

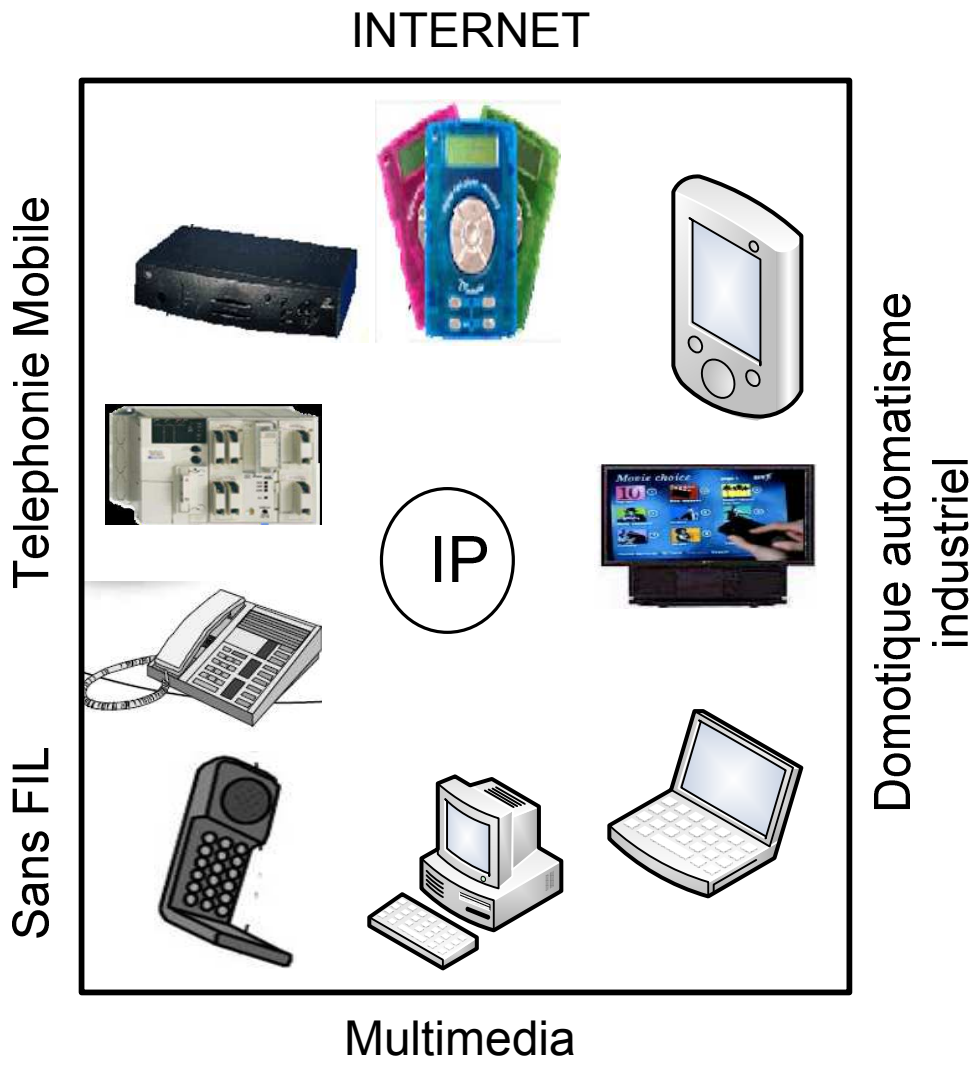
LES RESEAUX A TECHNOLOGIE

IPV6

Les technologies IPV6 (internet protocol)

1) Les limites de la technologie IPV4

On assiste ces dernières années à une saturation des demandes d'adressage IP à cause du développement général de l'Internet et des applications dérivées.



Les limites de l'IPV4 sont :

- Une Croissance de la taille des tables de routage (250 000 routes)
- IPv4 ne permet pas d'indiquer de façon pratique le type de données transportées (ToS ou Type of Service dans IPv4)
- IPv4 ne fournit pas intrinsèquement de mécanismes de sécurité comme l'authentification des paquets, leur intégrité ou leur confidentialité.

L'IPV6 a été mise place afin de remédier aux problèmes d'IPv4:

- Résoudre le problème de manque d'adresses
- Qualité de service
- Sécurité

- Mobilité
- Simplifier le traitement par les routeurs

On donne dans le tableau ci-dessous quelques définitions utiles

Nœud (node)	un module protocolaire qui implémente IPv6.
Router (routeur)	un nœud qui transmet des paquets IPv6 non explicitement adressés à lui-même.
Station (host)	tout nœud qui n'est pas un routeur
Interface	un attachement d'un nœud à une liaison.
Adresse (address)	un identifiant de la couche IPng pour une interface ou un groupe d'interfaces.
Liaison (link)	un moyen de communication ou médium sur lequel les nœuds peuvent communiquer avec la couche liaison (la couche immédiatement sous IPv6).
Double pile (Dual stack)	Une technique qui permet de fournir un support complet pour les protocoles IPV4 et IPV6

2) L'adressage IPV6

2.1) La représentation

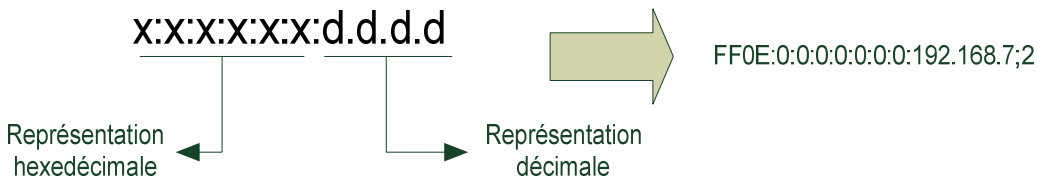
L'adresse IPV6 est constituée de **128 bits** soit 3.4 .10^{38} adresses possibles
La forme la plus appréciée est x:x:x:x:x:x:x:x, où les 'x' sont les valeurs hexadécimales des huit blocs de 2 octets chacun.

Exemples:
FEDC:BA98:7654:3210:4321:BA98:7654:3210

Pour alléger l'écriture on pourra supprimer certains zéros
1080:0:0:0:8:800:200C:417A équivaut à 1080 :0000:0000:0000:0008:0800:200C:417A
FF01:0:0:0:0:0:0:43 équivaut à FF01:0000:0000:0000:0000:0000:0000:0043

L'expression de deux "::" indiquera un ou de multiples groupes de 16 bits à 0 consécutifs
FF01::43 équivaut FF01:0:0:0:0:0:0:43
les "::" ne peuvent apparaître qu'une seule fois dans l'adresse.

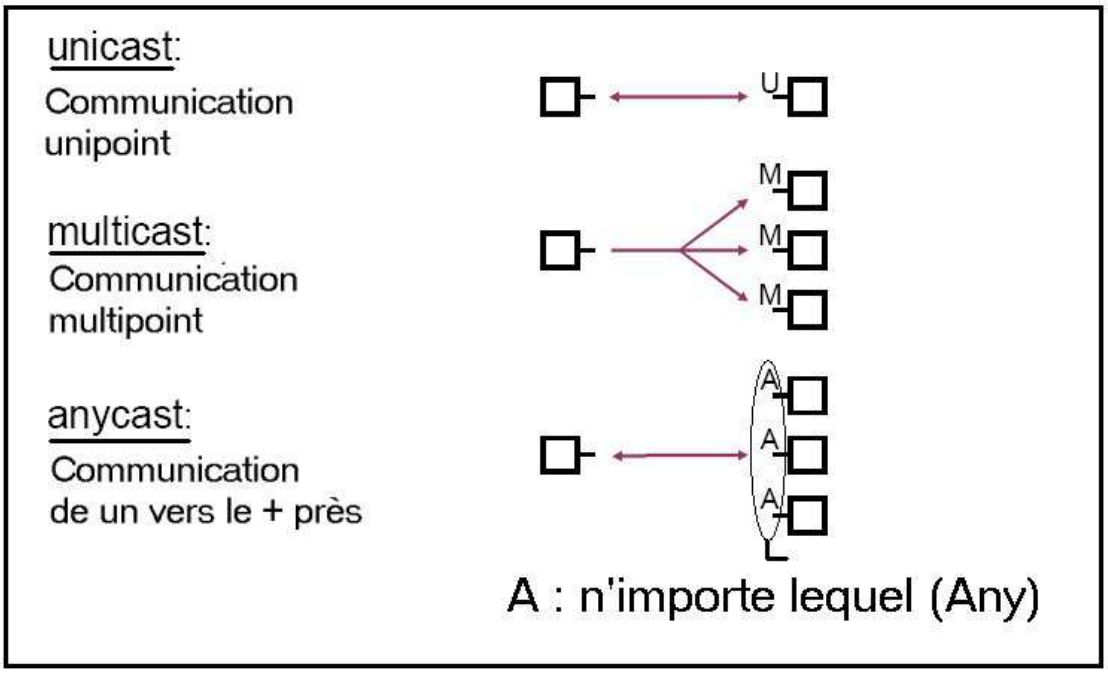
Lorsqu'on est dans un environnement mixte qui peuvent traiter des adresses IP du type IPV4 et IPV4, la notation est la suivante :



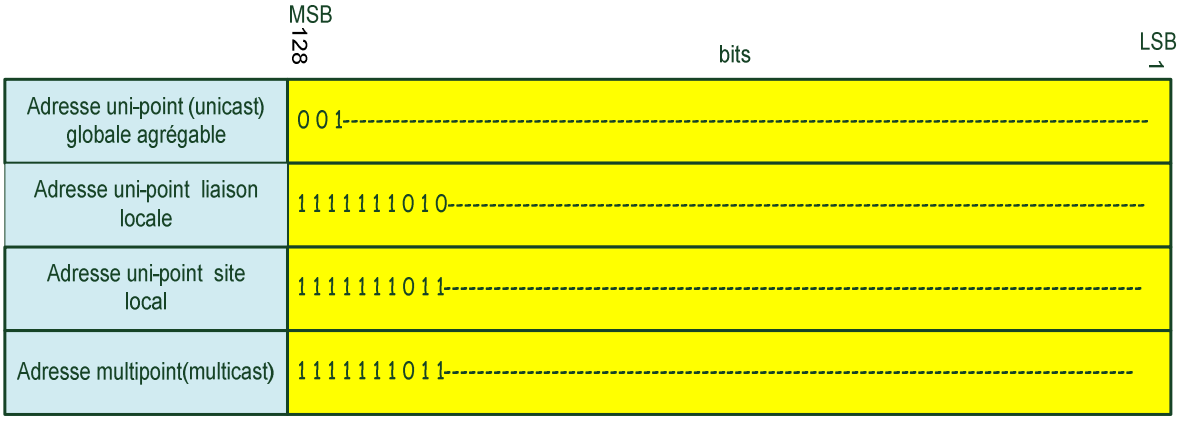
IPv6 : Préfixes
3FFE:B500::/32 L'adresse est abrégée et donnée sur 32 bits

2.2) Les 3 types d'adresses

On distingue 3 types d'adresses unicast, multicast, anycast



2.3) Le format binaire



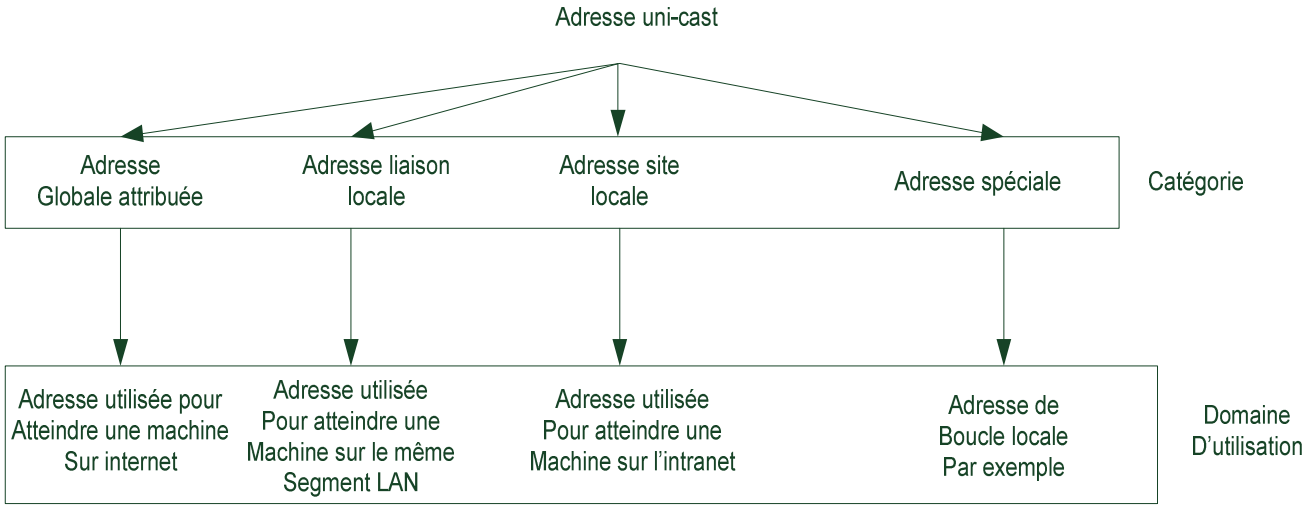
appellation	type
Nœud local	Même nœud
Lien locale	LAN
Site local	Intranet

2.4) Les adresses uni-point (unicast)

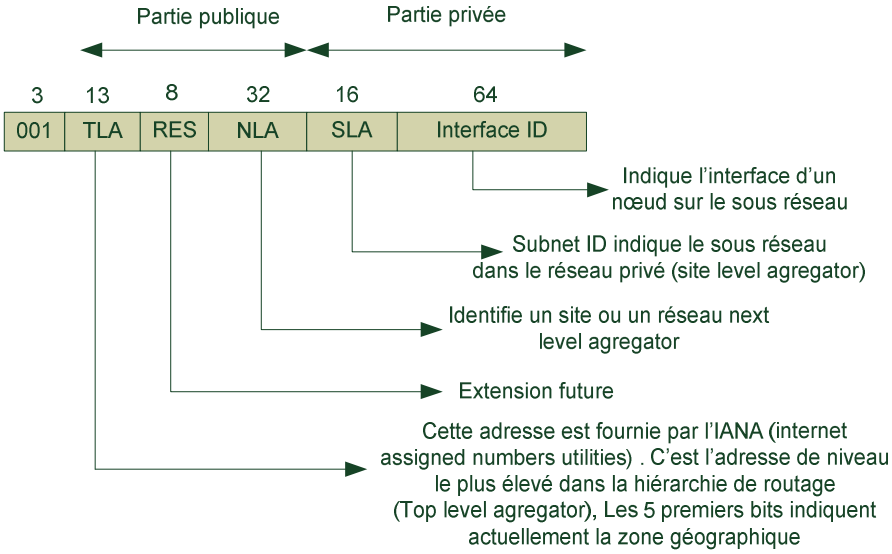
Une adresse unicast identifie une simple interface. Ceci peut être un combiné VOIP, un ordinateur personnel sur un LAN ….

2.4.1) Les différentes catégories d'adresses unicast

Une adresse unicast peut se décomposer en plusieurs catégories

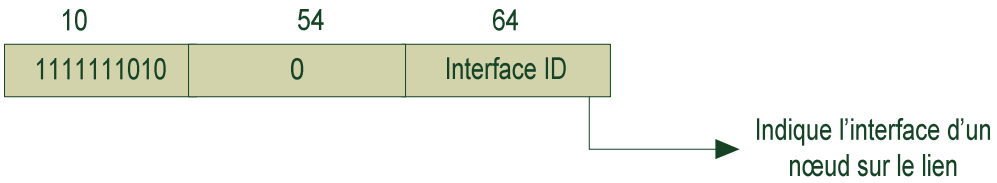


2.4.2) Adresse unicast globale attribuée



2.4.3) Adresse unicast de liaison locale

Les adresses de lien locales sont utilisées pour faire communiquer des machines sur le même lien sans l'aide d'un routeur (LAN, VLAN). Un routeur ne doit pas retransmettre un paquet ayant pour adresse source ou destination une adresse lien-local.



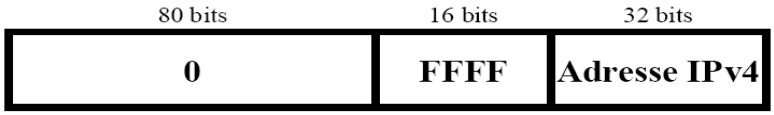
2.4.4) L'adresse unicast de boucle locale

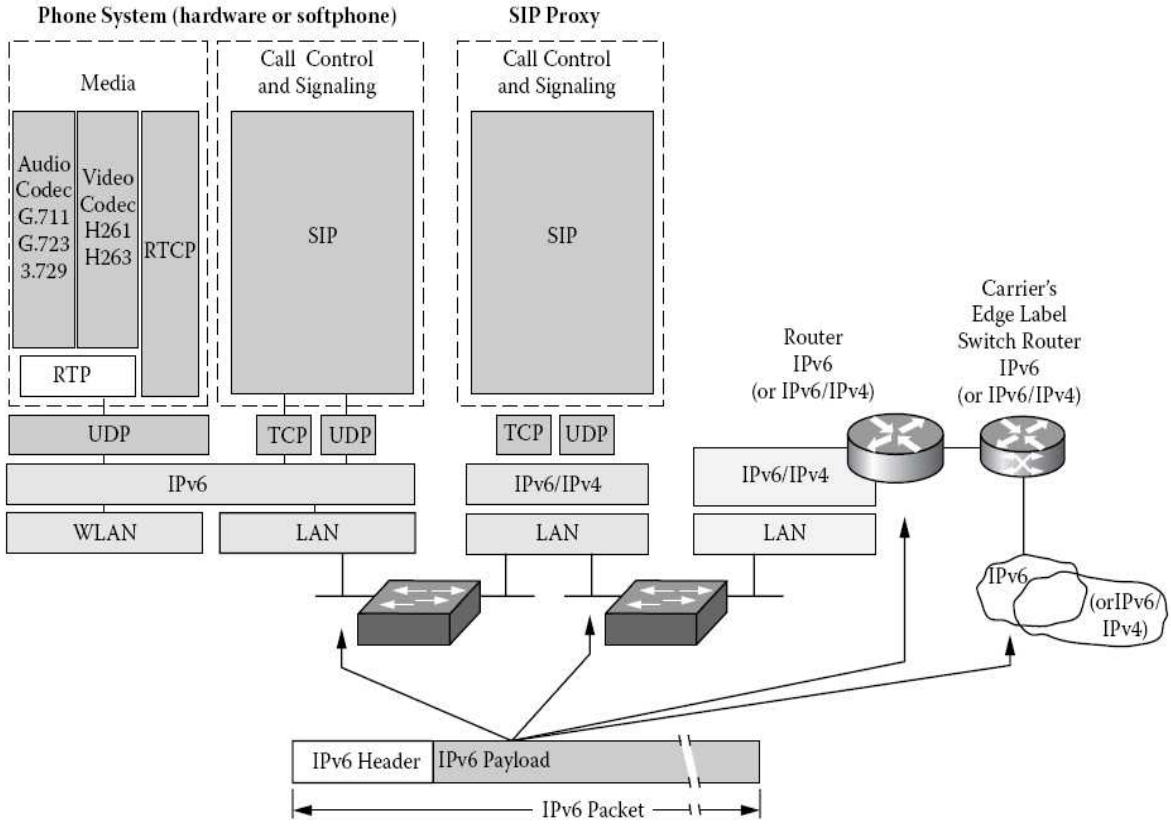
Elle est utilisée par un noeud pour s'envoyer à lui-même un paquet IPv6.

Sa valeur est 0:0:0:0:0:0:0:1 ou ::1

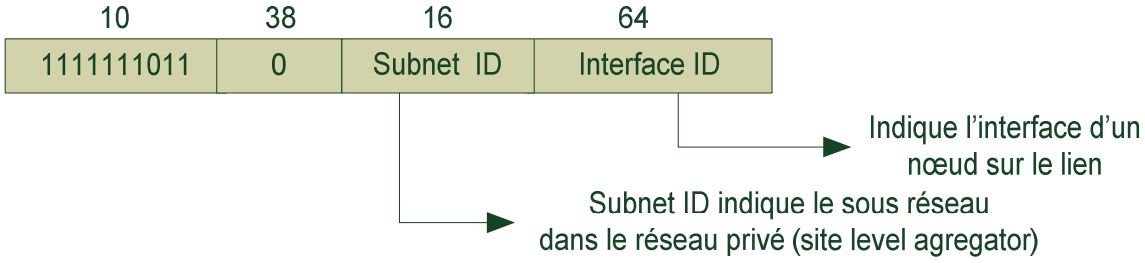
2.4.5) L'adresse unicast de IPV4 mapped IPV6

Cette forme d'adresse est conçue pour qu'une adresse d'un noeud IPv4 soit représentée en tant qu'adresse IPv6. Elle a la forme suivante :
Utilisée par les machines dual-stack pour communiquer à travers IPv4 en utilisant des adresses IPv6.





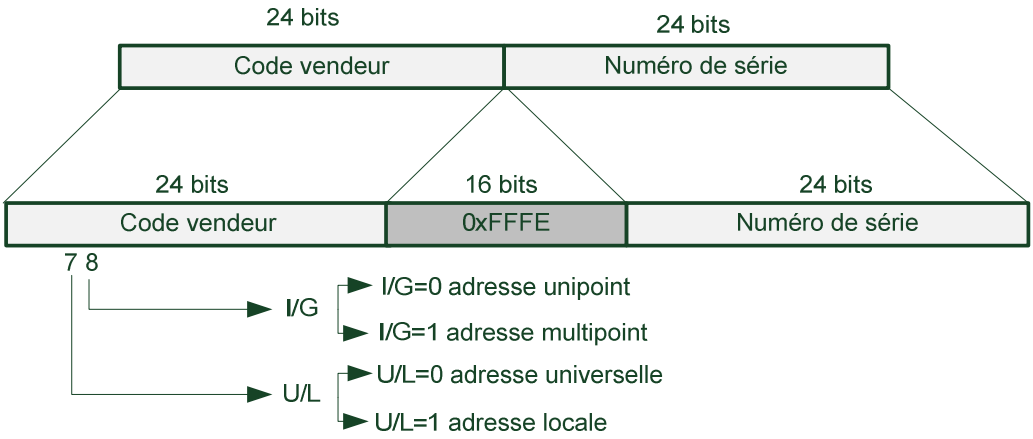
2.4.6) L'adresse unicast de site local



2.5) L'interface ID

Elle peut être l'adresse MAC de l'interface.

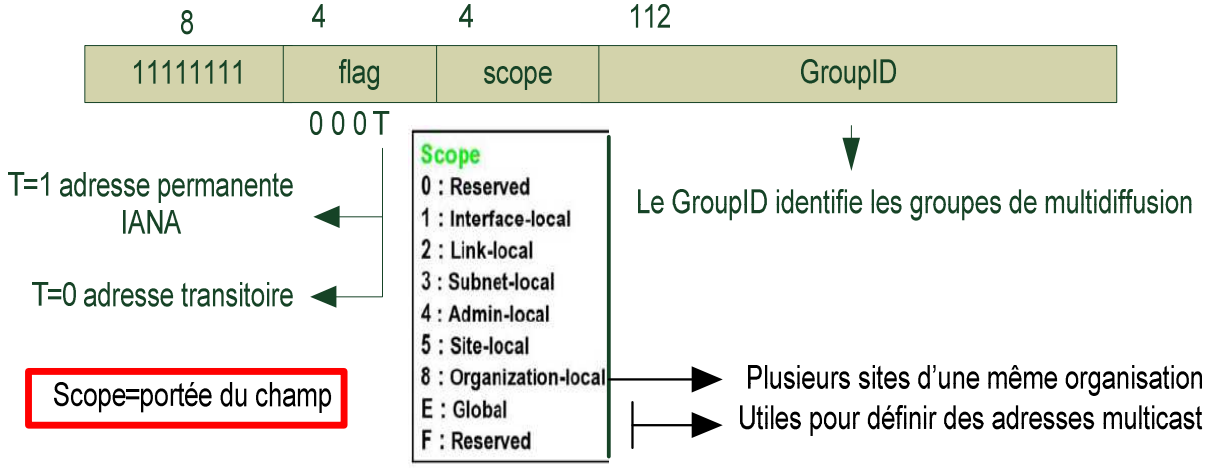
- Transformation d'une adresse MAC en identifiant d'interface (interface ID).



2.5) L'adresse multicast

Une adresse Multicast = un groupe d'interfaces. Elle remplace ainsi le Broadcast d'IPv4

- Les paquets sont transmis à **tous** les membres du groupe
- Une interface appartient à 0, 1, ou plusieurs groupes.



Les routeurs ne doivent pas router des paquets au delà de la portée du champ indiqué dans le scope.

Adresses multicast prédéfinies

Address	Description
Interface	
FF01:0:0:0:0:0:0:1	adresses de tous les noeuds
FF01:0:0:0:0:0:0:2	adresses de tous les routeurs
Lien local	
FF02:0:0:0:0:0:0:1	Adresse de tous les noeuds
FF02:0:0:0:0:0:0:2	Adresse de tous les routeurs
FF02:0:0:0:0:0:0:3	Unassigned
FF02:0:0:0:0:0:0:4	DVMRP routers
FF02:0:0:0:0:0:0:5	OSPFIGP
FF02:0:0:0:0:0:0:6	OSPFIGP designated routers
FF02:0:0:0:0:0:0:7	ST routers
FF02:0:0:0:0:0:0:8	ST hosts
FF02:0:0:0:0:0:0:9	RIP routers
FF02:0:0:0:0:0:0:A	EIGRP routers
FF02:0:0:0:0:0:0:B	Mobile agents
FF02:0:0:0:0:0:0:D	All PIM routers
FF02:0:0:0:0:0:0:E	RSVP encapsulation
FF02:0:0:0:0:0:1:1	Link name
FF02:0:0:0:0:0:1:2	All DHCP agents
FF02:0:0:0:0:1:FFXX:XXXX	Solicited-node address
Site-local scope	
FF05:0:0:0:0:0:0:2	adresses de tous les routeurs
FF05:0:0:0:0:0:1:3	All DHCP servers
FF05:0:0:0:0:0:1:4	All DHCP relays
FF05:0:0:0:0:0:1:1000 to FF05:0:0:0:0:01:13FF	Service location

2.6) L'Adresse anycast

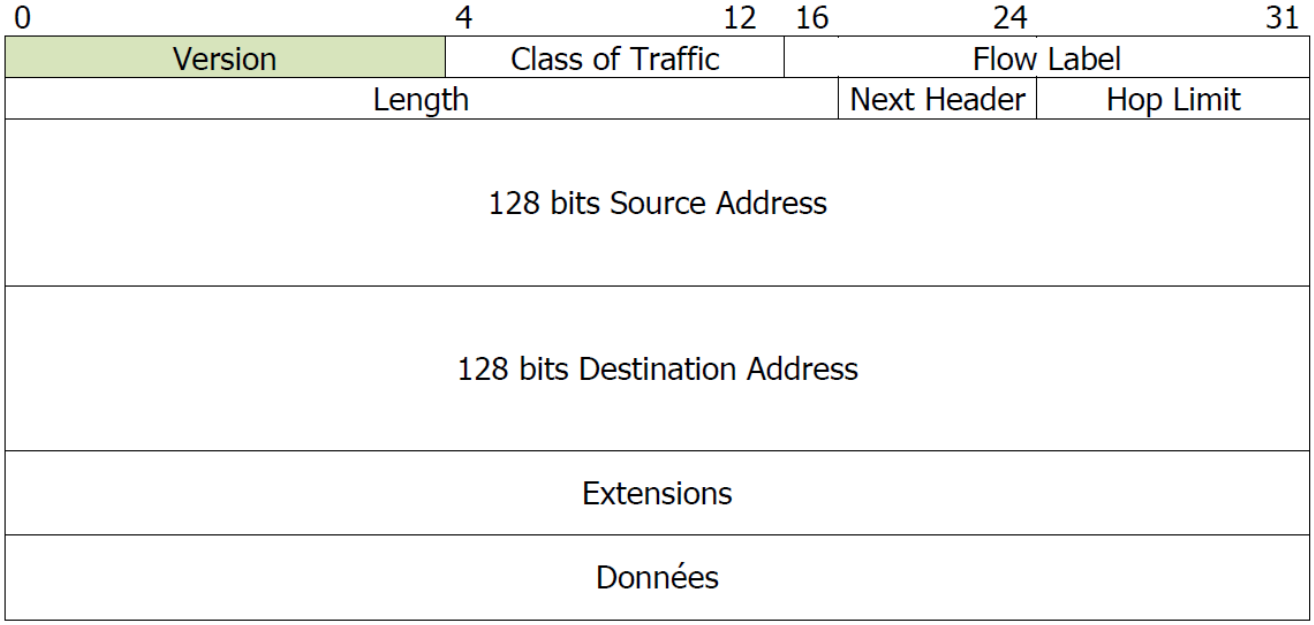
Une même adresse assignée à plusieurs interfaces.
Les paquets sont envoyés à l'interface la plus « proche »
Les Adresses **anycast** sont limitées (actuellement) à des sous-réseaux

n bits	*128 – n bits*
Subnet Prefix	00..00

Cette adresse peut être utilisée par exemple pour les applications où le noeud a besoin de communiquer avec un routeur quelconque appartenant à un ensemble de routeurs.
Une machine contenant une interface associée à une adresse anycast doit être configurée de telle sorte qu'elle sache que l'adresse est une adresse anycast.

3) Le protocole IPV6

3.1) L'entête IPV6

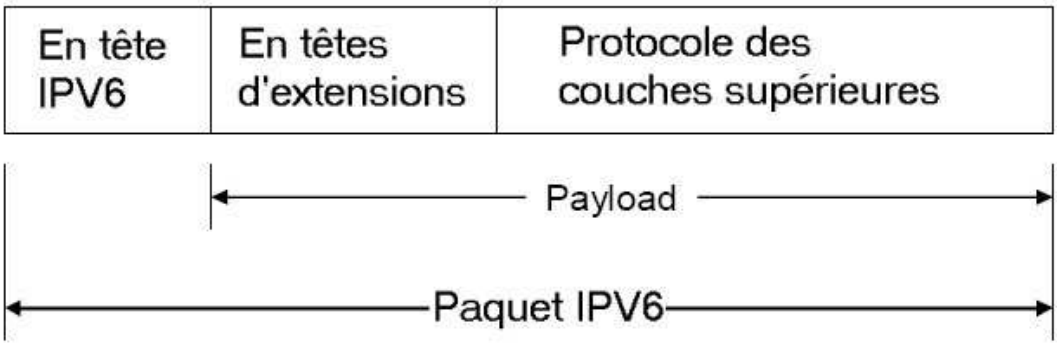


Description des différents champs

Version (4 bits): ce champ définit le numéro de version du Protocole IP. Il vaut 6. Pendant la période de transition de IPv4 vers IPv6, les routeurs devront examiner ce champ pour savoir quel type de datagramme ils routent.

Hop limit (8 bits): utilisé pour détruire les paquets qui pourraient rester dans le réseau à la suite de boucles dues aux tables de routage, ce champ est décrémenté d'une unité à chaque noeud qui retransmet le paquet (équivalent au Time To Live d'IPv4 - durée de vie). Le paquet est éliminé si le Hop limit arrive à zéro.

Payload Length (16 bits): elle représente la longueur des données après l'entête IPv6 en octets.



Next Header (8 bits): il identifie le type d'entête suivant immédiatement l'entête IPv6. Ce champ est le même que le champ « protocol » d'IPv4.

- **Source Address** (128 bits): champ adresse de l'émetteur du datagramme.
- **Destination address** (128 bits): champ adresse du destinataire du paquet. Il est possible que l'adresse ne soit pas celle du destinataire final si une option de routage est présente.

Flow Label (20 bits): peut être utilisé par une source pour nommer des séquences de paquets pour lesquels un traitement spécial de la part des routeurs IPv6 est demandé.
Ce traitement spécial pourrait être une qualité de service différente du service par défaut ou un service " temps réel ".

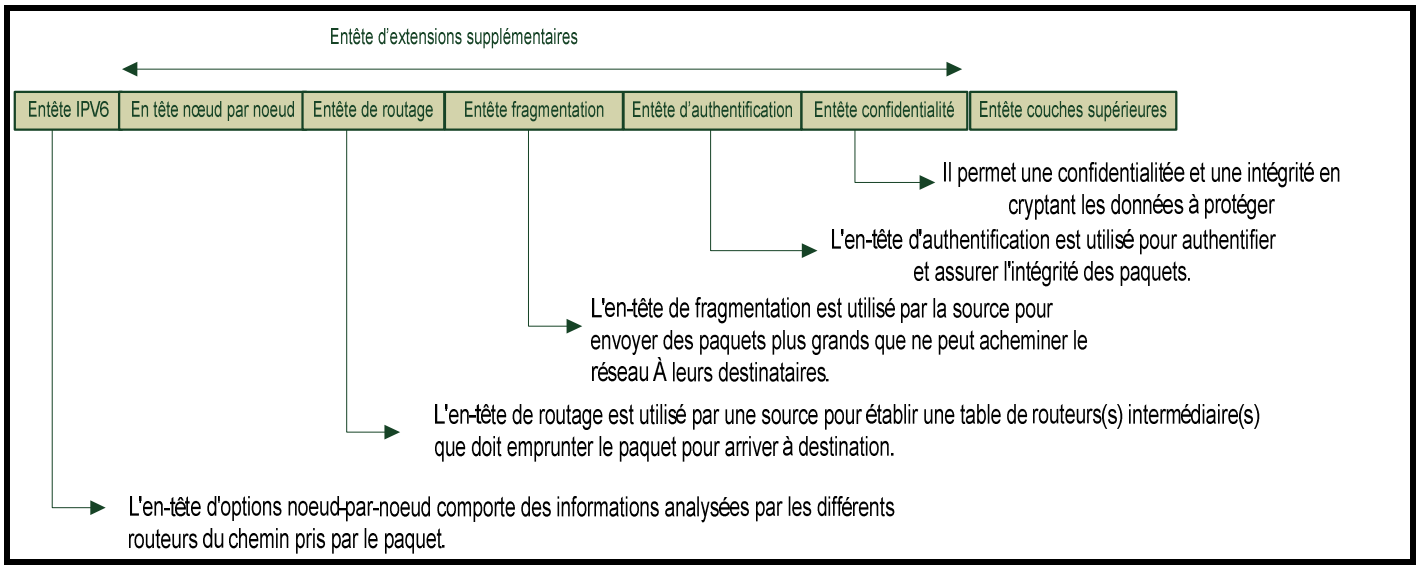
Trafic Class (8 bits) : il a été créé pour être utilisé par des noeuds origines et/ou des routeurs transmetteurs pour identifier et distinguer différentes classes ou priorités de paquets IPv6.
Dans le cas de l'architecture DiffServ (Differenciated Services), ce champ a la forme suivante :



- DSCP : DiffServ Code Point
- ECN : Explicit Congestion Notification

3.2) Les EN-TÊTES SUPPLÉMENTAIRES

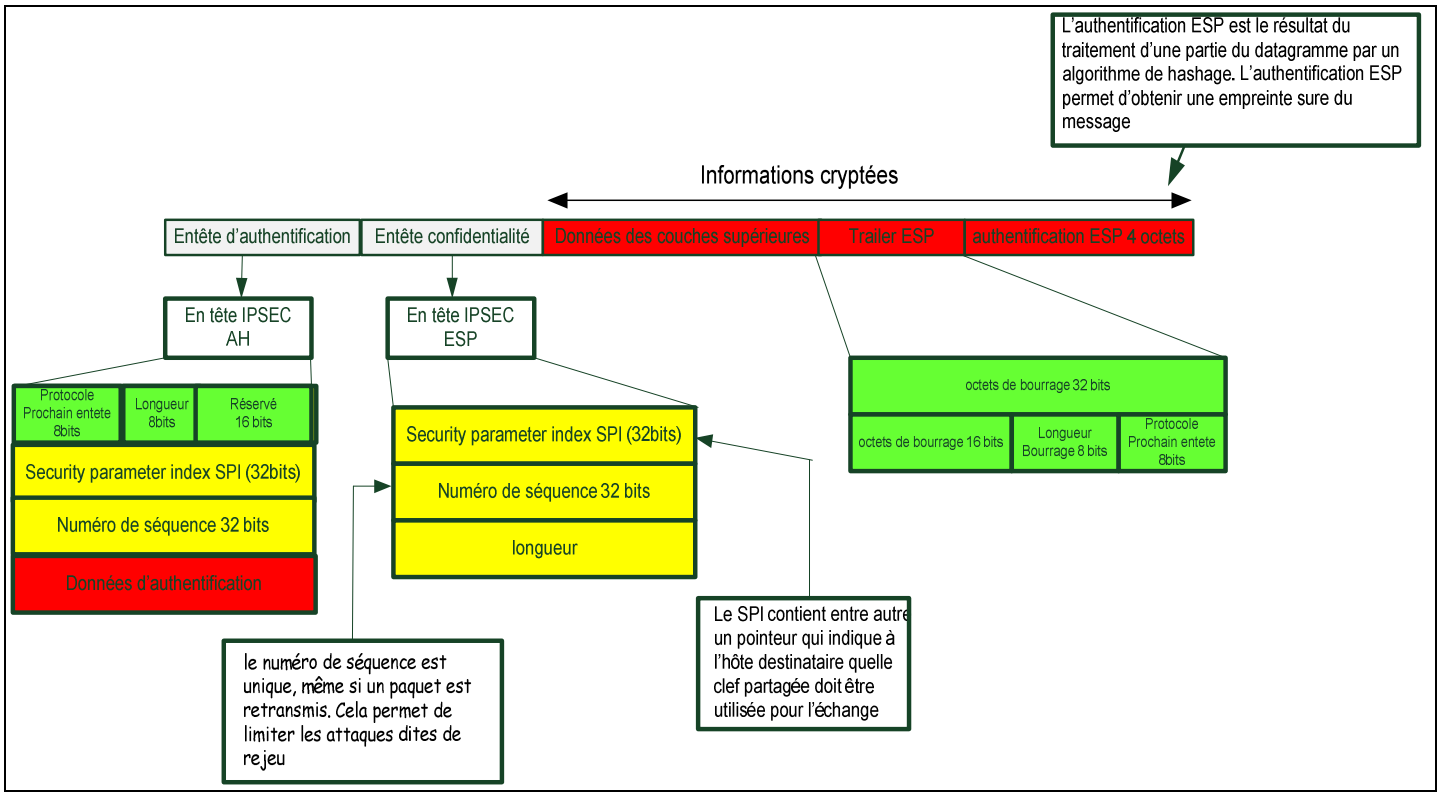
Dans la nouvelle version 6 d'IP, des informations complémentaires (en têtes d'extensions) sont codées dans des en-têtes qui doivent être placés dans le paquet entre l'en-tête IPv6 l'en-tête de la couche transport. Il y a un petit nombre d'extensions d'en-tête, chacun identifié par une valeur de Next Header distincte.
Un paquet IPv6 peut comporter aucune, une ou plusieurs en-têtes supplémentaires.
Les en-têtes supplémentaires ont un ordre :



Mise à part une exception, les en-têtes supplémentaires ne sont nullement examinés ou manipulés par les routeurs, jusqu'à ce que le paquet arrive au noeud (ou à chaque groupe de noeuds dans le cas du multicast) identifié par le champ adresse destinataire de l'entête IPv6.
A ce moment là, le premier en-tête supplémentaire, ou l'en-tête transport dans le cas d'absence d'en-tête supplémentaire, est traité. Le contenu de chaque en-tête déterminera s'il faut, ou pas, traiter l'en-tête suivant. La seule exception est l'en-tête de l'option noeud-par-nœud ("Hop-by-Hop" Options), elle porte des informations qui doivent être examinées par les noeuds du réseau.

4) securité

Ainsi toutes les implémentations d'une pile de protocole TCP/IP d'IPv6 intègre nativement le protocole IPsec (IP security), en revanche IPsec est optionnel pour la version actuelle d'IPv4 et n'est pas encore fourni en standard sur la plupart des systèmes courants.

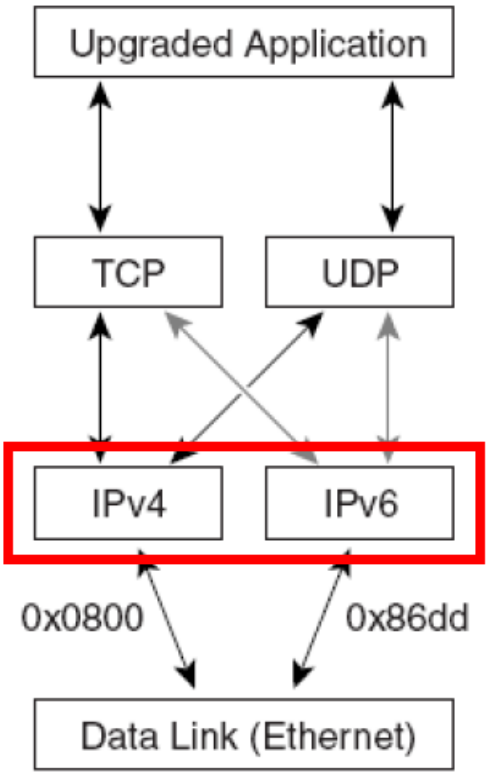


5) IPv6 techniques de transition

Les machines actuelles et à venir devront être capables de traiter des paquets IPv6 autant que les paquets IPv4. Pour transiter de la version 4 à la version 6 d'IP, deux techniques ont été mises au point : la double pile IP, l'encapsulation de Ipv6 dans Ipv4 (tunelling),.

5.1) Le modèle Dual Stack

Les équipements ont une adresse dans chacun des plans d'adressage Ipv4 et Ipv6. Ils **acheminent aussi bien les paquets Ipv6 qu'Ipv4**.
La majeure partie du code de la pile IPv4 peut être réutilisée pour IPv6. En effet, un seul branchement est nécessaire pour distinguer le bon code, en regardant le premier champ de l'entête IP qui donne le numéro de version.



Les principaux avantages de cette méthode sont **sa simplicité et sa rapidité de mise en œuvre**. Malheureusement, ce mécanisme n'est pas dénué d'inconvénients. Déployer des réseaux double pile ne résout pas le problème de la pénurie d'adresse et ne peut alors être qu'une solution à court terme. Cette technique permet néanmoins de tester rapidement le nouveau protocole sans remettre en cause l'architecture existante du réseau. De plus, déployer deux réseaux en parallèle impose de gérer et de maintenir deux réseaux logiques sur la même infrastructure physique et impose en conséquence également deux politiques de sécurité (une pour IPv4 et une pour IPv6). Cette technique n'est donc pas généralisable sur de grands réseaux à moins d'imposer une certaine surcharge de travail aux ingénieurs réseaux.

5.2) Les tunnels

L'encapsulation consiste à faire transiter des données d'un protocole donné à l'intérieur d'un autre. A l'heure actuelle, tous les routeurs ne sont pas capables de router des paquets IPv6. On place alors un paquet IPv6 à l'intérieur d'un paquet IPv4 pour le faire passer dans les réseaux anciens, et pouvoir retrouver un paquet IPv6 en sortie. On crée ainsi des tunnels Ipv6 à travers une infrastructure Ipv4. Cette méthode conserve les problèmes inhérents à IPv4 (adressage, routage, fragmentation) quoiqu'il arrive.

