6 pourrait être envisagé dans le cadre des travaux sur la directive 95/44/CE.

Annexes

1 Limitations du protocole IPv4

1.1 Adressage

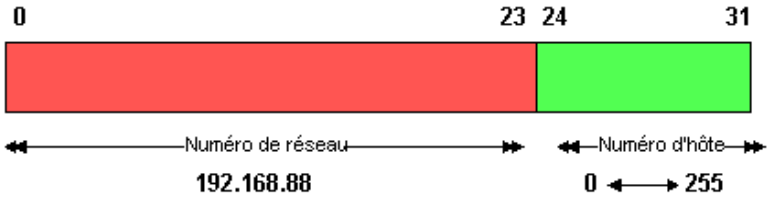
1.1.1 Adresses IPv4

Une adresse IPv4[74] est une suite de 32 éléments binaires séparés de manière hiérarchique en deux zones : l'une pour identifier le réseau sur lequel est rattachée la machine, l'autre pour identifier la machine elle-même sur ce réseau. Cette organisation hiérarchique permet de limiter la taille des tables de routage dans les routeurs.

Le nombre de bits alloué pour la partie réseau définissait à l'origine trois classes d'adresses : classe A, classe B, classe C. On ne parle plus aujourd'hui de classe. Les adresses sont désormais allouées sur la base d'un nombre de bits arbitraire (de 0 à 30) délimitant un agrégat de réseaux sur lequel se trouve la machine. Ce nombre définit le nombre de bits invariants de la plage d'adresses allouée. La taille de cet espace est alors désigné par le complément à 32 du nombre x de bits invariants, sous la forme « / 32-x ».

Ainsi une plage d'adresses « / 24 » comprend 24 bits invariants : il reste donc 8 bits pour affecter des adresses, ce qui permet d'affecter 28 (= 256) adresses IP. L'indication « / 24 » signifie que les 24 premiers bits identifient le réseau et les 8 bits restants désignent une machine sur ce réseau.

Par exemple, la plage d'adresses notée 192.168.88.0 / 24 peut être représentée sous la forme suivante :



1.2 Stock d'adresses limité

Avec un adressage sur 32 bits, on a longtemps cru que le stock d'adresses IPv4 disponibles serait largement suffisant pour satisfaire tous les besoins. Avec les développements récents de l'Internet, l'explosion prévue de ceux-ci du fait de pays émergents extrêmement peuplés (notamment en Asie), et l'arrivée d'une foule d'applications nouvelles, consommatrices d'adresses IP, le stock parait plus restreint. À cela, s'ajoute une répartition inégale des ressources entre les zones géographiques, la plus menacée par la pénurie étant la moins bien lotie.

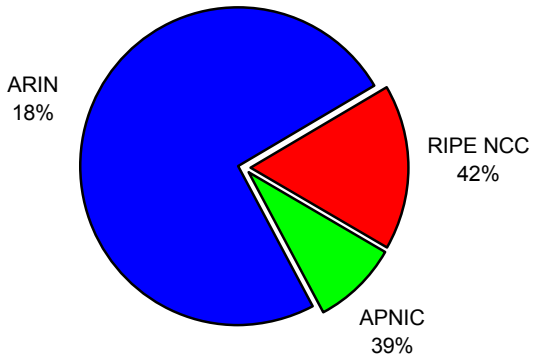
[74] Définie par la RFC 791 de septembre 1981.

L'adressage sur 32 bits permet de disposer d'un « stock » de 4.3 milliards d'adresses IP environ (2^{32} soit 4 294 967 296 adresses). À cette époque, et avec la vision qu'avaient alors les responsables, à savoir un réseau destiné aux militaires et scientifiques (donc assez éloignée de ce qu'allait devenir l'Internet que nous connaissons aujourd'hui), le stock paraissait plus que suffisant.

1.2.1 Inégalités géographiques

Aujourd'hui, on estime à moins d'un tiers du total les adresses non allouées à un registre régional (voir §9 infra), et que la majorité des adresses allouées le sont à la « zone américaine » (74% des adresses allouées) suivie de loin par les zones Européenne (17% des adresses allouées) et Asiatique (9% des adresses allouées), cette dernière étant pourtant la zone au plus fort potentiel en termes de besoin en adresses avec des pays comme la Chine ou l'Inde.

Figure 9 : Part des adresses attribuées à chaque organisme régional et ressources restant disponibles



Source : SpaWar

1.2.2 Nouveaux besoins

Le développement de l'électronique connectée, et notamment des objets nomades devrait induire, dans les années à venir, un besoin croissant en adresses IP. L'avènement du « always-on », et de nouvelles applications, comme la VoIP, fonctionnant en « end to end » et nécessitant des adresses IP fixes, ou encore les véhicules communicants ou le développement des réseaux de capteurs, comme le développement des communications machine à machine sous mode IP (s'appuyant sur des technologies comme Bluetooth ou 802.11) seront des facteurs accélérant la pénurie d'adresses IP.

Les classes d'adresses « B » ont été épuisées en 1994, et aujourd'hui, la plupart des experts prévoient un épuisement des adresses entre 2005 et 2010.

1.2.3 Précisions de l'étude ART sur la répartition géographique et le taux d'occupation des adresses IPv4

Au vu du nombre d'adresses non attribuées (près de 48% : ne pas confondre allocation et attribution), on pourrait penser que l'échéance de la pénurie est encore lointaine. Pourtant, on se rend compte, qu'en faisant l'hypothèse d'une croissance raisonnable sur l'ensemble du globe, on obtient effectivement une saturation des adresses IPv4 entre 2005 et 2010, comme l'annoncent les experts.

Les estimations du stock d'adresses non allouées varient entre 27 et 36% du total. Selon les RIR[75], 36% des adresses IPv4 ne sont pas encore allouées (en septembre 2001), soit environ 1,5 milliard d'adresses. En outre, les adresses allouées ne sont pas toutes utilisées (différence entre l'allocation et l'attribution). Une valeur moyenne à 31.5%, soit 1.35 milliard d'adresses est raisonnable.

Tableau 7 : Répartition des adresses par zones géographiques (10/2001)

Registre Internet Régional ou zone géographique (hors RIR)	Ressources allouées		Ressources disponibles (allouées et non attribuées)	
	% du total	Nombre (millions)	% du total	Nombre (millions)
ARIN – Amérique, Sud de l'Afrique	50.69 %	2 177	9.12 %	392
RIPE NCC – Europe, Afrique (Nord), Asie (Ouest), Moyen-Orient	11.65 %	500	4.89 %	210
APNIC – Asie-Pacifique	6.16 %	265	2.40 %	103
Non allouées	31.5 %	1 353	31.5 %	1 353
TOTAL	**100 %**	**4 295**	**47.91 %**	**2 058**

Source : IDATE

On parvient donc à un chiffre de 47.91% des adresses IPv4 non attribuées donc encore exploitables, soient environ 2 milliards d'adresses IPv4. La pénurie d'adresses IPv4 n'apparaît donc pas aussi critique qu'annoncée, et seule une indication du taux de croissance de l'utilisation de celles-ci pourrait mettre en évidence le risque de réelle pénurie à terme. Il faut cependant soustraire aux 4,3 milliards d'adresses théoriques l'ensemble de la classe D, réservée au multicast, ainsi qu'un ensemble d'adresses perdues pour les utilisateurs finaux (attribuées à des usages de fonctionnement, etc.) ; on peut estimer le stock total utilisable à environ 3.9 milliards d'adresses, soit, toutes choses égales par ailleurs, 1.9 milliard d'adresses encore disponibles dans ce cas de figure : ceci reste apparemment confortable. L'incertitude repose donc sur la croissance en besoin d'adresses, due à la « killer application » (développement des terminaux mobiles, du always-on, etc.) ou au « killer event » (explosion des besoins en Asie par exemple).

Le taux de croissance de l'Internet dans des pays tels que la Chine[76] ou l'Inde est extrêmement élevé. Ainsi, il est plus que raisonnable de tabler, en Asie, sur une croissance des besoins supérieure à 15% par an sur les prochaines années. 15% apparaît même comme une sous-estimation du taux. En effet, ces dernières années, le taux de croissance mondial d'Internet était supérieur à 30% par an, et on peut compter sur des rythmes de croissance soutenus, pour l'ensemble du monde, jusqu'en 2006 (Chine, Inde, etc. présenteront un taux élevé pendant encore plusieurs années après le reste du monde). On peut ainsi sans crainte estimer que le taux de croissance d'Internet dans le monde entier se trouvera entre 15 et 20% dans les cinq années à venir.

[75] près de 50% des adresses utilisées auraient été attribuées avant leur création, et ne seraient donc pas administrées directement par eux. Toutefois, par commodité, on peut les rattacher à leurs zones géographiques. Ces adresses sont considérées comme attribuées (et non seulement allouées). Les RIR sont définis par la RFC 1881

[76] Pour mémoire, 253% de croissance en Chine en 2000, et doublement du potentiel de croissance tous les six mois.

Tableau 8 : Calcul des dates de saturation en fonction de différents scenarii (10/2001)

Scénario		Nombre d'années pour atteindre la saturation	Date approximative de la saturation
Zone	**Taux de croissance**		
Asie seule	15% (sous-estimation)	18.75	Août 2020
	30%	9.99	Octobre 2011
Monde	5%	13.37	Mars 2015
	15%	4.67	Juin 2006
	20%	3.58	Mai 2005

Source : IDATE

Avec une hypothèse volontairement sous-estimée de 20% de croissance annuelle en Asie, on parviendrait, en admettant que le reste du monde cesse sa croissance (ou cesse celle-ci sur IPv4), à une saturation en 2020. L'hypothèse plus réaliste de 30% de croissance sur la zone amène à une saturation en 2011, c'est à dire dans la zone prévue par la plupart des experts (2005 à 2010 selon les experts).

En choisissant l'hypothèse extrêmement pessimiste de 5% de croissance annuelle des besoins en adresses IPv4 dans le monde entier, on parvient à saturation en 2015. Avec des hypothèses plus proches des prévisions généralement admises, de l'ordre de 15 à 20% de croissance annuelle, on arrive à une saturation aux alentours de 2005-2006.

Il faut noter que les Registres Internet Régionaux (RIRs) n'ont pris en charge l'attribution des adresses que longtemps après le début de l'utilisation de celles-ci. Ainsi, même si ces adresses peuvent être « imputées » à une zone géographique dépendant d'un RIR, celles-ci ne sont pas directement administrées par les RIR. Ces adresses « libres » compteraient pour 50% environ du total des adresses utilisées à ce jour. Au total, l'ARIN n'administrerait que 5% des adresses, le RIPE NCC 4% et l'APNIC 2%, soient au total, à peine 472 millions d'adresses.

1.3 Protocole non prévu pour l'usage commercial

Prévu à l'origine pour des usages non commerciaux, IPv4 n'a pas été conçu pour assurer les fonctions de QoS attendues aujourd'hui, ni non plus pour assurer les fonctions Multicast, ou plug and play, ou encore la sécurité, essentielles dans l'Internet commercial moderne. Des solutions ont été trouvées, alourdissant le protocole de couches supplémentaires, ou pour doper artificiellement la durée de vie du stock d'adresses, faisant exploser la complexité des tables de routage.

Le protocole IP était, rappelons-le destiné initialement aux réseaux de recherche et aux militaires.

1.3.1 Explosion des tables de routage

L'anarchie relative qui a pu régner un temps sur l'attribution des adresses, a mené à une perte de possibilité d'adressage hiérarchique. La désorganisation relative, ainsi que les solutions (type NAT, cf. infra) permettant de reculer l'échéance de la pénurie d'adresses ont eu pour effet d'alourdir les chemins de routage, et de surcharger les tables de routage.

1.3.2 Lacunes en termes de sécurité

Avec les développements des échanges commerciaux sur Internet, des échanges de données confidentielles, le besoin en sécurité s'est fortement accru. IPv4 n'est pas été conçu à l'origine pour un niveau de sécurité maximal, et les solutions proposées sont optionnelles et fonctionnent sous forme de couches supplémentaires par rapport au protocole initial.

1.3.3 Mobilité non prévue initialement

La mobilité d'un terminal dans des réseaux n'a pas été envisagée à l'origine pour IPv4, or, dans le contexte actuel, avec le développement du nomadisme, le sujet est brûlant, et les besoins croissants.

1.3.4 Gestion de la QoS non prévue

La QoS ou Qualité de service est un élément essentiel de l'Internet moderne. Opérateurs et utilisateurs attendent un fonctionnement optimal du réseau, et souhaitent mesurer cette QoS. IPv4 n'a pas été à l'origine prévu pour un usage « commercial » intense et ne prend pas en charge de façon native la gestion de la QoS.

1.3.4.1 Apports de l'étude ART

La Qualité de Service est généralement assimilée à la discrimination des services, autrement dit à la définition de classes différenciées de services. Mais cela signifie aussi garantir un service et pour cela réserver des ressources.

Pour implémenter ces classes ou garantir des ressources, il faut définir une ou plusieurs politiques sur les nœuds du réseau permettant d'implémenter la Qualité de Service demandée, en utilisant divers mécanismes (trafic shaping, admission control, gestion de la congestion etc...).

Enfin, pouvoir associer une classe de service et garantir des ressources à un certain trafic implique de pouvoir prédire le comportement du réseau. Pour cela, il est nécessaire de s'entendre sur la définition de critères de mesures ou métriques afin de pouvoir sélectionner le meilleur chemin, lorsque des chemins multiples existent (routage) et vérifier que les demandes en QoS sont satisfaites.

En définitive, la QoS englobe tous les mécanismes permettant de différencier les types de trafic, ceux-ci pouvant être classés et administrés différemment à travers le réseau.

La caractérisation de la qualité du service dans l'Internet est généralement exprimée par les critères suivants:

- **Délai** : temps écoulé entre l'envoi d'un paquet par un émetteur et sa réception par le destinataire. Le délai tient compte du délai de propagation le long du chemin et du délai de transmission induit par la mise en file d'attente des paquets dans les systèmes intermédiaires.
- **Gigue** : variation du délai de bout en bout
- **Bande passante ou débit maximum** : taux de transfert maximum pouvant être maintenu entre deux points terminaux
- **Disponibilité** : taux moyen d'erreurs d'une liaison

Plusieurs facteurs sont susceptibles d'avoir un impact sur ces critères :

- **l'infrastructure de l'Internet** : l'Internet est composé d'un ensemble de routeurs et de liaisons de transmission
    - Les liaisons possèdent des caractéristiques de délai (de propagation), débit maximum et disponibilité,
    - Les routeurs peuvent avoir un impact significatif sur le délai, la gigue et la disponibilité. En effet, les fonctions d'un routeur consistent à contrôler l'intégrité du paquet reçu sur l'interface d'entrée, déterminer l'interface de sortie en fonction de la destination souhaitée, puis stocker ce paquet dans la file d'attente associée à celle-ci.

Lorsque le fonctionnement se dégrade (trop de trafic compte tenu des capacités du routeur) les files d'attente se remplissent, introduisant un délai supplémentaire dans la transmission des paquets, puis le routeur est forcé de jeter des paquets. Ces différentes actions ont un impact sur le délai, la gigue et en augmentant la probabilité de paquets transmis dans le désordre, influent également sur la disponibilité

- **le comportement adaptatif du protocole TCP de bout en bout :**
  Pour tenir compte de l'évolution des réseaux, un mécanisme de contrôle du débit et de prévention de la congestion a été ajouté dans les implémentations actuelles du protocole TCP. L'idée de ce mécanisme est d'arriver à une situation dans laquelle l'émetteur injecte un nouveau paquet dans le réseau simultanément à la réception d'un paquet par le destinataire. Il est réalisé à l'aide de quatre algorithmes imbriqués, parmi lesquels, on distingue notamment le « slow start » ou le « congestion avoidance ».

- **l'instabilité des protocoles de routage :**
  L'instabilité dans les protocoles de routage influence la gigue ou variation du délai de bout en bout de manière significative, en forçant les routeurs à modifier le choix du chemin, lors de changement de topologies ou situation de congestion.
  Dans ce contexte, offrir un service de bonne qualité consiste à fournir un service avec un délai et une gigue minimum ainsi qu'une disponibilité et un débit maximum, assurant un service « best-effort » convenable pour tous les types de trafic.
  La Qualité de Service, quant à elle, peut-être interprétée comme une méthode permettant d'appliquer un traitement préférentiel à un certain type de trafic et d'augmenter ainsi le niveau de qualité des critères caractéristiques de cette catégorie de trafic.

Il faut noter qu'une grande partie des problèmes de performances est due à des implémentations insuffisantes de TCP, des mauvais paramétrages des buffers et des timers nécessaires.

1.3.5 Absence de configuration automatique

IPv4 n'a pas été prévu à l'origine pour un fonctionnement « plug and play », essentiel dans le développement des nouvelles applications et de l'électronique connectée, et fort utile pour simplifier l'administration des réseaux en général. On aboutit donc à la lourdeur de la gestion des réseaux IP, une captivité vis à vis des prestataires administrant le réseau, et un manque de souplesse prompt à décourager le grand public pour le développement des applications nomades, domotiques, etc.

1.3.6 Multicast

IPv4 n'est pas prévu de façon native pour gérer la possibilité de multicast (communication de données en direction d'un groupe de machines disséminées), bien qu'une classe d'adresse complète (classe D soient plus de 268 millions d'adresses) soit dédiée à la gestion de cette possibilité.

2 Solutions techniques développées afin de pallier les limitations d'IPv4

2.1 Pallier au manque d'adresses et aux difficultés de routage

Des solutions temporaires, permettant de retarder la pénurie d'adresses IPv4 ont été proposées : le NAT. Afin d'éviter la croissance exponentielle des tables de routage, la notion de classe d'adresse a disparu, et le CIDR est apparu ; toutefois, la croissance exponentielle a aujourd'hui repris après un répit.

2.1.1 CIDR

Le « Classless Inter Domain Routing », utilisé depuis 1993, a permis, en agrégeant des classes C IP contiguës de disposer de classes d'adresses de dimension raisonnable. Faisant de fait disparaître la notion de classe pour les adresses IPv4, cet artifice a permis de retarder la croissance des tables de routage, en permettant à celle-ci de ne plus être exponentielle mais linéaire pendant environ 5 ans. Aujourd'hui, la croissance exponentielle des tables de routage a repris.

2.1.2 NAT

Le « Network Address Translation » est un artifice très répandu, et encouragé par les RIR, qui permet de répondre à court terme à la pénurie d'adresses IPv4. Cette fonction de routeur d'extrémité de site permet d'isoler un domaine (inside) du réseau global (outside). L'Inside utilise alors un schéma d'adressage privé, et le NAT permet l'interfaçage avec le schéma d'adressage public.

2.2 Adaptation à l'usage commercial

Des couches supplémentaires de protocole ont été développées, afin de permettre la gestion de la sécurité, de la QoS, et le comblement des autres lacunes d'IPv4 pour un usage commercial. Pourtant, ces rajouts alourdissent IPv4 et ne présentent pas une efficacité optimale, notamment conjugués aux solutions développées pour pallier le manque d'adresses. Les solutions de mobile IP ne sont pas retenues pour les réseaux cellulaires et la gestion de la QoS devient extrêmement complexe, du fait d'outils lourds.

2.2.1 Sécurité

Les solutions de sécurisation sont multiples, et rencontrent des obstacles, notamment du fait du développement du Nat, qui nuit au fonctionnement en end-to-end. Toutes les solutions de sécurisation proposées pour IPv4 reposent sur des ajouts, ou couches de protocole supplémentaires. La sécurité est un élément optionnel.

2.2.2 Mobilité

Comme dit au paragraphe 3, IPv4 n'a pas été prévu pour gérer la mobilité. C'est donc une couche supplémentaire, Mobile IP qui est chargée de gérer cet élément essentiel des réseaux IP modernes.

2.2.2.1 Présentation de Mobile IP[77]

Mobile IP est un protocole, élaboré par l'IETF, qui permet à des terminaux mobiles de se déplacer dans différents réseaux tout en gardant valide son adresse IP et donc en évitant toute reconfiguration de la part de l'utilisateur final. Mobile IP a été d'abord conçu dans le contexte de la micro-informatique et des réseaux locaux (LAN). Mais dans la perspective du développement des réseaux mobiles et des réseaux locaux sans-fil (WLAN), l'utilisation de Mobile IP est envisagée également pour la gestion de la mobilité en temps réel pour des terminaux mobiles (téléphone et PDA).

Bien après la mise au point du protocole IPv4, le protocole Mobile IP a été développé pour gérer la mobilité au-dessus d'IPv4, qui n'a pas été conçu pour cela à l'origine. Mobile IP a pour objectif d'acheminer correctement des données qui proviennent ou qui sont à destination d'un terminal mobile, en conservant du point de vue des applications la validité de son adresse IP. Le mécanisme de Mobile IP introduit une nouvelle adresse IP, qui est celle du terminal dans le réseau visité. Les différents mécanismes définis dans Mobile IP sont alors chargés de faire la correspondance entre l'adresse IP d'origine du terminal et son adresse dans le réseau visité. Mobile IP fait complète abstraction du réseau visité : ainsi il peut aussi bien s'agir de mobilité dans des réseaux cellulaires comme de mobilité entre des réseaux hétérogènes, comme un réseau cellulaire et un réseau local sans-fil (WLAN).

Mobile IP existe en 2 versions : Mobile IPv4 (utilisant le protocole sous-jacent IPv4) et Mobile IPv6 (utilisant le protocole sous-jacent IPv6).

2.2.2.1.1 Mobile IPv4

Mobile IPv4 introduit 3 éléments fonctionnels :

- le « mobile node » est concrètement le terminal mobile (PC, PDA, …)
- le « home agent » est un serveur situé dans le réseau d'origine de l'utilisateur, qui permet à celui-ci de se déplacer vers d'autres réseaux.
- le « foreign agent » est un serveur situé dans le réseau visité par un utilisateur, qui permet à celui-ci de s'inscrire dans le réseau et de bénéficier d'un accès IP.

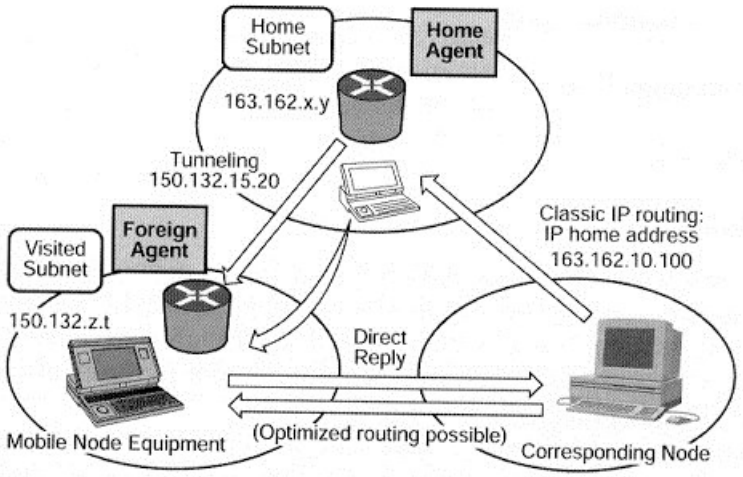
Le schéma ci-dessous explique le principe de Mobile IPv4. Dans le cas de figure présenté, le terminal mobile s'est déplacé de son réseau d'origine (adresse : 163.162.x.y) vers un autre réseau (adresse : 150.132.z.t). Dans son réseau d'origine le terminal est identifié sous l'adresse 163.162.10.100. Dans ce réseau visité, le terminal souhaite établir une connexion avec un ordinateur distant, appelé « corresponding node ». Cet ordinateur peut-être soit un serveur Internet soit un autre terminal mobile. Mobile IP permet d'associer une adresse temporaire dans le réseau visité (appelée « care-of-address ») à l'adresse d'origine (appelée « home address »). Dans le cas concret présenté, le terminal obtient la care-of-address 150.132.15.20, vers laquelle le home agent transfère les données reçues sur la home address. Le home agent utilise une procédure d'encapsulation des paquets IP (aussi appelée « tunnelling »).

L'identification d'un foreign agent sur un réseau visité se fait grâce au protocole « agent discovery ». Une fois le foreign agent découvert, le terminal mobile notifie son home agent de sa care-of-address.

Lorsque le terminal émet des paquets, ceux-ci sont envoyés directement à destination par le réseau visité. On constate en revanche que la réception de paquets est soumise à un routage triangulaire relativement inefficace. Une optimisation du routage a néanmoins été développée, comme une amélioration de Mobile IPv4.

[77] La mobilité dans IP est abordée dans plusieurs RFC, dont la RFC 2002, RFC 2005, la RFC 2026

Figure 10 : Mécanisme de Mobile IPv4



Source: « UMTS, mobile communication for the future », Flavio Muratore (2001)

Nous reviendrons plus longuement sur la gestion de la mobilité et en particulier dans les réseaux cellulaires dans le paragraphe consacré aux apports d'IPv6 en termes de gestion de la mobilité. Nous comparerons notamment dans ce paragraphe Mobile IPv4 et Mobile IPv6, mais aussi GTP, le protocole actuellement utilisé pour la gestion de la mobilité dans les réseaux cellulaires.

2.2.3 QoS

La QoS n'ayant pas été envisagée à l'origine dans IPv4, des solutions techniques sont développées en ajout au protocole. L'importance de cette notion de QoS dans l'Internet moderne implique qu'à chaque but recherché, pour l'amélioration de chaque critère, une solution technique différente soit apportée.

Apports de l'étude ART

Pour répondre aux attentes en termes de QoS de multiples solutions sont possibles, telles que :

- Pour implémenter des services différenciés :
  - l'implémentation de la QoS sur chaque routeur via des règles locales s'appliquant à l'en-tête du paquet
  - la modification de l'en-tête du paquet par chaque routeur d'accès pour indiquer le niveau du service
  - la définition d'un flux à travers une suite de routeurs et le marquage des paquets en tant que composant de ce flux.
- Pour la gestion des files d'attente :
  - Gestion FIFO, priority Queuing, Class Based Queuing (CBQ), Weighted Fair Queuing (WFQ)
- Le trafic shaping : en alternative ou en complément à ces techniques de gestion des files d'attente autres que FIFO, d'autres techniques sont utilisées, telles que « Trafic shaping » qui permet de contrôler le volume de trafic entrant dans le réseau ainsi que le débit avec lequel il est transmis. Les deux principales techniques de trafic shaping sont le Leary Bucket et le Token Bucket.
- Pour prévenir la congestion :
  - on utilise principalement deux techniques : le Random Early Detection (RED) et le Weighted Random Early Detection (WRED)

- Le modèle « Integrated Service » de l'IETF :
    - Le modèle repose sur deux principes fondamentaux :
        - le réseau doit être contrôlé et soumis aux mécanismes de contrôle d'admission
        - des mécanismes de réservation de ressources sont nécessaires pour fournir des services différenciés
- RSVP : un protocole de réservation de ressources

  RSVP est un mécanisme de signalisation, le signal étant constitué par l'information de contrôle QoS.

  RSVP établit et maintient un état logiciel entre les nœuds constituant le chemin réservé. Par opposition à la réservation d'un chemin statique (par exemple l'établissement d'un circuit virtuel), cet état logiciel est caractérisé par des messages périodiques de rafraîchissement envoyés le long du chemin pour maintenir l'état.

  RSVP fournit aussi une QoS dynamique tenant compte des modifications de ressources pouvant survenir du fait du destinataire ou de l'émetteur ou encore par l'introduction de nouveaux membres dans un groupe multicast

Nous allons ci-dessous exposer les solutions apportées pour la gestion de la QoS sur les réseaux IPv4 (les paragraphes suivants se basent essentiellement sur les travaux de Claudine Chassagne – CNRS).

2.2.3.1 Routage et Qualité de Service

Le routage est un aspect important dans l'implémentation de la Qualité de Service, en particulier pour les aspects suivants:

- **Choix du meilleur chemin**

Les protocoles actuels tels que OSPF, RIF sont basés sur le choix du chemin le plus court calculé suivant une métrique unique arbitraire (poids administratif ou nombre de sauts). Ils ne permettent pas d'utiliser d'autres chemins qui pourraient convenir pour transporter du trafic moins prioritaire.

- **Stabilité du réseau**

Intégrer des coûts variables basés sur des métriques caractéristiques de la QoS (délai, gigue, disponibilité etc..) permettant un routage optimal entraîne, en contrepartie, l'instabilité et le manque de convergence des protocoles de routage, obligés de s'adapter aux changements. Actuellement, aucun protocole de routage n'offre un bon compromis entre stabilité et adaptation dynamique aux flux de trafic.

- **Existence de politiques différentes**

Le problème est encore plus complexe, lorsqu'il s'agit de routage « interdomain », mettant en jeu différentes administrations et différentes politiques de routage. Il n'est, en général, pas possible d'influencer le choix du chemin pour le trafic entrant dans son propre domaine.

Plusieurs directions orientent les recherches actuellement dans ce domaine:

- QoSR (Quality of Service Routing) étudié par le groupe de travail QOSR de l'IETF avec pour objectif d'intégrer les métriques de la QoS et les critères de choix d'un chemin dans les protocoles de routage existants,
- MPLS (Multi Protocol Label Switching) du groupe de travail MPLS de l'IETF pour développer un modèle de transmission associant le niveau 2 et le niveau 3,
- Extensions RSVP pour intégrer le routage au protocole RSVP.

QoS Routing (QoSR)

Le routage avec QoS peut-être défini comme un mécanisme par lequel les chemins associés aux flux sont déterminés à la fois par la connaissance des ressources disponibles dans le réseau et les demandes en QoS de ces flux.

Au-delà de l'apport de RSVP et du modèle IS dans ce domaine, il semble qu'un nouveau modèle de routage intégrant la QoS soit nécessaire pour tenir compte des aspects de re-calcul d'un chemin à la suite de modifications topologiques et des aspects d'asymétrie.

Pour cela, un RFC (RFC 2386) définissant les conditions auxquelles doit satisfaire ce modèle a été rédigé par le groupe de travail QoSR, avec pour objectifs :

- encourager l'évolution des architectures de routage intra domaines basées sur la QoS,
- favoriser les interactions simples, cohérentes et stables entre les domaines administratifs (AS) implémentant les solutions de routage ainsi définies.

Intradomain QoSR

Étant donné un ensemble clairement défini de paramètres QoS, un mécanisme de routage robuste et raisonnable doit calculer le chemin approprié sans dégrader la performance globale du réseau. Aussi, des concessions sur le calcul du chemin ont été faites, quitte à ne pas obtenir le chemin optimal. De plus, les mécanismes de contrôle d'admission ou utilisation des bits IP Precedence dans le rejet des paquets peuvent aider à réduire le trafic pour lequel le chemin doit être calculé.

Un protocole de routage avec QoS doit:

- acheminer un flux le long d'un chemin satisfaisant les demandes en QoS ou bien fournir un mécanisme pour indiquer que le flux n'a pas été admis,
- indiquer les perturbations dues aux changements de topologies,
- satisfaire le service best-effort sans réservation de ressources,
- supporter le trafic multicast,
- tenter de diminuer l'overhead induit par la consommation des ressources et le calcul,
- fournir des mécanismes de contrôle d'admission.
- Un protocole de routage « à état de liens » dont la caractéristique est de détecter rapidement les modifications de topologies et les transmettre à ses voisins, peut convenir. Mais des modifications sont nécessaires pour intégrer les exigences QoS et minimiser les informations échangées dans les annonces de liens. Deux propositions ont été faites pour utiliser OSPF en ce sens.

Interdomain QoSR

L'aspect principal dans le routage entre domaines différents (AS) est la stabilité. C'est pourquoi, un protocole de routage à état de liens, qui communique les modifications de topologies à ses voisins, semble peu adapté, là où il est préférable de minimiser les échanges d'informations entre AS voisins.

Actuellement le protocole BGP (Border Gateway Protocol) largement implémenté dans l'Internet, fournit le routage interdomain dans l'Internet. Dans BGP, le chemin est basé sur la destination et est sélectionné suivant le plus long préfixe correspondant. Plusieurs mécanismes basés sur les attributs de BGP peuvent influencer le choix de celui-ci, sans toutefois offrir un bon niveau de fonctionnalité. Cependant, ils conservent une certaine importance, tant que des méthodes de choix du chemin basé sur les métriques QoS ne sont pas disponibles.

Un autre problème affectant la Qos est le routage asymétrique du fait des politiques différentes de routage des diverses organisations. Le chemin de la source vers la destination peut-être différent de celui revenant de la destination vers la source. Les métriques sont alors différentes (délai, gigue etc...), des filtres de trafic peuvent intervenir. Ceci affecte surtout les nouvelles applications temps réel audio et vidéo, mais aussi le protocole RSVP qui nécessite la symétrie des chemins pour fonctionner.

Multi-Protocol Label Switching (MPLS)

Suite à la prolifération des techniques développées pour accélérer la transmission des paquets (Label switching, Tag switching), le groupe de travail MPLS de l'IETF, s'est fixé pour objectifs de :

- rassembler dans un cadre standard unique ces différents concepts,

- développer une technologie minimisant la surcharge du routage et permettant l'introduction de nouveaux services sans modification du modèle sous-jacent de transmission.

Cette architecture est basée sur le concept de « label swapping » et consiste à insérer une étiquette de longueur fixe entre la couche de niveau 2 et celle de niveau 3, utilisée dans les décisions de routage et de transmission, à la place du choix du plus long préfixe (variable) correspondant utilisé dans les protocoles de routage. Déterminer le meilleur chemin grâce à un ensemble de valeurs de longueur fixe nécessite moins de ressources et de temps.

Les étiquettes sont distribuées en utilisant un protocole dynamique de distribution (LPD). L'association entre une étiquette et un préfixe (ou un ensemble de préfixes) est faite par un nœud d'extrémité MPLS (un routeur capable de cette fonctionnalité).

Parmi les possibilités d'implémenter la QoS dans MPLS, la contribution Tag Switching de Cisco propose d'utiliser les 3 bits IP Precedence de l'en-tête du paquet IP. Lors de l'entrée d'un paquet IP sur un routeur MPLS d'extrémité, celui-ci traduit les bits IP Precedence dans le champ CoS de l'en-tête MPLS.

Extensions RSVP pour le routage

RSVP utilise la table de routage locale dans les routeurs pour déterminer les routes vers les destinations appropriées. La QoS étant nécessaire dans le routage, il est important de fournir une sorte d'interface entre ces deux mécanismes distincts (réservation et routage).

Une proposition du groupe de travail RSVP de l'IETF définit une interface entre RSVP et routage appelée RSRR: Routing Support for Routing Reservation. La communication entre ces deux protocoles est réalisée via l'échange de questions et réponses asynchrones. Cette interaction permet à RSVP de s'adapter aux modifications de routage.

2.2.3.2 QoS et ATM[78]

Outre les fonctionnalités de haut débit, ATM comporte un ensemble complexe de mécanismes de gestion du trafic, établissement de circuits virtuels (VCs) et paramètres variés de la QoS. Mais ces mécanismes sous-jacents ne sont pas réellement exploités par de nombreuses organisations qui n'utilisent que les fonctions de transport dans l'Internet aujourd'hui.

Sans entrer dans les détails des nombreuses fonctionnalités d'ATM relatives à la QoS (fonctions de gestion de trafic, paramètres de trafic, classes de services QoS), l'impression générale est que la QoS ATM est complexe.

D'autre part, dans un réseau hétérogène tel que Internet, il ressort que :

- si ATM n'est pas déployé de bout en bout, les efforts pour délivrer la QoS en utilisant les fonctionnalités de ce protocole peuvent être inefficaces : le stockage en file d'attente introduit par les routeurs et hôtes non ATM a une influence sur le calcul du délai et de la gigue,
- les applications natives ATM n'existent pas dans la plupart des cas, aujourd'hui, hormis de rares endroits tels que des universités ou organismes de recherche, ayant développé des applications temps réel capables d'exploiter les paramètres QoS,
- la philosophie de base de l'Internet est d'offrir des services de transmission de bout en bout, cohérents et indépendants de toute technologie de transport sous-jacente. TCP/IP et ATM ont des comportements différents face à la congestion. Pendant qu'ATM jette des cellules et signale la perte du paquet IP au système terminal (dans un intervalle de temps bien inférieur à un unique RTT), TCP réduit sa fenêtre d'émission et adapte son débit, alors que la congestion ATM a été déjà traitée.

[78] ATM : Asynchronous Transfer Mode ; Le protocole ATM est né de l'idée que les réseaux destinés à la transmission de la voix (réseau téléphonique), de la video (réseau cablé), et des données (jusqu'alors dominé par le système BISDN pour Broadband Integrated Services over Digital Network) devaient fusionner et n'utiliser plus qu'un réseau de câbles commun, ainsi qu'un protocole commun. Les caractéristiques du protocole reflètent les objectifs alors visés par le forum ATM : le protocole ATM s'appuie sur la notion de circuit virtuel, ce qui constitue un compromis entre des protocoles basés sur des circuits physiques comme ISDN, et ceux basés sur des paquets envoyés sans qu'une connexion soit préalablement établie (Switched Virtual Connexion) comme ethernet.

L'objectif de la QoS dans l'Internet consiste principalement à prévenir ou éviter complètement l'impact de la congestion, en jetant des paquets. Dans le cas d'IP sur ATM, il n'existe pas de relations entre les directives de ces deux niveaux. Cependant, augmenter la complexité des mécanismes de rejet des cellules ATM pour préserver les directives IP, ralentirait le traitement et serait improductif. Si le réseau ATM est correctement dimensionné pour éviter les problèmes de congestion à large échelle, il n'est pas nécessaire de mettre en œuvre les mécanismes IP de gestion de la congestion.

En revanche, l'utilisation de la technologie ATM offre la réservation de bandes passantes à des trafics différenciés, entre deux routeurs, implémentant ainsi des services différenciés.

2.2.3.3 « Utilisation » de la QoS

Suivant l'importance et la diversité du réseau administré ainsi que le niveau de services requis, les politiques de QoS peuvent varier de l'implémentation de simples mécanismes au déploiement de solutions commerciales par des constructeurs.

Cependant certaines règles simples mises en œuvre conjointement sur la station et dans le réseau peuvent apporter une amélioration sensible de la Qualité de Service. Ces règles visent toujours à améliorer les quatre critères de performance cités précédemment : délai, gigue, débit maximum et disponibilité.

Stations

L'utilisation des implémentations du protocole TCP comportant les options de fenêtrage adaptatif, conjointement avec la définition de gros buffers, peut apporter des améliorations significatives de la performance de bout en bout.

En effet, le débit est basé sur le volume de données chargé de bout en bout divisé par le délai de propagation. Ce dernier est la somme des délais de propagation le long du chemin et des temps de mise en file d'attente dans les nœuds intermédiaires. Si les mécanismes QoS vus précédemment permettent de réduire le délai relatif aux files d'attente, il est important également de bien dimensionner les buffers.

Une grande partie des problèmes de performances est due à des implémentations insuffisantes de TCP, des mauvais paramétrages des buffers et des timers nécessaires. Il n'est pas certain que des structures QoS imposées à l'entrée du réseau puissent compenser ces déficiences.

Une bonne implémentation peut être encore améliorée par les considérations suivantes :

- Implémenter le mécanisme de « TCP Selective Acknowledgment » décrit dans le RFC 2018. Ce mécanisme permet de limiter les dégâts induits par la perte de paquets multiples envoyés à partir d'une seule fenêtre. Le destinataire envoie à l'émetteur des paquets SACK (Selective Acknowledgment) l'informant des paquets, effectivement reçus, ce qui lui permet de ne retransmettre que les paquets manquants.
- Implémenter des buffers importants sur l'émetteur avec les options de fenêtre adaptatives. En autorisant la transmission de plus gros volumes de trafic, cela permet à l'émetteur de s'adapter à une plus grande diversité de chemins réseaux,
- Utiliser un débit initial plus élevé que la valeur de 1 MSS choisie par défaut dans le mode slow-start de TCP. MSS ou Max Segment Size est le plus gros « morceau » de données qu'un émetteur et un récepteur peuvent s'échanger par TCP. Lorsque la connexion est établie, chacun envoie sa valeur de MSS (par défaut, 536 octets). La valeur initiale de cwnd est fixée initialement à 1 MSS, alors que 4 parait une valeur plus adaptée. Si le réseau ne peut pas faire face à cette rafale initiale, il fera diminuer la fenêtre. S'il possède les fonctionnalités, alors le débit initial permettra de transmettre 4 fois plus de données pendant le même temps.

Des expérimentations récentes publiées dans les RFC 2414, RFC 2415, RFC 2416 sur l'utilisation d'une fenêtre initiale TCP plus importante devraient tenir compte de ces considérations.

Le RFC 2398 fournit un certain nombre d'outils permettant de tester une implémentation TCP ou de donner des informations sur TCP (dbs, tcpanaly, Netperf, Tracelook, Ttcp etc...).

Réseau

Les performances peuvent être améliorées en autorisant le réseau à signaler les conditions naissantes de congestion afin que les systèmes terminaux puissent réduire le trafic et éviter ainsi le rejet des paquets. Pour cela, il est conseillé de :

- Implémenter le mécanisme RED (Random Early Detection)
- Séparer les queues TCP et UDP dans un routeur, par exemple, en plaçant les trafics TCP et UDP dans des files d'attente de sortie séparées et en utilisant un algorithme du type WFQ pour choisir les paquets. Outre l'effet d'adaptation de TCP résultant sur les systèmes terminaux, cela permet aussi de limiter les dégâts que pourrait causer un flux UDP.
- Implémenter le « Trafic Shaping » en utilisant un mécanisme « token bucket » aux extrémités du réseau

Lorsque les machines connectées et le réseau possèdent un niveau de qualité de service convenable, d'autres mesures QoS peuvent avoir une influence sur la congestion, sans dégrader sensiblement les performances.

- Support du champ IP Precedence pour éviter la monopolisation des ressources par certaines classes de trafic,
- Weighted RED (WRED) avec la pondération gérée via le champ IP Precedence. Cela permet au réseau de demander aux flux de trafic moins prioritaire de s'adapter au profit du trafic plus prioritaire,
- Weighted Fair Queuing (WFQ). Ce mécanisme de gestion des files d'attente pondéré par le champ IP Precedence permet au trafic prioritaire d'être mis en tête des files d'attente et donc d'avoir un meilleur temps de transmission.

2.2.3.4 Conclusion sur la QoS

La Qualité de Service dans l'Internet est encore un vaste chantier, à tel point qu'il est difficile d'en faire la synthèse.

Aujourd'hui de multiples groupes de travail de l'IETF travaillent dans des domaines touchant la Qualité de Service. Certains tiennent compte de nouveaux développements dans les réseaux tels que la spécification 802.1p ou les techniques de « label switching », tandis que d'autres se focalisent sur les politiques de contrôle dans les réseaux ou la définition de nouveaux protocoles de routage. Tous ces travaux sont néanmoins étroitement imbriqués et permettent de construire progressivement les morceaux du puzzle QoS adapté à l'Internet.

Plusieurs alternatives existent aujourd'hui. Cependant, parallèlement au modèle de réservation de ressources et de services intégrés posant des problèmes de déploiement à large échelle, il semble que les efforts s'orientent maintenant vers l'allocation prioritaire de ressources permettant de créer des distinctions de classes au sein du service « best-effort ». Ce type de modèle étudié actuellement au sein du groupe diffserv (« Differentiated Services ») repose essentiellement sur un champ dans l'en-tête du paquet IP, de telle sorte que les mécanismes de mise en file d'attente et de rejet des paquets puissent être mis en œuvre sur chaque nœud intermédiaire (IPv6, nous le verrons prend ce concept en compte).

L'implémentation de tels algorithmes ajoutés au déploiement d'architectures adéquates (offrant un service prévisible, stable et cohérent) pourront offrir à terme des niveaux de services différenciés tout en offrant une bonne stabilité.

Pour plus de détails sur les stratégies déployées par les équipementiers, le lecteur pourra se référer à la fiche technique Cisco en annexes ; qui bien que « publicitaire », décrit avec détails les stratégies de QoS possibles.

2.2.4 Précisions sur les standards de QoS et les actions des industriels

Au-delà des outils de gestion de la QoS, la façon de les utiliser dépend d'une politique de QoS : en effet, si on peut attribuer des priorités aux paquets en fonction de leur contenus, etc. il n'est pas spécifié par les RFC une fonction priorité = f (nature du paquet). Ceci relève de la politique de QoS. Dans ce domaine, les acteurs, et notamment les équipementiers, qui développent aujourd'hui des outils de gestion de la QoS tentent d'imposer les systèmes de gestion de la politique de QoS implémentés dans leurs matériels.

2.2.4.1 COPS

Parmi les politiques de QoS, on peut distinguer COPS (Common Open Policy Services), notamment promue par l'équipementier leader du marché, à savoir Cisco, dont les membres participent activement à la définition des spécifications en prenant part à la rédaction des RFC qui les définissent.

COPS est définie initialement par la RFC 2748 de janvier 2000 (The COPS Protocol), complétée par la RFC 2749 (janvier 2000 : COPS usage for RSVP), la RFC 2940 (octobre 2000 : Definition of Managed Objects for COPS Protocol clients), la RFC 3084 (mars 2001 : COPS Usage for Policy Provisioning – COPS PR-) et RFC 3181 (octobre 2001 : Signaled Preemption Priority Policy Element).

COPS et Cisco :

Les services QPM-COPS (QoS Policy Manager Common Open Policy Services) s'intègrent notamment dans la politique de QoS intégrale et de gestion du réseau en fonction du contenu de ses principaux promoteurs (Cisco en particulier), pour assurer la gestion intelligente du trafic par un contrôle des politiques à base d'annuaires, tenant compte de l'application et de l'utilisateur. Les services QPM-COPS forment une offre de politiques de qualité de service, qui autorise la différentiation et la signalisation des services pour assurer une qualité de haut niveau sur la totalité des infrastructures réseau.

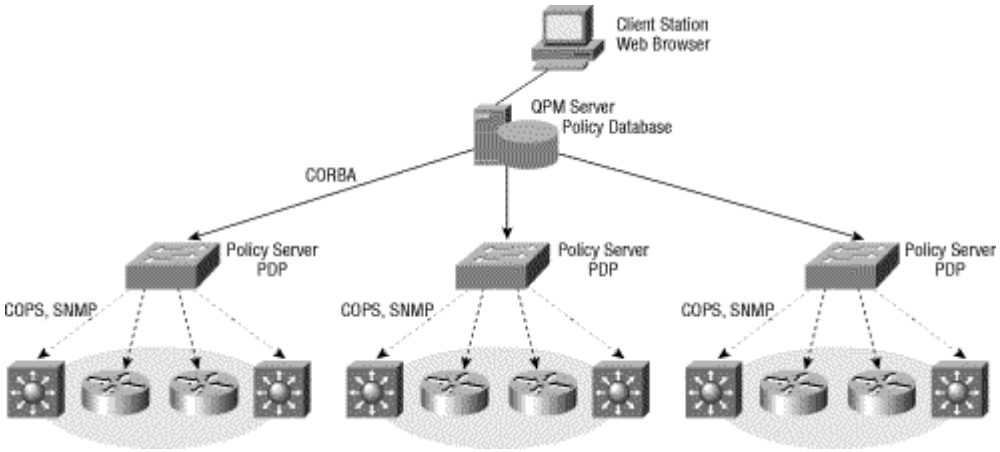
Concernant Cisco, disponibles depuis mi 2000, les services QPM-COPS disposent notamment des fonctions suivantes :

- Administration de politiques utilisateurs dynamiques avec une technologie réseau exploitant des annuaires
- Performances garanties des services vocaux et vidéo de haute qualité avec contrôle d'admission et gestion des politiques RSVP (Resource Reservation Protocol)
- Intégration très forte des politiques QoS du serveur et du réseau grâce à QPM-COPS et à des autres applications exploitant les annuaires
- Haute disponibilité permanente des applications et des utilisateurs grâce à une architecture ouverte et distribuée s'appuyant sur les protocoles standards COPS, RSVP et LDAP (Lightweight Directory Access Protocol).

On retiendra principalement qu'un seul point du réseau permet de définir des politiques et des services de bout en bout applicables à un parc étendu de routeurs et de commutateurs, QPM-COPS se répartit en trois composants :

- La station cliente, dotée d'une interface de navigation Web standard pour QPM.
- Le serveur QPM qui centralise, définit et coordonne les politiques du réseau.
- Les points de décision PDP (Policy Decision Point) qui peuvent se répartir sur différentes zones géographiques ou administratives du réseau. Un PDP est chargé de distribuer les politiques aux routeurs et commutateurs de son domaine. Il communique avec le serveur QPM central pour déterminer les rôles et les politiques à mettre en œuvre sur les périphériques dont ils ont la charge.

Figure 11 : COPS selon Cisco



Source : Cisco

2.2.4.2 AAA :

Les concepts AAA (Authentication, Authorization, Accounting) sont apparus au début des années 1990 avec la volonté des prestataires ISP d'offrir à leurs clients en déplacement la possibilité de se connecter à l'Internet via un modem. Il fallait en effet proposer une authentification fiable des utilisateurs, l'authentification ne pouvant plus reposer sur la connaissance de la position géographique des utilisateurs (numéro de téléphone). Ce service d'authentification est d'autant plus crucial que le système de facturation ou d'accès à certains services comme le VPN reposent sur une bonne authentification. Pour éviter toute fraude, il est donc nécessaire que les équipements du réseau sachent mettre en œuvre les fonctions AAA, c'est-à-dire :

- S'authentifier et s'identifier les uns les autres ;
- Gérer les droits des mobiles ;
- Collecter et stocker des informations sur les connexions des mobiles.

En outre, l'AAA est un groupe de travail de l'IETF qui travaille sur ces problématiques qui sont jouent également dans la QoS.

2.2.4.3 Diameter :

Un nouveau protocole implémentant AAA et appelé Diameter est en cours de finalisation à l'IETF. Ce protocole se présente comme la suite du protocole RADIUS (Remote Authentication Dial-In User Service) largement utilisé actuellement par les ISP pour rendre un service AAA auprès de leurs clients PPP dont l'accès est fixe. Le protocole Diameter ambitionne de faire de l'AAA dans les environnements de mobilité IP et d'accès PPP[79] mobiles.

Comme COPS, Diameter est soutenu par des industriels, dont les membres participent activement à la définition du protocole. L'industriel le plus actif pour Diameter est Sun Microsystems.

Il n'existe pas de RFC traitant de Diameter, mais des « Drafts » (dont le format est défini par la RFC 2026 de l'IETF, et qui sont des documents de travail de l'IETF, donc mouvants) : on recense à ce jour 18 de ces Drafts, consacrés à la définition de différentes spécifications de Diameter, rédigés entre mars et octobre 2001 ; les bases de Diameter ont été décrites dans le « Draft-ietf-aaa-diameter-framework-01 », du 5 mars 2001, rédigé par Pat Calhoun, de Sun Microsystems.

Diameter est donc encore inabouti à ce jour.

Par rapport à COPS, Diameter n'est pas défini comme un protocole de gestion de la QoS, mais comme un protocole participant au processus AAA, donc à l'authentification. Certes, les procédures AAA participent le la QoS globale, mais elles ne sont pas prises en compte dans la définition communément admise de QoS. Diameter et COPS ne remplissent donc pas les mêmes fonctions dans la « chaîne de QoS ».

2.2.5 Multicast

La fonctionnalité n'a pas été prévue de façon native. De ce fait, une classe d'adresses complète (la classe D) a été dédiée à la gestion de la fonction MultiCast. Afin d'assurer cette fonction, plusieurs solutions ont été retenues, et notamment celle du « Edge Casting ».

[79] PPP : Point-to-Point Protocol

3 Avantages techniques d'IPv6

Outre un format d'adressage qui permet de disposer d'un stock d'adresses extrêmement important, IPv6 prévoit un adressage hiérarchique, permettant d'optimiser le routage. L'usage commercial est envisagé, et le nouvel IP peut supporter de façon native le multicast, l'auto configuration (utile dans la gestion de la mobilité), la gestion de la mobilité (même si Mobile IPv6 ne sera pas, a priori, utilisé sur les réseaux cellulaires dans l'immédiat), la sécurisation par défaut, et un format de données permettant de simplifier la gestion de la QoS, et notamment d'ouvrir la voie à de nouvelles applications.

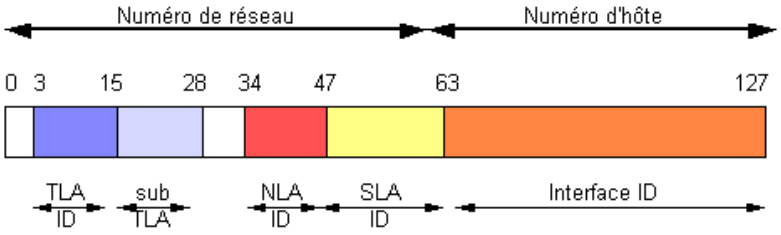
3.1 Adressage sur 128 bits

IPv6 dispose d'un adressage sur 128 bits, et non plus sur seulement sur 32 comme dans IPv4. On dispose ainsi d'un stock de 2^{128} adresses, soient 2^{96} fois plus qu'avec IPv4. Ce stock très important permet d'envisager l'avenir avec sérénité, et de considérer qu'il sera ainsi possible de faire face à la croissance d'Internet dans toutes les zones géographiques, mais aussi de faire face aux besoins induits par l'apparition de nouvelles applications consommatrices d'adresses IP.

3.1.1 Apport de l'étude ART

Les 128 bits d'une adresse IPv6[80] sont regroupés en deux parties de 64 bits: une portion désignant un numéro de réseau et une portion désignant un numéro d'hôte correspondant à l'adresse physique de l'interface connectée.

La portion allouée à l'identification du réseau dans la topologie du réseau public est constituée d'un préfixe lui-même hiérarchisé par la juxtaposition de trois numéros (le TLA ID[81], le sub-TLA et le NLA ID[82]) et d'un préfixe identifiant la machine dans la topologie du site raccordé sur ce réseau (SLA ID[83] sur 16 bits), comme l'indique le schéma ci-dessous :



[80] Définie par la RFC 2460
[81] Top-Level Aggregation Identifier, numéro attribué par les RIRs aux TLA registries, identifiant une plage d'adresses qu'ils peuvent ensuite redistribuer auprès de fournisseurs d'accès notamment
[82] Next-Level Aggregation Identifier, numéro attribué généralement aux fournisseurs d'accès par les TLA registries identifiant une plage d'adresses IPv6
[83] Site-Level Aggregation Identifier

3.2 Adressage hiérarchique et agrégation

IPv6 permet un adressage hiérarchique[84], réduisant le nombre de routes pour les routeurs de cœur de réseau IP. Cet adressage hiérarchique permet de simplifier les agrégations d'adresses (par fournisseur ou par nœud d'échange). Dans IPv6, il y a séparation entre l'adresse du terminal et l'identification du réseau. Cette séparation permet de renuméroter un réseau très simplement (cf. auto configuration).

3.2.1 Apport de l'étude ART : conséquences de l'adressage hiérarchique sur les procédures d'attribution

L'intérêt du nouveau format d'adresses IPv6, outre son allongement, est son organisation hiérarchique. L'utilisation de préfixes séparés pour les adresses affectées à un fournisseur et les adresses affectées à une zone géographique constitue un compromis entre deux différentes visions du futur réseau Internet (à savoir, une gestion 100% par zone géographique et une gestion 100% par prestataire de service). Chacun de ces fournisseurs dispose d'une fraction réservée de l'espace d'adressage (1/8 de cet espace). Les 5 premiers bits qui suivent le préfixe 010 sont utilisés pour indiquer dans quel « registre » se trouve le fournisseur d'accès. Actuellement, trois registres sont opérationnels (ARIN, APNIC, RIPE NCC), et jusqu'à 29 nouveaux registres pourront être ajoutés ultérieurement.

Chaque registre est libre de diviser les 15 octets restants comme il l'entend. Une autre possibilité est d'utiliser un octet pour indiquer la nationalité du fournisseur et de laisser toute liberté aux octets suivant pour définir une structure d'adresses spécifique.

Le modèle géographique est le même que celui du réseau Internet actuel, dans lequel les fournisseurs d'accès ne jouent pas un grand rôle. Dans ce cadre, IPv6 peut gérer 2 types d'adresses.

Les adresses de liens et de sites locaux n'ont qu'une spécification locale. Elles peuvent être réutilisées par d'autres organisations sans qu'il y ait de conflit. Elles ne peuvent pas être propagées hors des limites des organisations, ce qui les rend bien adaptées à celles qui utilisent des gardes-barrières pour protéger leur réseau privé du réseau Internet.

Les conséquences de l'adressage hiérarchique sur les modes d'attribution ne sont donc pas extrêmement visibles. Toutefois, on peut noter que les politiques mises en œuvre sont particulièrement rigoureuses et structurées, afin d'éviter de reproduire la confusion survenue avec IPv4. Le risque est de provoquer des réactions de rejet de la part des utilisateurs, face à des procédures rigides qui semblent pour certains plus adaptées à une gestion de pénurie (ce qui n'est pas le cas d'IPv6) qu'à une volonté d'éviter une dispersion géographique des préfixes.

Ainsi, sans changer fondamentalement les modes d'allocation ou d'attribution des adresses, l'adressage hiérarchique permet, notamment du fait que l'adressage IPv6 est encore neuf et n'hérite pas d'un adressage anarchique comme ce fut le cas avec IPv4, de structurer « proprement » la répartition des adresses. Les procédures d'agrégation en seront donc simplifiées, et, par voie de conséquence, les tables de routage allégées. La gestion globale de l'adressage étant correctement et rationnellement ordonnée, c'est l'ensemble de l'Internet qui fonctionnera mieux.

[84] adressage multipoint et hiérarchique : par zone géographique et/ou prestataire de service.

3.3 Multicast

La fonctionnalité est prévue en natif dans IPv6. Cette fonction va de pair avec le nouvel adressage et simplifie le routage des données.

Globalement, le routage est simplifié, fluidifié et donc amélioré.

3.4 Auto configuration et gestion de la mobilité

IPv6, contrairement à IPv4, prévoit la possibilité pour un terminal IPv6 (ou nœud IPv6) de s'auto configurer dans un réseau. On parle alors d'un mode « plug and play ». Cette fonctionnalité est particulièrement utile en vue du développement des réseaux privés, et des applications domotiques et nomades, qui s'accommodent mal de lourdes procédures d'administration. La gestion et l'administration des réseaux IP en général est simplifiée, au bénéfice des utilisateurs.

La fonctionnalité a en outre une utilité en termes de gestion de la mobilité, elle-même prévue en natif dans IPv6 : même si Mobile IPv6 est une couche supplémentaire de protocole, celle-ci est envisagée dès la spécification d'IPv6.

3.4.1 Apports de l'étude ART

3.4.1.1 Mobile IPv6

Le protocole Mobile IPv6 partage avec Mobile IPv4 de nombreux points communs. Néanmoins la version Mobile IPv6 est complètement intégrée dans IPv6, à la différence de Mobile IPv4 qui apparaît davantage comme une couche supplémentaire au-dessus d'IPv4. De plus Mobile IPv6 apporte certaines améliorations à Mobile IPv4. Résumé des différences entre les 2 versions du protocole :

- Support de l'optimisation du routage : Mobile IPv6 intègre l'optimisation du routage (« Route Optimisation ») comme une fonctionnalité fondamentale à la différence de Mobile IPv4, qui en fait une extension optionnelle. L'optimisation du routage permet d'éliminer le routage triangulaire.
- Support intégré de la gestion des adresses d'origine (home address) et adresses temporaires (care of address) de Mobile IP : lorsque le terminal mobile envoie des données, il intègre sa care of address dans le champ Source Address de l'entête du paquet IPv6. Cette adresse sera prise en compte dans le réseau pour le routage des paquets qui lui seront envoyés. En revanche, la home address doit être conservée du point de vue des applications (adresse unique), et celle-ci est placée dans le champ Home Address du paquet IPv6. Pour que ce mécanisme fonctionne et traite correctement la core of address et la home address, il requiert que l'ensemble des terminaux (mobiles ou fixes), routeurs et serveurs mis en jeu soient compatibles IPv6.
- L'utilisation directe de la care of address dans le champ Source Address de l'entête du paquet IPv6 évite l'opération d'encapsulation – ou de tunnelling – de Mobile IPv4. Les équipements distants envoient directement les paquets à la care of address.
- Il n'y a plus besoin de serveur foreign agent comme en Mobile IPv4. Dans Mobile IPv6, le terminal mobile utilise directement les fonctionnalités IPv6 « Neighbor Discovery » et « Address Autoconfiguration ».

3.4.1.2 Synthèse

Tableau récapitulatif des différences entre Mobile IPv4 et Mobile IPv6 :

	Mobile IPv4	Mobile IPv6
Mécanisme général	Mécanisme d'encapsulation des paquets IP et de transfert vers l'adresse IP temporaire dans le réseau visité	Suppression du foreign agent, devenu inutile grâce aux fonctionnalités de gestion de la mobilité intégrées dans IPv6
Routage	Routage triangulaire lors de la réception des paquets par le terminal mobile L'optimisation du routage est développée et disponible comme une option	Support intégré de l'optimisation du routage (« Route Optimisation »)
Adressage	Seule l'adresse IP du réseau d'origine est connue du correspondant ; le foreign agent assure la correspondance entre l'adresse IP d'origine et celle dans le réseau visité	Les 2 adresses IP (dans le réseau d'origine et dans le réseau visité) sont codées dans l'adresse IPv6, permettant à l'équipement distant de connaître directement l'adresse de destination et d'éviter l'encapsulation.

3.4.1.3 Auto configuration et mobilité

3.4.1.3.1 Principe

La première exigence de l'opération « plug and play » est qu'une station puisse être capable d'acquérir une adresse de manière dynamique, soit lorsqu'elle est attachée à un réseau pour la première fois, soit lorsque la station a besoin d'être reconfigurée parce que la station a bougé ou parce que l'identité du réseau a été modifiée. Il y a bien d'autres fonctions qui nécessitent un environnement de « plug and play ». La plupart de celles-ci doivent se faire en-dehors du protocole IPv6, mais le protocole d'auto configuration d'adresse d'une station sera exécuté par IPv6.

Une station IPv6 peut auto configurer deux types d'adresses :

- les adresses intra-liaison (intra-link scope address),
- les adresses inter-liaison (inter-link scope address).

Une adresse d'environnement intra-liaison est auto configurable en l'absence de routeur, alors qu'une adresse inter-liaison est auto configurable lorsqu'un routeur est présent sur la liaison.

Il n'y a qu'une seule façon de former une adresse inter-liaison, en revanche, il y a deux manières pour former une adresse inter-liaison. Dans le premier mécanisme, une station obtient son adresse inter-liaison en concaténant un préfixe de réseau annoncé par un « Router Advertisement » [IPv6-DISC-PROC] à un jeton unique par liaison. L'autre mécanisme disponible pour les stations est d'utiliser le protocole de configuration dynamique des stations pour IPv6 [Dynamic Host Configuration Protocol - DHCPv6]. Le choix du protocole à utiliser est proposé par le routeur, et le choix est configurable par l'administrateur système.

Le premier processus de formation de l'adresse inter-liaison convient pour des environnements où aucune gestion administrative n'est désirée. Ce protocole est spécialement conçu dans le but particulier de faire de la configuration simple d'adresse. DHCPv6 est un protocole plus complexe permettant une affectation flexible des adresses; sous le contrôle de l'administrateur système. Ce protocole nécessite tout particulièrement un important gestionnaire de système (serveur et base de données).

3.4.1.4 Gestion de la mobilité

L'objet de ce paragraphe descriptif est de définir la mobilité, les apports d'IPv6 dans la gestion de la mobilité au sein et entre des réseaux, et l'apport de l'auto configuration dans ce contexte.

Le concept de mobilité signifie, dans le cas présent, la séparation des identificateurs et des adresses, ces deux éléments possédant un format similaire. L'identificateur d'un nœud mobile ne change jamais quel que soit ses déplacements tandis que son adresse est spécifique à son point de rattachement à Internet. L'adresse est seulement utilisée pour le routage des paquets et non pour l'identification du nœud à l'inverse de l'identificateur qui peut même éventuellement servir d'adresse par défaut.

Deux options ont été rajoutées dans les options de l'en-tête de type Hop-by-Hop afin de rendre possible la mobilité. L'une est utilisée pour la communication de données et l'autre pour le contrôle.

TCP/UDP[85] identifie un nœud par son identificateur et non son adresse. Afin d'optimiser le routage, chaque nœud dispose d'une partie cachée ou Address Mapping Table (AMT). IPv6 résout le problème de l'identificateur et de l'adresse en utilisant AMT, puis en renvoyant le paquet avec la prise en compte de son adresse complète.

Les entrées AMT sont créées puis mises à jour en fonction de la réception ou de l'envoi de paquets selon les options de mobilité choisies après, bien entendu, l'authentification du paquet.

Cependant, avant d'aborder les différentes techniques développées pour la mobilité, il convient de définir un certain nombre de concepts :

- AAA[86] : Authentication, Authorization, Accounting. Fonction de gestion de la sécurité pour les réseaux cellulaires définie par l'IETF ; elles concernent le contrôle d'accès lors de l'interconnexion à un réseau plus large que le réseau d'origine.
- Un nœud : Il s'agit d'un terme général utilisé pour évoquer à la fois une station de travail et/ou un routeur.
- Un nœud mobile : C'est un nœud qui a la possibilité de changer de point de rattachement sur l'Internet.
- Une adresse : C'est un numéro qui spécifie le point de rattachement à l'Internet. Une adresse est attribuée à chaque interface réseau d'un nœud. Nous avons vu que, pour IPv6, la taille d'une adresse est de 128 bits. L'adresse d'une interface change lorsque le nœud se déplace sur un autre réseau.
- Un identificateur : C'est un numéro attribué à un nœud unique. Chaque nœud dispose de son propre identificateur indépendamment du nombre d'interfaces réseaux dont il bénéficie. Non seulement un identificateur est unique et définitif quel que soit le nœud de rattachement à l'Internet, mais il bénéficie du même format qu'une adresse classique ce qui lui permet éventuellement de se substituer à une adresse.
- Un réseau maison (home subnet) : Il s'agit du réseau indiqué par l'identificateur d'un nœud mobile.
- Une résolution d'adresse (address resolution) : C'est une fonction qui oriente l'identificateur vers l'adresse correspondante.
- Un « résolveur » d'adresse (address resolver) : C'est un nœud qui utilise une résolution d'adresse. Il existe deux types de résolveurs d'adresses pour un nœud mobile.
    - le résolveur primaire : Un résolveur d'adresse est connecté au réseau maison d'un nœud mobile. Un nœud mobile indique périodiquement le(s) résolveur(s) primaire(s) de son identificateur ainsi que son adresse courante.
    - le résolveur temporaire : Dans le cas d'un résolveur d'adresse non connecté au réseau maison d'un nœud mobile, un résolveur temporaire crée et met à jour ses paquets AMT reçus ou envoyés (avec l'option mobile dans l'en-tête).

[85] TCP : Transmission Control Protocol ; UDP : User Datagram Protocol
[86] Cf. infra, précisions sur le concept AAA dans le paragraphe « authentification dans un réseau mobile »

- Address Mapping Table (AMT) : Une table constituée d'entrées pour chacune desquelles il y a l'information de routage entre l'identificateur et l'adresse. Chaque nœud doit disposer d'une AMT pour la résolution d'adresse.

Deux options pour la mobilité sont possibles via les propriétés de l'en-tête IPv6 Hop-by-Hop : l'option de mobilité pour les données utilisateur et l'option de mobilité pour le contrôle.

La raison principale pour laquelle ces options sont inclues dans l'en-tête IPv6 Hop-by-Hop est la possibilité de créer et de mettre à jour des entrées AMT sur chaque nœud le long du chemin suivi par le paquet envoyé.

Les options de mobilité utilisent deux méthodes d'authentification, « keyed MD5 » et « RSA digital signature ».

- Keyed MD5 est utilisée dans le cadre de l'authentification end-to-end d'un paquet via l'option de mobilité pour les données utilisateurs ce qui nécessite de partager une clé secrète commune entre le nœud authentifiant et le nœud authentifié. La taille de la clé est de 128 bits, les calculs couvrent les champs suivants : Source Address (dans l'entête IPv6), Source Identifier, Source Address Version, Holding Time et Timestamp.
- La méthode RSA digital signature est utilisée pour l'authentification de nœuds intermédiaires utilisés pour l'envoi de paquets avec l'option de mobilité pour le contrôle. La taille de la clé est de 512 bits, les calculs couvrent les champs suivants : Identifier, Address, Address Version, Holding Time et Timestamp.

Lorsqu'un nœud est connecté à un réseau, il lui est attribué une adresse IPv6 temporaire dans le sous réseau par le mécanisme d'auto configuration d'adresses. A l'inverse, l'identificateur du nœud mobile ne change pas. Le nœud mobile transfère un paquet IPv6 via l'option de mobilité pour le contrôle situé dans son réseau maison. Lors de toute cette procédure, les entrées AMT pour le nœud mobile sont créées et mises à jour à la fois sur les nœuds intermédiaires et ceux du réseau maison.

Processus de gestion de la mobilité :

- **Procédures utilisées sur le nœud mobile :** Lorsqu'un nœud mobile est connecté à un réseau, il transmet un paquet IPv6 via l'option de mobilité pour le contrôle à son réseau maison.
- **Procédures utilisées sur un nœud intermédiaire :** Lorsqu'un nœud intermédiaire reçoit un paquet via l'option de mobilité pour le contrôle, il peut exécuter les procédures suivantes après ou avant l'envoi des paquets.
- **Authentification :** le nœud intermédiaire authentifie le paquet s'il connaît la clé publique du nœud mobile spécifié par le champ Identifier de l'option de mobilité. Si l'authentification réussit alors la modification AMT est exécutée.
- **Modification AMT :** le nœud intermédiaire crée une entrée AMT pour le nœud mobile spécifié par le champ Identifier de l'option de mobilité s'il ne la connaît pas déjà ; ou bien, il met à jour l'entrée AMT existante à condition qu'elle ne soit pas obsolète (le numéro de l'option de mobilité ne doit jamais être plus grand que celui de l'entrée AMT). Dans le cas où l'entrée AMT est obsolète, le nœud intermédiaire peut diffuser le paquet reçu à toutes ses interfaces.
- **Procédures utilisées sur un nœud situé à la frontière (Boundary Node) du réseau maison :** lorsqu'un paquet avec une option de mobilité pour le contrôle est reçu, un nœud situé à la frontière du réseau maison du nœud mobile désigné par le champ Identifier de l'option exécute les procédures d'authentification et de modification AMT, puis diffuse le paquet dans le réseau maison s'il s'agit d'un réseau de type diffusion. Si le nœud situé à la frontière dispose d'une entrée AMT obsolète, il transmet alors le paquet à l'adresse désignée par le champ Address de l'entrée AMT obsolète.
- **La communication des données :** dans les données de communication, l'option de mobilité pour les données des utilisateurs est intégrée dans chaque paquet IPv6. TCP/UDP désigne le nœud de destination avec l'identificateur. La résolution d'adresse pour le nœud de destination est exécutée soit au niveau du nœud source, soit au niveau du nœud intermédiaire, ou bien au niveau d'un nœud localisé au sein du réseau maison du nœud de destination, puis le paquet est routé vers le nœud de destination.

- **Procédures appliquées au nœud source :** le nœud source crée un paquet IPv6 via l'option de mobilité pour les données des utilisateurs. Dans l'option, les champs relatifs au nœud source (Source Identifier, Source Address Version, Holding Time et Timestamp) sont remplis avec les valeurs appropriées, puis les données d'authentification sont calculées et attribuées au champ Authentication Data.
- Une requête de transmission de la couche supérieure précise le nœud de destination et son identificateur (champ Destination Identifier) mais pas l'adresse. Le nœud source essaie de résoudre la correspondance de l'identificateur et de l'adresse grâce à la technique AMT. Si l'entrée AMT pour le nœud de destination existe, l'adresse et son numéro de version sont attribués respectivement au champ de destination de l'en-tête IPv6 ainsi qu'au champ du numéro de version de l'adresse de destination de l'option.
- **Procédures appliquées au nœud intermédiaire :** il existe deux procédures dans le cas d'un nœud intermédiaire avec l'option de mobilité des données des utilisateurs, à savoir la modification AMT et la résolution d'adresse.
- Lors de la modification AMT, l'entrée AMT pour le nœud mobile désigné par le champ Source Identifier de l'option peut être créée ou modifiée. Dans un premier temps, le nœud intermédiaire authentifie le paquet si ce dernier connaît la clé commune du nœud source. Si l'authentification réussit, les procédures suivantes sont exécutées. Si une entrée AMT pour le nœud mobile désigné par le champ Source Identifier de l'option n'existe pas, elle est alors créée. S'il n'y a pas d'entrée AMT (information obsolète), alors des modifications sont réalisées en accord avec les valeurs de l'option.
- Dans le cas de la résolution d'adresse, l'adresse de destination dans l'en-tête IPv6 et le numéro de version de l'adresse de destination de l'option peuvent être modifiés. Si l'entrée AMT pour le nœud de destination du paquet existe, alors il faut comparer le numéro de version de l'adresse de destination du paquet avec le numéro de version de l'adresse de l'entrée. Si l'entrée AMT dispose d'informations plus récentes, alors le champ Destination Address de l'en-tête IPv6 et le numéro de version de l'adresse de destination de l'option sont modifiés conformément à l'entrée.
- **Procédures appliquées au nœud de destination :** le nœud de destination exécute la procédure de modification AMT décrite ci-dessus puis la signale à la couche supérieure de réception du paquet avec l'identificateur du nœud source mais pas son adresse.

3.4.1.5 Mobilité dans les réseaux cellulaires

3.4.1.5.1 Présentation générale

L'évolution des réseaux GSM introduit, avec le GPRS, le transfert en mode paquet, plus adapté au transport des données que le mode circuit. De plus, le GPRS introduit une nouvelle infrastructure de réseau cœur qui utilise le protocole IP (version 4). Enfin, le GPRS définit un protocole pour la gestion de la mobilité dans le réseau GPRS, qui a pour but de garantir le routage des paquets entre le terminal mobile et le serveur et qui doit assurer la continuité des transferts de données lorsque le mobile se déplace (passage d'une cellule à une autre) : le protocole GTP (GPRS Tunnel Protocol) est mis en œuvre pour gérer la mobilité dans les réseaux GPRS. Celui-ci est d'un principe assez proche de celui de Mobile IPv4 avec encapsulation des paquets IP dans des paquets IP.

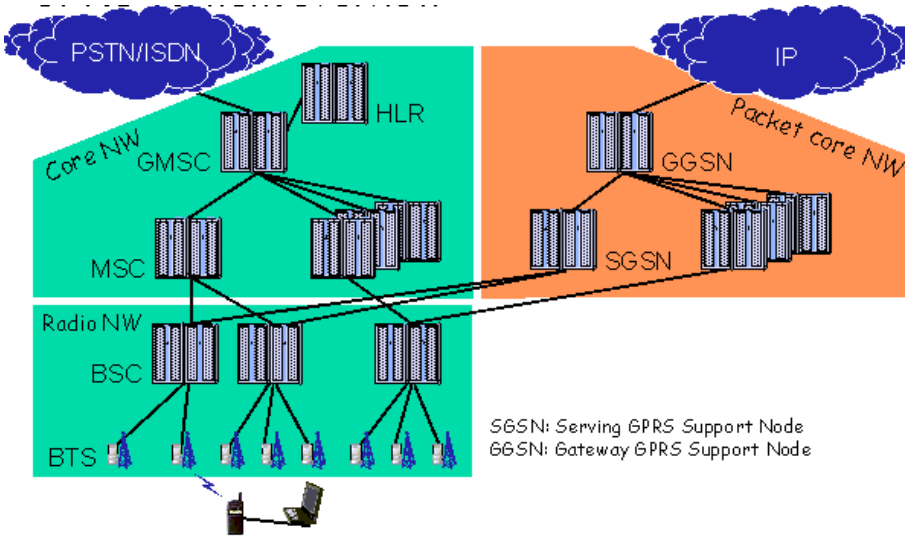
Le même réseau cœur et donc la même gestion de la mobilité seront utilisés pour les premiers déploiements de l'UMTS, dans les versions release 99 puis release 4 de 3GPP. L'utilisation d'IPv6 est obligatoire à partir de la version release 5 du standard UMTS, finalisée d'ici la mi-2002. Ainsi les déploiements des premières versions des réseaux UMTS (d'abord en release 99 puis en release 4) utiliseront IPv4 et le protocole GTP. L'UMTS release 5 marque le passage vers le « tout-IP », c'est à dire l'utilisation du protocole IP de l'application dans le terminal jusqu'au serveur hébergeant le service. Le support du tout-IP implique par ailleurs le support de différentes classes de qualité de service en fonction de la nature du flux transporté (voix, vidéo, contenu Internet, …).

3.4.1.5.2 Les différents niveaux de gestion de la mobilité

3.4.1.5.2.1 Description de l'architecture de réseau

Commençons par un rappel de l'architecture du réseau GPRS (qui est similaire à celle du réseau UMTS release 99 et release 4) : la figure ci-après présente l'architecture du système GSM/GPRS. Le GPRS introduit un réseau cœur fonctionnant en mode paquet, en parallèle du réseau cœur circuit du GSM. 2 nouveaux équipements sont constitutifs de ce réseau paquet : le SGSN (Serving GPRS Support Node) et le GGSN (Gateway GPRS Support Node).

Figure 12 : Architecture GPRS



3.4.1.5.2.2 Les différents niveaux de mobilité

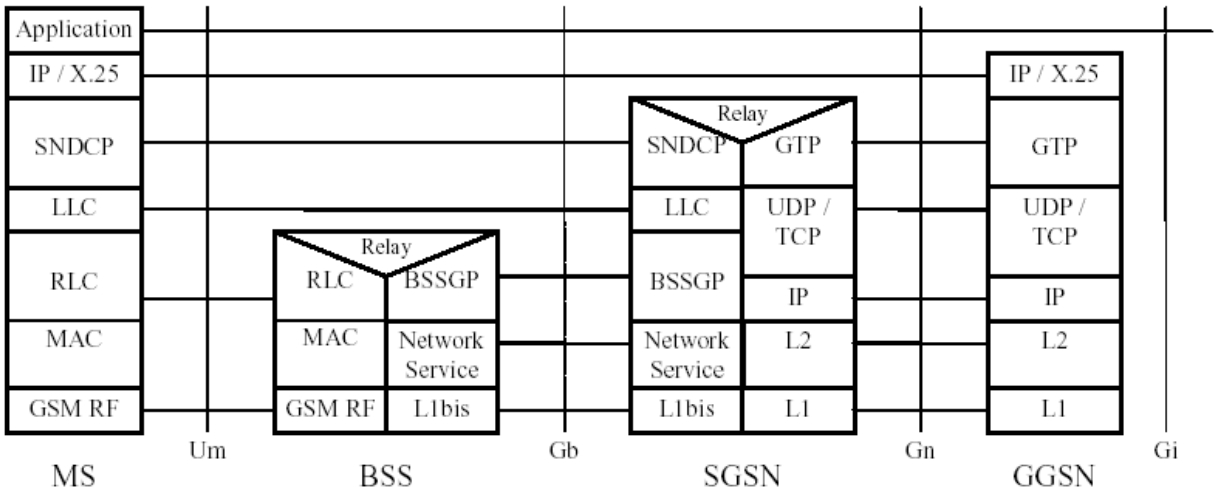
On peut distinguer plusieurs niveaux de mobilité dans les réseaux sans-fil, gérés par différents mécanismes :

- **La mobilité au sein du réseau cellulaire** (appelée « handover » pendant la transmission de données et « re-sélection » lorsque le terminal se déplace en état de veille)
  - Dans le cas du GSM/GPRS, différentes procédures de handover peuvent être appliquées car il existe différents types de handover : par exemple handover intra BSC (donc de même BSC), handover inter BSC avec encore 2 distinctions : intra MSC ou SGSN et intra MSC ou SGSN. L'ensemble de ces cas de handover mettent en jeu l'ensemble {MS[87], BTS, BSC, MSC/SGSN} ou seulement un sous-ensemble de ces équipements. Par exemple, le handover intra BSC ne met en jeu que les équipements du sous réseau radio (BTS et BSC). **Les procédures mises en jeu entre les équipements {MS, BTS, BSC, MSC/SGSN} sont gérées par les protocoles de couche 2 et 3 de ces équipements.**
  - Dans le cas de la mobilité lors de la transmission de données en GPRS et UMTS, **le protocole GTP (GPRS Tunnel Protocol) est utilisé pour gérer la mobilité entre le GGSN et le SGSN qui gère l'abonné**. Le protocole GTP n'intervient pas directement dans les procédures de handover, qui sont laissées à la charge des protocoles du réseau d'accès radio et de l'interface entre BSC et MSC/SGSN.

À titre d'illustration, le détail des protocoles mis en jeu dans le plan de transmission GPRS et le modèle en couche sont donnés dans la figure ci-dessous :

[87] MS : Mobile Station

Figure 13 : Modèles en couche du plan de transmission GPRS



Source : GSM 3.60 – Figure 4

- **La mobilité entre différents réseaux cellulaires d'une même technologie** (roaming) : Dans le cas du GPRS et de l'UMTS (release 99 et release 4), les procédures générales définies dans le GSM sont utilisées. Au niveau de GTP, le GGSN du réseau d'origine route les paquets vers le SGSN qui gère l'abonné dans le réseau visité.
- **La mobilité entre réseaux hétérogènes**. Plusieurs cas de figure : de GPRS vers UMTS, d'un réseau cellulaire GPRS ou UMTS vers un accès Internet fixe, ou vers un WLAN, d'UMTS vers CDMA 2000. La gestion de ces cas de figure relève de Mobile IP.

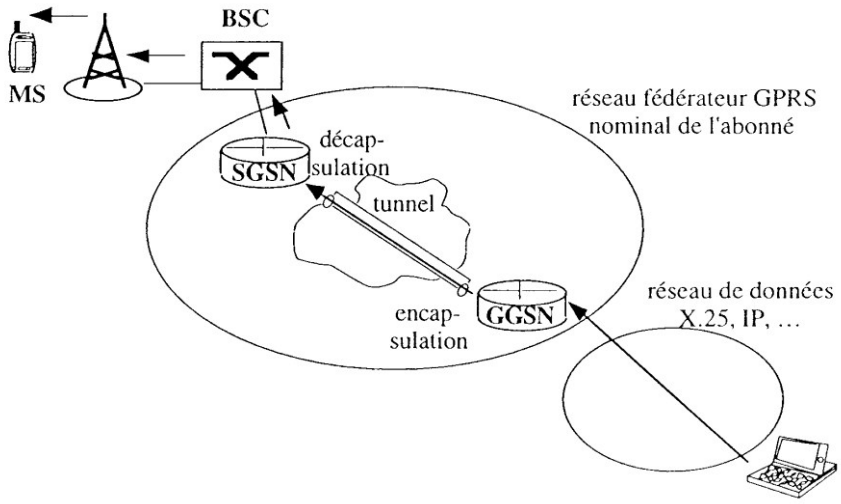
3.4.1.6 Description de GTP

Le protocole GTP assure la gestion de la mobilité dans le réseau cœur des systèmes GPRS et UMTS release 99 et release 4. Comme expliqué ci-dessus, le protocole GTP intervient à l'interface entre les équipements GGSN et SGSN du cœur de réseau, au-dessus des couches TCP/UDP et IP et consiste à encapsuler les paquets IP à destination du mobile dans des paquets IP. Un tunnel IP est créé entre le GGSN, directement relié au réseau IP externe, et le SGSN. En revanche la liaison entre le SGSN et le terminal est gérée par d'autres protocoles qu'IP. GTP ne gère que la mobilité sur l'interface GGSN-SGSN.

GTP ne gère que la macro-mobilité, c'est à dire la mobilité dans le cœur de réseau.

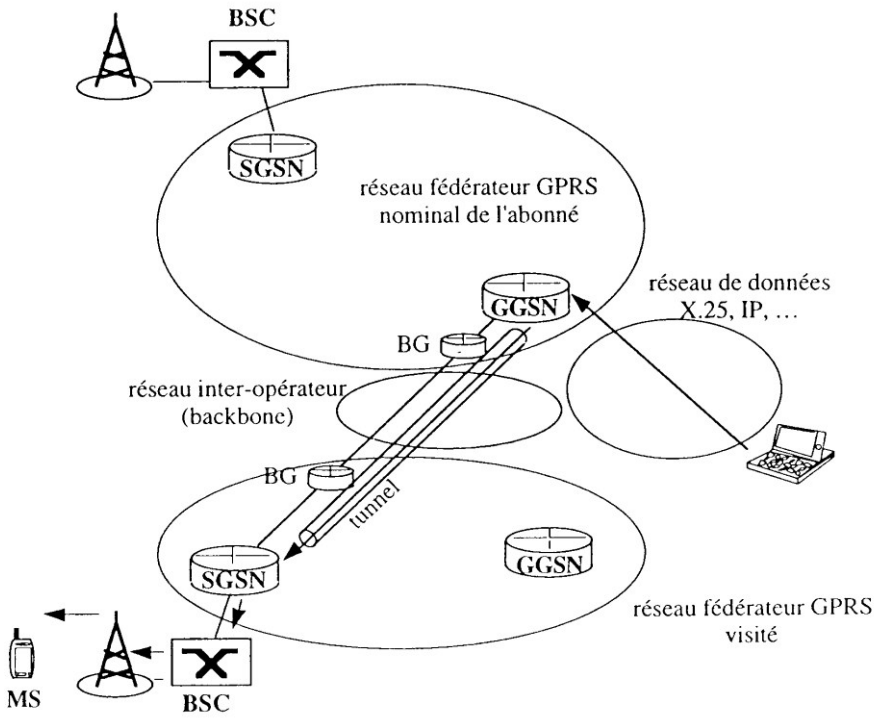
La spécification GSM 09.60 de l'ETSI définit en détail ce protocole GTP. Dans le cadre de ce document, nous nous contenterons des 2 figures ci-dessous illustrant le principe de GTP :

Figure 14 : Principe de la transmission de données vers un mobile GPRS



Source : Réseaux GSM-DCS (X. Lagrange, P. Godlewski, S. Tabbane), éditions Hermes

Figure 15 : Principe du transfert de données lors de l'itinérance sur un autre réseau



Source : Réseaux GSM-DCS (X. Lagrange, P. Godlewski, S. Tabbane), éditions Hermes

3.4.1.6.1 GTP et handover

GTP ne gère que la macro-mobilité et donc n'intervient pas dans les procédures de handover, qui sont gérées au niveau de réseau d'accès radio et du SGSN.

3.4.1.6.2 GTP et l'effet « trombone »

GTP définit le GGSN du réseau d'origine comme le passage obligé des paquets à la fois en émission et en réception. Il introduit donc potentiellement un effet « trombone », équivalent à un routage non optimal des transmissions de données.

La solution à ce problème semble passer par l'utilisation de Mobile IP.

3.4.1.6.3 Comparaison de GTP avec Mobile IP

3.4.1.6.3.1 Les similitudes

GTP et Mobile IPv4 assurent des fonctionnalités similaires :

- **Utilisation de l'encapsulation (ou « tunneling ») pour la transmission de paquets IP** : dans les 2 cas, une seule adresse IP est utilisée pour identifier l'utilisateur du point de vu de l'application quel que soit la position de l'utilisateur et un équipement est chargé d'établir un tunnel afin d'assurer le lien entre cette adresse IP et l'équipement auquel l'utilisateur est rattaché :
    - dans le cas de GTP, le GGSN établit le tunnel vers le SGSN, auquel l'abonné est rattaché
    - dans le cas de Mobile IP, le Home Agent établit le tunnel vers le Foreign Agent, du réseau auquel l'utilisateur est rattaché

Par conséquent, il y a une forte similitude fonctionnelle entre d'une part le GGSN et le Home Agent et d'autre part, le SGSN et le Foreign Agent. Dans le cas de GTP, le SGSN constitue le bout du « tunnel » de routage. Dans Mobile IP, le bout du tunnel correspond à la care-of-address, qui est soit l'adresse du Foreign Agent, soit l'adresse du terminal dans le réseau local.

- **Procédures d'enregistrement** : des fonctionnalités d'enregistrement du terminal mobile auprès du Home Agent – respectivement du GGSN – sont définies à la fois dans GTP et dans Mobile IP.

3.4.1.6.3.2 Les différences

GTP est un protocole intégré dans le standard GPRS. Il répond donc à une exigence précise qui est la gestion de la mobilité dans le réseau cœur du système GPRS. Le système GPRS est un système télécoms standardisé, avec des architectures et des interfaces entre éléments spécifiées. En revanche, Mobile IP est un protocole destiné à gérer la mobilité d'équipements fonctionnant sous IP, sur divers réseaux IP. Dans Mobile IP, la technologie de transmission sous-jacente utilisée par le réseau est transparente.

Outre cette différence fondamentale, d'autres différences existent entre les 2 protocoles :

- **Connectivité au réseau IP externe** : à la différence du Foreign Agent de Mobile IP, le SGSN n'est pas connecté à un réseau IP externe, de sorte que les paquets émis par le terminal mobile sont forcément routés via le GGSN (impliquant un routage triangulaire non optimal).
- **Support des autres protocoles cellulaires** : GTP interagit avec d'autres protocoles utilisés dans les réseaux cellulaires (MAP – Mobile Application Part, chargé de la communication avec le HLR, est un exemple). Mobile IP doit pouvoir s'intégrer dans ces protocoles, tout en préservant le fait que Mobile IP doit rester indépendant du réseau sous-jacent. Du point de vue des opérateurs mobiles, des procédures spécifiques doivent être supportées par le protocole Mobile IP (par exemple, des procédures d'autorisation d'accès au réseau mobile).

Des différences supplémentaires d'ordre technique existent : techniques d'identification sensiblement différentes (Mobile IP ne supporte pas l'Access Point Name utilisé largement dans les réseaux mobiles pour identifier le GGSN); support de PPP ;

Figure 16 : Tableau de synthèse de la comparaison entre Mobile IPv4 et GTP :

	Mobile IPv4	GTP
Similitudes	Similitudes fonctionnelles entre le GGSN et le Home Agent et entre le SGSN et le Foreign Agent ; notamment : • Procédure d'encapsulation des paquets IP, • Procédure d'enregistrement du terminal mobile Le but des 2 protocoles est de gérer la macro-mobilité.	
Différences	• Protocole destiné à gérer la mobilité d'équipements fonctionnant sous IP, sur divers réseaux IP • Protocole indépendant du réseau sous-jacent • Le Foreign Agent est connecté au réseau IP externe	• Protocole intégré dans le standard GPRS, qui est un système télécom • Interconnexion avec des protocoles spécifiques du réseau GPRS • Le SGSN n'est pas relié au réseau IP externe : tout paquet émis est routé via le GGSN

3.4.1.6.3.3 Convergence entre Mobile IP et GTP ?

Il est vraisemblable que Mobile IPv4 ne sera pas utilisé dans les réseaux mobiles et que d'ici la release 5 de l'UMTS, ce soit GTP qui sera utilisé. En revanche, la convergence pourrait avoir lieu à partir de release 5 avec IP6 et Mobile IPv6. Mais, comme expliqué ci-dessous, l'adoption de Mobile IPv6 par les réseaux cellulaires n'est pas acquise.

3.4.1.7 Statut de l'adoption d'IPv6 et de Mobile IPv6 dans les réseaux cellulaires

L'adoption d'IPv6 dans les réseaux cellulaires est le fruit d'un travail commun entre 3GPP, l'organisme international responsable de la standardisation de l'UMTS, et l'IETF, l'organisme international responsable de la standardisation des protocoles et des langages de l'Internet. IPv6 et Mobile IP sont à l'origine conçus par l'IETF, donc par la communauté Internet. Mais 3GPP rassemble des acteurs des télécommunications, issus d'une culture différente des acteurs de l'Internet et il semble que l'adoption des standards de l'IETF dans les réseaux cellulaires soient encore loin d'être concrétisée.

Si les acteurs des télécoms mobiles s'accordent pour reconnaître la nécessité de disposer d'IPv6 pour pouvoir associer une adresse IP à chaque terminal mobile dans le futur, en revanche l'adoption des fonctionnalités associées à IPv6 pour l'UMTS n'est pas établie. On peut donner 2 exemples :

- **L'UMTS release 5 préconise l'usage d'IPv6 end-to-end mais ne rend pas obligatoire l'usage de Mobile IPv6** (statut à octobre 2001). Toutefois l'usage de Mobile IPv6 n'est pas exclu et est à l'étude au sein de 3GPP.
- Alors qu'IPv6 doit utiliser IPSEC pour la sécurité, l'UMTS release 5 n'a pas encore accepté ce protocole de sécurisation, pour cause d'incompatibilité avec certains aspects du standard UMTS (au niveau de la compression de l'entête IP, préconisée par 3GPP et incompatible avec IPSEC).

Or, tel que définie par l'IETF, une implémentation IPv6 doit supporter Mobile IPv6 et IPSEC.

Ainsi, à ce jour, il semble que l'utilisation d'IPv6 prévue dans les réseaux cellulaires UMTS reste encore très restrictive, notamment dans le domaine de la mobilité. De plus, l'implémentation effective d'UMTS release 5 n'est envisageable qu'à partir de 2004/2005. Ainsi, à court et moyen terme, la gestion de la mobilité dans les réseaux cellulaires va continuer à utiliser les procédures définies dans le GPRS (handover et encapsulation par GTP). L'utilisation de Mobile IP peut être contournée pour la gestion de la mobilité dans un réseau cellulaire, en revanche, elle semble incontournable pour permettre de gérer la mobilité entre des réseaux hétérogènes (cellulaire et WLAN par exemple).

Résumé de l'intérêt de l'utilisation de Mobile IPv6 dans les réseaux cellulaires :

- Support de la mobilité multi-accès (WLAN, cellulaire, Bluetooth), tout en conservant une adresse IP unique
- Amélioration du routage lors du roaming dans un réseau et de l'utilisation de services locaux
- Possibilité d'utilisation de la même adresse IP lors de l'utilisation d'un GGSN différent pour un service spécifique

3.4.1.8 Synthèse

Résumé des éléments essentiels portant sur la gestion de la mobilité dans les réseaux cellulaires :

- Le GPRS et l'UMTS (release 99 et release 4) utilisent le protocole GTP pour la gestion de la mobilité dans le réseau cœur (macro-mobilité), à l'interface entre le GGSN et le SGSN
- La gestion de la micro-mobilité (notamment le handover) est gérée par des protocoles spécifiques du réseau d'accès radio et du SGSN.
- Le protocole GTP est similaire en termes de fonctionnalités par rapport à Mobile IP mais a été défini de façon à parfaitement s'intégrer dans l'environnement du réseau cellulaire. En revanche il ne peut pas gérer la mobilité vers des réseaux avec d'autres technologies.
- À partir de la release 5 de l'UMTS, IPv6 est obligatoire de bout en bout, le but principal étant de pouvoir disposer d'une adresse IP unique par terminal mobile
- En revanche l'adoption de Mobile IPv6 dans les réseaux cellulaires est encore à l'étude par 3GPP. Mobile IPv4 ne devrait pas pour sa part être intégré dans les réseaux mobiles au profit de GTP.
- La mobilité entre réseaux de technologie différente (WLAN, …) requiert l'adoption de Mobile IP

3.4.1.9 Note sur ENUM

Le protocole ENUM n'est pas spécifiquement lié à la mobilité, toutefois, il permet (entre autres) d'associer, à une adresse IP, un identifiant unique en numérotation E.164. Cet identifiant peut être utilisé comme identifiant, tout comme l'adresse d'un terminal dans le « réseau maison ». La plupart des avis sur ENUM sont relativement neutres, mais concordent sur un point : l'impact sur IP est non significatif, et les évolutions des deux protocoles seront parallèles, mais pas croisées. Ainsi, on peut penser qu'ENUM pourrait trouver une légitimité grâce notamment à la mobilité. Cette question reste ouverte.

On peut signaler que l'UIT procède actuellement à l'élaboration des principes et des procédures d'administration du protocole. L'approbation des textes régissant la mise en application du protocole ne devrait pas intervenir avant novembre 2002.

3.5 Sécurisation

Alors que la sécurité est optionnelle dans IPv4, elle est native et par défaut dans IPv6, avec l'intégration en natif du protocole IPSec.

Le fait que la grande quantité d'adresses disponibles permette d'éviter un recours aux NATs et autres artifices permet également d'accroître le niveau global de sécurité.

3.6 Gestion de la QoS et différentiation des types de flux

IPv6 est prévu pour différencier les flux de données et gérer la QoS.

3.6.1 Apports de l'étude ART

Les spécifications d'IPv6 sont contenues dans la note RFC 2460. Nous allons donc ici inventorier les spécifications d'IPv6 répondant à des critères de QoS. Les détails de ces améliorations sont contenus dans la RFC 2460 (nous procédons ici à une synthèse)

- **Simplification du format de l'en-tête :**

Certains champs de l'en-tête IPv4 ont été enlevés ou rendus optionnels, pour réduire dans les situations classiques le coût (en ressources de traitement) de la gestion des paquets et pour limiter le surcoût en bande passante de l'en-tête IPv6.

- **Support amélioré des options et des extensions futures :**

Des changements dans la façon dont les options de l'en-tête IP sont encodés permettent une transmission (forwarding) plus efficace, des limites moins strictes sur la longueur des options et une plus grande flexibilité dans l'introduction par la suite de nouvelles options.

- **Fonctionnalité d'étiquetage de flux d'informations :**

Une nouvelle fonctionnalité est ajoutée pour étiqueter des paquets appartenant à des « flux » d'informations particuliers pour lesquels l'émetteur demande une gestion spéciale, comme un service « sans perte d'information » ou un service « temps réel ».

- **Dans le processus de routage :**

À part une exception, les en-têtes d'extension ne sont pas examinés ou traités par un quelconque nœud le long du chemin emprunté par le paquet (packet's delivery path), jusqu'à ce que le paquet atteigne le nœud (ou l'ensemble de nœuds, dans le cas du multicasting) identifié par le champ " Adresse Destination " de l'en-tête IPv6.

L'exception à laquelle fait allusion le précédent paragraphe est l'en-tête des options sauts après sauts (Hop-by-Hop Options Header), qui transporte les options qui doivent être examinées et traitées par chaque nœud le long du chemin emprunté par le paquet, incluant les nœuds source et destination.

- **Problème de la longueur des paquets[88] :**

[88] paquet (packet) : un en-tête IPv6 avec sa « charge utile » (ce qu'il transporte).

IPv6 exige que chaque lien inter-réseaux ait un MTU[89] supérieur ou égal à 1280 octets. Sur tout lien qui ne peut pas transporter un paquet de 1280 octet en un seul morceau, les services de fragmentation et d'assemblage spécifique au lien doivent être fournis par la couche en-dessous d'IPv6.

Cette fonctionnalité permet d'homogénéiser et de rendre plus efficace la transmission des paquets sur le réseau.

- **Labels relatifs aux flux[90] d'informations :**

Le champ Label du Flux sur 20 bits dans l'en-tête IPv6 peut être utilisé par une source pour nommer des séquences de paquets pour lesquels un traitement spécial de la part des routeurs IPv6 est demandé. Ce traitement spécial pourrait être une qualité de service différente du service par défaut ou un service « temps réel ».

- **Classes de trafic :**

Le champ Classe du Trafic sur 8 bits dans l'en-tête IPv6 a été créé pour être utilisé par des nœuds origines et/ou des routeurs transmetteurs pour identifier et distinguer différentes classes ou priorités de paquets IPv6.

- **Durée de vie maximale d'un paquet :**

Contrairement à IPv4, les nœuds IPv6 ne sont pas obligés d'imposer un temps de vie maximum des paquets. On peut ainsi envisager une réduction des pertes d'information du fait d'une absence de paquets jetés à la fin de leur durée de vie.

La QoS passant également par la gestion de la sécurité, on peut ajouter que des extensions prévues pour gérer l'authentification, l'intégrité des données ou une (optionnelle) confidentialité de celles-ci sont spécifiées pour IPv6.

Tableau 9 : Synthèse des critères de QoS et des apports d'IPv6 par rapport aux solutions IPv4

Critère de QoS	Apport d'IPv6	Solutions IPv4
Délai	Simplification du format de l'en-tête Support amélioré des options et extensions Fonctionnalité d'étiquetage du flux d'informations, label des flux Amélioration du processus de routage	Modification de l'en-tête du paquet par chaque routeur d'accès pour indiquer le niveau de service Définition d'un flux à travers une suite de routeurs et marquage des paquets en tant que composant de ce flux WRED, WFQ
Gigue	Support amélioré des options et extensions Amélioration du processus de routage	Gestion des files d'attente Trafic Shaping
Bande passante	Simplification du format de l'en-tête Longueur des paquets Classes de trafic	Trafic Shaping Techniques de prévention de la congestion RSVP

[89] MTU de lien (link MTU) : l'unité maximum de transmission (Maximum Transmission Unit), i.e., la taille maximale en octets d'un paquet qui peut être transmis sur le lien.
MTU de chemin (path MTU) : le plus petit MTU de lien de l'ensemble des liens constituant le chemin entre le nœud source et le nœud destination.

[90] Un flux est une séquence de paquets envoyée par une source particulière vers une destination particulière (unicast ou multicast) pour lequel la source désire un traitement spécial de la part des routeurs intermédiaires. La nature de ce traitement spécial pourrait être communiquée aux routeurs par un protocole de contrôle, tel qu'un protocole de réservation de ressources, ou par des informations à l'intérieur même des paquets du flux, par exemple, dans une option sauts après sauts.

Critère de QoS	Apport d'IPv6	Solutions IPv4
Disponibilité	Fonctionnalité d'étiquetage du flux d'informations, label des flux Classes de trafic Durée de vie maximale d'un paquet Gestion de la sécurité	RSVP IPSec et autres Modification de l'en-tête du paquet par chaque routeur d'accès pour indiquer le niveau de service

Source : IDATE

3.6.1.1 Compléments d'information sur les apports d'IPv6 et la QoS

3.6.1.1.1 Apports d'IPv6 pour la VoIP (et autres applications temps réel) :

Outre le fait que les communications IP sont possibles en mode end-to-end, grâce à l'abondance des adresses IP, IPv6 permet, grâce à sa propension à l'amélioration de la QoS, d'améliorer la performance de la VoIP.

- le mode end-to-end permet de communiquer entre deux terminaux IP, directement reliés au réseau IP sans passer par le réseau commuté pour aboutir sur un téléphone standard, ni sans transiter par un ordinateur qui transformera les paquets IP en voix : les terminaux sont des « téléphones IP », qui transforment la voix en paquets de données et inversement, et sont directement connectés comme des nœuds du réseau. C'est dans ce contexte que peut apparaître l'utilité d'ENUM ou d'un protocole comparable

IPv6 permet, nous venons de le voir, de fixer des priorités pour certains paquets de données, et plus généralement, de classer les flux et d'améliorer la fluidité du trafic. **Cette propriété est de façon évidente un réel apport pour la qualité des applications temps réel**, comme la VoIP, la Vidéo sur IP, etc.

4 Avancement du déploiement d'IPv6 dans les différentes zones géographiques

4.1 Impact sur les politiques commerciales des acteurs IP et nouvelles applications

Ce sont les fournisseurs de services qui, en proposant une offre alléchante basée sur les avantages d'IPv6, devraient permettre de susciter la demande qui motivera opérateurs et ISP à développer leurs offres commerciales. Aujourd'hui, les équipementiers, conscients de ce fait, se tiennent prêts à répondre à la demande avec des produits, parfois non finalisés, mais globalement disponibles. Le Japon est globalement en avance sur l'Europe, et les américains rattrapent aujourd'hui rapidement leur retard.

4.1.1 Équipementiers

Les américains, leaders du marché dans le domaine d'IPv4 semblaient un temps distancés par les Européens, et surtout par les Japonais dans la course à IPv6. En effet, peut-être du fait du stock important d'adresse dont dispose la zone américaine, les acteurs « locaux » ne semblaient pas s'inquiéter de la pénurie qui menace. Aujourd'hui, l'ensemble des équipementiers d'outre atlantique semble avoir pris conscience des enjeux liés à IPv6 et des nouveaux marchés qui s'ouvrent en Asie-Pacifique : tous proposent une gamme IPv6, en général en phase d'upgrade logiciel, mais proposent également les services commerciaux correspondants. Ainsi, la zone américaine semble combler son retard, notamment par rapport à **l'Europe**, qui avait pourtant pris conscience des enjeux d'IPv6 bien avant l'Amérique, notamment au travers d'acteurs comme Ericsson (premier routeur IPv6 en 1996 avec Telebit), Nokia, ou 6Wind, un spin off de Thomson qui produit des routeurs IPv6.

Les Japonais, profitant notamment de l'initiative WIDE sont en tête de la course, et proposent déjà des gammes complètes de produits destinés à IPv6 (routeurs). En outre, la structuration du consortium WIDE et de l'industrie nippone en général leur permet de déjà penser au marché du grand public et aux applications futures (électronique connectée). En outre, l'Asie-Pacifique, leur marché « naturel et domestique » présente un énorme potentiel de croissance, auquel répond parfaitement IPv6 et que le Japon semble décidé à exploiter.

En ce qui concerne les OS, si la plupart des UNIX sont aujourd'hui capables de supporter IPv6, et que Windows XP est censé également disposer d'une gestion du nouveau protocole, celui-ci n'est pas prévu par défaut dans l'OS leader du marché. Une décision de **Microsoft** allant dans ce sens pourrait jouer le rôle de déclencheur d'une phase d'accélération du passage à IPv6.

4.1.2 Opérateurs

En Europe, France Telecom et BT travaillent activement sur IPv6, mais en sont encore à l'état de la R&D (même si FT, par l'intermédiaire de sa filiale Wanadoo Belgique, propose un service IPv6 reposant sur du 6to4).

En Suède Telia propose depuis juin 2001 un service commercial IPv6. En revanche, les autres grands opérateurs Européens restent attentistes et adoptent une position de suiveurs. Les opérateurs historiques sont les plus privilégiés quant au développement d'IPv6, car ils sont a priori les seuls à disposer d'une capacité de R&D suffisante. Les opérateurs alternatifs se placent systématiquement en suiveurs.

Cette règle connaît une exception aux **États-Unis**, où Zama Networks, créé en 1998, se positionne comme un opérateur de réseaux IPv6 natifs, les autres opérateurs américains ne communiquant pas sur le sujet, peut-être du fait de leur vision rassurante d'un monde IPv4 qu'ils contrôlent largement, ne pressentant pas la pénurie. Sa cible est explicitement la zone Asie-Pacifique. Cette zone est par ailleurs la cible des opérateurs **Japonais** : NTT et IIJ proposent des services commerciaux IPv6 (mais les capacités très restreintes amènent à considérer ces réseaux comme des réseaux de test de commercialisation plus que des réseaux commerciaux à part entière), et Matsushita propose depuis peu un service d'ISP IPv6.

4.1.3 ISP

Au Japon, NTT, IIJ et Matsushita proposent donc des offres d'ISP IPv6, comme Wanadoo Belgique (à l'aide d'un 6to4), Telia, et Zama. Toutefois, les offres sont extrêmement rares, et les ISP semblent à ce jour en position d'attente.

4.1.4 Applications

Parmi les applications qui seront des moteurs d'IPv6, on peut distinguer :

- Les applications nomades, gourmandes en adresses, et notamment, à terme, les terminaux UMTS
- Les applications domotiques
- La VoIP
- Les applications ayant un besoin accru en sécurité
- Les réseaux de capteurs

4.1.5 Utilisateurs

Les utilisateurs adoptent une position attentiste face à IPv6, se souciant plus de la qualité des prestations qui leurs sont offertes que des éléments techniques sous-jacents.

4.1.6 Nouveaux entrants

Les équipementiers grand public, les constructeurs automobiles, les éditeurs de jeux vidéo semblent particulièrement concernés par IPv6, de par la nature des innovations qu'ils présentent : les apports du nouveau protocole en termes de sécurité, de gestion de la mobilité, d'auto configuration sont des éléments essentiels au développement de leurs nouvelles applications.

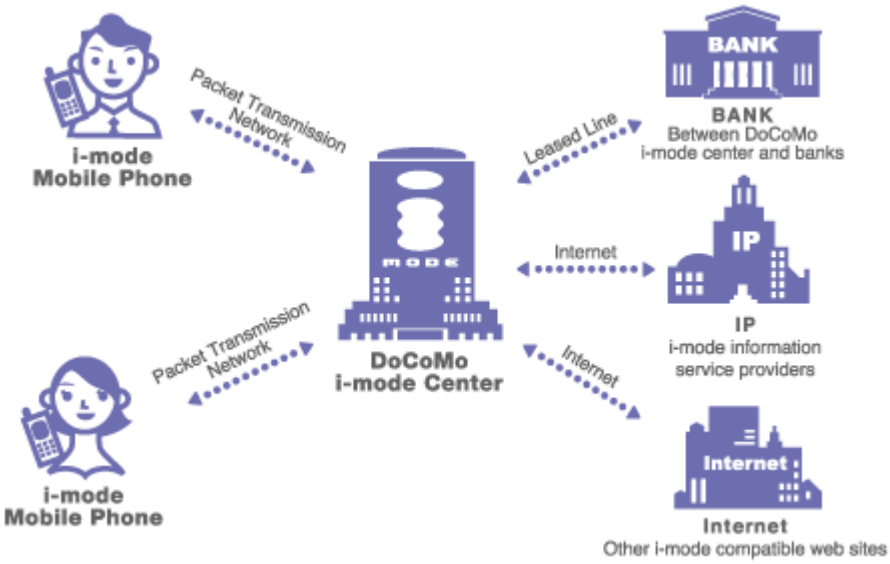
5 Les enseignements de l'i-mode

L'enjeu de cette note est de mieux comprendre la manière dont l'i-mode fonctionne et d'éclaircir en particulier la manière dont la signalisation et l'adressage IP est réalisé.

L'i-mode utilise un réseau de communication de paquets, qui fonctionne sur la même fréquence que la norme de la téléphonie cellulaire PDC (*Personnal Digital Cellular*), soit 800Hz et dont le débit maximal est le même que celui du GSM, soit 9,6 kbps.

La particularité consiste dans le fait que toutes les communications transitent par le centre NTT DoCoMo. À cet endroit se trouvent deux bases de données. La première contient les informations relatives aux abonnés, la seconde est utilisée pour la facturation. La Figure 17 montre la structure de l'accès Internet mobile avec i-mode. Comme dans le cas de GPRS, le réseau de transmissions par paquets est séparé de celui de la voix. Le réseau paquet en overlay est appelé PDC-P (*Personnal Digital Cellular-Packet*). Dans l'architecture i-mode, l'équipement réseau chargé de séparer les réseaux en mode circuit et mode paquet est appelé M-SCP (*Mobile Service Control Point*).

Figure 17 : Structure haut-niveau du système i-mode

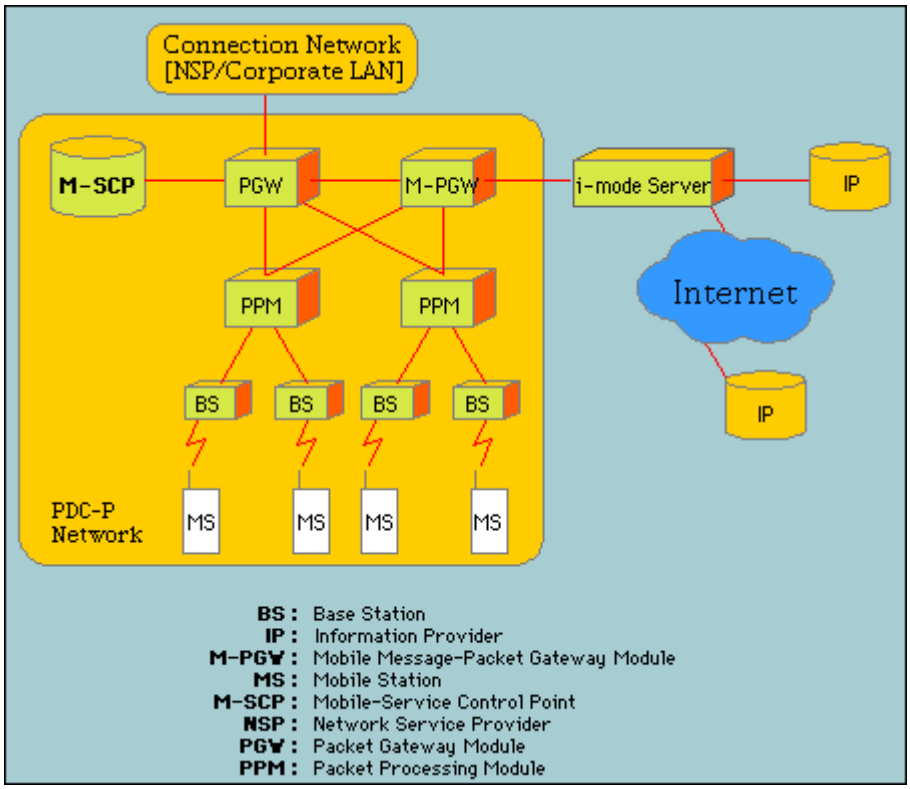


Source : NTT DoCoMo

Les équipements réseaux mis en jeu dans le réseau PDC-P sont représentés sur la Figure 18. Les éléments de réseaux sont le PPM (Packet Processing Module) et le M-PGW (Mobile message-Packet Processing Module) :

- les PPM fournissent le passage entre l'interface radio et le cœur de réseau de l'opérateur.
- le M-PGW procure le passage du réseau privé vers Internet ou des lignes sécurisées vers des serveurs spécialisés.

Figure 18 : Configuration du réseau PDC-P (réseau overlay du réseau PDC)



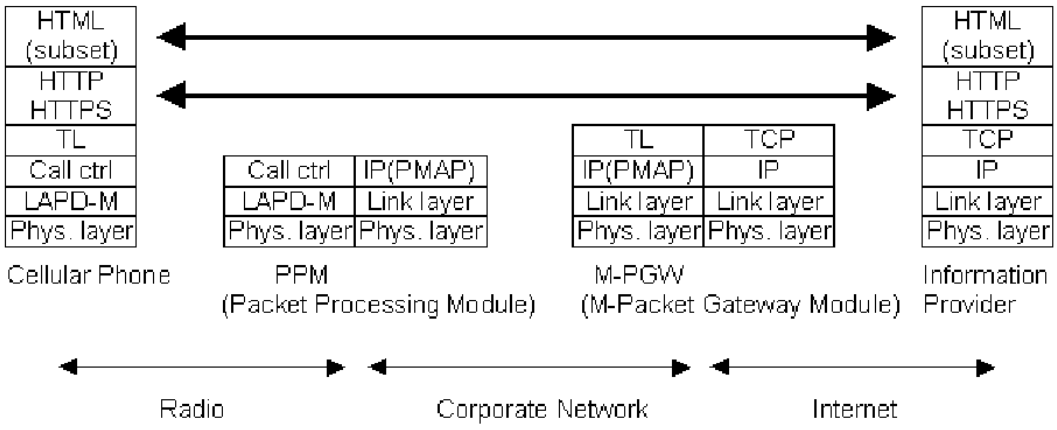
Source : NTT DoCoMo

La Figure 19 montre une représentation en couches des protocoles mis en jeu dans l'i-mode. Chaque terminal compatible i-mode possède un navigateur permettant l'accès au Web, qui utilise le langage c-HTML, langage dérivé du HTML. La transmission des pages utilise les protocoles classiques HTTP et HTTPS (dans le cas d'envois de données confidentielles comme les transactions bancaires).

La passerelle M-PGW entre le monde Internet et le réseau PDC-P convertit le protocole TCP en un protocole de transport propriétaire, le TLP (*Transport Layer Protocol*). Au niveau de la couche réseau, IP est utilisé pour transporter les données dans le cœur de réseau.

Les terminaux disposent d'adresses IP provenant de classes privées. La passerelle M-PGW met en place un dispositif basé sur le NAT (*Network Addresses Translation*). Ce mécanisme a pour but de substituer l'IP de destination du paquet par celle d'une adresse machine du réseau interne.

Figure 19 : Protocoles mis en jeu avec l'i-mode lors de la transmission de données



Source : NTT DoCoMo

Conclusion et synthèse sur l'adressage IP

Les terminaux i-mode ne sont pas pour l'instant munis d'adresses IP permanentes. L'adresse IPv4 est une adresse privée déterminée par le système d'adressage NAT. L'adresse est déterminée lors de la demande de connexion data du terminal i-mode puis est relâché lorsque la connexion est terminée.

Les abonnés i-mode sur le réseau PDC-P ne bénéficient pas d'une connexion permanente (always-on) mais d'une connexion à la demande, ce qui permet de libérer les ressources lorsque les terminaux sont inactifs. Cette situation devrait évoluer avec l'arrivée de la 3G avec la fourniture d'une véritable connexion data permanente. Dans cette perspective, IPv6 devrait être la solution utilisée par DoCoMo pour fournir une adresse IP unique à chaque terminal.

Dans le cas d'applications en mode « push », le mobile est d'abord appelé par le PPM pour que la connexion s'établisse puis la réception de données peut s'effectuer.

Le système actuel permet à DoCoMo de gérer l'adressage de plus de 30 millions d'abonnés i-mode. Selon DoCoMo, cette solution avec IPv4 et NAT est satisfaisante et n'occasionne pas de problèmes majeurs.

6 Commission Européenne et IPv6

Synthèse Communication IPv6
Task Force Mobile Wireless WG (1/3)

- **Choix d'une version du protocole IP :**

➢ **Les standards GPRS et UMTS permettent le choix entre v4 et v6➢ GPRS :**

• Tous les réseaux GPRS utilisent aujourd'hui IPv4. Dans le futur, certains opérateurs pourraient déployer IPv6

• Des équipements compatibles IPv6 ont été annoncés mais la réelle disponibilité de produits (même expérimentaux) n'est pas avant 2002

➢ **UMTS**

• release 99 et release 4 : Situation équivalente au GPRS mais avec plus de déploiements optionnels d'IPv6 attendus

• release 5 : Obligations d'utiliser IPv6 dans les réseaux et les terminaux, mais seulement pour l'IMS (IP Multimedia Subsystem)

- **Trois éléments déclencheurs :**

1) Le respect des standards pour lesquels IPv6 est obligatoire (à partir des fonctionnalités IP Multimedia)

2) Éviter les problèmes dus au manque d'adresses IP

3) Bénéficier des nouvelles fonctionnalités offertes par IPv6

Synthèse Communication IPv6 Task Force Mobile Wireless WG (2/3)

Phase	Cœur de réseau (SGSN, GGSN, …)	Terminaux et services	Eléments de réseaux pour le multimédia IP
GPRS release 98	IPv4	IPv4 ou IPv6	En pratique, ce sera IPv4; IPv6 optionnel
UMTS release 99 et 4	IPv4, IPv6 optionnel	IPv4 ou IPv6	En pratique, ce sera IPv4; IPv6 optionnel
UMTS release 5	Non décidé	A priori, identique à la release 99	IPv4 et IPv6 (IPv6 exclusivement pour IP Multimedia)	IPv6 exclusivement

- **Pour le réseau cœur, avant Release 5, le problème principal est le support de GTP (GPRS Tunnelling Protocol)**

Synthèse Communication IPv6 Task Force Mobile Wireless WG (3/3)

- **Recommandations (extraits)**

➢ La Commission Européenne doit s'assurer que les adresses IPv6 soient rendues disponibles à tous les secteurs de l'industrie, y compris les opérateurs UMTS, en nombre suffisant et à des prix raisonnables.

➢ Afin de mettre en place IP Multimedia (release 5) en 2003-2004, les industriels sont invités à soumettre des contributions à 3GPP pour accélérer les travaux de spécifications sur IPv6 pour l'UMTS.
(Release 5 est censée être achevée par 3GPP en mars 2002, avec quelques fonctionnalités repoussées à Octobre 2002. Toute déviation par rapport au plan repoussera des fonctionnalités à de futures releases)

➢ Les spécifications 3GPP dépendent fortement d'autres groupes (ex: IETF). La Task Force doit vérifier que les spécifications de 3GPP et les Drafts RFCs répondent aux objectifs des opérateurs et de l'IP Multimedia Subsystem

➢ Au plus tard en 2004-2005, les opérateurs auront déployé IPv6 dans leur réseau pour IP Multimedia. La Task Force devrait recommander une stratégie technique pour réaliser ceci sur la base de critères précis (marchés, coûts, …).

Synthèse Communication IPv6 Task Force
Points clés

- **Un discours volontariste et optimiste sous l'angle de la mobilité**

- **Date critique avancée pour l'adoption d'IPv6 : 2005**

- **Des recommandations visant :**

➢ **Les états membres :**

Exemplarité sur les réseaux publics, Programmes éducatifs, Promotions d'IPv6 (ISP, opérateurs, PME, consommateurs), Soutien financier des réseaux académiques pour IPv6, mettre en place un comité national IPv6,…

➢ **Des actions complémentaires de la Commission (6ème PCRD) :**

• Recentrer le 6ème PCRD sur les sujets : IPv6 et accès haut débit, interopérabilité, équipements IPv6, test à grande échelle, production d'un code ouvert source européen IPv6, …

• Renouveler et élargir la Task Force aux industriels et organismes de standardisation

➢ **Les industriels :**

• Participation au 6ème PCRD sous l'angle IPv6, intégration d'IPv6 dans leurs plans stratégiques, participations actives aux standards, veiller à l'interopérabilité des équipements,…

- **Les recommandations de la Task Force seront abordées lors du Conseil européen de Barcelone les 15 et 16 mars 2002**

7 La composition et la mission des différents intervenants dans la définition de la politique IPv6

- **L'IETF (Internet Engineering Task Force)** assisté par l'IAB (Internet Architecture Board) organise le consensus de la communauté mondiale des chercheurs et des développeurs avec le soutien financier des industries concernées.
  Cette organisation, qui n'a pas de personnalité juridique, édicte de facto l'ensemble des protocoles qui assure l'interopérabilité des usages Internet.
  Le travail technique de L'IETF est effectué dans le cadre des groupes de travail organisés en fonction de différents sujets et par le biais des listes de mailing. C'est dans le cadre d'un de ces groupes de travail que la politique d'IPv6 a été conçue.
  Le rôle de l'IETF a été prépondérant dans le processus d'élaboration des spécifications du nouveau protocole par voie de RFC mis en ligne sur le site de l'IETF.[91] Il a d'abord fait publier un livre blanc (RFC 1550)[92] pour définir les fonctionnalités du nouvel IP. À l'issue d'un travail d'analyse et de débats, les critères techniques pour choisir le nouveau protocole (RFC 1726)[93] ont été publiés.

  Les documents préparés essentiellement par l'IETF ont, par la suite, été soumis à l'appréciation des trois RIR.

- **Les RIR (Regional Internet Registry)** sont les organismes chargés de l'allocation des préfixes IPv6 de haut niveau dans leurs régions respectives.
  C'est dans le cadre de ces trois RIR (APNIC[94], ARIN[95], RIPE NCC[96]) et avec l'étroite collaboration de leurs communautés d'Internet qu'a été développé le « Provisional IPv6 Assignment and Allocation policy document » de 1999. Les discussions relatives au projet de révision de la politique d'adressage ont eu lieu dans le cadre des réunions, des groupes de travail et des forums sur Internet, au sein des RIR. Ce projet, suite à diverses modifications opérées par les RIR, a été soumis à l'IANA[97] qui l'a approuvé le 14 juillet 1999.
  En Europe, le RIPE compétent est une association de droit néerlandais.

- **L'IANA (Internet Assigned Numbers Authority)**[98] est l'autorité, à l'origine, responsable de la surveillance et de la gestion du protocole d'allocation, de coordination et d'attribution des adresses IP. Aujourd'hui la majorité de ses missions a été transférée à l'ICANN[99]. Toutefois et sous la responsabilité de ce dernier, l'IANA continue à coordonner les activités techniques de l'IETF et à distribuer les adresses aux RIR, et ce jusqu'à la mise en œuvre de l'accord formalisant les relations entre l'ICANN et les RIR, actuellement en projet.

- **ICANN (The Internet Corporation For Assigned Names and Numbers)**

91 http://www.ietf.org/.
92 http://faqs.org/rfcs/rfc1550.html.
93 http://faqs.org/rfcs/rfc1726.html.
94 http://www.apnic.net.
95 http://www.arin.net.
96 http://www.ripe.net/ripencc/.
97 Les nouvelles compétences de l'ICANN et de l'ASO sont devenues effectives en octobre 1999.
98 htpp://www.iana.org/
99 IETF/ICANN Memorandum of Understanding Concerning the technical work of the IANA : http://www .icann.org/general/ietf-icann-mou-01mar00.htm

La nature juridique et les missions de l'ICANN

L'ICANN est une société de droit privé à but non lucratif et d'intérêt public, dont le siège est à Los Angeles, California. Les fonctions exercées par l'ICANN lui ont été déléguées par le gouvernement américain au terme d'un accord dit transitoire.[100]

L'ICANN a été créé en 1998 et a pour vocation première de servir l'intérêt commun en assurant la stabilité opérationnelle de l'Internet[101]. D'après ses statuts[102], sa mission, surtout à l'égard des IP, consiste à :

- Coordonner les différents éléments techniques de l'Internet de manière à préserver la connectivité universelle au Réseau des Réseaux ;
- Assurer et superviser les tâches liées à l'attribution et au fonctionnement des adresses sur le protocole d'Internet ("adresses IP") ;
- Engager toutes actions juridiques nécessaires à l'accomplissement des missions précédentes.

Les tâches confiées à ICANN sont celles où une coordination et des choix centralisés s'imposent soit en raison du caractère globalement unique de certains éléments (adresses IP) soit pour assurer l'interopérabilité générale du système (protocoles).

Les principales composantes de l'ICANN jouant un rôle dans la mise en place de la politique IPv6

- **Le conseil d'administration**[103] est l'organe principal de l'ICANN composé de 19 administrateurs qui doivent refléter la communauté mondiale et les différents milieux concernés par l'Internet. Neuf de ces membres sont élus par les trois organisations de support de l'ICANN (DNSO, ASO (Address Council), PSO) qui représentent les milieux économiques, techniques, non commerciaux et universitaires, neuf autres administrateurs at-large, représentant les utilisateurs, sont désignés au terme d'une procédure de scrutin électronique mondial.

  Les décisions de l'ICANN sont prises par le conseil d'administration ou sous sa direction. Le mécanisme de prise de décision par l'ICANN est destiné à assurer le consensus et la représentation de la communauté d'Internet.

  Les normes, politiques, procédures ou pratiques sont élaborées selon un processus bottom-up au sein de l'ICANN. Ces normes ne sont ensuite adoptées par le conseil d'administration de l'ICANN que s'il y a consensus[104].

  L'ICANN délègue toute question à propos de laquelle une politique doit être élaborée au comité d'une des trois Supporting Organisations qui est invité à préparer des propositions. L'ICANN publie largement ses propositions sur son site Web, invite à des prises de position et organise ses auditions. Compte tenu des résultats de la consultation effectuée pour chaque proposition, le comité compétent soumet une recommandation à l'ICANN qui fait état du consensus existant ou non sur chaque point. Le conseil d'administration décide sur cette base de l'adoption ou non de la politique proposée.

[100] Memorandum of Understanding between ICANN and US department of Commerce du 25 novembre 1998.
[101] Articles Of Incorporation du 21 novembre 1998, article 3 : htpp://www.icann.org/general/articles.htm.
[102] Articles Of Incorporation du 21 novembre 1998, article 3 .
[103] By-laws de l'ICANN, article V : http://icann.org/general/bylaws.htm.
[104] ICANN Bylaws Article 4 : http://www.icann.org/general/bylaws.htm.

- **L'ASO (Address Supporting Organisation)**[105] : Le Memorandum of Understanding du 18 octobre 1999[106] signé entre les trois RIR et l'ICANN prévoit la création de l'ASO comme une organisation de support de l'ICANN. Sa mission est d'examiner et de développer les recommandations relatives à la politique d'adresse IP ainsi que de conseiller l'ICANN sur ces recommandations[107].

  L'ASO dispose d'une sous-organisation appelée Address Council constitué de neuf membres élus par les RIR (trois par RIR) et chargé d'administrer l'ASO[108]. Les missions de l'ASO relatives à la politique d'adresses sont exercées au sein de ce conseil.

- **Le GAC (Government Advisory Committee)**[109] est un comité consultatif composé des représentants des gouvernements nationaux, des organisations gouvernementales multinationales. Ce comité a pour mission de conseiller le conseil d'administration de l'ICANN sur les objectifs de politique publique et de la communauté internationale des États[110]. Il fonctionne comme un forum de discussion des intérêts des gouvernements et des consommateurs.

105 www.aso.icann.org
106 www.aso.icann.org/docs/aso-mou.html
107 Point 4 du MOU du 18 octobre 1999
108 Point 2 et 4 du MoU de l'ASO : www.aso.icann.org/docs/aso-mou.html
109 http://www.noie.gov.au/Projects/international/DNS/gac/index.htm
110 Les Principes de Fonctionnement, article 1er : http://www.noie.gov.au/Projects/international/DNS/gac/Operating_Principles-French .htm

8 Le processus d'adoption des politiques IPv6

Les étapes chronologiques

- Les protocoles IPv6 ont été préparés par IETF en 1998 : IETF Draft Standard du 10 août 1998[111] et soumis à l'approbation de l'IANA ;
- Le « Provisional IPv6 Assignment and Allocation Policy Document » a été approuvé, le 14 juillet 1999, par l'IANA et publié le 20 juillet 1999 ;
- Les réunions de l'ASO[112] le 19 mai 2000, le 4 avril 2001 et le 5 mars 2002 ont concerné le « IPv6 Address Allocation and Assignment Global Policy » ;
- Réunions de l'APNIC en août 2001, de RIPE et de l'ARIN en octobre 2001 relatives aux politiques d'IPv6 : au cours de ces réunions un consensus a été obtenu sur la nécessité d'adopter une nouvelle politique d'IPv6 ;
- Diffusion du projet de « IPv6 Address Allocation and Assignment Global Policy » le 22 décembre 2001 ;
- Suite aux discussions du projet du 22 décembre 2001 au sein des trois RIR, un nouveau projet de politique IPv6 en date du 25 avril 2002 a été mis en ligne le 23 mai 2002 par les trois RIR;
- En application de l'article 4 des statuts de l'ASO, le nouveau projet du 22 décembre 2001, suite aux modifications apportées par les RIR, va être transféré à l'Address Council de l'ASO pour examen puis au conseil d'administration de l'ICANN pour adoption. Toutefois, nous n'avons pas d'indication sur le calendrier de l'adoption du projet en vue de sa transmission à l'ASO et à l'ICANN.

Les étapes théoriques du nouveau processus d'adoption

Ces étapes sont déterminées par les statuts du RIPE NCC, de l'ICANN et le Memorandum of Understanding de l'ASO.

Selon les dispositions de l'article 4 du Memorandum of Understanding de l'ASO du 18 octobre 1999, les propositions de politiques globales (comme « IPv6 Address Allocation and Assignment Global Policy ») sont développées dans le cadre des RIR et transmis à l'Address Council de l'ASO[113] pour examen.

La transmission du RIPE à l'ASO suppose une décision de l'Assemblée Générale[114].

Au sein de cette Assemblée Générale, les décisions sont prises à la majorité des voix. Toutefois, le nombre des voix des membres (les « Internet Registry ») de l'Assemblée Générale est fonction du nombre des allocations détenues par les différents IR :

- Petits IR = 1 voix
- Moyens IR = 2 voix
- Grands IR = 3 voix

111 http://playground.sun.com/pub/ipng/html/ipng-DS.txt.
112 http://www.aso.icann.org/meetings/.
113 Dans certains cas, l'Address Council de l'ASO peut être saisi par l'ICANN, voire accepter d'examiner des propositions spontanées de tout intéressé.
114 Selon les statuts de RIPE NCC, l'Assemblée Générale est compétente pour discuter et mettre en place la politique d'adressage. Les membres de l'Assemblée Générale sont les entités qui ont conclu un « RIPE NCC Service Agreement ».

Une telle répartition des voix en fonction de la taille des IR donne **aux grands IR un poids particulier, mais pas nécessairement déterminant,** dans le processus d'adoption[115].

Dans tous les cas, lorsque l'Address Council examine les propositions de nouvelles politiques globales ou de modification des politiques existantes, il sollicite, en premier lieu, l'opinion des trois RIR et du public. L'Address Council prend en considération ces opinions pour décider de l'approbation de la proposition en question.

Pour qu'une proposition puisse être acceptée et transmise au conseil d'administration de l'ICANN, il faut l'accord du 2/3 des membres (donc six membres) de l'Address Council.

Le conseil d'administration de l'ICANN doit ensuite, avant tout vote sur la proposition[116] :

- mettre en ligne une note publique (sur le Web Site de l'ICANN) qui explique les politiques à adopter et les raisons de cette adoption ;
- laisser une opportunité aux personnes intéressées par la proposition, pour présenter leurs commentaires sur l'adoption de la politique en question ;
- tenir un forum public dans le cadre duquel la politique proposée va être discuté.

Le conseil d'administration de l'ICANN[117] adopte les politiques à la majorité des voix[118].

[115] Il existe, à ce jour, approximativement 1.500 petits IR, 500 moyens IR et 100 grands IR.
[116] Article 3, section 3 des statuts de l'ICANN : htpp://www.icann.org/general/bylaws.htm.
[117] Composé de 19 membres.
[118] Article 4 des statuts de l'ICANN.

9 Les conditions requises pour accéder aux adresses IPv6

Comme nous l'avons précisé ci-dessus, les conditions prévues par le document RIPE 196 et par le nouveau projet de politique ne sont pas les mêmes. Par ailleurs, le document RIPE 196 prévoit des conditions différentes pour la période d'amorçage et pour la période de croisière.

La période d'amorçage semble presque terminée

Le document RIPE 196 indique que la condition relative aux accords de peering crée un problème pendant la durée initiale de transition au réseau d'adressage IPv6 et prévoit un mécanisme intérimaire d'éligibilité.

Selon le document susvisé, les RIR peuvent effectuer une allocation initiale d'adresses sub-TLA aux IR qui remplissent les critères (a) ET (b) ET (c) ou (d)

> (a) L'IR demandeur doit avoir des accords de peering avec au moins trois autres Systèmes Autonomes de la zone libre.
>
> ET
>
> (b) L'IR demandeur doit montrer (par plan d'architecture ou de déploiement) qu'il planifie de fournir un service IPv6 dans les 12 mois suivants la réception des adresses allouées.
>
> ET l'un des critères suivants :
>
> (c) L'IR demandeur doit être un fournisseur transit d'IPv4 et doit montrer qu'il a déjà 40 clients (usagers finaux) qui peuvent remplir le critère pour une attribution d'a /48. Dans ce cas, l'IR doit avoir une politique d'acheminement enregistrée dans une base de données de l'IRR (Internet Routing Registry).
>
> Ou
>
> (d) L'IR demandeur doit démontrer une expérience d'IPv6 par une participation d'au moins six mois au projet 6bone, au cours de laquelle il a exploité pendant trois mois un pseudo TLA.

En période de croisière :

- **Les critères prévus par le document RIPE 196**

Les critères prévus pour une allocation initiale de sub-TLA sont basés sur des considérations techniques et tendent à atteindre le but d'agrégation.

L'article 4.2.1 du document RIPE 196 prévoit que :

Les RIR vont uniquement allouer des sub-TLA adresses aux IR qui remplissent le critère (a) et au moins une partie du critère (b) :

> (a) Le réseau IPv6 de l'IR demandeur doit avoir des accords de peering avec le réseau d'au moins trois autres IR ayant bénéficié d'un sub-TLA.
>
> ET
>
> (b) L'IR doit avoir attribué des adresses IPv6 à au moins 40 usagers finaux de SLA qui ont des réseaux connectés par des liens permanents et semi-permanents.
>
> Ou
>
> (ii) L'IR demandeur doit justifier (par des documents comme plan d'architecture ou de déploiement) d'une intention claire pour fournir un service IPv6 dans les 12 mois suivants la réception des adresses qui lui sont allouées.

- **Les critères prévus par le projet du 22 décembre 2001**

Le projet en cours prévoit qu'un IR demandeur peut recevoir une allocation initiale en démontrant qu'il aura, dans les trois mois, une demande pour au moins un préfixe /36 (soit au moins 776 usagers finaux ayant besoin d'une attribution d'adresse IPv6). Ce chiffre de 776 usagers correspond à blocs d'adresses /48 qui peuvent être attribués en dehors de blocs d'adresses a /36 qui doivent atteindre un ratio HD[119] de 0.8.

Une discussion est ouverte sur le point de savoir si ce seuil est trop exigeant : lors de la réunion du RIPE (mai 2002), il aurait été ramené à deux cents usagers dans les deux ans.

Lorsque le demandeur a déjà une infrastructure IPv4, la base de clients IPv4 est prise en compte pour justifier des demandes d'allocation d'adresses IPv6.

[119] Un ratio HD est un système métrique d'utilisation proposé dans le RFC 3194.

Table des illustrations