Protocole IPv6

Préambule

Ce cours vous présente la conversion Binaire/Hexadécimal indispensable pour aborder l'adressage IPv6. Il aborde également les changements qu'apporte ce protocole (adressage, VoIP…) et les différentes techniques de transition.

Conversion en Hexadécimal pour IP V6

Bin	0	1	10	11	100	101	110	111	1000	1001	1010	1011	1100	1101	1110	1111
Hexa	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
Dec	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15

Tableau de conversion Binaire-Hexadécimal-Décimal

Convertir L'hexadécimal

Binaire – Hexa

1111 (binaire) = 1×2^3 + 1×2^2 + 1×2^1 + 1×2^0
1111 (binaire) = 1×8 + 1×4 + 1×2 + 1×1
1111 (binaire) = 8 + 4 + 2 + 1 = 15 (décimal) = **F** (hexa)

Hexa – Décimal

3BF = 3×16^2 + Bx16^1 + Fx16^0
3BF = 3×256 + 11×16 + 15
3BF = 768 + 176 + 15 = **959**

Décimal – Hexa

172= 172/16 = 10 (A) reste 12 (C)
172= AC

IPV6

Avec l'explosion du nombre d'utilisateurs, de réseaux et donc des besoins, l'actuelle version d'IP devait subir des modifications. Depuis les années 70, l'internet utilise un protocole quasi inchangé alors que les matériels sont devenus de plus en plus puissants et que le nombre de personnes et de réseaux s'est multiplié.

Les raisons de changer

Pénurie d'adresses IPV4

C'est en 1981 que le système d'adressage sur 32 bits avec répartition des classes est normalisé.
Depuis, la consommation des adresses IP n'a cessé de progresser et ce plus vite que prévu. En effet, l'arrivée des nouveaux matériels (smartphone, tablette, objet connecté et les box pour les particuliers) fait que l'épuisement des adresses disponibles est actuellement un vrai problème.

Pour retarder l'échéance, des techniques ont été mises au point mais souvent au détriment de l'objectif originel d'IP, c'est-à-dire une adresse directement accessible pour des communications point à point.

Ces techniques sont les suivantes :

- **Le NAT** avec l'adressage privé
- **La récupération des adresses inutilisées** (ex. Université de Stanford qui a rendu des adresses au profit de L'APNIC)
- **La récupération de la classe E** (abandonnée car certains des matériels et logiciels ne le supportaient pas)
- **Le virtual Hosting** qui permet de gérer plusieurs sites web avec une seule adresse en jouant sur le nom DNS.

Cependant, même ces technologies ne permettent plus d'assurer la pérennité du réseau.

Voix sur IP

Le principe de communication en VoIP (téléphonie, visioconférence) est d'établir un lien direct entre l'émetteur et le récepteur. Le problème est que la plupart du temps, le poste téléphonique se trouve dans un réseau IP privé derrière un système NAT.

Cela implique que la passerelle externe, qui ne possède qu'une seule adresse IP publique, la partage avec de multiples adresses privées (SIP par exemple), ce qui en termes de qualité induit une dégradation. De plus, il est nécessaire de faire des acrobaties techniques (time out, keep alive) pour arriver à communiquer.

Accès aux serveurs internes

De même, l'accès aux serveurs internes se fait également au prix d'acrobaties (redirection de ports, VPN) avec toutes les difficultés inhérentes à ce type de technologies, notamment la difficulté à gérer les VPN et la translation.

Chiffrement des données

Pour avoir une communication chiffrée de bout en bout, on se heurte également au problème de translation. Même si des solutions propriétaires existent, les solutions apportées peuvent être coûteuses et ne sont jamais très élégantes.

Les conflits d'adressage

En utilisant un système d'adressage privé, on peut rencontrer un certain nombre de conflits.
Imaginons 2 entreprises souhaitant communiquer ensemble et ayant choisi un plan d'adressage interne équivalent (172.20.0.0/16) Que va-t-il se passer quand une machine de l'entreprise A va vouloir communiquer avec le réseau de l'entreprise B ? Comment le routeur va-t-il s'y retrouver ?

Imaginons maintenant que ces deux entreprises souhaitent fusionner. Le problème de renumérotation peut s'avérer insurmontable (Datacenter, applications serveur, matériel, vlan, firewall…)

Les diffusions

Ipv4 est en grande partie basé sur la diffusion (ARP, DHCP, Netbios) Ces requêtes ne passent pas les routeurs et ont tendance à inonder le réseau.

Principaux objectifs de l'IPV6

Supporter des milliards d'équipements.
Réduire les tables de routage.
Simplifier le protocole, pour permettre aux routeurs de router plus rapidement.
Fournir une meilleure sécurité que l'actuel protocole IP.
Accorder plus d'attention au type de service, et notamment aux services associés au trafic temps réel.
Faciliter la diffusion multi-destinataires en permettant d'en spécifier l'envergure.
Donner la possibilité à un ordinateur de se déplacer sans changer son adresse.
Permettre au protocole une évolution future, telles que la mobilité, la domotique, le multimédia etc.
Accorder à l'ancien et au nouveau protocole une coexistence pacifique.

Les principales améliorations d'IPv6

Le passage d'un adressage sur 2 puissance 32 à un adressage sur 2 puissance 128 soit 667 millions de milliards d'adresses IP disponibles par mm^2 de la surface de la Terre ou **60 000 milliards de milliards d'adresses par habitant**.
Des mécanismes d'auto configuration et de renumérotation automatique.
Adresses multiples par interface.
Adressage privée unique.
La sécurité avec IPSEC.
La prise en compte de la qualité de service.
En-tête simplifié facilitant le routage.
Les champs d'extension de l'en-tête qui laissent la place aux nouvelles technologies.
La gestion du multimédia.
Le multicast à la place du broadcast.
La gestion de la mobilité.

https://6lab.cisco.com/stats/

IPv6 dans le monde

Adressage IPV6

Types d'adresses

Adresses unicast

Ces adresses peuvent être locales ou globales, elles représentent un équipement sur le réseau.

Adresses multicast

Vers un groupe de routeurs, de serveurs DHCP
Groupe internet = équivalent au Broadcast

Anycast (RFC 1546)

Désigne un groupe d'interfaces, mais la remise du paquet s'effectue à un membre et non pas à tout le groupe comme le multicast. Cela peut être le plus proche au sens du routage (nb saut, RDT minimale…). Ces adresses sont expérimentales pour l'instant.

Les préfixes

La notion de classes d'adresses disparaît au profit de la notion de longueur de préfixe. Les réseaux sont notés en utilisant la notation CIDR. Par exemple, le préfixe 2001:db8:85a3::/48 représente l'ensemble des adresses qui commence à 2001:db8:85a3:0:0:0:0:0 et qui finit à 2001:db8:85a3:ffff:ffff:ffff:ffff:ffff.

1. Adresse non spécifiée 00..0 ou ::/128
2. Adresse de bouclage 00..1 ou ::1/128
3. Adresse multicast 1111 1111 ou ff00 ::/8
4. Adresse de lien local 1111 1110 10 ou fe80 ::/10

5. Adresse unicast unique (ULA) 1111 1101 fd00 ::/8
6. Adresse Unicast Globale (GUA) 0010 ou 2xxx :: et 3xxx ::

IPv6 généralise le plan d'adressage CIDR, les préfixes restent la propriété des opérateurs. Ils ne peuvent plus être attribués "à vie" aux équipements.

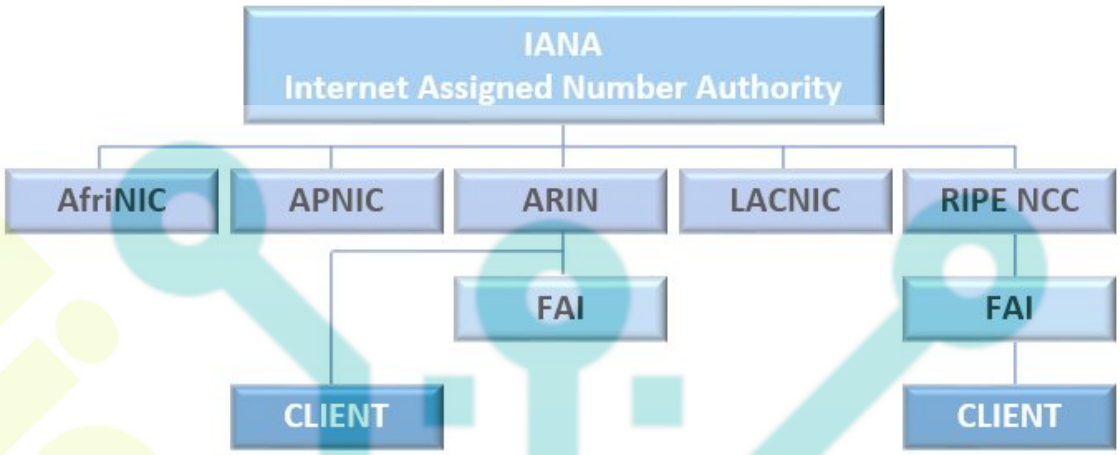
Sous IPv6, le stock d'adresses est de 2 puissance 128 adresses soit 16 octets. De ce fait, la représentation au format décimale pointée est abandonnée au profit de la notation hexadécimale par bloc de 2 octets séparés par **:**

- Format utilisé – **FE80:011A:0000:0000:0000:0000:0E3E:38D9**
- Notation abrégée – **FE80:11A::E3E:38D9**, entre les 2 points, il n'y a que des zéros.
- Notation avec suppression des 0 de tête – **FE80:11A:0:0:0:0:DE3E:38D9**

Distribution des préfixes

1 - Préfixe Global Unicast

Les adresses **Unicast Global** sont routables sur Internet. C'est en sorte l'équivalent des adresses publiques dans IPv4.



Ripe (Europe), Arin (USA, Canada, Apnic (Asie), Afrinic (Afrique), Lapnic (Amsud)

Les adresses IP Unicast sont distribuées par l'IANA aux registres Internet régionaux (RIR). Les RIR gèrent les ressources d'adressage IPv4 et IPv6 dans leur région. L'IANA alloue des blocs dans l'espace unicast global (**2000::/3**) aux cinq RIR.

Les **5 premiers bits** qui suivent le préfixe 010 (2000::/3) sont utilisés pour indiquer dans quel " registre " se trouve le fournisseur d'accès.

> **Exemple** l'adresse 2001:688:1f99:1:250:baff:febe:712 correspond :
> 2001 : une adresse unicast globale attribuée par les autorités régionales
> 688 : est le préfixe attribué par RIPE-NCC à France Télécom
> 1f99 : est attribué à l'ENST Bretagne par France Télécom
> 1 : est le réseau définit sur le site de l'ENST

Grâce à cette structure, la plupart des sites finaux (entreprises et organisations , par opposition aux fournisseurs de services Internet) seront affectés avec un préfixe de 48 bits.

Les 16 bits de sous-réseau ID permettent à chaque site une flexibilité considérable dans la création de sous-réseaux.

- Une petite organisation peut mettre tous les bits dans l'ID de sous-réseau à zéro et avoir une structure interne "à plat".
- Une organisation de taille moyenne peut utiliser tous les bits de l'ID de sous-réseau pour effectuer l'équivalent d'un sous-réseau IPv4. Il y a 16 bits ici, ce qui permet 65536 sous-réseaux.

- Une grande organisation peut utiliser les bits pour créer une hiérarchie de plusieurs niveaux de sous-réseaux, exactement comme IPv4. Par exemple, l'entreprise peut utiliser deux bits pour créer quatre sous-réseaux. Puis prendre les trois bits suivants pour créer huit sous-sous-réseaux. Il y aurait encore 11 autres bits pour créer des sous-sous-sous-réseaux et ainsi de suite.

2-Préfixe Unique Local Unicast (ULA)

Les adresses uniques locales sont créées en utilisant un identifiant global (Global ID) généré pseudo-aléatoirement. Ces adresses suivent le format suivant :
• Préfixe (7 bits) : **FC00::/7** préfixe identifiant les adresses IPv6 locales (ULA)
• Bit L : positionné à 1 si local et 0 pour le futur
• Global ID : Numéro du réseau

> Les adresses **unique local unicast** sont destinées à l'équivalent des adresses IP privées IPV4. Elles sont générées aléatoirement et permettront d'interconnecter des réseaux par VPN. Elles sont indépendantes des fournisseurs d'accès à l'Internet et ne nécessitent pas de connectivité.

3-Préfixe Link Local Unicast

Les adresses lien-local sont configurées automatiquement à l'initialisation de l'interface et permettent la communication entre nœuds voisins. L'adresse est obtenue en concaténant le préfixe **FE80::/10** aux 64 bits de l'identifiant d'interface.

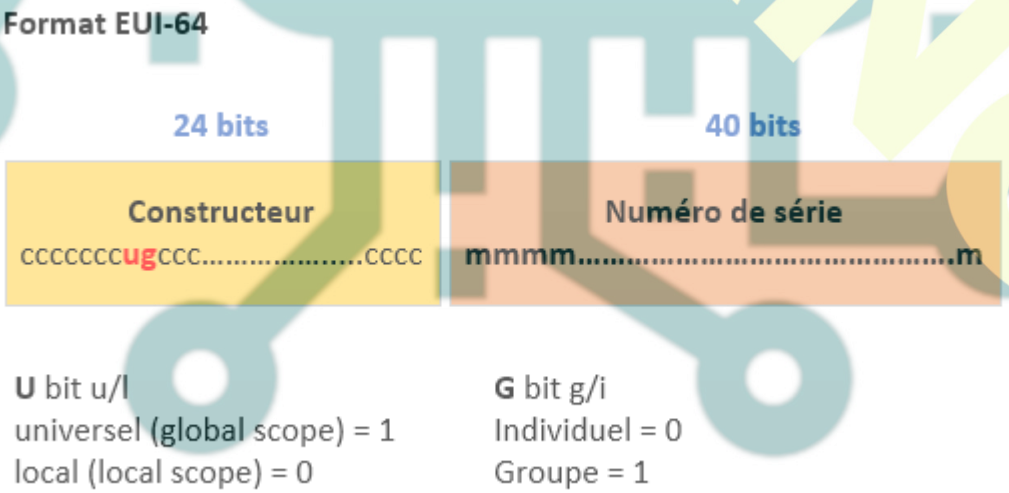
Elles n'ont qu'une spécification locale sur l'interface. Toutes ces adresses sont créées automatiquement avec 8 octets qui représentent le réseau et 8 octets représentant l'interface sur ce réseau. Elles ne sont pas routables. C'est un peu l'équivalent des adresses APIPA de la version 4.

4-Préfixe Multicast

Cette adresse spécifie un groupe d'interfaces appartenant au groupe de diffusion. Elle peut être permanente ou temporaire. Typiquement, une vidéo-conférence est temporaire. L'étendue de la diffusion peut être indiquée, ce qui permet d'indiquer si la demande doit être confinée au lien local, au site, ou au-delà.

Le préfixe vaudra donc FF00::/8, les bits du flags sont utilisés pour indiquer des cas particuliers (adresse dynamique ou permanente par exemple), le scope est utilisé pour indiquer si la portée du message est globale, site ou locale.

Cas de la construction dérivé de l'adresse MAC



Bit u et g inversé dans ipv6 pour permettre de commencer la numérotation à 1

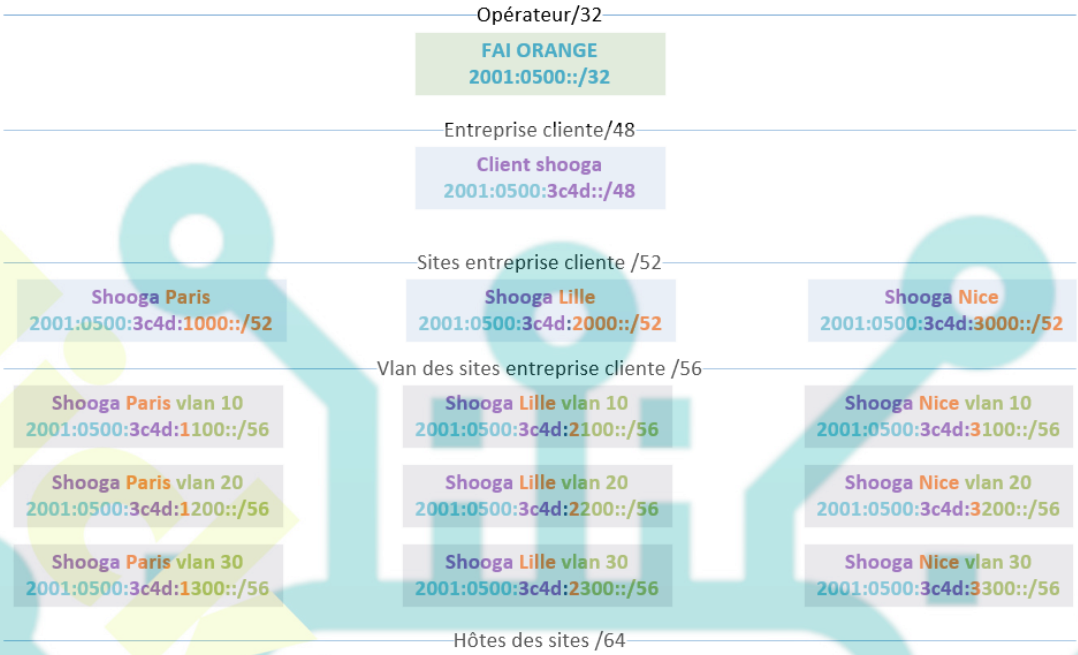
Format EUI-48

Créer un plan d'adressage IPv6

Exemple simple de découpage avec un préfixe d'adresse globale en comparaison avec ce qui peut être fait en ipv4.

192.168.1.0/24 – 2001:db8:3c4d:1::/64
192.168.2.0/24 – 2001:db8:3c4d:2::/64
192.168.3.0/24 – 2001:db8:3c4d:3::/64
192.168.4.0/24 – 2001:db8:3c4d:4::/64

Exemple complexe avec sous découpage



Les mécanismes d'adressage

Communication entre équipements

Détection d'inaccessibilité des voisins ou NUD (Neighbor Unreachability Detection) Cette fonction n'existe pas en IPv4. Elle permet d'effacer des tables de configuration d'un équipement, les voisins qui sont devenus inaccessibles (panne, changement d'adresse…) Si un routeur devient inaccessible, la table de routage peut être modifiée pour prendre en compte une autre route.

Découverte des routeurs. Ce protocole permet aux équipements de déterminer les routeurs qui sont sur leur lien physique. Dans IPv4, ces fonctionnalités sont assurées par le protocole ICMP Router Discovery.

Découverte des paramètres. Ce protocole permet aux équipements d'apprendre les différents paramètres du lien physique, par exemple, la taille du MTU, le nombre de sauts maximal autorisé, si la configuration automatique avec état (comme DHCPv6) est active… Il n'existe pas d'équivalent en IPv4.

Indication de redirection. Ce message est utilisé quand un routeur connaît une route meilleure (en nombre de sauts) pour aller à une destination.

Le rôle du routeur est important dans l'auto-configuration. Il indique à la machine via un message d'annonce de routeurs, la méthode à retenir et fournit éventuellement les

informations nécessaires à sa configuration.

Configuration manuelle

L'administrateur fixe l'adresse. Les adresses constituées entièrement de 0 ou de 1 ne jouent pas de rôle particulier dans IPv6.

https://www.site24x7.com/fr/tools/ipv6-sous-reseau-calculatrice.html

Calcul CIDR IPv6

Configuration automatique

La configuration automatique peut utiliser 3 méthodes :

Auto configuration sans état basée sur l'adresse MAC
Auto configuration DHCPv6 avec état
Auto configuration DHCPv6 sans état

Auto configuration sans état basée sur l'adresse MAC

L'autoconfiguration sans état, **SLAAC** (Stateless Automatic Auto Configuration) est une méthode par défaut de configuration IPv6 dans un environnement routé pour les routeurs **RADVD** (Router Advertisement Daemon) et les nœuds.

- Le routeur (RA-Router Advertisement) envoie les paramètres préfixe avec le Flag A activé, la MTU, la préférence, la passerelle, les Flags M et O
- L'interface construit elle-même son identifiant d'interface selon différentes méthodes MAC EUI 64 ou de manière aléatoire.

Cette méthode est utilisée pour configurer des adresses lien-local en échangeant des messages (sollicitation et annonce) avec les routeurs de voisinage.

Configuration automatique des adresses avec état basée sur DHCP

Utilisé pour configurer les adresses lien-local à l'aide d'un protocole de configuration tel que DHCP.

Ce mode est appelé DHCPv6 Stateful. Il est similaire au DHCP IPv4. Le serveur assigne l'adresse complète et des paramètres optionnels
RA Flags activés M=1 et O=1.

Configuration automatique des adresses sans état basée sur DHCP

Dans un adressage sans états, le serveur DHCP ne fournit que des informations optionnelles : serveur DNS, NTP, SIP, etc. Il ne donne aucune adresse, elles sont alors générées par SLAAC. Il ne maintient aucun état dynamique des clients qui le sollicitent.
Le RA flags M=0/1 et O=1 selon le déploiement choisi.

Les flags

Ces quatre méthodes peuvent se combiner au choix et servir à la gestion de l'adressage IPv6 ainsi qu'à la re-numérotation IPv6. Elles sont indiquées dans le champ Flags :

Configuration	Flag M	Flag O
Configuration statique ou nulle seul	0	0
Stateless Automatic Autoconfiguration (SLAAC)	0	0
DHCPv6 (Stateful) avec ou sans SLAAC	1	1
DHCPv6 Stateless avec SLAAC	0	1

Affectation des flags pour l'adressage

- Le bit **M** (*Managed address configuration*) mis à 1 indique que l'équipement ne doit pas construire lui-même l'adresse à partir de son identifiant d'interface et des préfixes reçus, mais doit demander une adresse auprès d'un serveur d'adresses.

- Le bit **O** (*Other stateful configuration*) indique que l'équipement doit interroger le serveur de configuration pour obtenir des paramètres autre que l'adresse.

https://www.youtube.com/watch?v=zFD1Pr9Qaic

Adressage IPv6

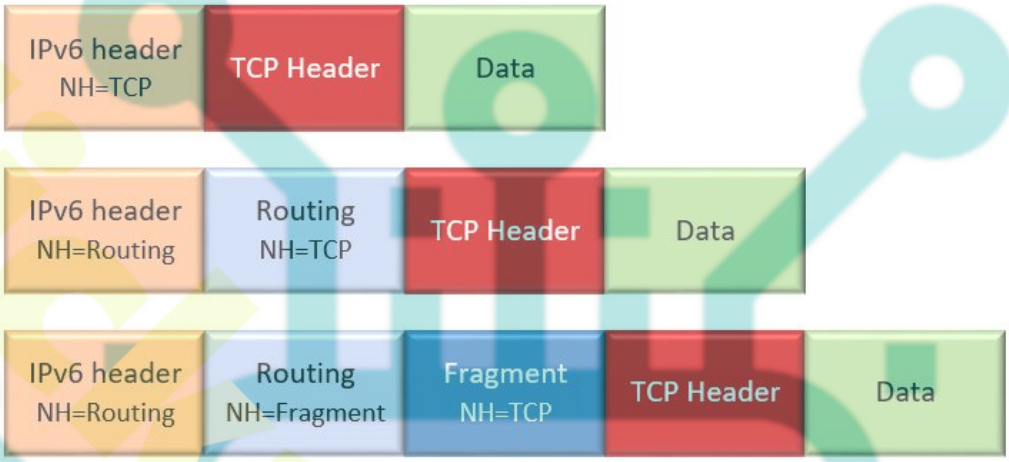
En-tête IPv6

L'en-tête du paquet IPv6 a été fixé à 40 octets, soit 2 fois plus qu'IPv4 sans les options.

La signification des champs est la suivante :

- **Version** (4 bits) : valeur du numéro de protocole internet
- **Traffic Class** (8 bits) : utilisé dans la qualité de service
- **Flow Label** (20 bits) : peut être utilisé par une source pour un traitement spécial des paquets. Ce traitement spécial pourrait être une qualité de service différente du service par défaut ou un service "temps réel".
- **Payload length** (16 bits) : taille de la charge utile en octets.
- **Next Header** (8 bits) : identifie le type de header qui suit immédiatement selon la même convention qu'IPv4.
- **Hop Limit** (8 bits) : décrémenté de 1 par chaque routeur, le paquet est détruit si ce champ atteint 0 en transit.
- **Source Address** (128 bits) : adresse source
- **Destination Address** (128 bits) : adresse destination

Il est possible qu'un ou plusieurs en-têtes d'extension suivent l'en-tête IPv6. L'en-tête de routage permet par exemple à la source de spécifier un chemin déterminé à suivre.



Les extensions les plus significatives sont :

Proche-en-Proche : cette extension, permet au routeur traitant le paquet d'échanger de l'information avec les routeurs suivants quand il rencontre un champ étrange. L'une des options la plus inquiétante du point de vue de la sécurité est l'option «Router Alert». En effet, cette option demande au routeur suivant d'examiner le contenu des paquets qu'il relaie (comme les protocoles RSVP et multicast l'exigent), au risque d'augmenter sa charge de travail (déni de service) et de le voir effectuer une mauvaise interprétation.
Fragmentation : Pour réduire le travail des routeurs intermédiaires, le processus de fragmentation se fait sur l'équipement émetteur, qui fragmente, puis sur l'équipement du récepteur, qui réassemble.
Sécurité : deux extensions de sécurité, AH pour l'authentification et ESP pour la confidentialité.
Mobilité : cette option sert à maintenir une relation entre le système mobile distant et son réseau d'origine.
Jumbogramme : cette option signale aux éléments du réseau qu'ils doivent traiter un paquet de taille extrêmement grande. Bien que cette option semble offrir une optimisation de la bande passante, elle peut perturber un ensemble d'éléments dans le réseau qui n'ont pas la capacité de gérer de tels paquets (sondes IDSs, pare-feux)

ICMPv6

ICMPv6 combine des fonctions antérieurement subdivisées à travers différents protocoles, tels qu'ICMPv4 , IGMP et ARP.

Utilisation ICMPv6

- **Résolution d'adresses** (remplace ARP)
- **Détection d'inaccessibilité des voisins**, qui permet de mettre à jour les tables de configuration (par exemple la table de routage)
- **Configuration des routeurs** (remplace ICMP router Discovery de Ipv4)
- **Apprentissage des préfixes** en fonction des annonces faites par les routeurs
- **Détection des adresses dupliquées** (équivalent de l'ARP gratuit)
- **Découverte des paramètres** (notamment le MTU, nombre de sauts avec DHCPv6)
- **Redirection** (remplace ICMP redirect d'Ipv4)

DNS

Dans le Domain Name System, les noms d'hôtes sont associés à des adresses IPv6 grâce à l'enregistrement AAAA.

```
www.ipv6.ripe.net. IN AAAA 2001:610:240:22::c100:68b
```

L'enregistrement inverse est réalisé sous ip6.arpa en inversant l'adresse écrite sous forme canonique :

```
b.8.6.0.0.0.1.c.0.0.0.0.0.0.0.0.2.2.0.0.0.4.2.0.0.1.6.0.1.0.0.2.ip6.arpa. IN PTR
www.ipv6.ripe.net
```

IPv6 sur les couches liaison et transport

Les protocoles TCP et UDP fonctionnent comme en IPv4. Le pseudo en-tête utilisé pour le calcul du code de contrôle est cependant modifié et inclut les adresses IPv6 source et destination. L'utilisation du code de contrôle est obligatoire pour UDP.

Les protocoles de la couche de liaison de type 802.3 sont adaptés pour le transport d'IPv6. Au niveau Ethernet par exemple, la valeur du champ type attribué à IPv6 est **0x86DD.**

Sur les réseaux X.25 ou Frame Relay, des adaptations sont prévues pour permettre le fonctionnement du Neighbor Discovery.

Routage IPV6

Le routage IPv6 est quasiment identique au routage IPv4. La seule différence est la taille des adresses. Avec des extensions simples, il est possible d'utiliser la totalité des algorithmes de routage d'IPv4 comme OSPF ou RIP.

IPv6 comprend également des extensions de routage simples qui prennent en charge de nouvelles capacités de routage puissantes.

- Sélection de fournisseur en fonction de la stratégie, des performances, des coûts, etc.
- Hébergement de mobilité, routage vers emplacement actuel.
- Réadressage automatique, routage vers nouvelle adresse.

Publication de routeur

Sur des liens compatibles multicast et des liens point à point, chaque routeur envoie régulièrement un paquet de publication au groupe multicast pour lui annoncer sa disponibilité. Un hôte reçoit des publications de la totalité des routeurs, constituant une liste des routeurs par défaut.

Protocole de routage

RIPng est quasiment identique à RIPv2, mais n'inclut plus d'authentification, car celle-ci repose sur les moyens de sécurité mis en place au niveau d'IPv6.

OSPF passe à la version 3. Une opération a été effectuée afin de rendre le cœur du protocole indépendant du protocole réseau IPv6, et de le restreindre au transport les informations d'adressage.

BGPv4 l'adaptation s'est limitée à changer le format de l'adresse et le numéro AS qui doit passer de deux à quatre octets.

Technologies de transition

Pour que le passage de l'IPv4 vers l'IPv6 se fasse correctement, des technologies de transition ont été mises en place. Elles permettent de supporter les réseaux mixtes (ipv4 et ipv6) car un basculement total immédiat est impossible.

Les différentes méthodes:

Dual Stack, double pile IPv4/IPv6
Traduction, exploitée chez les ISP pour connecter IPv6 à IPv4
Tunnels : solution de transition pour transporter de l'IPv6 sur de l'IPv4 et, à terme, de transporter de l'IPv4 dans de l'IPv6.

La double-pile IP, ou Dual Stack

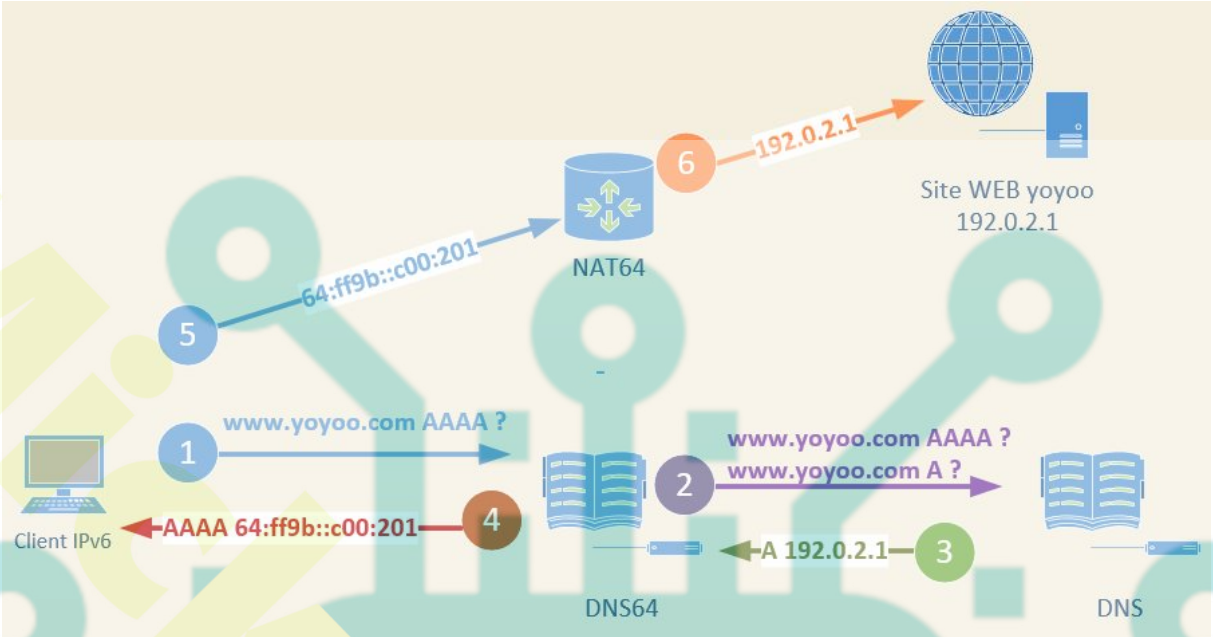
La double pile IP consiste à affecter à un équipement une adresse IPv4 et une adresse IPv6. Dans ce cas-là, les deux protocoles sont installés sur le même système, ils communiquent directement entre eux et séparément avec l'extérieur. Ce qui peut engendrer quelques problèmes de sécurité.

Si une application parle en v4 alors on passe par v4 si une application parle v6 alors on passe par v6.

Si une application passe par les deux, on privilégie v6 sauf si la portée de v4 est la plus grande (si v4 utilise une adresse publique et que v6 utilise une adresse locale)

Traduction NAT64

Pour permettre le transport des datagrammes IPv6 dans un réseau intermédiaire ne supportant qu'IPv4, on peut utiliser la fonctionnalité de NAT64 et de DNS64.



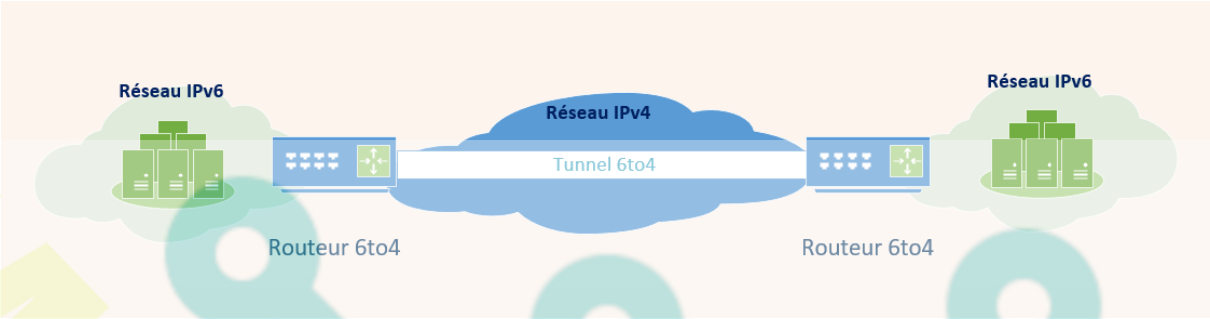
Shéma DNS64/NAT64 simplifié

Tunnels automatiques IPv6 dans IPv4

Dans le cas d'un tunnel automatique, une liaison fixe point à point est établie entre les routeurs.
Il existe à l'heure actuelle trois technologies principales pour effectuer l'acheminement d'IPv6 sous IPv4 : 6to4, ISATAP et Teredo.

1. 6to4

6to4 utilise un principe d'encapsulation du trafic IPv6 dans des paquets IPv4. Une adresse IPv6 est automatiquement attribuée dans le réseau 2002::/16
Il permet d'interconnecter deux îlots IPv6. Par contre, il a besoin de passerelles relais pour s'interconnecter au monde global IPv6



2. ISATAP

ISATAP (Intra Site Automatic Tunnel Addressing Protocol) est une technique de tunneling IPv6 qui permet de connecter IPv6 sur un réseau IPv4, similaire au tunnel 6to4 automatique .

Sur un réseau IPv4, on peut configurer un routeur en tant que routeur ISATAP « tête de réseau » auquel les hôtes IPv6 peuvent se connecter. L'adresse source IPv4 des clients et du routeur ISATAP est intégrée à l'adresse IPv6 afin que chaque périphérique sache comment se rendre de l'autre côté du réseau IPv4.

https://www.youtube.com/watch?v=F4EDPRJfD0s

Isatap Windows

3. TEREDO

Teredo est une extension de 6to4 avec traversée de NAT utilisée par Microsoft. Elle permet à un hôte connecté à un réseau IPv4 de communiquer en IPv6 avec l'extérieur sans routeur particulier sur son réseau. Le datagramme IP est encapsulé dans de l'UDP et non de l'IP ce qui permet la traversée du NAT.

CLIENT TEREDO

Un client Teredo est un nœud IPv6/IPv4 qui prend en charge une interface de tunneling Teredo. Un client Teredo communique avec un serveur Teredo pour obtenir un préfixe d'adresse à partir duquel une adresse IPv6 basée sur Teredo est configurée la communication avec d'autres clients ou hôtes Teredo sur Internet IPv6.

SERVEUR TERADO lien ICI

Un serveur Teredo est un nœud IPv6/IPv4 connecté à la fois à l'Internet IPv4 et à Internet IPv6, et prend en charge une interface de tunneling Teredo sur laquelle les paquets sont reçus. Le serveur Teredo écoute le trafic Teredo sur le port UDP 3544.

Microsoft a déployé des serveurs teredo sur Internet IPv4.

Relais TERADO Lien ICI

Un relais Teredo est un routeur IPv6/IPv4 qui peut transférer des paquets entre des clients Teredo sur Internet IPv4 et des hôtes IPv6 uniquement.

Les relais Teredo ne sont pas requis pour communiquer avec les relais Teredo spécifiques à l'hôte.

Sous Windows les fonctionnalités Direct Access et Forefront permettent de gérer les différentes technologies de tunnel et de NAT64.

https://www.youtube.com/watch?v=zbRydun1gxg

TERADO

4 . Les tunnels Broker

Pour obtenir une connectivité IPv6 on peut également faire appel à un fournisseur de tunnel IPv6 indépendant du FAI.

LE CDN

Un "réseau de livraison de contenu" (CDN –Content Delivery Network) est un service qui récupère votre contenu et le rend disponible à travers un réseau mondial de serveurs de distribution.
Le CDN peut mettre à disposition le contenu de vos serveurs sur un réseau IPv6 même si votre propre infrastructure n'est pas en capacité de le faire.

Dans le cas où l'adresse IPv6 est directement mise dans l'URL d'un site, celle-ci doit apparaître entre crochets
http://[XXX:XXXX:XXXX::XXXX:XXXX]/index.html, parce que «:» a une autre signification dans une URL.