MOOC

Objectif IPv6 !

vers l'internet nouvelle génération

Document Compagnon

Séquence 0

Internet

Licence Creative Nommons CC BY-SA 4.0 International

Attribution - Partage dans les Mêmes Conditions 4.0 International (CC BY-SA 4.0)

Avertissement Ce résumé n'indique que certaines des dispositions clé de la licence. Ce n'est pas une licence, il n'a pas de valeur juridique. Vous devez lire attentivement tous les termes et conditions de la licence avant d'utiliser le matériel licencié.

Creative Commons n'est pas un cabinet d'avocat et n'est pas un service de conseil juridique. Distribuer, afficher et faire un lien vers le résumé ou la licence ne constitue pas une relation client-avocat ou tout autre type de relation entre vous et Creative Commons.

Clause C'est un résumé (et non pas un substitut) de la licence.

http://creativecommons.org/licenses/by-sa/4.0/legalcode

Vous êtes autorisé à :

- **Partager** — copier, distribuer et communiquer le matériel par tous moyens et sous tous formats
- **Adapter** — remixer, transformer et créer à partir du matériel
- pour toute utilisation, y compris commerciale.

L'Offrant ne peut retirer les autorisations concédées par la licence tant que vous appliquez les termes de cette licence.

Selon les conditions suivantes :

Attribution — You must give **appropriate credit**, provide a link to the license, and **indicate if changes were made**. You may do so in any reasonable manner, but not in any way that suggests the licensor endorses you or your use.

Partage dans les Mêmes Conditions — Dans le cas où vous effectuez un remix, que vous transformez, ou créez à partir du matériel composant l'Oeuvre originale, vous devez diffuser l'Oeuvre modifiée dans les même conditions, c'est à dire avec **la même licence** avec laquelle l'Oeuvre originale a été diffusée.

No additional restrictions — Vous n'êtes pas autorisé à appliquer des conditions légales ou des **mesures techniques** qui restreindraient légalement autrui à utiliser l'Oeuvre dans les conditions décrites par la licence.

Notes: Vous n'êtes pas dans l'obligation de respecter la licence pour les éléments ou matériel appartenant au domaine public ou dans le cas où l'utilisation que vous souhaitez faire est couverte par une **exception.**

Aucune garantie n'est donnée. Il se peut que la licence ne vous donne pas toutes les permissions nécessaires pour votre utilisation. Par exemple, certains droits comme l**es droits moraux, le droit des données personnelles et le droit à l'image** sont susceptibles de limiter votre utilisation.

Les informations détaillées sont disponibles aux URL suivantes :

- http://creativecommons.org/licenses/by-sa/4.0/deed.fr
- http://fr.wikipedia.org/wiki/Creative_Commons

Les auteurs

Bruno Stévant

Bruno STEVANT est enseignant chercheur à l'IMT Atlantique. Il intervient dans l'enseignement et sur les projets de recherche autour d'IPv6 depuis plus de 10 ans. Il est secrétaire et responsable des activités de formation de l'association G6, association pour la promotion et le déploiement d'IPv6 en France.

Jacques Landru

Enseignant chercheur au CERI - Systèmes Numériques à l'IMT Nord Europe, Jacques est responsable de l'UV de spécialisation ARES (Architecture des RESeaux) à la fois dans le mode traditionnel présentiel que dans sa déclinaison à distance dans le cadre de la filière apprentissage.

Jean-Pierre Rioual

Ingénieur Conseil Réseaux – EURÊKOM. Fort de 30 années d'expérience dans le domaine des réseaux, il intervient auprès des entreprises pour des missions d'expertise sur leurs réseaux de transmission de données (intégration, mesures, optimisation, administration), conçoit et anime des actions de formation "réseaux".

Véronique Vèque

Véronique Vèque est Professeur des Universités à l'Université Paris-Saclay. Elle enseigne les réseaux depuis plus de 20 ans en Master Réseaux et Télécoms. Elle poursuit ses recherches au sein du L2S (Laboratoire des Signaux et Systèmes) où elle est responsable de l'équipe Réseaux, optimisation et codage. Elle est directrice-adjointe de l'école doctorale STIC de l'Université Paris-Saclay.

Pascal Anelli

Pascal ANELLI est enseignant-chercheur à l'Université de la Réunion. Il enseigne les réseaux depuis plus 20 ans. Il est membre du G6 depuis sa création. A ce titre, il est un des contributeurs du livre IPv6. En 1996, il a participé au développement d'une version de la pile IPv6 pour Linux.

Remerciements à :

- Vincent Lerouvillois, pour son travail de relecture attentive ;
- Joël GROUFFAUD (IUT de la Réunion) ;
- Pierre Ugo TOURNOUX (Université de la Réunion) ;
- Bruno Di Gennaro (Association G6) ;
- Bruno Joachim (Association G6) pour sa contribution à l'activité « Contrôler la configuration réseau par DHCPv6 » ;
- Richard Lorion (Université de la Réunion) pour sa contribution à l'activité « Etablir la connectivité IPv6 tunnels pour IPv6 ».

----- oOo -----

Tables des activités

Activité 01 : Qu'est ce que le réseau Internet ?

Internet et l'interconnexion de réseaux

Qu'est-ce que l'Internet ? Littéralement, Internet est la contraction d' *"Inter-networking"* qui signifie "interconnexion de réseaux". À ce stade, nous ne voyons pas la différence avec l'Internet qui répond aussi à cette définition. Mais Internet est bien plus qu'un simple réseau car c'est une interconnexion de réseaux à l'échelle mondiale. L'Internet est aussi appelé le réseau des réseaux. Sa couverture mondiale permet à des personnes partout dans le monde de communiquer grâce à de nombreuses applications.

Un réseau de communication

Qu'est-ce qu'un réseau ? Un réseau est un système de transmission capable de transférer des données d'un point à un autre de ce réseau. Un réseau de communication fournit une infrastructure pour l'échange d'informations entre n'importe quelles machines numériques qui y sont connectées. L'infrastructure du réseau comprend

L'infrastructure du réseau comprend --des liens de communication, qu'ils soient filaires ou sans fil, --des équipements comme les stations de base, les points d'accès WiFI, les commutateurs, ou les routeurs, --des programmes ou des logiciels qui réalisent les protocoles de l'Internet et les applications. Les machines numériques encore appelées *"hôtes*" sont par exemple un ordinateur, un serveur, un robot, un guichet automatique bancaire, une montre connectée, ou un smartphone. Les hôtes exécutent les applications de communication qui sont les sources et les destinations du trafic.

Les applications pour utiliser l'Internet

Les applications sont des programmes informatiques exécutés sur plusieurs machines et qui collaborent pour permettre à des personnes de communiquer directement entre elles ou d'échanger des données à travers le réseau. Certaines applications sont qualifiées d'historiques comme le mail ou le transfert de fichiers car elles ont été développées au tout début d'Internet. Leur particularité est de transférer des données ou des fichiers. De nos jours, les internautes utilisent massivement le Web, les réseaux sociaux, la télévision ou les jeux en réseau. Ces applications récentes permettent l'échange de contenus plus riches tels que l'audio ou la vidéo. Citons par exemple, les applications suivantes : Web, VoIP, e-mail, jeux, e-commerce, calcul réparti, transfert de fichiers, vidéo à la demande, réseaux sociaux.

Accéder à l'Internet

Pour communiquer, l'utilisateur dispose d'un terminal de communication, généralement un PC, une tablette ou un smartphone. L'application de communication s'exécute sur ces terminaux et envoie et/ou reçoit des informations de différentes natures (textes, images, audio, video). Ces terminaux utilisateurs sont connectés à des réseaux d'accès à Internet. Le réseau d'accès est le premier maillon pour accéder à Internet et le principal chose ressentie par l'utilisateur. On distingue plusieurs types de réseau d'accès. Le réseau d'accès résidentiel permet aux

utilisateurs d'accèder à Internet depuis leur domicile. Le particulier est abonné à un opérateur Internet ou fournisseur d'accès à Internet (FAI) via une offre d'abonnement Internet qui a un coût mensuel forfaitaire. Le réseau résidentiel est le plus souvent constitué autour d'une « box », qui est un routeur paramétré par l'opérateur. Cette box permet une interconnexion des machines de la maison en sans fil, grâce au Wi-Fi ou en filaire, grâce à Ethernet. Elle est relié au réseau de l'opérateur par la ligne téléphonique de l'abonné, en ADSL (Asymetric Digital Subscriber Line) ou en fibre optique.

Avec la généralisation des « smartphones », légers et puissants, le réseau mobile ou cellulaire est largement utilisé pour accéder à l'Internet notamment aux réseaux sociaux. Le réseau mobile est déployé par un opérateur pour couvrir des territoires avec des communications sans fil. Sur un territoire sont disséminées des stations de base munies d'antennes qui couvre une cellule géographique. Les utilisateurs peuvent ainsi se connecter par des liaisons radio partagées. Les stations de base forment un réseau d'accès connecté par fibre optique au réseau filaire de l'opérateur. Le réseau mobile permet aux utilisateurs de téléphoner partout et même en mobilité. Depuis leur déploiement à la fin des années 90, les réseaux mobiles ont connu des innovations technologiques majeures qui ont amélioré leur couverture et augmenté le débit d'accès. Ainsi avec la quatrième génération, on peut désormais transférer des données avec des débits de plusieurs Mbit/s et regarder des vidéos en streaming. Le troisième type de réseau d'accès est celui de l'entreprise. Ce réseau utilise le plus souvent la technologie Ethernet mais aussi le Wi-Fi. Ethernet est basé sur une infrastructure constituée du câblage en paires torsadées et de prises Ethernet (RJ45) et d'équipements dédiés. Le câblage est déployé dans tous les bureaux ou salles de l'entreprise et relie ainsi les hôtes aux équipements réseau : commutateurs Ethernet et routeurs.

Structure de l'Internet

L'Internet est une interconnexion de réseaux différents appartenant à différentes organisations. Une communication entre deux utilisateurs, de réseaux différents voire de pays différents passent par plusieurs réseaux. Comme le montre la figure 1, la communication entre Alice et Bob passe par plus d'un réseau : elle part du réseau résidentiel d'Alice, puis passe par le réseau X de son FAI. Le réseau X est lui-même connecté à un réseau régional, plus important. Pour simplifier, le réseau régional est connecté au réseau Backbone. Il interconnecte un autre réseau régional auquel est connecté le réseau d'opérateur Y auquel est abonné l'utilisateur B. Les réseaux de l'opérateur de Bob ou du FAI d'Alice sont des réseaux de collecte : ils donnent accès à Internet à une multitude d'abonnés. Ils couvrent une région ou un seul pays.

Le backbone ou épine dorsale d'Internet est constitué d'un ensemble de réseaux qui couvre plusieurs continents, fédérant ainsi tous les réseaux régionaux. Ils disposent d'une très grande capacité d'acheminement du trafic. Leurs clients sont d'autres réseaux de FAI et jamais des particuliers. Internet est donc composé d'un ensemble de réseaux différents, interconnectés de manière hiérarchique, mis en place et maintenu par des opérateurs privés. Leur interconnexion assure une connectivité globale entre les usagers et les services.

La communication à travers des réseaux différents est possible grâce à la technologie de l'Internet. Internet semble être un réseau logique ou virtuel qui est en réalité une suite de réseaux physiques reliés les uns aux autres.

Figure 1 : Interconnexion de réseaux dans l'Internet.

L'adressage IPv4 dans Internet

Nous avons vu qu'Internet était une interconnexion de nombreux réseaux, publics, privés, FAI régionaux ou internationaux. A la manière d'une adresse postale ou d'un numéro de téléphone, chacun de ces réseaux est identifié de manière unique par une adresse réseau ou adresse IP. L'adresse IP est un élément essentiel car elle identifie de manière unique un réseau sur l'Internet. C'est une information indispensable pour effectuer le routage d'un paquet entre la source et son destinataire. Chaque réseau interconnecte de nombreux hôtes et routeurs qu'il faut pouvoir identifier de manière unique. L'adresse IP est hiérarchique à deux niveaux. Une partie de l'adresse, appelé préfixe réseau, identifie un réseau particulier sur l'Internet. La deuxième partie de l'adresse, appelée champ hôte, identifie de manière unique un hôte ou une interface de routeur sur ce réseau particulier. Grâce à cette adresse, on peut localiser sur quel réseau la machine est connectée, ce qui est indispensable pour le routage. Les adresses IP sont distribuées par un organisme appelé *Registry*, différent pour chaque grande région du monde.

Structure hiérarchique de l'adresse IPv4

L'adresse est définie sur 32 bits ou 4 octets, selon un format hiérarchique en 2 champs (voir Fig.2). Le préfixe ''réseau'' porte sur les bits de poids fort (à gauche des 32 bits). On l'appelle encore ''préfixe réseau'' et ''NetID'' (Network Identifier) en anglais. Le champ ''Hôte'' porte sur les bits de poids faible (à droite des 32 bits). On l'appelle encore ''numéro d'hôte'' ou ''HostID'' (Host Identifier) en anglais.

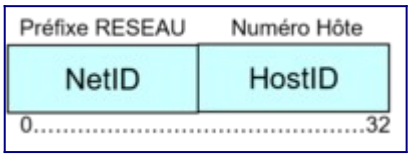


Figure 2 : Format de l'adresse IPv4.

Système de classes d'adresse dans IPv4

Ces deux champs ont une longueur variable selon la taille du réseau. Initialement, tel que défini dans le RFC xx, le découpage de ces 2 champs dépendait d'un système de classes, notées de A à E (voir Fig.3). Pour différencier à quelle classe appartient une adresse réseau, il faut

examiner les 3 premiers bits de poids fort. Ainsi, le premier bit de poids fort identifie la classe A. La valeur binaire ‘’10’’ identifie la classe B et la valeur binaire ‘’110’’ identifie la classe C. La classe D est identifiée par la valeur ‘’1110’’ et la classe E par ‘’1111’’. La classe A est associée aux très grands réseaux car 8 bits sont dédiés au préfixe réseau et 24 bits pour la partie hôte, offrant une capacité de 2^24 adresses possibles d’hôte, soit plus de 16 millions d’adresses. La classe B est associée aux grands réseaux car avec un préfixe et un champ hôte sur 16 bits, elle permet d’adresser jusqu’à 65536 hôtes. La classe C est dédiée aux petits réseaux connectant moins de 256 hôtes, avec un préfixe réseau sur 24 bits et un champ hôte sur 8 bits. La classe D est réservée pour l’adressage multicast et la classe E est non utilisée jusqu’à présent.

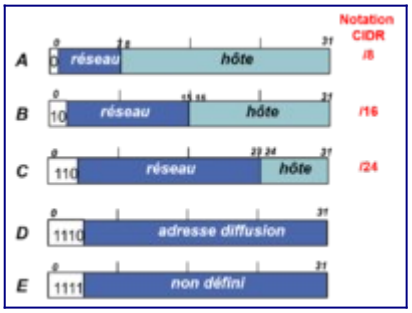


Figure 3 : Système de classes d’adresses (RFC).

Notation décimal pointé d’une adresse IPv4

L’adresse IP est un nombre qui identifie un hôte particulier sur un réseau particulier. C’est un nombre binaire qui est utilisé notamment pour les routeurs qui décide du routage en comparant deux préfixes réseau par une opération booléenne : 2 machines sont sur le même sous-réseau si la disjonction exclusive (XOR) de leurs préfixes respectifs est égal à zéro. On utilise la notation ‘’décimale pointée’’ pour faciliter leur manipulation par des humains. Cela consiste à représenter en décimale la valeur de chaque octet de l’adresse, chaque octet étant délimité par un point. Ainsi la figure 4 montre une adresse binaire et sa notation décimale en dessous. Cette adresse commençant par ‘’10’’, il s’agit d’une adresse de classe B qui définit le préfixe réseau sur 16 bits et le numéro d’hôte sur 16 bits aussi.

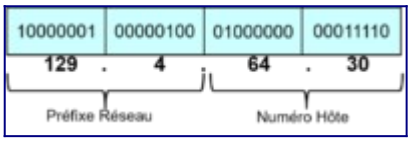


Figure 4 : Notation de l’adresse réseau en décimal.

Par convention, on note l’adresse réseau avec une valeur à zéro dans tous les bits du numéro. Sur l’exemple de la figure 4, l’adresse réseau est donc : 129.4.0.0.

Système sans classe : CIDR

En 1993, la solution CIDR (Classless Internet Domain Routing) permet de s’affranchir du système de classes. Au départ, il s’agit d’allouer plusieurs classes C contigües afin d’allouer un nombre d’adresses au plus près de la demande. Ainsi, un réseau qui demande 500 adresses se verra allouer deux classes C contigües, par exemple les blocs 193.56.64.0 et 193.56.65.0. Cela revient à numéroter les hôtes sur 9 bits puisque la valeur binaire du préfixe réseau est :

‘’’11000001.00111000.0100000|0.00000000’’’. Avec CIDR, les premiers bits de l’adresse ne permettent plus d’en déduire la longueur de chacun des champs réseau et hôte. L’information sur la longueur du préfixe réseau a donc été ajoutée à la fin de l’adresse. Ainsi une adresse est notée *a.b.c.d/x* où x est un entier qui indique le nombre de bits du préfixe réseau. Dans l'exemple précédent, l’adresse 129.4.0.0 de classe B sera maintenant notée 129.4.0.0/16. Dans le deuxième exemple de 2 classes C contigües, on notera l’adresse réseau : 193.56.64.0/23. Avec cette notation, on connaît le nombre x de bits consacrés au préfixe réseau et par soustraction à 32, on peut en déduire le nombre de bits dédiés au numéro d’hôte.

En conclusion

Le réseau Internet se définit comme une interconnexion de réseaux offrant aux machines numériques connectées à ces réseaux, un service de connectivité globale. Internet est organisé hiérarchiquement en interconnectant des milliards de réseaux d'accès à des réseaux régionaux, internationaux jusqu'aux réseaux de backbone. Tous les jours de nouveaux réseaux sont interconnectés à l'Internet sans que cela change les réseaux déjà connectés. L'adresse Internet est au coeur de cette connectivité globale mais dans sa version IPv4, sa capacité limitée et son mode d'attribution en font aussi son point faible.

Activité 02 : Principes de l'Internet

Pour comprendre les principes d'Internet, nous allons tout d'abord introduire le rôle du routeur qui est l'équipement d'interconnexion des réseaux. Nous décrirons le protocole IP, qui réalise l'interconnexion, et son unité de données, le paquet. Puis nous expliquerons comment les paquets sont transférés dans le réseau.

Introduction

Internet est une interconnexion de réseaux qui sont différents à la fois par leur technologie et par leur adresse. Le routeur est un équipement clé dans cette interconnexion car il appartient à chacun des réseaux et leur sert de passerelle. Le protocole IP (Internet Protocol) définit le format de son unité de données, appelée paquet ainsi que les règles d'échanges de paquets entre routeurs et hôtes. Le routeur réalise le routage des paquets dans le réseau.

Le routeur

Dans cette interconnexion de réseaux qui constitue l'Internet, il faut un équipement qui permet de passer d'un réseau à l'autre : le routeur. Deux réseaux sont différents car ils appartiennent à des entités différentes, utilisent un préfixe réseau différent sur chaque réseau et quelques fois, une technologie de transmission différente (par exemple : cellulaire versus Ethernet). En interconnectant deux réseaux différents, le routeur est l'équipement qui réalise cette interconnexion et joue le rôle de *passerelle relais*. Il est le seul équipement capable d'avoir une adresse IP sur chaque réseau.

- Par exemple, à la maison, Alice est raccordée à Internet grâce à une box qui utilise la plage d'adresses 192.0.0.0/24. Son FAI utilise la plage d'adresse 129.4.0.0/16. Le routeur possède une interface sur chaque réseau, et une adresse sur chaque réseau sera associée à chaque interface. Par exemple, sur le réseau d'Alice, le routeur aura l'adresse 192.0.0.1 et sur le FAI, il aura l'adresse 129.4.128.37.

Le routeur

Alice et Bob communiquent grâce à une chaîne de segments de communication qui forme une interconnexion de réseaux. À la maison, Alice est connectée à Internet par son opérateur X, et Bob par son opérateur mobile Y. Pour réaliser l'interconnexion entre les différents réseaux, il faut ajouter un équipement clé : le routeur.

Le routeur réalise deux fonctions complémentaires : le relayage et le routage.

Un routeur, comme son nom l'indique, effectue le routage qui définit la route à emprunter en fonction de l'adresse du destinataire. Le routage est effectué grâce à un *protocole de routage* qui intervient entre les routeurs. Chaque routeur échange avec les routeurs de son domaine des informations qui leur permettent de reconstituer la carte ou graphe du réseau. Avec cette carte, le routeur est alors capable de calculer une *table de routage* qui indique pour chaque destination connue sur ce réseau, la meilleure route à prendre. Dans cette table, il existe toujours une route par défaut qui est l'adresse d'un routeur qui permet d'aller vers l'Internet. A

l'aide de sa table de routage et en fonction de leur destination, le routeur retransmet ou relaie les données reçues d'un réseau vers le suivant.

- Dans l'exemple d'Alice, en plus d'assurer les communications locales, la *box* est aussi le routeur qui interconnecte le réseau local domestique d'Alice au réseau de l'opérateur (voir Fig.1). Dans cet exemple très simple, déterminer la route à prendre en fonction de la destination des données signifie, pour le routeur, choisir entre le réseau local ou le réseau de l'opérateur. Si, par exemple, Alice envoie un mail à Bob, le routeur envoie les données (le mail) vers le réseau de son opérateur car la destination est extérieure au réseau résidentiel d'Alice. Par contre, si Alice envoie un document à imprimer à son imprimante, le routeur ne retransmettra pas les données (le document) vers l'opérateur car l'imprimante est interne au réseau d'Alice.

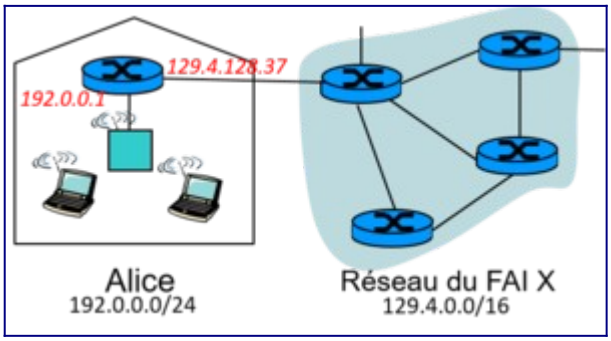


Figure 1: Une box et un routeur.

IP, le protocole de l'Internet

Pour communiquer, deux personnes doivent parler la même langue et utiliser les mêmes coutumes. De la même façon, pour communiquer, deux entités réseau doivent pour se comprendre et parler la même langue et utiliser les mêmes principes d'échange. Le protocole de communication définit les règles et le format des échanges entre des entités distantes ainsi que la synchronisation de ces échanges dans le temps. Il y a des protocoles pour toutes sortes de fonctions réseau : routage, liaison de données, partage du support, client-serveur, navigation multimédia, courrier électronique...

Le protocole IP (*Internet Protocol*) est le protocole dédié à l'interconnexion de réseaux différents. IP définit le format des unités de données (*PDU - Protocol Data Unit*) échangées entre les réseaux : les paquets, ainsi que les règles d'échange des paquets. Il ne modifie pas les données qui lui sont confiées et se contente de les relayer vers un autre réseau. Il a pour objectif d'être rapide et efficace. Il a été simplifié au maximum : il transmet directement les données dans le paquet par un fonctionnement en mode non connecté, c'est à dire sans établir une connexion logique au préalable. D'ailleurs, pour marquer cette caractéristique, les paquets se nomment également *datagramme*.

Pour assurer la continuité du transfert des paquets dans tout l'Internet, le protocole IP est non seulement dans tous les routeurs ou *nœuds* du réseau, mais aussi, dans les hôtes qui veulent

transmettre des données qu'ils doivent encapsuler dans des paquets IP. Ce protocole est implanté dans une couche logicielle du système d'exploitation des hôtes et des routeurs. Il permet d'uniformiser le réseau et de s'affranchir des différentes technologies de transmission. C'est en quelque sorte le langage commun (une espèce d'Espéranto) à l'ensemble des équipements de l'Internet. Le protocole IP définit, avec l'adresse IP, un système d'adressage global qui permet à tout hôte connecté de communiquer avec n'importe quel hôte disposant d'une adresse IP. Ainsi, parce qu'il est présent dans chaque hôte connecté au réseau et dans chaque routeur, le protocole IP permet la communication de bout-en-bout.

Le paquet IP

Le paquet IP ou datagramme est l'unité de transfert des données pour tous les réseaux connectés à l'Internet. Le paquet a une taille maximale qui dépend de la taille de la trame au niveau liaison. En effet, selon le principe d'encapsulation des protocoles, sur chaque segment de communication, le paquet est *transporté* dans le champ de données (ou *charge utile*) d'une trame.

Le paquet IP est composé de 2 parties (voir Fig.2):

- l' *en-tête IP* contient les informations nécessaires à son routage vers sa destination finale, à savoir les deux *adresses* source et destination ;
- le *champ de données* contient les données de l'application - par exemple, tout ou partie d'un mail, d'une page Web ou d'un document à imprimer.

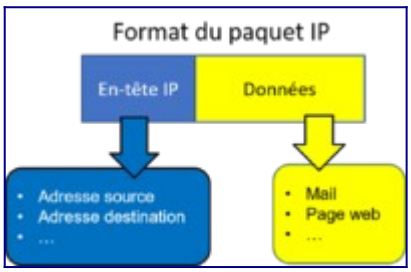


Figure 2: Le format du paquet IP.

Ces données applicatives doivent être découpées en blocs transportables par un paquet. Par exemple, une application de transfert de fichier découpe un fichier en blocs de données, puis chaque bloc est encapsulé dans un paquet par ajout de l'en-tête. Ensuite, chaque paquet est transmis indépendamment les uns des autres dans le réseau.

Acheminement par paquet et relayage par les routeurs

Le transfert du fichier entre la machine d'Alice et le terminal de Bob consiste à envoyer une suite de paquets sur l'Internet. Les paquets sont envoyés en mode *datagramme*, indépendamment les uns des autres, de manière analogue aux lettres ou aux cartes postales échangées sur le réseau postal. Ils sont transférés de routeur en routeur, passant d'un réseau à un autre, conformément au routage calculé dans les tables de routage.

Sur chaque routeur, le relayage consiste à recevoir un paquet depuis une interface réseau en entrée, d'examiner son en-tête, en particulier l'adresse de destination du paquet, et décider de l'interface de sortie, c'est-à-dire le prochain réseau sur lequel il sera retransmis pour atteindre le réseau auquel Bob est connecté. Le choix de l'interface de sortie en fonction de la destination a été précalculé par la fonction de routage et enregistré dans une table. Comme le montre la figure 3, les paquets circulent ainsi de la source à la destination.

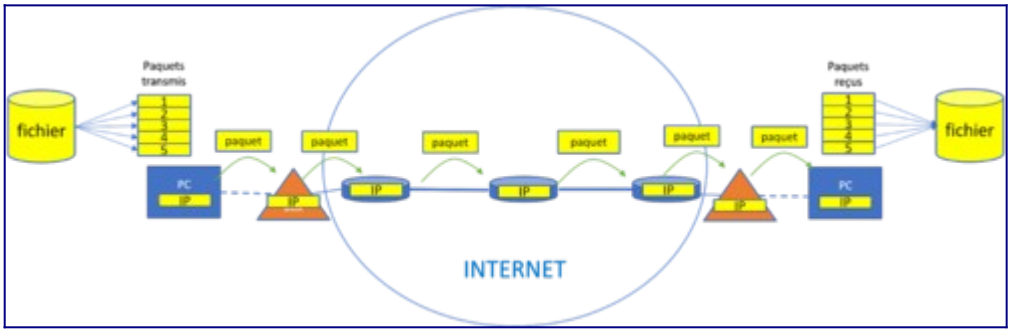


Figure 3: Acheminement d'un paquet IP relayé d'un routeur à l'autre.

Conclusion : points clés d'IP

Pour résumer, le protocole IP utilise un mode de communication par paquets, de taille réduite, et acheminés en mode datagramme. Le protocole IP est mis en œuvre par les routeurs, équipements spécialisés qui assurent l'interconnexion et le relayage des paquets d'un réseau à l'autre entre la source et la destination.

Parce qu'il est présent dans tous les hôtes et les routeurs, le protocole IP permet d'uniformiser le réseau et de s'affranchir des différentes technologies de transmission sous-jacentes.

Activité 03 : Évolution de l'Internet

Introduction

En 40 ans, Internet a connu une croissance exponentielle en termes de nombre de réseaux connectés et de nombre d'hôtes connectés. Internet connecte aujourd'hui 4,8 milliards d'utilisateurs soit 59 % de la population mondiale. A travers des graphiques et l'histoire récente des technologies associées, nous allons voir comment cette évolution s'est produite.

Les différentes phases de l'évolution d'Internet

La figure 1 reprend le graphique de Peter Magnusson [1] qui présente des années 70 à 2000, une croissance en 3 phases, pour arriver à environ 100 millions d'hôtes connectés.

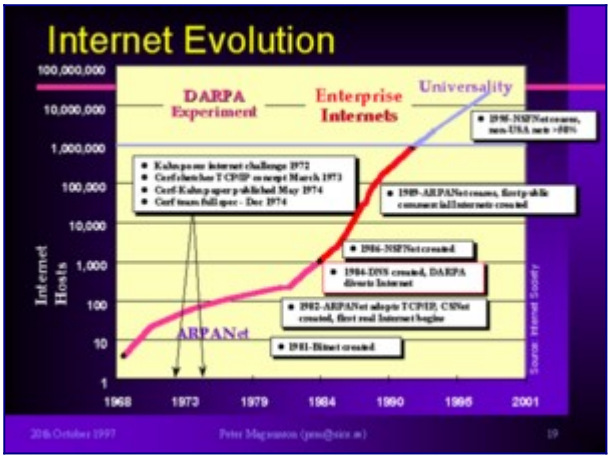


Figure 1: Internet Evolution (Internet Society).

La première phase : expérimentale

La première phase est dite expérimentale et court de 1969 à 1986 [2], environ. En pleine guerre froide, le DARPA (Département de la Défense Américaine) souhaite interconnecter différents sites avec un contrôle décentralisé afin d'éviter une attaque du centre de contrôle qui pourrait affecter le fonctionnement de tout le réseau et des autres sites. Sur la figure 2, on voit le plan du réseau ARPANET en 1973. En 1971, ce réseau comprend 23 nœuds et 111 nœuds en 1977.

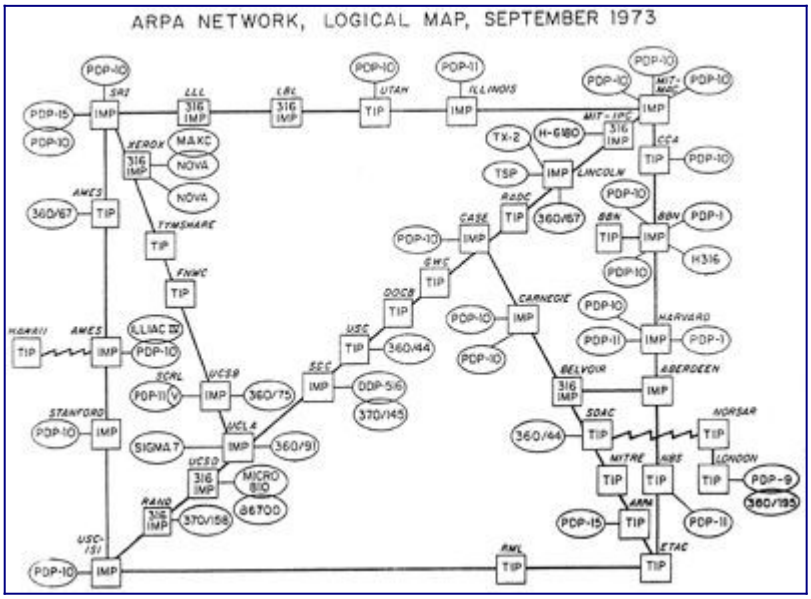


Figure 2: Carte d'ARPANET en 1973.

Les fondements : intelligence répartie et mode non connecté

L'intelligence répartie sur tous les éléments est le principe fondateur de l'Internet. Ce qui est révolutionnaire pour l'époque où tous les réseaux de télécommunication mais aussi les sytèmes informatiques étaient bâti sur un contrôle centralisé. Dans ces réseaux centralisés, le centre de contrôle gérait tout le fonctionnement du réseau, notamment pour construire les tables de routage utilisées par les noeuds, mais aussi pour établir une connexion entre deux utilisateurs afin de transférer des données (en mode connecté). Le mode réparti va donc être décliné dans les premiers protocoles développés. Contrairement au routage centralisé, tous les noeuds du réseau participent au routage en s'envoyant des informations de connectivité afin que chaque routeur construise sa table de routage.

IPv4

Au début des années 1980, alors que s'opérait l'interconnexion de différents réseaux informatiques pour créer l'Internet que nous connaissons aujourd'hui, IP (Internet Protocol) s'est imposé comme le protocole standard de l'Internet. L'organisme de standardisation IETF spécifie la version 4 du protocole IP (IPv4) dans le document RFC 791, daté de 1981. Ce RFC définit d'une part, l'adresse sur 32 bits et son format en 2 champs de longueur variable et d'autre part, le paquet, son unité de données de transfert. En 1983, le réseau étasunien ARPANET choisit la pile TCP/IPv4 comme le standard de communication pour les équipements et les réseaux souhaitant se connecter. Ce choix s'est ensuite imposé sur l'ensemble des réseaux et des systèmes de ce qui allait devenir ensuite l'Internet. Le protocole IPv4 a été un élément décisif dans le passage à l'échelle de l'Internet. Ses spécifications généralisent les propriétés importantes de connectivité globale et de contrôle de bout en bout. Elles définissent pour les adresses IP une longueur fixe de 32 bits. IPv4 permet ainsi de définir un nombre important d'adresses (2^{32} soit plus de 4,3 milliards), donc autant d'identifiants attribués à chaque équipement connecté. Au moment où ont été définies ces spécifications, le réseau ARPANET comptait quelques centaines d'équipements. En 1987, ce nombre dépassa les 10 000 puis 160

000 à la fin de l'année 1989 [3]. La capacité d'adressage d'IPv4 semblait alors suffisante pour pouvoir répondre au besoin de nouvelles connexions, même si celui-ci augmentait rapidement.

La seconde phase : l'expansion

En 1983, le réseau Arpanet a été séparé du réseau militaire pour rester utilisé par des écoles et des universités américaines. L'intégration par l'Université de Berkeley des protocoles TCP/IP dans le noyau du système d'exploitation Unix est un événement très important qui va accélérer la diffusion des protocoles de l'Internet et son adhésion par le plus grand nombre.

Les années 80 voient la généralisation des stations de travail sous Unix autonomes mais avec des capacités limitées en termes de puissance de calcul et de capacité de stockage disque. Ces stations ont besoin de communiquer entre elles pour l'accès à des ressources partagées comme le système de fichiers ou les imprimantes. La pile TCP/IP va être massivement utilisée pour ces communications locales puis mondiales.

En effet, les protocoles Internet proposent des applications de communication inter-personnelle comme le mail, le transfert de fichiers, ou les news. Très vite, les chercheurs et les ingénieurs vont les adopter pour échanger des informations scientifiques entre collègues du monde entier. Ces utilisateurs experts vont réaliser des tests en vraie grandeur de l'Internet.

La troisième phase : l'universalité

Au début des années 1990, le réseau précurseur ARPANET a laissé sa place à l'interconnexion des réseaux que nous appelons aujourd'hui l'Internet. L'Internet devint alors mondial, se structurant par l'interconnexion des opérateurs publics et privés des différents pays. En 1992, le nombre d'équipements connectés à l'Internet dépasse le million. En parallèle, dans les années 90, la micro-informatique se développe dans les entreprises et chez les particuliers qui commencent à s'équiper d'ordinateurs personnels assez basiques mais très économiques. Et grâce à la technologie ADSL, dès la fin des années 90, le débit d'accès va être dopé en utilisant toute la capacité des paires téléphoniques. Une autre avancée technologique vient de la généralisation des interfaces graphiques qui va simplifier l'accès des utilisateurs aux informations et aux commandes du système. Ainsi, grâce à la souris, aux fenêtres, boutons et autres barres de défilement, l'utilisateur n'a plus besoin de connaître les commandes Unix !

Les informations contiennent toujours des textes mais sont aussi enrichies par des images, des sons et des vidéos. Dès cette époque, dans l'Internet se pose le problème de la recherche d'informations dans ce réseau mondial avec des contenus toujours plus nombreux. Les premiers moteurs de recherche font leur apparition [ref sur moteurs] . Mais le progrès le plus significatif a été le développement de l'application Web, connu aussi sous le nom *World Wide Web*. Cette application, dite client-serveur, se compose d'un navigateur, programme qui s'exécute sur le terminal de l'utilisateur et d'un serveur Web qui gère des contenus. La communication entre navigateur et serveur se fait à travers l'Internet. Le serveur Web propose des contenus tels que des pages HTML, des sons, des images ou des vidéos. Un fichier HTML est une description de la page Web à afficher et des objets qu'elle contient. Le navigateur

envoie des requêtes au serveur pour obtenir cette page et ses objets. En réponse, le serveur lui envoie le fichier HTML et les objets. Le navigateur réalise le formattage des contenus reçus pour les afficher sur le terminal de l'utilisateur. Dans cette page, des éléments sont mis en évidence et peuvent être ''cliqués'' pour accéder directement à une nouvelle page. Grâce aux liens 'hypertexte' qui chaînent les pages entre elles, les contenus sont faciles à trouver. Au fur et à mesure, les contenus se sont enrichis dans toutes les langues et dans tous les pays du monde, rendant le Web plus proche et plus attractif pour les particuliers.

La quatrième phase : l'explosion

Dès les années 2010, la croissance a continué de manière exponentielle pour arriver à 4,5 milliards d'utilisateurs soit 59% de la population mondiale. La 4ème phase que nous vivons actuellement pourrait s'appeler l'explosion ! Quatre phénomènes expliquent cette croissance sans précédent.

- D'abord, le nombre d'hôtes utilisant Internet a augmenté car les consoles de jeux, les tablettes ou les télévisions sont maintenant connectés à Internet . Il y a désormais 4 à 5 terminaux ou ''écrans'' par personne.
- Les 3èmes et 4èmes générations des réseaux mobiles permettent désormais à des terminaux intelligents comme les smartphones, de transférer non seulement de la voix mais aussi des données, des images et des vidéos.

Comme on le constate sur ce schéma qui représente une minute d'utilisation d'Internet, de nouvelles applications sont massivement utilisées par les internautes comme la vidéo à la demande et le streaming, les réseaux sociaux, le pair-à-pair ou les jeux. Les communications inter-personnelles vidéo se généralisent.

- Enfin, ces 20 dernières années, de nombreux pays émergents, en Asie, en Amérique du Sud ou en Afrique, ont connu un développement économique sans précédent. Il s'est accompagné de leur développement technologique conduisant à leur adhésion massive à l'Internet.
- De nouveaux usages ont dopé la demande de débit sur Internet. Ainsi la figure 3 représente une minute d'utilisation d'Internet. On constate ainsi que les nouvelles applications, telles que la vidéo à la demande et le streaming, les réseaux sociaux, le pair-à-pair ou les jeux sont massivement utilisées par les internautes. De même, les communications inter-personnelles vidéo se généralisent.

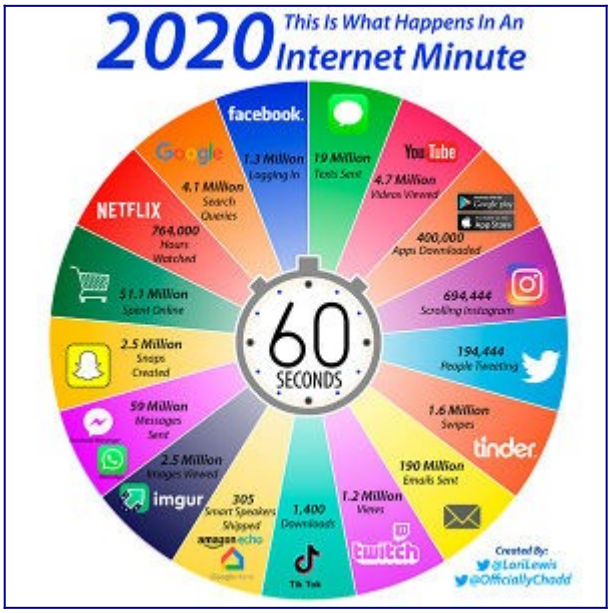
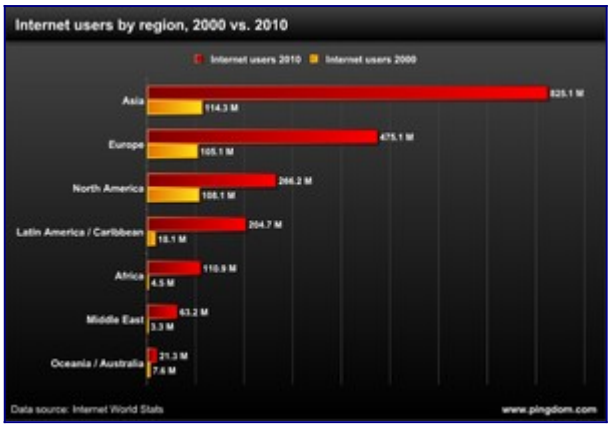
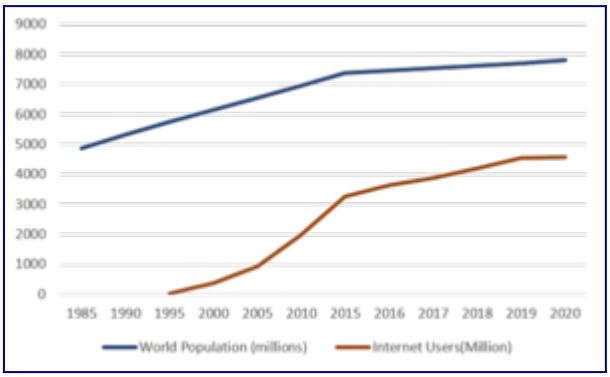


Figure 3:.

Sur le graphique de la figure 4(a), on voit la forte progression du nombre d'utilisateurs d'Internet entre 2000 et 2010, pour chaque région du monde. Le développement économique de l'Asie lui a donné la croissance la plus forte. Le nombre d'utilisateurs a été multiplié par 7 pour prendre la tête du nombre d'internautes, à la place de l'Europe et des Etats-Unis. En fait, le nombre d'utilisateurs de l'Internet augmente plus vite que la croissance de la population mondiale (voir Fig.5).



(a)



(b)

Figure 4: (a) Nombre d'internautes en 2000 et 2010, par régions du monde[Internet World Stats: www.pingdom.com]. (b) Croissance de la population et du nombre depuis 1985. .

Le nombre d'internautes en 2020 est d'environ 4,8 milliards et représente 59% de la population mondiale. L'Internet n'avait pas été prévu pour supporter une telle croissance. La capacité d'adressage des 32 bits d'adresse, en théorie 4,3 milliards, est donc largement dépassée.

Mesures d'urgence pour lutter contre la pénurie d'adresses

L'Internet vit depuis des années en situation de pénurie d'adresses. Cette pénurie d'adresses a été prédite dès le milieu des années 1990, peu après la naissance du Web. Des mesures palliatives ont été prises pour ralentir la consommation des adresses et ralentir l'apparition de la pénurie complète des adresses IPv4.

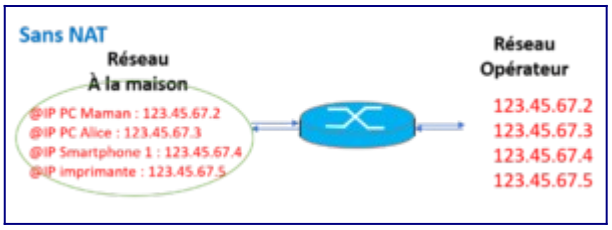
Mesure 1 : CIDR (Classless Inter Domain Routing)

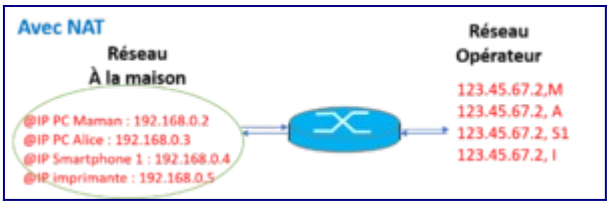
Comme on l'a vu sur la figure 4, l'accroissement du nombre d'hôtes date du début des années 90 ce qui a alerté les instances de l'Internet qui ont pris plusieurs mesures d'urgence. La première mesure a consisté à abandonner le système de classes d'adresses. En effet, les classes d'adresse utilisent une granularité d'allocation trop grossière menant à un gaspillage excessif. Un deuxième inconvénient était une représentation trop importante des très grands réseaux aux détriments des petits réseaux, qui étaient les plus nombreux. La méthode sans classe ou [4], a été mise au point en 1993, de sorte que la totalité de l'espace d'adressage unicast soit disponible. La longueur du préfixe réseau qui est variable, comme on l'a vu, est spécifiée pour chaque adresse en ajoutant à la fin "/x" où x est le nombre de bits dans le préfixe réseau. Par exemple, si un FAI a besoin de 8000 adresses, avec les classes, on lui aurait allouer une classe B qui dispose de 65536 adresses d'où un énorme gaspillage ! Sans classe, on peut allouer à ce FAI un bloc /19 soit 8192 adresses ce qui est proche de son besoin.

Mesure 2 : NAT (Network Address Translation)

La deuxième mesure, appelée NAT ou Network Address Translation, consiste à translater en sortie de réseau, une adresse privée vers une adresse publique. Cela permet d'économiser les adresses publiques en combinant un adressage privé dans le sous-réseau, et le partage de l'adresse publique entre les hôtes en sortie du sous-réseau. Cette translation est effectuée sur tous les paquets traversant les routeurs et les box. L'adressage privé est défini dans la [5], et permet d'utiliser 3 plages d'adresses réservées à cet usage et donc non routables : 10.0.0.0/8, 172.16.0.0/12, et 192.168.0.0/16.

Par exemple, sur la figure 8(a), Alice doit connecter 5 machines à la maison et son FAI lui a donc distribué 5 adresses : 123.45.67.2, 123.45.67.3, 123.45.67.4, 123.45.67.5, 123.45.67.6. Cependant, le FAI ne dispose pas d'un bloc d'adresses suffisant pour distribuer autant d'adresses que demandées par ses clients. En effet, les FAI ne proposent qu'une seule adresse publique dans leur forfait standard d'abonnement à Internet. En utilisant NAT, le fournisseur d'Alice ne lui alloue plus qu'une seule adresse routable et Alice a affecté à ses hôtes une adresse privée. Dans la figure 8(b), les 5 hôtes d'Alice dispose respectivement des adresses : 192.168.0.2, 192.168.0.3, 192.168.0.4, 192.168.0.5, 192.168.0.6.



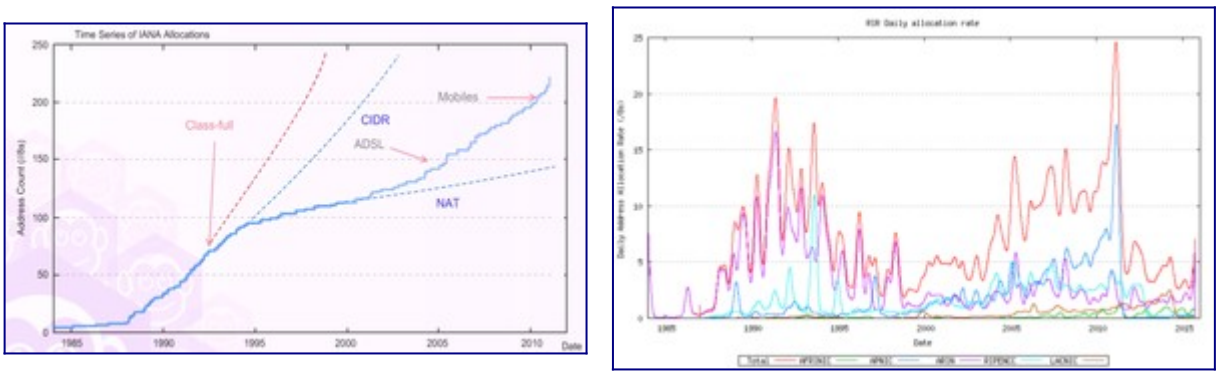


(a) **(b)**

Figure 8 : (a) Plan d'adressage sans NAT. (b) Plan d'adressage privé et NAT

Le mécanisme NAT a été ajouté aux fonctions classiques du routeur. Il consiste à translater les adresses privées internes au réseau vers l'adresse publique, routable sur l'Internet. A chaque fois qu'un paquet IP sort vers l'Internet, le routeur effectue la translation de l'adresse source de ce paquet en l'adresse publique attribuée à cet abonné. Comme plus d'une machine est connectée sur le réseau, il faut utiliser un autre champ de l'en-tête pour distinguer les hôtes sources. On utilise le port source qui est dans l'en-tête TCP ou UDP. Une table de translation NAT est maintenue par le routeur qui mémorise ainsi 4 informations : adresse IP source, numéro de port source, adresse IP translatée, numéro de port translaté. En sortie, il translate (adresse IP source, numéro de port source) vers (adresse IP translatée, numéro de port translaté) c'est-à-dire qu'il réécrit les adresse et port source dans les en-têtes IP et TCP du paquet. Quand un paquet de réponse arrive en entrée du routeur, la translation inverse est effectuée avec toujours réécriture de l'adresse et du port. Le mécanisme NAT engendre donc des opérations supplémentaires pour le routeur qui doit les faire pour chaque paquet.

La figure 9 représente le cumul des adresses IPv4 consommées et l'effet des différentes mesures de réduction de consommation des adresses. [6]. Les adresses IPv4 sont exprimées par le préfixe de longueur 8 bits. Cette figure montre bien une diminution du taux de consommation des adresses IPv4. Ce qui a permis de gagner du temps avant de passer à une solution définitive. Mais le développement de l'Internet dans la téléphonie mobile et la banalisation des accès ADSL ont accéléré la pénurie. Le graphique (b) de la figure 9 montre que, depuis 2011, la pénurie est aigüe par cette chute du taux de consommation des adresses.



(a) **(b)**

Figure 9 : Cumul de consommation des adresses IPv4 et taux de consommation.

Notation "/8"

Dans les diagrammes montrant l'usage des adresses IPv4, celles-ci sont agrégées par "/8". Comme l'espace d'adressage IPv4 est un champ de 32 bits, il y a 4 294 967 296 valeurs uniques représentées dans ce contexte par une séquence de 256 "/8" bits où chaque "/8"

correspond à 16 777 216 adresses uniques.

Limites des mesures d'urgence

Fin du bout-en-bout

Cependant, la solution NAT rend la connectivité Internet coûteuse et complexe. Les serveurs qui sont dans un réseau avec adressage privé et NAT ne sont plus atteignables et des techniques de contournement ont dû être mise en œuvre pour que les applications retrouvent une connectivité globale (à savoir, pouvoir être appelées ou appelantes). De plus, le NAT introduit un état dans le réseau qui fragilise la robustesse du système de communication. Il convient ici de ne pas oublier qu'un principe fondateur de l'Internet est de rendre le fonctionnement de l'infrastructure de communication indépendante du fonctionnement des producteurs et consommateurs de données. Ce principe connu sous le nom de "bout-en-bout" a conduit à définir le service réseau en mode "non connecté". Aucune marque ou état, issu d'une communication, n'est mémorisé dans le réseau : tout est indiqué dans le paquet. On parle d'unité de transfert auto-descriptive. L'en-tête du paquet comporte toutes les informations pour aller de la source à la destination. Le NAT est en complète contradiction avec ce principe. Le paquet n'est plus auto-descriptif de la source à la destination car chaque passerelle NAT traversée modifie les informations de l'acheminement du paquet. On peut considérer que chaque NAT traversé conduit à constituer un tronçon du chemin pour atteindre la destination. C'est cette succession de tronçons qui devient le chemin de la source à la destination. On peut voir que, d'une infrastructure de communication de bout-en-bout, l'Internet a évolué vers une infrastructure de communication devant gérer des changements de tronçons. Or, ces changements de tronçons demandent des états complexes à gérer en mode "non connecté", ce qui rend le système fragile. En effet, une panne d'un NAT suffit à interrompre toutes les communications le traversant, ce qui n'est pas le cas quand cela arrive à un routeur. Certes, des solutions existent, à base de redondances de NAT, pour maintenir la disponibilité de ce dispositif. Ces solutions sont coûteuses et complexes à mettre en œuvre et ne constituent pas le cas courant.

L'introduction du NAT a donc changé l'architecture de l'Internet, supprimant la propriété de bout-en-bout [RFC 2993]. La conséquence est que déployer des nouveaux services ou des nouveaux protocoles de transport est devenu quasi impossible. Car, non seulement NAT change l'adresse IP, mais il modifie souvent aussi le numéro de port situé au niveau de la couche de transport, ce qui a pour conséquence de figer les protocoles de transport actuels. L'ajout d'un nouveau protocole de transport nécessite de mettre à jour le code de tous les NAT en activité, ce qui représente une opération quasi impossible du fait de la diversité des NAT et de leur nombre. Cette idée de rigidification de l'Internet est nommée par le terme d'"ossification". Devant cet état de fait, des réflexions sont menées dans les instances de la gouvernance Internet pour essayer de sortir de cette impasse [RFC 7663].

Complexité accrue

Le routeur doit effectuer plus d'opérations pour chaque paquet à relayer mais NAT a aussi des

conséquences sur les applications notamment client-serveur. Le modèle d'interaction se trouve aussi, d'une certaine manière, rigidifié. Dans le modèle d'interaction client-serveur, les clients qui sont derrière le NAT peuvent s'accommoder de partager une simple adresse IP. Il en est tout autrement pour les serveurs qui ont besoin d'une adresse IP qui leur soit propre afin d'être contactés. Ainsi, ce changement architectural de l'Internet l'a transformé petit à petit en un système minimaliste à l'image des services télématiques utilisés à l'époque du minitel. Il est composé de clients et de serveurs. Les possédants d'un adressage public ont ainsi un avantage pour promouvoir leur service. Une certaine forme de contrôle des services est ainsi donnée aux hébergeurs et opérateurs. La conséquence de cette évolution est qu'il est très difficile pour un utilisateur derrière un NAT d'offrir un service. Il en est de même pour les applications de type "pair à pair" (comme la téléphonie sur IP, les jeux répartis...) qui sont devenues terriblement complexes pour contourner les difficultés introduites par le NAT pour les connexions entrantes [RFC 5128]. De fait, l'innovation dans ce type d'application est d'une certaine manière réduite. Le NAT est le composant qui participe à limiter l'apparition de nouveaux acteurs et à maintenir une certaine forme de rente pour les acteurs en place.

NAT et la sécurité

Enfin, certains ont vu dans le NAT un élément de sécurité d'un réseau local, dans la mesure où le NAT agit comme un filtre en bloquant les paquets entrants non sollicités. Les attaques sont de nos jours dans le contenu, au niveau de l'application, comme les chevaux de Troie ou les codes malveillants (*malware*) dans les pages Web. Le NAT n'améliore donc pas la sécurité car il n'apporte aucune protection contre ces attaques [7]. Le RFC 4864 montre comment avoir le même niveau de sécurité qu'un NAT en IPv6 sans en reprendre les inconvénients.

Double-NAT

La pénurie d'adresses ne faisant que s'aggraver avec le temps, on en arrive à la situation que les adresses publiques ne sont plus suffisantes pour être attribuées aux opérateurs eux-mêmes. C'est ce que montre la figure 10[8]. Cette figure représente, sous forme d'un histogramme, l'état des allocations et donc la situation de l'adressage dans l'Internet IPv4. L'histogramme est composé de 256 barres indiquées par la valeur du premier octet de l'adresse d'IPv4 (notée ici "/8"). Pour la même valeur du premier octet, est alors indiqué l'état de l'usage des 3 autres octets. Cette figure montre qu'il ne reste quasiment plus rien à allouer (en vert). Les RIR (*Regional Internet Registries*) sont sur leur réserve. Ils allouent maintenant les dernières adresses publiques sous des conditions draconiennes et donc, le plus souvent, n'allouent plus d'adresses publiques.

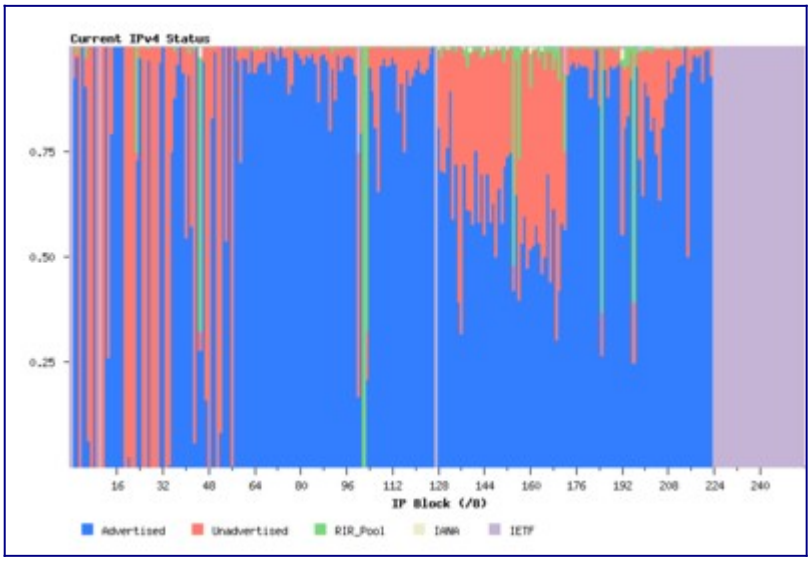


Figure 10 : État du plan d'adressage IPv4 en 2015.

Aussi, certains opérateurs, par manque d'adresses publiques, ont recours au NAT444, encore appelée technique du "double NAT" ou CGN (Carrier Grade Nat) RFC 6888. Le réseau de l'opérateur est, lui-même, en adressage privé. Ainsi, le client de l'opérateur n'a même plus une adresse publique. Le NAT du client final se retrouve à faire un passage d'un adressage privé à un autre adressage privé. D'un point de vue de la terminologie, le NAT du client est dorénavant qualifié de NAT44 pour un changement d'adressage de derrière (le coté client) à devant (le coté opérateur) cet équipement.

Un NAT ou des NAT ?

La traduction, qui se veut une solution provisoire, s'est intégrée dans l'architecture de l'Internet comme une technique classique. À tel point qu'elle se décline en différents usages. Stéphane Bortmeyer parle du "zoo des sytèmes de traduction d'adresse IP"[9] lorsqu'il en recense les différentes évolutions.

Le déploiement des super NAT, ou NAT444, pose de nombreux problèmes. Par exemple, il était complexe pour un client d'un opérateur d'héberger un serveur derrière un NAT44, mais ceci devient maintenant impossible derrière un NAT444. Les RFC 5684 et RFC 7021 dressent d'ailleurs une liste des ennuis apparus par l'introduction des NAT444. La seule solution a toutes ces complexités réside dans le passage à IPv6 pour sortir enfin de la pénurie.

Conclusion

La demande d'adresses va exploser avec l'Internet des objets et l'industrie 4.0. Dans un rapport en 2020, CISCO recense environ 20 milliards d'objets connectés, avec environ 200 objets par personne. Ce nombre pourrait augmenter jusqu'à 50 milliards à terme. Il est à relativiser car le plus souvent, seulement une passerelle qui connecte les objets, accèdera à Internet.Mais même si on divise 50 milliards par 100 ou 1000, c'est colossal !

Le protocole IPv6 en donnant une capacité d'adressage immense va permettre d'intégrer ces nouveaux usages et de redonner sa simplicité au réseau. Les institutions de la gouvernance de

l'Internet ne cessent d'ailleurs d'avertir et de demander d'accélérer le passage à IPv6. Par exemple, en mai 2016, le président du RIPE a lancé un avertissement solennel sur l'épuisement des ressources en adressage IPv4 et l'impérieuse nécessité de passer sans délai à IPv6 [10]

Références bibliographiques

1. ↑ The Internet Revolution – History and Significance https://petersmagnusson.org/2010/06/06/the-internet-revolution-history-and-significance/
2. ↑ Internet Society: Brief History of the Internet https://www.internetsociety.org/internet/history-internet/brief-history-internet/
3. ↑ Internet History of 80s, https://www.computerhistory.org/internethistory/1980s/
4. ↑ Classless Inter-Domain Routing (CIDR) [1]
5. ↑ RFC 1918 [2]
6. ↑ Huston, G (2013). APNIC Labs. A Primer on IPv4, IPv6 and Transition
7. ↑ Bortzmeyer, S. (2012) La traduction d'adresses (NAT) apporte-t-elle vraiment de la sécurité ?
8. ↑ Huston, G. IPv4 Address Report
9. ↑ Bortzmeyer, S. (2010), "Le zoo des systèmes de traduction d'adresse IP"
10. ↑ Col, P. (2016). ZDNet. *IPv6 : avertissement solennel du RIPE*. http://www.zdnet.fr/actualites/ipv6-avertissement-solennel-du-ripe-39837614.htm

Pour aller plus loin

RFC et leur analyse par S. Bortzmeyer :

- RFC 1918 Address Allocation for Private Internets Analyse

Activité 04 : Pourquoi IPv6 ?

Motivations

Le problème de pénurie des adresses Internet est principalement dû à l'explosion de la demande qui dépasse largement la capacité d'adressage IPv4. Ce problème qui est devenu critique ces dernières années, milite pour l'adoption rapide d'IPv6. En effet, il faut aujourd'hui un grand espace d'adressage pour adresser tous les appareils connectés et par la suite, les futurs objets connectés issus des applications IoT. Dépasser la pénurie d'adresses, c'est aussi ouvrir la voie à de nouveaux services, à de nouveaux acteurs innovants, c'est créer de nouveaux marchés pour de nouveaux besoins. Le passage à IPv6 devient une nécessité car, en attribuant une adresse à chaque nœud du réseau, la connectivité en IPv6 retrouve les principes qui ont fait le succès du fonctionnement de l'Internet.

La technologie de l'infrastructure de communication retrouve sa simplicité originelle. Il n'est pas soutenable que la croissance du réseau s'effectue avec une complexité croissante comme avec IPv4. Tout ceci est bien connu et cette évolution est qualifiée par "non passage au facteur d'échelle" (*not scalable*). Ainsi, avec cette simplicité retrouvée, de nouveaux champs d'application s'ouvrent à l'Internet en IPv6. Le [RFC 7368] en donne une illustration avec la domotique.

En plus de la simplicité retrouvée, IPv6 apporte de nouvelles fonctionnalités, comme la configuration automatique d'un réseau. En IPv4, chaque équipement doit se voir attribuer une adresse et obtenir sa configuration depuis un serveur qui reste à gérer. Avec IPv6, le réseau peut se gérer uniquement au niveau des routeurs, les stations construisant leurs adresses automatiquement. Ce qui est très intéressant lorsque le réseau comporte un grand parc de machines.

Nous allons introduire les points clés de la nouvelle version du protocole d'interconnexion IP : le protocole IPv6. Nous expliquerons pourquoi il y a beaucoup plus d'adresses et comment le protocole IP a été simplifié et modernisé. Les deux protocoles étant différents, le passage d'IPv4 à IPv6 a fait l'objet de scénarios spécifiés dans des RFC. Un grand nombre d'équipements et de services reposent toujours sur IPv4 et une cohabitation s'est installée pour encore de nombreuses années. Néanmoins, IPv6 est un passage obligé pour l'Internet du 21^{e} siècle.

IPv6 : une nouvelle version d'IP

Depuis le premier RFC sur IPv6 publié en décembre 1995, la version IPv6 a quitté les laboratoires. L'étape de standardisation des protocoles de base de IPv6 (*core specs*) est achevée depuis le début des années 2000. La nouvelle version d'IP reprend ses principes fondateurs : encapsulation des données dans des paquets, adresses source et destination dans l'en-tête, transfert en mode datagramme, routage paquet par paquet.

Le réseau utilise des équipements intermédiaires simples et transparentes aux données transférées. Il n'effectue aucune reprise sur erreurs et tout le contrôle est reporté sur les extrémités dans d'autres protocoles. L'adressage est toujours hiérarchique mais de nouveaux niveaux sont ajoutés à la demande.

Deux points clés permettent à IPv6 de résoudre les problèmes que nous avons évoqués dans les activités précédentes :

- IPv6 offre une adresse plus longue qui passe de 32 bits à 128 bits. Cette capacité immense va résoudre la pénurie à très long terme ;
- les concepteurs d'IPv6 ont voulu moderniser le protocole par la même occasion pour prendre en compte de nouveaux besoins qui n'avaient pas été envisagés dans les années 70-80.

Par exemple, il n'avait pas été imaginé le développement de la diffusion de chaînes de télévision sur Internet. Dans IPv6, la diffusion à un groupe de récepteurs, le *multicast*, a été défini dès le départ.

Un système d'adressage avec une capacité immense

L'espace d'adressage IPv6 a une capacité immense. Une adresse IPv6 est longue de 128 bits (16 octets), contre 32 bits pour IPv4. On dispose ainsi d'environ $3{,}4 \times 10^{38}$ adresses (soit plus de 340 sextillions). Pour reprendre l'image usuelle, on aurait plus de 667 millions d'adresses IPv6 par millimètre carré de surface terrestre.

La notation d'une adresse IPv6 se fait maintenant en hexadécimal, codé sur 16 bits. Une adresse IPv6 est alors représenté par 8 mots de 2 octets séparés par un ":", comme le montre l'exemple de la figure 2.

```
2001:0db8:0000:0000:0000:ff00:0042:8329
```

Figure 1 : Exemple d'adresse IPv6 notée en héxadécimal.

Le format de l'adresse est hiérarchique avec de multiples niveaux. L'opérateur dispose d'un bloc d'adresses plus long qui lui donne plus de liberté pour allouer des sous-blocs. On peut découper par exemple l'adresse en 4 champs qui sont :

- le préfixe FAI ;
- le préfixe de réseau ;
- le préfixe de sous-réseau ;
- et l'adresse hôte.

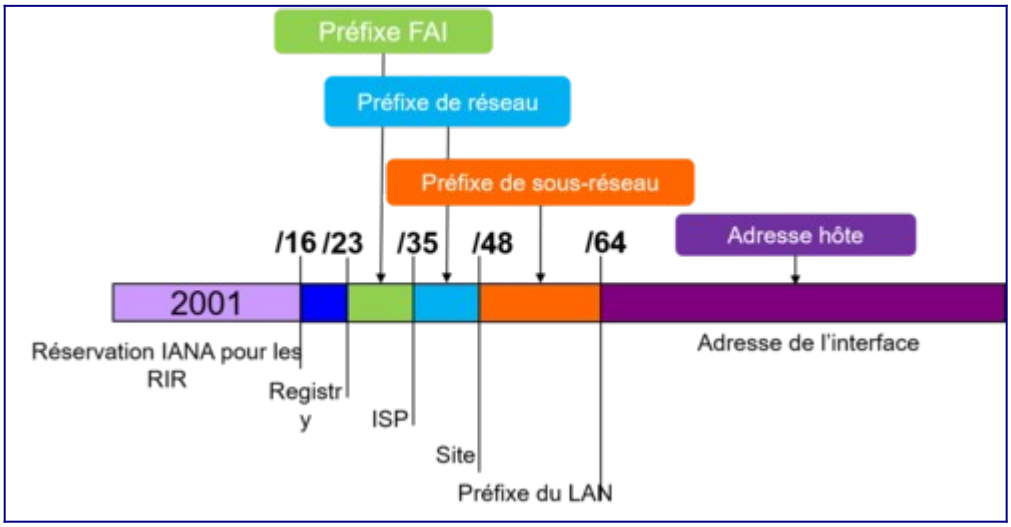


Figure 2 : Format de l'adresse IPv6.

En IPv6, l'auto-configuration d'adresse permet à un hôte d'utiliser son adresse physique ou MAC pour créer son adresse réseau. Pour réaliser la transition en douceur, il est aussi possible de dériver l'adresse IPv6 de l'adresse IPv4. De nouvelles fonctionnalités définissent des adresses génériques pour, par exemple, trouver immédiatement le serveur DNS sur un réseau, ou n'importe quel autre service.

Une simplification des fonctions d'IP

La conception d'IPv6 est aussi l'occasion de dépoussiérer le protocole. Fort de l'expérience acquise avec IPv4, certaines fonctions d'IP on été redéfinies et optimisées, d'autres ont été supprimées.

Ainsi, la protection des erreurs du paquet IPv4 par un *checksum* est finalement inutile puisque déjà réalisée au niveau liaison ; le champ *checksum* n'est plus présent dans l'en-tête IPv6.

La fonction de fragmentation d'un paquet par le routeur a été elle aussi supprimée. Cette fonction a pour but d'adapter la taille du paquet à celle de la trame du réseau suivant. Cela signifie que lorsque le routeur veut envoyer un paquet qui est plus grand que la taille de la trame, il doit fragmenter ce paquet et ainsi l'envoyer dans plusieurs trames consécutives. Les différents fragments sont identifiés pour permettre en réception de reconstituer le paquet initial. La fragmentation a de multiples inconvénients qui sont l'accroissement du temps de traitement du paquet par le routeur, une probabilité plus importante de perte de paquets puisque un seul frgment perdu entraîne la perte de tout le paquet et enfin, en réception, la mémorisation des fragments, leur éventuel remise en ordre avant la livraison à la couche supérieure. Pour éviter la fragmentation par les routeurs, le protocole IPv6 préconise d'apprendre la taille minimale de paquet supportée **sur tout le chemin** et ainsi, d'envoyer des paquets de la bonne taille. Les trois champs de l'en-tête dédiés à cette fonction ont donc été supprimés.

Un inconvénient d'IPv4 est qu'il n'y a aucune relation entre les adresses de niveau réseau et de niveau liaison. Or l'adresse physique est nécessaire pour transmettre la trame qui contient le paquet. Avec IPv4, il faut donc chercher et récupérer cette adresse physique avant d'encapsuler

le paquet dans la trame. Pour éviter cette recherche, IPv6 fournit l'auto-configuration d'adresse réseau à partir de l'adresse physique.

Le protocole IPv4 ayant été conçu il y a 40 ans, de nouveaux usages sont apparus qu'il a fallu ajouter de manière artificielle. Dans IPv6, il sera possible d'ajouter de nouvelles fonctionnalités assez facilement grâce aux extensions d'en-tête.

De IPv4 à IPv6

Une transition pas si simple

IPv4 et IPv6 sont des protocoles différents : les adresses ainsi que le format des paquets n'ont pas la même structure. De fait, les deux technologies vont cohabiter sur Internet, chacune dans un plan d'adressage différent. Ceci a pour conséquence que la communication entre un hôte IPv4 et un hôte IPv6 ne peut pas se faire directement. Pour connecter tous les utilisateurs de manière transparente, les routeurs et les hôtes devront avoir une connectivité IPv4 et IPv6. On parle de double pile. Les équipements disposent alors à la fois d'une adresse IPv4 et d'une adresse IPv6.

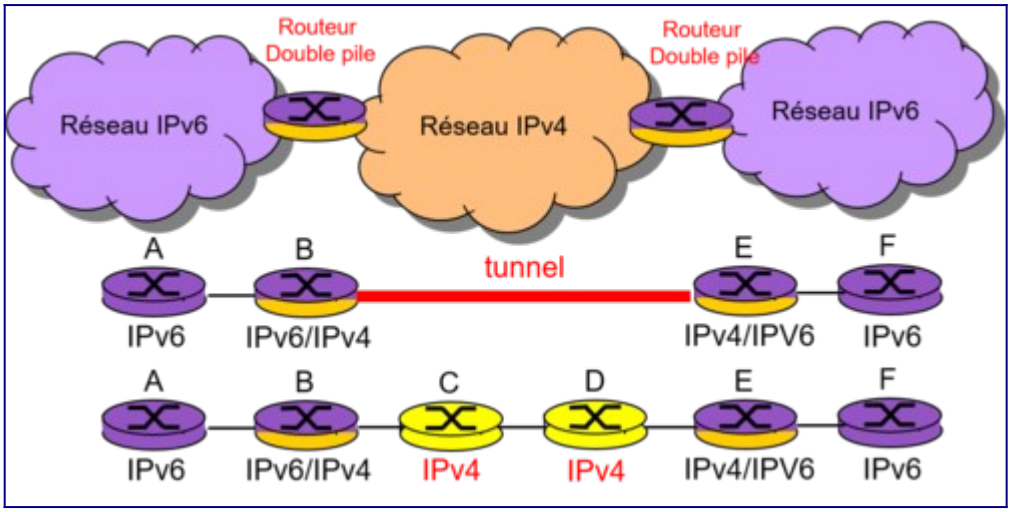


Figure 3 : Scénario de transition IPv6 avec routeurs double pile.

Lorsqu'une des connectivités est manquante, il est possible de recourir à des solution de tunnels. Un tunnel permet à deux hôtes IPv4 de communiquer au travers d'un réseau IPv6, ou inversement. Cependant, il faut noter que le recours à un mécanisme de tunnels est complexe et nuit aux performances.

D'autres scénarios de transition ont été étudiés et sont spécifiés dans plusieurs RFC.

Une cohabitation forcée

Le premier standard IPv6 date de 1995 et a été amélioré et complété durant une dizaine d'années. Depuis, la transition vers IPv6 n'est toujours pas finie alors même que les opérateurs ont quasiment tous épuisé leurs adresses IPv4.

En France, dans son baromètre annuel de la transition vers IPv6 [1], l'ARCEP pointe les nombreux freins au déploiement généralisé d'IPV6 (voir figure.4). Les causes sont multiples car cette transition nécessite des compétences techniques et des ressources adaptées. C'est un vrai projet. Et ce rapport met en évidence le rôle joué dans cette transition par les multiples acteurs de l'Internet : fournisseurs d'accès, hébergeurs de contenus, opérateurs mobiles, équipementiers, services DNS, réseau de transit et terminaux.

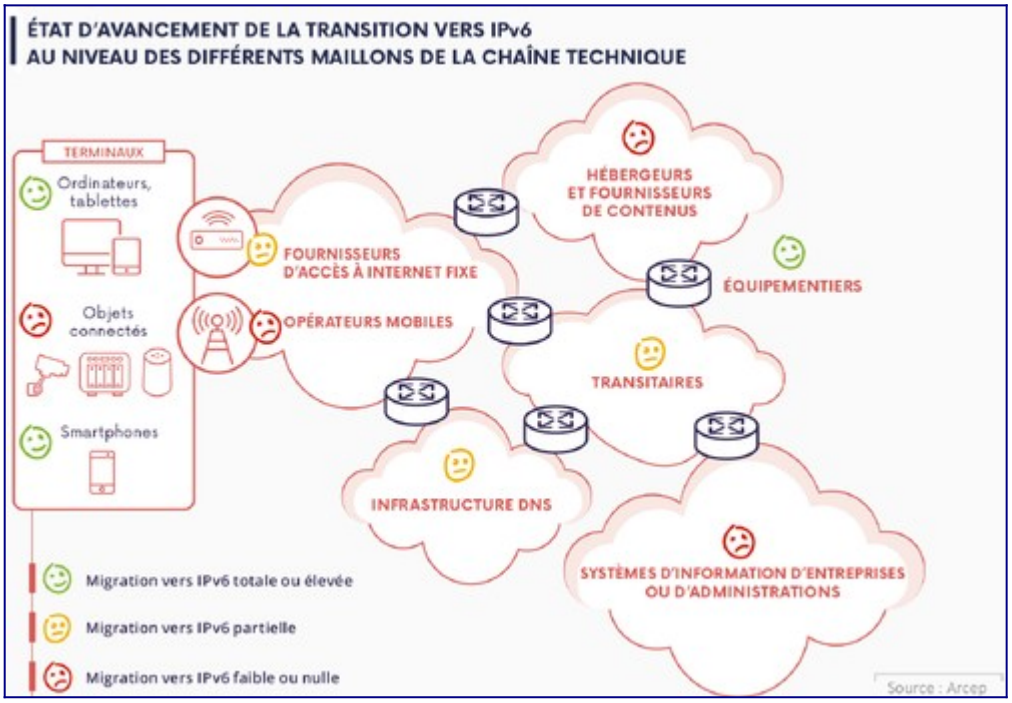


Figure 4 : Etat de la transition vers IPv6 selon les acteurs [ARCEP].

La figure 4, tirée du rapport de l'ARCEP, montre l'état d'avancement de la transition IPV6 au niveau des différents acteurs de l'Internet. Les équipementiers (ou fabricants de routeurs), les systèmes d'exploitation et les terminaux ont achevé leur mise en conformité avec les standards d'IPv6. Pour d'autres acteurs, comme les opérateurs, l'adoption d'IPv6 est plus longue. Carton rouge aux hébergeurs dont l'adoption d'IPv6 reste encore assez faible. Sur le plan international, la situation est aussi différente selon les pays. Les Etats-unis, le Canada et quelques pays d'Europe ont largement déployé IPv6. Cependant, en majorité, les pays sont encore très faiblement impliqués comme le montre la figure 5.

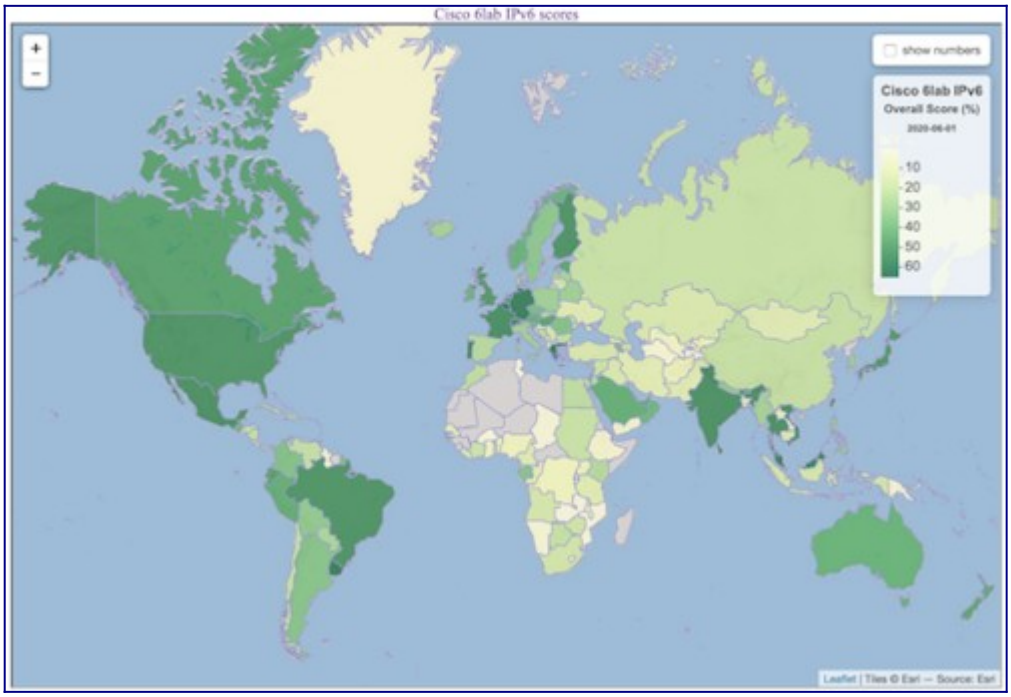


Figure 5 : Carte de l'adoption d'IPv6 par CISCO.

En 2022, l'usage d'IPv6 vu par les serveurs de Google est proche de 40 %. La figure 6 montre l'évolution des usages[2]. Cette courbe montre un quasi-doublement de l'adoption d'IPv6 tous les ans depuis 2010. Les utilisateurs de Google peuvent émettre des requêtes en IPv6 s'ils ont un accès IPv6 offert par leur fournisseur d'accès à Internet. En aout 2016, aux USA, IPv6 représente plus de la moitié du trafic mobile vers Facebook[3].

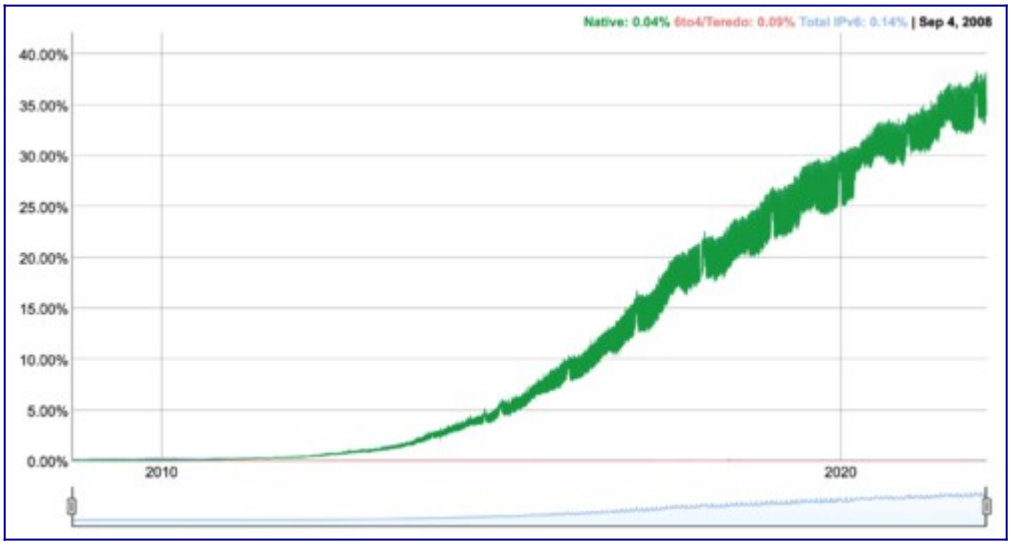


Figure 6 : Évolution du pourcentage de requêtes reçues en IPv6 par Google en 2022.

La figure 7[4] montre le pourcentage des organisations annonçant un préfixe IPv6. L'Europe, de manière générale, est active dans le déploiement d'IPv6 et la Belgique en particulier [5]. Pour suivre l'évolution de l'adoption d'IPv6, la page web de *world ipv6 launch* référence les mesures faites par différents opérateurs[6].

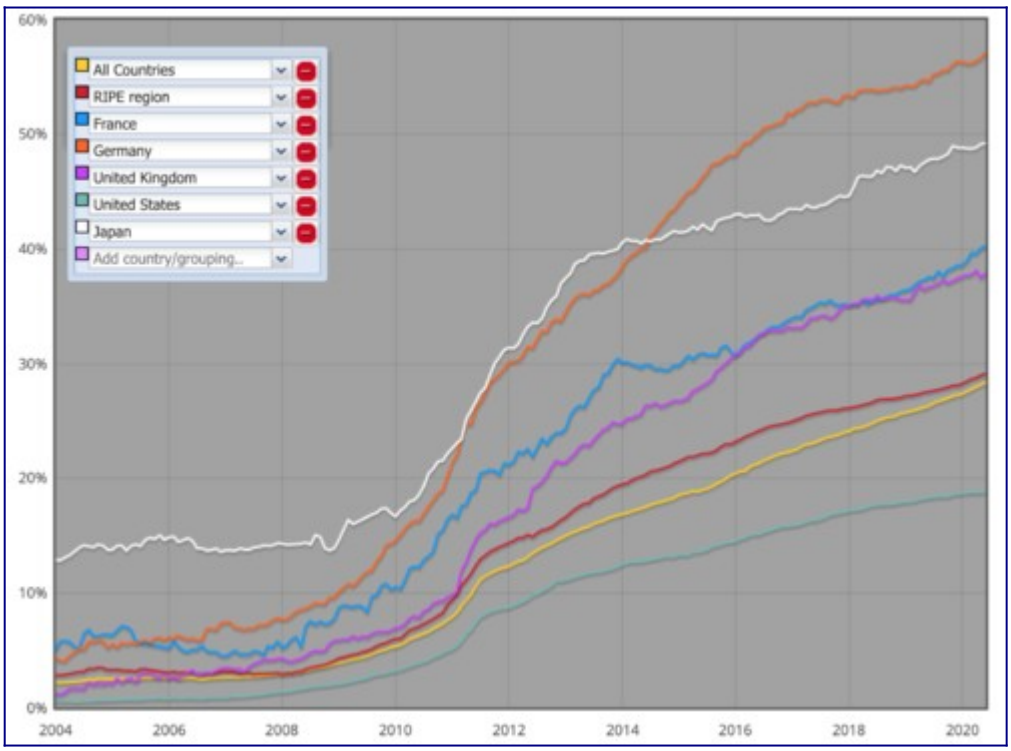


Figure 7 : Évolution du pourcentage d'organisations annonçant au moins un préfixe IPv6 par région.

IPv6 : un passage obligé

Restons optimistes cependant car les nouveaux services ou les nouveaux usages se tournent de plus en plus vers IPv6 car ils ne trouvent pas dans IPv4 les solutions techniques nécessaires à leur développement.

Les distributeurs de contenus qui déploient une infrastructure de caches répartis sur tout l'Internet ont besoin de beaucoup de flexibilité, de beaucoup de bande passante et d'une latence faible. Les nouveaux réseaux d'accès sont de plus en plus en IPv6. Enfin, l'Internet des objets, les villes intelligentes ou les réseaux de véhicules ne peuvent se développer qu'en IPv6.

L'adoption d'IPv6 est aussi une question de formation. Le protocole IPv6 n'est plus au stade expérimental ; il est indispensable pour un fonctionnement normal de l'Internet. Nous entendons par "normal", un fonctionnement respectant les principes fondateurs de l'Internet, dont celui du "bout-en-bout". Si les principes de ces deux versions d'IP sont très similaires, IPv4 adopte de plus en plus des principes non conventionnels pour continuer à fonctionner.

L'apprentissage du fonctionnement de l'Internet doit se faire de nos jours principalement avec IPv6, et accessoirement avec IPv4. Il faut rendre banale la nouvelle version du protocole IP. Dans un article[7], Geof Huston dresse une liste de fausses assertions et de rumeurs pour justifier de ne pas commencer le travail de migration vers IPv6. Si ces fausses assertions circulent, elles démontrent à quel point le besoin de formation et d'information sur la situation de l'Internet est nécessaire. Nous espérons que ce cours contribuera à combler ce manque.

Conclusion

Pour conclure, l'heure de la pénurie d'adresses IPv4 a sonné depuis quelques années et IPv6 est un passage obligé pour développer les nouveaux usages et simplifier le fonctionnement du réseau. IPv6 est le protocole de l'Internet du 21e siècle. Il est incontournable. L'IoT (*Internet of Things*) et les nouveaux usages seront les moteurs de son déploiement massif dans les dix prochaines années. Comme il modernise effectivement IPv4, il nécessite une étude approfondie de ses mécanismes de fonctionnement pour faciliter son appropriation par l'ensemble des acteurs impliqués dans un monde de plus en plus numérique.

IPv6 permet de retrouver les principes qui ont fait le succès de l'Internet comme, notamment, une connectivité simplifiée. Il est admis aujourd'hui qu'IPv6 est indispensable pour le développement des services innovants.

1. ↑ Baromètre annuel de la transition vers IPv6 en France (Nov. 2021) [1]
2. ↑ Google. Statistics. IPv6 Adoption
3. ↑ Col P. (2016) ZDNet. IPv6 représente plus de la moitié du trafic mobile vers Facebook aux USA
4. ↑ RIPE NCC. IPv6 Enabled Networks
5. ↑ Cole, P. (2016). ZDnet. La Belgique championne du monde d'IPv6, bien loin devant la France !
6. ↑ World IPv6 Launch IPv6 Measurements
7. ↑ Huston, G. (2011). Cisco Internet Protocol Journal, Vol. 14, No. 1, pp. 14-21, March. Transitional Myths