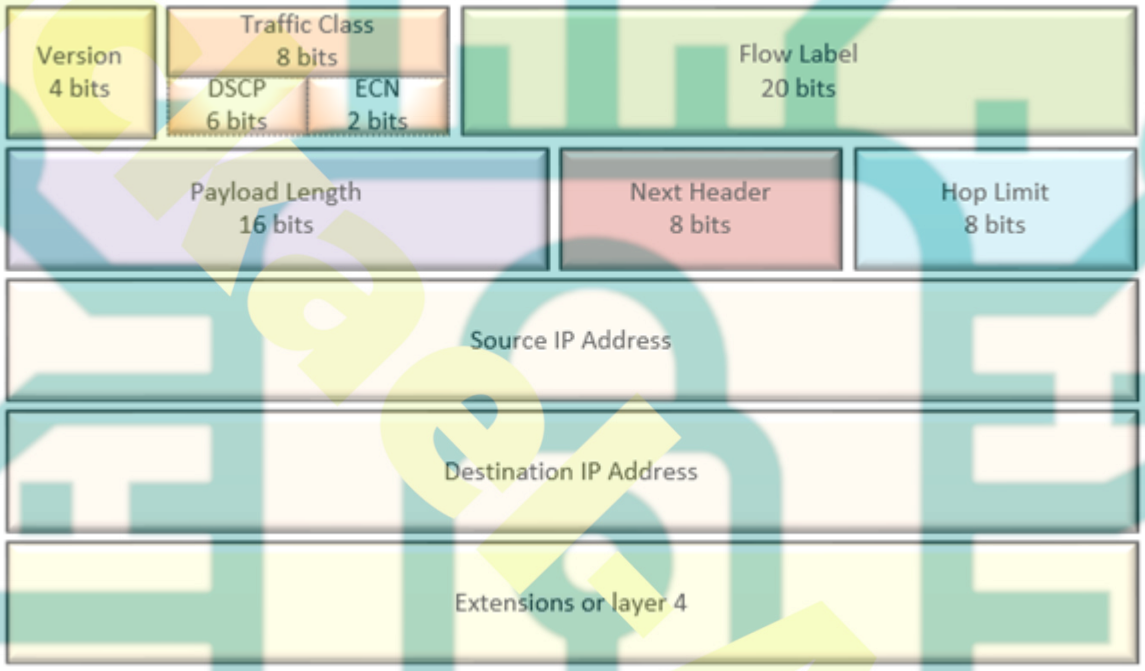
IPv6 avancé

En-tête IPv6



- **Version** – version d'IP (valeur 6 pour IPv6)
- **Traffic Class** – représente la classe de trafic, ce bloc est décomposé en 2 parties (DSCP – Différential Services Code Point) (ECN – Explicit Congestion Notification)
- **Flow Label** – conçu pour accélérer le traitement de la QOS, car la QOS peut être disséminé dans plusieurs champs IP et transport, comme : protocole de transport, numéro de port, @ip source et destination. Pour une suite de paquets, la source détermine une valeur aléatoire pour faciliter le travail des routeurs intermédiaires (le routeur n'a plus besoin de lire 5 champs pour déterminer l'appartenance à un paquet).
- **Payload Length** – détermine la longueur de la charge utile du paquet (jusqu'à 64 ko). En IPv6 on ne prend pas en compte la taille de l'en-tête. Pour des tailles supérieures à 64 Ko, le champ est mis à 0 et on utilise l'option jumbogramme du champ d'extension (la taille de la charge utilise peut-être portée jusqu'à 4 Go)
- **Next Header** – identifie le prochain en-tête de protocole (ICMP, TCP, UDP, Tunnel, sécurité…)

- **Hop Limit** – limite du nombre de sauts (64 par défaut), chaque routeur décrémente cette valeur de 1. Si un routeur reçoit la valeur 1 il détruit le paquet et envoie un message ICMP de type 3 à l'expéditeur, ce qui permet de déterminer un problème de routage.

Champ TRAFFIC CLASS

DSCP (diffserv)

RFC-4594 Service Classes (Cisco Classes)	Per Hop Behavior	PHB	IP Precedence Bits	DSCP (Binary)	Queuing	Cisco Application Examples
Standard (Best Effort)	Default Forwarding	DF	000	000000	Default + RED	Default Class
Low Priority (Scavenger)	Class Selector 1	CS1	001	001000	Min BW	Bittorrent, Games
High Throughput (Bulk Data)	Assured Forwarding 11	AF11	001	001010	BW + WRED	E-Mail, FTP, Backups
	Assured Forwarding 12	AF12	001	001100	BW + WRED	
	Assured Forwarding 13	AF13	001	001110	BW + WRED	
OAM (Network Management)	Class Selector 2	CS2	010	010000	BW	SNMP, SSH, Syslog
Low Latency (Transactional Data)	Assured Forwarding 21	AF21	010	010010	BW + WRED	WebEx, MeetingPlace, ERP
	Assured Forwarding 22	AF22	010	010100	BW + WRED	
	Assured Forwarding 23	AF23	010	010110	BW + WRED	
Broadcast Video (Cisco Signaling)	Class Selector 3	CS3	011	011000	BW	SCCP, SIP, H.323
Multimedia Streaming	Assured Forwarding 31	AF31	011	011010	BW + WRED	Video on Demand
	Assured Forwarding 32	AF32	011	011100	BW + WRED	
	Assured Forwarding 33	AF33	011	011110	BW + WRED	
Real Time Interactive	Class Selector 4	CS4	100	100000	Optional PQ	TelePresence
Multimedia Conferencing	Assured Forwarding 41	AF41	100	100010	BW + WRED	Cisco Unified Personal Communicator
	Assured Forwarding 42	AF42	100	100100	BW + WRED	
	Assured Forwarding 43	AF43	100	100110	BW + WRED	
Signaling (Cisco Broadcast Video)	Class Selector 5	CS5	101	101000	Optional PQ	IPTV, IP Video Surveillance
Telephony	Expedited Forwarding	EF	101	101110	PQ	IP Phones
Network Control	Class Selector 6	CS6	110	110000	BW	Routing Protocols

517 Pour les classe de famille (ex. AF11,12 et 13 ou AF 21,22,23ž plus la valeur est haute, moins elle est prioritaire.

ECN

4 valeurs sont définies, les 3 premières pour indiquer si l'équipement est capable de gérer la congestion. Quand les deux extrémités de la transmission prennent en charge ECN, ils marquent leurs paquets avec ECT(0) ou ECT(1).

Champ ECN		Désignation
0	0	NON ECT
0	1	ECT (1)
1	0	ECT (0)
1	1	CE (paquets ont traversés un équipement saturé)

TCP utilise deux drapeaux de l'en-tête TCP, ECN **Echo** qui sert à informer l'émetteur qu'un paquet IP marqué a bien été reçu et **CWR** (Congestion Window Reduced) qui informe le récepteur que des mesures ont été prises par l'émetteur en réduisant sa fenêtre de congestion.

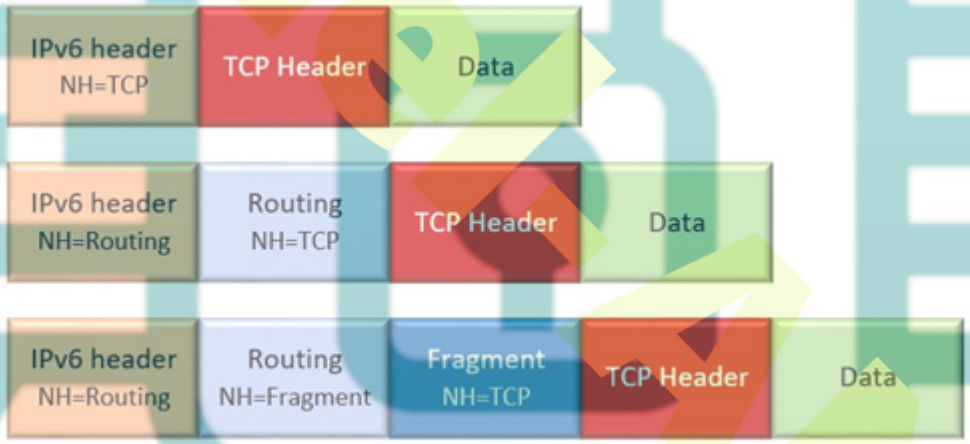
Intérêt des champs d'extension

C'est l'émetteur qui définit les en-têtes d'extension, Ils permettent d'offrir des fonctionnalités supplémentaires permettant d'impliquer le destinataire ou le routeur intermédiaire. Les options ne sont présentées que lorsqu'elles sont nécessaires. Les équipements non impliqués dans le traitement, n'ont pas besoin d'analyser les extensions.

Les extensions ne modifient pas la structure originale de l'en-tête IPv6, grâce au champ Next Header.

Codage	Description	Rôle
0	Proche en proche	Extension devant être traitée par tous les routeurs intermédiaires
4	IPv4	Transporté par IPv6 (tunnel)
6	TCP	Transporté par IPv6
17	UDP	Transporté par IPv6
41	IPv6	
43	Routage	Permet d'imposer une route différente du routage mis en œuvre
44	Fragmentation	Fragmentation du paquet si nécessaire
50	ESP	Chiffrement IPSEC
51	AH	Authentification IPSEC
58	ICMPv6	Transporté par IPv6
59	IPv6 No Next	Pas d'en-tête suivant
60	Destination	Options traitées par la destination
135	Mobilité	Mobilité
136	UDP-Lite	Transporté par IPv6 (sans checksum)
140	Shim6	Pour le multihoming
194	Jumbogramme	Taille de paquets supérieure à 64 Ko

- Les extensions peuvent se cumuler les unes aux autres



Gestion du MTU

La taille des paquets IPv6 est conditionnée par la couche de niveau 2 qui définit la trame maximum possible. Lorsqu'un datagramme IP circule, il est possible qu'il traverse des réseaux n'ayant pas les mêmes possibilités. Il faut donc, qu'il utilise la MTU la plus faible de tous les liens par lesquels il passe. Cette taille est appelée Path MTU (PMTU).

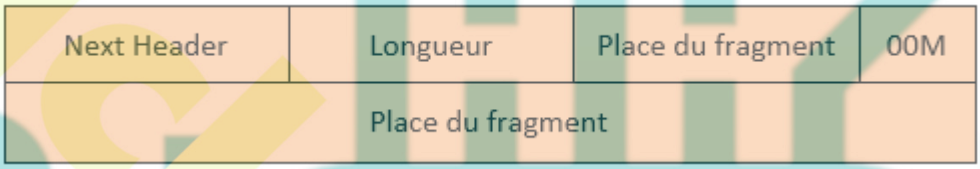
Si la taille est incompatible entre la supposition de l'expéditeur et un des routeurs traversés. Dans ce cas le routeur envoie un message

ICMP error:packet too big

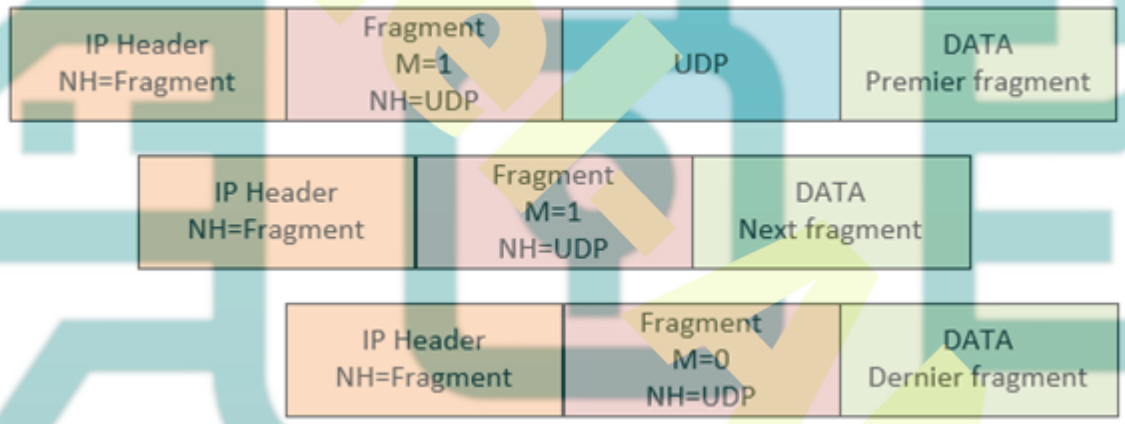
et envoie la taille recommandée. Ainsi, le reste de l'acheminement se fera avec cette nouvelle PMTU.

La fragmentation est utilisée lorsque IP la couche réseau ne peux pas adapter la MTU (UDP/NFS par exemple).

Extension de fragmentation.



Place du fragment : Indique lors du réassemblage ou les données doivent être insérées
Le bit M : s'il vaut 1 indique qu'il y aura d'autres fragments



Identification : permet de repérer les fragments appartenant à un même paquet

Découverte du MTU

Au départ, l'équipement émetteur fait l'hypothèse que le **PMTU** (Path Discovery MTU) d'un chemin X est égal au MTU du lien auquel il est directement attaché. Lorsqu'il envoie ses paquets vers le routeur, soit le paquet correspond et le routeur le transfère, soit le paquet excède la taille maximale autorisée et dans ce cas le routeur le détruit et envoie un message d'erreur ICMPv6 **« paquet trop grand »** en indiquant la MTU à utiliser.

Ensuite, le client peut utiliser la bonne taille de MTU

La MTU peut être revue en cours de transfert si, à la suite d'un changement de route, un lien de MTU plus faible est traversé.

L'émetteur vérifie aussi que le PMTU n'a pas augmenté en envoyant de temps en temps un paquet plus grand. Si celui-ci traverse le réseau sans problème, la valeur du PMTU est augmentée.

ICMPv6

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

Même s'il reprend les fonctions de la version 4, ICMPv6 intègre des fonctions supplémentaires telles que la gestion des groupes de multicast (Multicast Listener Discovery – **MLD**), la résolution d'adresse IP en adresse physique.

Avec ICMPv6, la résolution d'adresse en IPv6 s'effectue par la procédure de découverte des voisins (Neighbor Discovery Protocol ou **NDP**). Pour être voisin, deux nœuds doivent être connectés sur le même lien et utiliser le même préfixe réseau.

Message ICMPv6

Les messages ICMPv6 sont encapsules dans un paquet IPv6 avec le Next Header de valeur 58.

Type

Le champ type indique la nature du message ICMPv6 (message d'informations ou message d'erreur).

La distinction se fait grâce au bit de poids fort.

- Pour les messages d'erreurs le bit est positionné sur 0 (le champ Type utilise une valeur comprise entre 0 et 127).

- Pour les messages d'informations la valeur du champ Type est comprise entre 128 et 255.

Code

Le champ Code s'interprète en fonction de la valeur du champ Type. Il est utilisé pour ajouter une précision sur l'information ou l'erreur.

Checksum

Vérifie l'intégrité du message ICMP.

Options

Fournit les informations utiles à la fonction (configuration par exemple)

- Dans le cas d'un message d'erreur elle contient, le paquet ayant provoqué l'erreur ou un fragment de ce paquet, si la taille est supérieure à 1 280 octets.
- Pour les messages de découverte du voisinage ce champ fait le distinguo entre les messages de sollicitation de voisin ou d'une annonce de voisin.
- Les messages de test d'accessibilité embarquent des données de taille et de contenu quelconque.

Liste des messages

Type	Code	Utilisation
Gestion des erreurs		
1		Destination inaccessible
	0	- aucune route vers la destination
	1	- la communication avec la destination est interdite
	2	- hors portée de l'adresse source
	3	- l'adresse est inaccessible
	4	- le numéro de port est inaccessible
	5	- l'adresse source est filtrée par un firewall
	6	- l'adresse destination est rejetée
2		Paquet trop grand
3		Temps dépassé :
	0	- limite du nombre de sauts atteinte
	1	- temps de réassemblage dépassé
4		Erreur de paramètre :
	0	- champ d'en-tête erroné
	1	- champ d'en-tête suivant non reconnu
	2	- option non reconnue
Information		
128		Demande d'écho
129		Réponse d'écho
Gestion des groupes multicast (MLD, RFC 2710)		
130		Requête d'abonnement
131		Rapport d'abonnement
132		Fin d'abonnement
Découverte de voisins inverse (RFC 3122)		
141		Sollicitation
142		Annonce
Gestion des groupes multicast (MLDv2, RFC 3810)		
143		Rapport d'abonnement MLDv2
Mobilité (RFC 3775)		
144		Découverte d'agent mère (requête)
145		Découverte d'agent mère (réponse)
146		Sollicitation de préfixe mobile
147		Annonce de préfixe mobile
Découverte de voisins sécurisée (SEND, RFC 3971)		
148		Sollicitation de chemin de certification
149		Annonce de chemin de certification

Filtrage d'ICMP

Attention de ne pas filtrer inconsidérément ICMP car il est nécessaire à la communication (voir RFC 4890)

Découverte des voisins

Il permet à deux éléments réseau de se découvrir et d'échanger des informations de configuration (résolution @mac/@IP, adresse dupliquée)

Le protocole de découverte des voisins ou **NDP** (Neighbor Discovery Protocol) permet à un équipement de s'intégrer dans le réseau local en dialoguant avec les éléments connectés

au même support. Ce protocole n'est pas utilisé pour découvrir tout le réseau, mais il permet à un élément de connaitre les autres équipements avec lesquels il doit dialoguer.

Le champ **Hop Limit** de l'en-tête IPv6 contient la valeur 255. Les datagrammes ayant une valeur différente de 255 doivent être ignorés par le récepteur (parce que venant d'un autre réseau).

Le protocole utilise cinq types de messages

Découverte de voisins (RFC 2461)	
133	Sollicitation du routeur
134	Annonce du routeur
135	Sollicitation d'un voisin
136	Annonce d'un voisin
137	Redirection

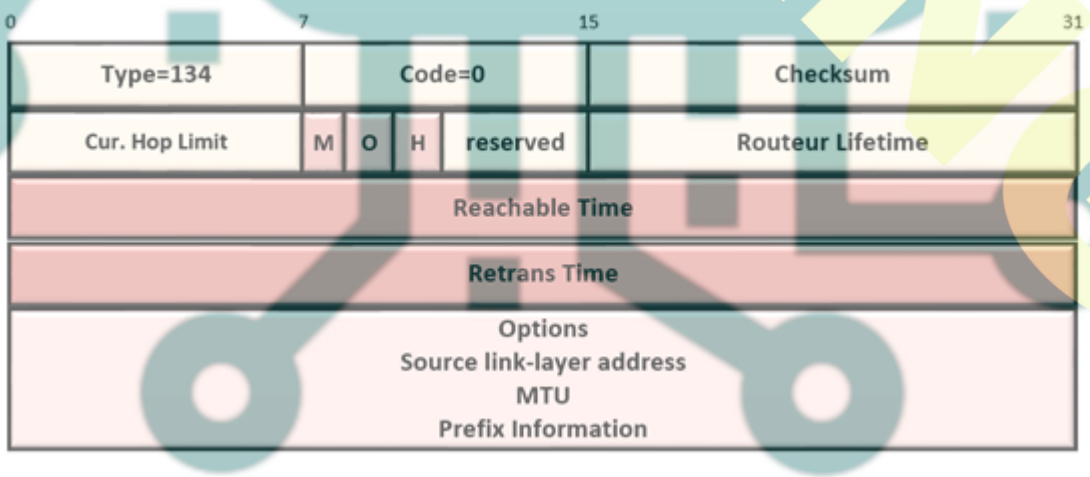
Sollicitation du routeur

Le message de sollicitation d'un routeur est émis par un équipement au démarrage pour recevoir plus rapidement des informations du routeur. Ce message est émis à l'adresse IPv6 de multicast réservée aux routeurs sur le même lien ff02::2.

Si l'équipement ne connaît pas encore son adresse source, l'**adresse non spécifiée ::/0 est utilisée**.

Le champ option contient généralement l'adresse physique de l'équipement.

Annonce du routeur



Ce message est émis périodiquement par les routeurs ou lors d'une réponse à un message de sollicitation d'un équipement.

Le champ **adresse source** contient l'**adresse de lien local du routeur**, le champ **destination** contient, l'**adresse de l'équipement** qui a émis la demande, ou l'**adresse multicast** vers de toutes les stations (**ff02::01**).

Le champ **Hop Limit** (saut max) non nul donne la valeur qui est placée dans le champ nombre de sauts des paquets IP émis.

- Le bit **M** indique que l'adresse de l'équipement doit être obtenue avec un protocole de configuration. Si l'adresse ne peut être obtenue d'un serveur, l'équipement utilise la configuration sans état en concaténant son identifiant d'interface aux préfixes obtenus.
- Le bit **O** indique que la récupération d'informations doit être obtenue (à l'exception de l'adresse).
- Le bit **H** indique que le routeur peut être utilisé comme « agent mère » pour un mobile.

Le champ **Router LifeTime** (durée de vie du routeur en secondes) donne la période pendant laquelle le routeur qui effectue les annonces sera considéré comme routeur par défaut. La valeur maximale correspond à 18 heures 12 minutes, cependant, ce message étant émis périodiquement la durée de vie d'un routeur n'a pas réellement de limites.

> Si la valeur est à 0 cela implique que l'équipement ne remplit pas les fonctions de routeur par défaut.

Le champ **Reachable Time** (durée d'accessibilité en millisecondes) indique la période pendant laquelle une information contenue dans le cache de la machine peut être considérée comme valide. A la fin de cette période, un message de détection d'inaccessibilité est émis pour vérifier l'exactitude de l'information.

Le champ **Retrans Time** (temporisation de retransmission en millisecondes) donne la période entre deux émissions non sollicitées de ce message. Il sert à la détection d'inaccessibilité pour les équipements.

> Ce message peut transporter les options : adresse physique de la source, MTU, information sur le préfixe (une ou plus)

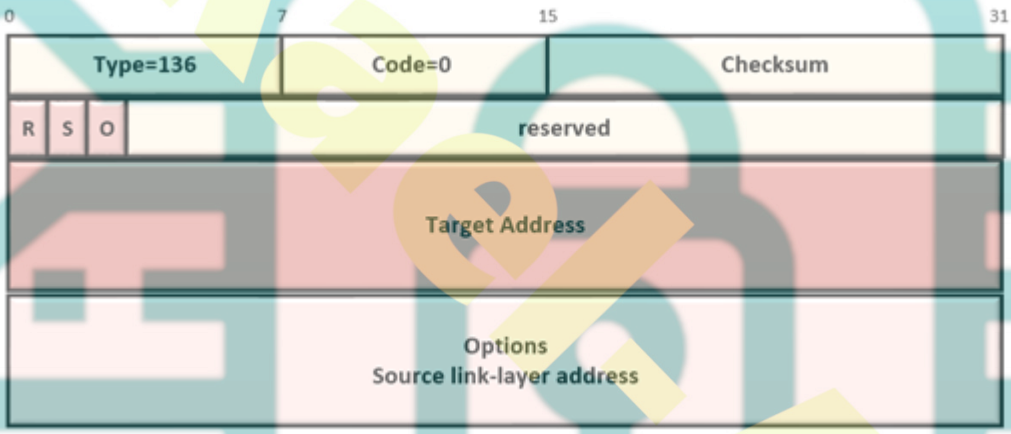
Sollicitation d'un voisin

Ce message sert à récupérer les informations d'un équipement voisin (même lien physique). Le message peut utiliser l'adresse unicast ou multicast.

Le champ adresse **source** du paquet IPv6 contient l'**adresse de lien-local**, l'adresse globale, ou l'adresse non spécifiée. Le champ **destination** contient l'**adresse de multicast** sollicité correspondant à l'adresse recherchée, ou l'**adresse de l'équipement** (dans le cas d'une détection d'inaccessibilité des voisins, NUD)

Le champ option contient le plus souvent l'adresse physique de la source.

Annonce d'un voisin



Ce message est la réponse à une sollicitation, mais il peut également être émis spontanément pour propager une information de changement d'adresse physique, ou de statut de routeur.

- Le bit **R** à 1 indique que l'émetteur est un routeur. Il est utilisé pour la détection d'un routeur qui perd son rôle de routeur par défaut.
- Le bit **S** est à 1 si l'annonce est utilisée en réponse à une sollicitation.
- Le bit **O** est à 1 indique que cette annonce doit effacer les informations se trouvant dans les caches des équipements, association adresse IP / adresses physiques.

Le champ Target Address contient :

- Si le bit S est à 1, l'adresse de la cible auquel ce message de sollicitation répond.
- Si le bit S est à 0, ce champ contient l'adresse IPv6 lien-local de l'équipement émetteur.
- L'option adresse physique de la cible contient l'adresse physique de l'émetteur.

Indication de redirection

Ce message est utilisé lorsqu'un routeur connaît une route meilleure (en nombre de sauts) vers à une destination. Dans IPv6, un matériel ne connait pas tous les préfixes de son réseau local, cela veut dire qu'une machine peut envoyer un message vers le routeur alors que le destinataire se trouve sur le même segment. Dans ce cas, le routeur émet un message de redirection pour corriger la demande de l'émetteur.

Le champ adresse **cible** contient l'adresse IPv6 de l'équipement vers lequel les paquets doivent être émis. Le champ adresse **destination** contient l'adresse IPv6 de l'équipement pour lequel la redirection s'applique.

Les options contiennent l'adresse physique du nouveau routeur et l'en-tête du paquet redirigé.

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
```

Le RR de type AAAA (quad A) enregistre les correspondances nom/adresse IPv6. Le code réservé de ce nouveau type d'enregistrement de ressources vaut 28.

Le nouveau sous-domaine ip6.arpa. est dédié à la résolution DNS inverse en IPv6. La résolution DNS inverse utilise, pour IPv6, la notion de quartet (nibble correspond à un chiffre hexadécimal).

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

```
b.8.6.0.0.0.1.c.0.0.0.0.0.0.0.0.2.2.0.0.0.0.4.2.0.0.1.6.0.1.0.0.2.ip6.arpa. IN PTR
www.ipv6.ripe.net
```

Cependant, il faut faire attention avec une telle configuration car certains résolveurs recherchent prioritairement un enregistrement AAAA avant un enregistrement A, et ce,

même si l'hôte exécutant le résolveur n'a qu'une connexion IPv6 limitée (une simple adresse locale au lien).

Découverte de la liste de serveurs DNS récursifs

La communauté IPv6 a mis en œuvre 3 mécanismes de découverte automatique des serveurs DNS récursifs avec ou sans DHCPv6.

UDP et TCP

Les modifications apportées aux protocoles de niveau 4 UDP et TCP sont minimes.

La principale modification à ces protocoles concerne le checksum, il a été adapté au format de paquet IPv6 et englobe le pseudo-en-tête. De plus, pour UDP, le checksum qui était facultatif en IPv4, devient obligatoire.

Un autre changement au niveau des protocoles de niveau 4 concerne la prise en compte de l'option jumbogramme de l'extension proche-en-proche.

Gestion des jumbogrammes

Pour le protocole UDP, si la longueur des données excède 65 535 octets, le champ longueur est mis à 0. Le récepteur détermine la longueur des données par la connaissance de la taille dans l'option jumbogramme.

Le protocole TCP pose plus de problèmes. En effet, bien que les messages TCP ne contiennent pas de champ longueur, plusieurs compteurs sont codés sur 16 bits.

UDP-lite

UDP-lite permet de remonter aux couches supérieures des données erronées pendant leur transport. En principe, comme l'intégrité n'est pas respectée on rejette ces paquets. Cependant, la plupart des décodeurs de flux multimédias sont capables de supporter un certain nombre d'erreurs binaires dans un flux de données.

> Pour améliorer la qualité perçue par l'utilisateur, il est donc préférable d'accepter des paquets erronés plutôt que de rejeter un bloc complet

d'information.

Le format de la trame reste le même qu'UDP, seul le contenu du champ longueur change. Si la longueur est 0, UDP-lite considère que tout le checksum couvre tout le paquet.

- La valeur **8** indique que seul l'en-tête UDP est protégé par le checksum.
- Les valeurs comprises entre **1 et 7** sont interdites car le checksum UDP-lite doit toujours couvrir l'en-tête.
- Une valeur supérieure à **8** indique qu'une partie des données sont protégées.

IPv6 sur les couches liaison

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 :

- La 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.

Routage statique

Routage pour ipv4

ip route 0.0.0.0 0.0.0.0 10.0.24.1

Routage pour ipv6

ipv6 route ::/0 2001:cafe:deca:12::2

Protocoles de routage internes

Ces protocoles de routage profitent des propriétés intégrées dans la nouvelle version comme l'authentification ou le multicast.

RIPng

RIPng est le premier protocole de routage dynamique proposé pour IPv6 (RFC 2080) RIPng est une simple extension à IPv6 du protocole RIPv2 d'IPv4. Il en hérite les mêmes limitations d'utilisation (maximum de 15 sauts par exemple).

Fonctionnement

Le format des paquets RIPng, est très proche de celui des paquets du protocole RIPv2. Seule la fonction d'authentification a disparu. Du fait de l'apparition d'IPsec dans IPv6.

Pour résoudre les problèmes de convergence ("comptage jusqu'à l'infini"), la valeur maximale de métrique ("infini") est 16.

Si le champ métrique d'une entrée vaut 0xFF, le champ préfixe de cette entrée donne l'adresse d'un routeur (prochain saut).

Dans RIPv2, cette possibilité était indiquée dans chaque information de routage, dans RIPng l'indication du prochain saut est valable pour toutes les routes qui suivent jusqu'à la fin du paquet ou jusqu'à la prochaine entrée de ce type. Ainsi, bien que les adresses soient quatre fois plus grandes qu'en IPv4, la taille des informations de routage est la même que dans RIPv2.

Les paquets RIPng sont émis vers l'adresse de multicast all-rip-router **FF02::9** et encapsulés dans un paquet UDP avec le numéro de port 521.

OSPFv3

En IPv6, la notion IPv4 de sous-réseau est remplacée par celle de lien.

Un lien correspond à un ensemble de machines directement connectées au niveau de la couche liaison. Une aire correspond à un ensemble de réseaux interconnectés. La notion de portée (lien, aire, …) utilise le mécanisme de portée d'IPv6.

OSPF a réalisé à une modification du format des champs adresses pour accepter les adresses IPv6. Les informations d'adressage ont été retirées des formats des paquets et des LSA (Link State Advertisements) mais conservées pour les LSUA (Link State Update Packets) qui utilisent un champ "LSA payload" contenant une adresse IPv6.

Les LSA contiennent uniquement des informations sur la topologie du réseau, les routeurs voisins étant identifiés par un numéro de routeur (Router_ID). Un champ diffusion a été ajouté afin de déterminer la portée des paquets (diffusion sur le lien-local, dans l'aire ou dans le domaine de routage).

Un lien peut supporter plusieurs instances du protocole OSPFv3, ce qui permet de l'utiliser plus facilement sur des liens partagés entre plusieurs domaines de routage. OSPFv3 utilise des adresses lien-local pour l'échange sur les liens.

Le mécanisme de sécurité de OSPFv2 a été remplacé par IPsec.

Routage externe

BGP

En IPv4 comme en IPv6, cette notion de domaine d'administration est représentée par un numéro de système autonome codé actuellement sur 2 octets (AS : Autonomous System).

BGP4 est le protocole de routage externe actuellement utilisé pour le routage global de l'Internet IPv4. Ce protocole contient une évolution (RFC 2858) qui rend BGP4 multi-protocole en introduisant la notion de famille d'adresse (ex. IPv4, IPv6, IPX…) et de sous-famille d'adresse (ex. unicast, multicast).

L'adaptation multi-protocole de BGP4 est assez simple car elle ne concerne que les trois attributs dont le format dépend de l'adresse soit :

- **NLRI** : Network Layer Reachability Informations (suite de préfixes)
- **NEXT_HOP** : Adresse IP où il faut router les NLRI
- **AGGREGATOR** : Adresse IP du routeur qui a fait une agrégation de préfixes.

Pour réaliser cette adaptation, BGP4+ introduit deux nouveaux attributs qui indiquent que l'on annonce des informations de routage autres que les routes unicast IPv4.

- **MP_REACH_NLRI** (Multiprotocol Reachable NLRI)
- **MP_UNREACH_NLRI** (Multiprotocol Unreachable NLRI)

Les implémentations du RFC 2858 sont souvent appelées MBGP (pour le multicast) ou BGP4+ (pour IPv6).

> Les numéros d'AS utilisés pour IPv4 servent aussi pour IPv6.

Règles d'annonce et d'agrégation

Pour assurer une bonne administration du routage IPv6 :

- Ne pas annoncer les différents sous-réseaux d'un site à l'extérieur de ce site, mais au contraire annoncer une route unique pour tout le site ;
- Aux frontières du plan d'adressage agrégé, regrouper les différents NLA en un seul préfixe ;
- Les adresses non globales (lien local, site local) ne doivent pas être annoncées.
- Un site ne doit pas annoncer de préfixe plus long que /48.

> Dans le routage entre nœuds d'interconnexion, seuls existent des annonces de longueur /35 pour les préfixes "plan autorités régionales" (2001:xxx) et 2002::/16 (6to4).

IPv6 et la mobilité (MIPv6)

Le groupe de travail Mobile IP s'est donc appuyé sur une solution basée sur deux adresses IP et sur le routage « normal » des paquets pour assurer la gestion de la mobilité des nœuds. MIPv6 définit l'emploi des éléments suivants :

- Les en-têtes d'extension protocolaire (protocole 135)
- Les en-têtes de routage (nouveau type 2)
- Les en-têtes destination
- Les mécanismes d'annonce des routeurs (ICMPv6)
- La gestion de l'obsolescence des adresses
- La sécurisation des paquets (IPsec).

Vue générale de la gestion de la mobilité IPv6

Le mécanisme de configuration sans état permet au terminal mobile (MN : *Mobile Node*) d'acquérir une adresse IPv6 globale topologiquement valide et peut dès lors communiquer normalement. La détection de mouvement profite du mécanisme d'annonce des routeurs.

MIP (Mobile IP) permet au mobile de conserver l'adresse utilisée dans son réseau d'attachement le **home address** (HoA) ou adresse du réseau mère Ainsi, du point de vue des couches supérieures, le mobile conserve son adresse mère (HoA) quelle que soit sa position géographique. Par ailleurs, il acquiert une adresse nouvelle temporaire appelée **care-of address** (CoA) locale dans chacun des réseaux visités (réseaux étrangers).

Cette adresse temporaire est utilisée pour localiser le mobile.

> **Du point de vue de la pile IPv6** le nœud mobile communique toujours avec l'adresse temporaire (sauf lorsqu'il est attaché à son réseau mère).
> **Du point de vue des couches supérieures** le mobile communique toujours avec son adresse mère.

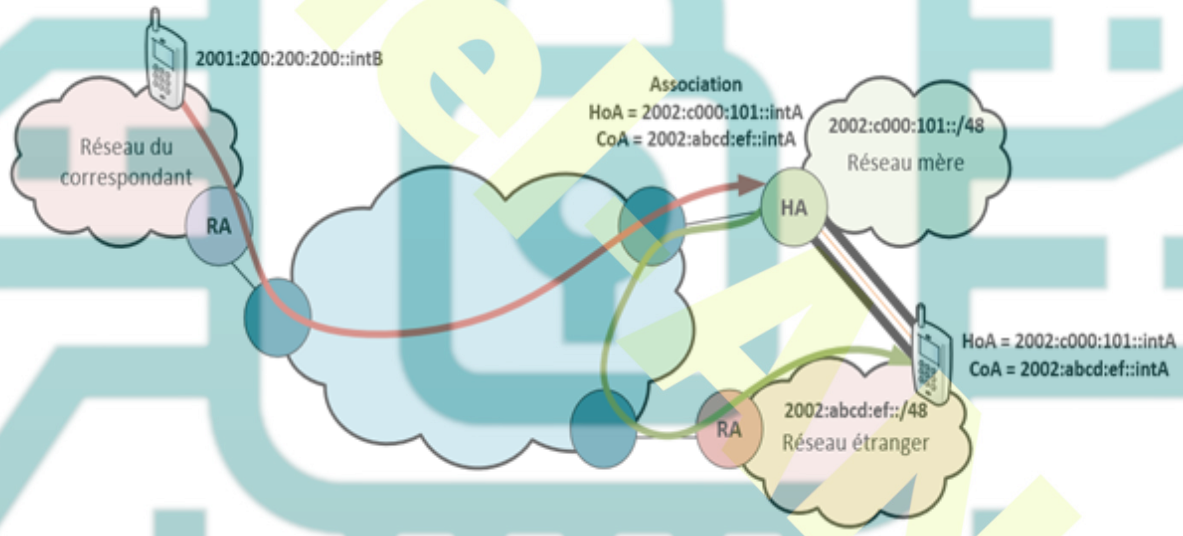
Une nouvelle entité, le **home agent** (HA) ou agent mère, située dans le réseau mère est chargé d'assurer la correspondance entre la HoA et la CoA du mobile lorsque celui-ci est attaché à un réseau étranger. Cet agent est également chargé de réacheminer les paquets IP à destination de l'adresse mère du mobile vers l'adresse temporaire dans son réseau visité.

Le mobile dans son réseau mère

Quand le mobile est attaché au réseau mère, il dispose de son adresse mère et communique normalement en utilisant sa HoA comme adresse source. Les paquets qui lui sont destinés comprennent l'adresse mère comme adresse destination et sont routés en fonction du préfixe du réseau mère. L'agent mère est inactif. le mobile communique de la même manière que n'importe quel nœud IPv6 sur l'Internet.

Le mobile dans un réseau étranger

Lorsque le mobile est attaché à un réseau étranger, il dispose de son adresse mère, et d'une adresse temporaire routable acquises via l'auto-configuration avec ou sans états. L'adresse temporaire est transmise à l'agent mère pour créer une association entre la HoA et cette CoA.



Cette association lui permet de faire suivre les paquets à destination de la HoA d'un des mobiles vers la CoA de ce dernier.

Il encapsule les paquets en utilisant l'extension d'en-tête IP-IP d'IPv6. Les paquets ainsi encapsulés sont protégés par IPsec.

Le paquet IP retransmis vers le mobile comporte comme adresse source celle du HA et comme adresse destination la CoA du mobile. Le mobile reçoit le paquet et aperçoit l'extension d'en-tête IP dans IP. Il supprime l'en-tête et remet le paquet aux couches supérieures comme s'il avait reçu le paquet dans son réseau mère.

Le quintuplé TCP créée lors d'une session n'est pas modifié. La communication n'est pas rompue lors du déplacement.

Lors de la réponse le principe est le même, ainsi le correspondant voit la communication comme venant directement du réseau mère du mobile.

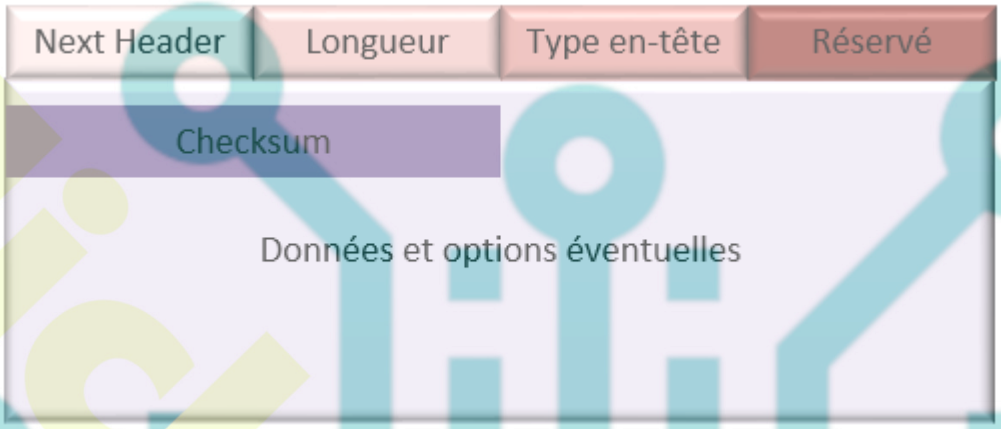
Mise à jour de l'association

Dès que le mobile a changé de CoA, il doit en informer l'agent mère en envoyant une mise à jour d'association (*binding update*). Une mise à jour d'association est envoyée régulièrement, avant le délai d'expiration, pour maintenir l'association.

Retour dans le réseau mère

Lors de son retour dans le réseau mère, le mobile doit en informer l'agent mère pour que ce dernier cesse de faire suivre les paquets à l'ancienne localisation du mobile. Il utilise une annonce de routeur contenant le préfixe de sa home address.

Format général du paquet



- Le champ en-tête suivant est pris dans le même espace de numérotation que les en-têtes d'extension d'IPv6. Dans le cas de la signalisation de mobilité, il doit valoir 59 (pas d'en-tête suivant).
- Le champ longueur de l'en-tête, en octets, ne prend pas en compte les 8 premiers octets de l'en-tête.
- Le champ type d'en-tête décrit les messages de signalisation donné au tableau Type des en-têtes de mobilité.

Type des en-têtes de mobilité	
0	Demande de rafraîchissement émise par le nœud correspondant
1	Initialisation de test d'adresse mère (HoTI)
2	Initialisation de test d'adresse temporaire (CoTI)
3	Test d'adresse mère (HoT)
4	Test d'adresse temporaire (CoT)
5	Mise à jour d'association (émise depuis le nœud mobile)
6	Acquittement de mise à jour d'association
7	Erreur de mise à jour d'association

Tableau Type

Technologies de transition

Principe du tunnel IPv6 sur IPv4

Un tunnel consiste encapsuler une unité de transfert (PDU) dans la charge utile d'un autre protocole de la même couche.

Dans le cas d'IPv6, cette technique a été définie dans le RFC 4213 sous le nom de **6in4**. L'encapsulation du paquet IPv6 dans le paquet IPv4 s'effectue en insérant le paquet IPv6 dans le champ « données » du paquet IPv4. Le champ « protocol » de l'en-tête IPv4 prend alors la valeur **41** pour indiquer IPv6. Les extrémités du tunnel (hôtes, routeurs) sont appelées **tunnel end point.**

Déploiement d'IPv6 dans les réseaux

Mécanismes de transition	Cœur de réseau	ISP	Entreprises	Particuliers
Double pile	X	X	X	X
6PE (MPLS)	X	X	X	
6to4		X	X	X
Tunnel Broker		X	X	X
TSP		X	X	X
ISATAP			X	
TEREDO		X	X	X
Relais applicatifs		X	X	X
NAT-PT		X	X	X
DSTM		X	X	X
SOCKS			X	X
VPN		X	X	X
L2TP		X	X	X

6in4

6In4 encapsule directement le paquet IPv6.
Dans un paramétrage manuel, on indiquera sur un hôte son adresse IPv6, l'adresse IPv4 du Endpoint (routeur distant) et l'adresse de la passerelle IPv6 du EndPoint.

Double pile

Cela consiste à configurer une ou plusieurs adresses IPv6 et une ou plusieurs adresses IPv4 sur les équipements du réseau. Les fournisseurs gérant le cœur de réseau supportent ce mécanisme, qui a l'avantage d'être progressif et ne concerner qu'une partie du cœur de réseau dans un premier temps.

6PE (MPLS)

Le cœur du réseau MPLS reste inchangé. 6PE permet à un fournisseur de ne faire évoluer que la partie périphérique de son réseau (*Provider Edge*) pour pouvoir transporter aussi le trafic IPv6 de ses usagers. Le routage IPv6 est réalisé par les équipements de périphérie qui attribuent une étiquette à chaque paquet IPv6.

6PE, propose l'utilisation de BGP pour créer automatiquement des tunnels dans un système autonome. Grâce aux extensions multi-protocole de BGP, il est possible de transporter des préfixes IPv6 et les étiquettes MPLS associées à ces préfixes.

Le routeur de bordure en entrée du réseau peut associer le préfixe IPv6 et le champ Next Hop correspondant à l'adresse IPv4 du routeur ayant fait l'annonce iBGP.

6to4

Le mécanisme 6to4 permet d'interconnecter entre eux des sites IPv6 isolés en créant des tunnels automatiques IPv6 dans IPv4. Le mécanisme repose sur différents composants.

- La machine terminale 6to4
- Le routeur de bordure connecté à IPv4 et IPv6, qui encapsule les paquets IPv6 dans des paquets IPv4
- Le relais 6to4 est un équipement réseau dont l'adresse est bien connue (adresse anycast).

6to4 bénéficie d'un préfixe IPv6 réservé : **2002::/16** (RFC 3587). Le préfixe IPv6 de 48 bits est créé en utilisant l'adresse IPv4 du nœud en bordure des réseaux IPv4 et IPv6.

De cette manière, 6to4 peut générer un préfixe IPv6 conforme au plan d'adressage global (16 bits pour les sous réseaux et 64 bits pour l'identifiant) pour un site en toute autonomie.

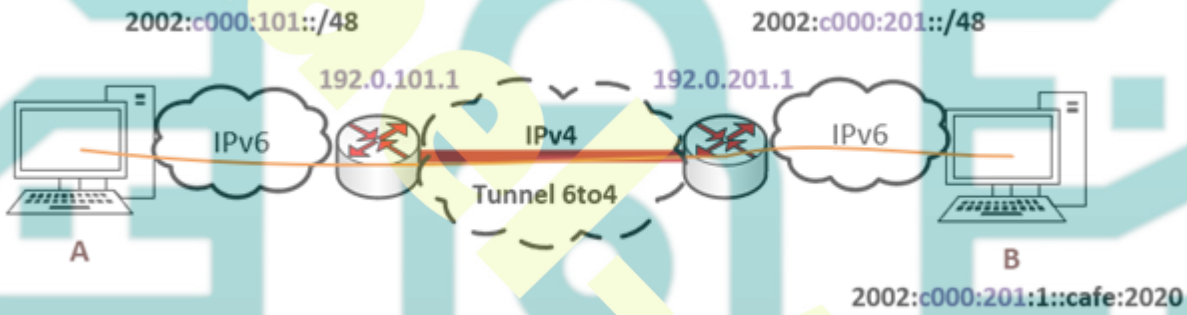
6to4 peut relier deux réseaux IPv6 à travers un nuage IPv4, cependant, les routes ne sont pas optimales car, un site isolé utilisant 6to4 n'est pas directement connecté à l'Internet v6 et doit passer par un relais qui est connecté au 2 mondes.

Dans le rfc3068, il est proposé d'utiliser une adresse anycast commune à tous ces relais à travers le monde, ce qui permettrait de joindre le routeur le plus proche et ainsi optimiser en partie le trafic.

> Actuellement, aucun fournisseur n'a intérêt à offrir un tel service mutualisé, car le trafic IPv6 de ses concurrents va charger son infrastructure au détriment de ses propres clients.

Par exemple un routeur 6to4 double pile est connecté à la fois à l'Internet v4 et à un site IPv6. Il possède une adresse IPv4, 192.28.88.1 qui va servir pour construire le préfixe 2002:c000:201::/48 (0xc0 = 192). Ce préfixe de 48 bits va être utilisé par l'ensemble des nœuds IPv6 du site.

Au niveau du routage, la figure représente l'envoi d'un paquet IPv6 de l'hôte A vers l'hôte B. Il est important de noter ici que A et B sont des hôtes ayant une adresse IPv6 prise dans le plan d'adressage 6to4.



1. La station **A** interroge le DNS pour connaître l'adresse IPv6 de la station **B** (2002:c000:201:1::cafe:2020).
2. La station **A** émet le paquet vers cette destination via le tunnel 6to4.
3. Le routeur 6to4 du site de **A** analyse l'adresse IPv6 de destination et trouve l'adresse IPv4 de l'autre extrémité du tunnel (192.0.201.1).
4. Le routeur encapsule le paquet IPv6 dans un paquet IPv4.
5. Le routeur 6to4 du site **B** désencapsule le paquet IPv6 et le route vers la station **B**.

6rd

6rd (IPv6 Rapid Deployment – RFC 5569) améliore la performance et la fiabilité par rapport au 6to4.

Ce mécanisme est utilisé par un opérateur qui souhaite offrir une connectivité IPv6 alors que son infrastructure repose sur IPv4.

Contrairement à 6to4 qui utilise un préfixe commun, 6rd utilise un préfixe IPv6 propre à l'opérateur. Ce dernier doit donc installer ses propres relais pour offrir la connectivité avec l'Internet v6. Le relais est un routeur de bordure double pile.

Le préfixe 6rd est automatiquement calculé par la box fournie par le FAI en concaténant le préfixe 6rd du FAI et tout ou partie de l'adresse IPv4 allouée sur l'interface WAN IPv4 de la box.

Le FAI contrôle les tunnels. Il peut ainsi garantir une symétrie entre l'aller et le retour et créer des tunnels plus courts. Les relais installés par l'opérateur sont propres à ses clients ce qui le différencie du 6to4 ou les relais sont mutualisés et publics.

Exemple

- L'adresse IPv4 192.0.1.200 (c000:01c8 en hexadécimal) est attribuée à une box
- L'opérateur dispose du préfixe IPv6 2001:cafe::/32 pour son domaine 6rd.
- Les adresses de toutes les box agrègent le préfixe 192.0.0.0/8 (supernetting).
- L'opérateur garde les 24 bits de poids faible comme partie significative pour distinguer les différentes box de son réseau.

Le préfixe IPv6 de chaque box aura une longueur de 56 bits, correspondant à l'association du préfixe (2001:cafe) avec la partie significative de l'adresse IPv4 (0001:00c8)
Le préfixe IPv6 pour cette box pourra être 2001:cafe:1:c8::/64

Pour permettre au client de créer des sous réseaux, le préfixe calculé pourra être 2001:cafe:1:c8::/56 Il restera alors 8 bits, au titre du SID (Subnet Identifier), pour la numérotation des sous-réseaux internes du site.

Le NAT

NAT 64/46

Pour le protocole IP, il s'agit bien de faire communiquer 2 machines, chacune n'utilisant qu'une version du protocole, IPv4 ou IPv6.

Le client ne parle qu'IPv6 et le serveur ne parle qu'IPv4 (NAT64)
Le client ne parle qu'IPv4 et le serveur ne parle qu'IPv6 (NAT46)

Un moyen, pour offrir cette connectivité, est de traduire automatiquement les paquets IPv6 du client en IPv4 pour les envoyer au serveur, et de faire la traduction inverse au retour.

Ce dispositif n'effectue pas une simple translation d'adresse, il traduit de l'en-tête IP.

Le traducteur assurant le relais entre un réseau IPv6 (coté client) et un réseau IPv4 (coté serveur) est appelé NAT64.

Quant à NAT66, il s'agit de traduction entre IPv6 et IPv6 destinée aux personnes persuadées que le NAT améliore la sécurité.

Le RFC 5202 détaille ainsi la question du NAT sur IPv6 et explique que, bien que ce soit une mauvaise idée, il faut sans doute s'attendre à le voir arriver.

Le RFC 6144 détaille les cas d'utilisation de la traduction entre IPv6 et IPv4 en distinguant l'Internet (plan d'adressage non modifiable) et un réseau (plan d'adressage modifiable).

Principe de la traduction entre protocoles IP

Les traductions peuvent utiliser le **mode sans état** (stateless)
Chaque paquet est traité isolement et contient toutes les informations nécessaires à la traduction. Cette solution est plus performante car elle traite plus de paquets.

La traduction d'adresses utilisant une adresse IPv6 embarquant une adresse IPv4 est qualifiée de sans état lorsqu'il y a une correspondance de 1 vers 1 (une adresse IPv4 = une adresse IPv6)

Le NAT peut utiliser également le **mode avec état**, le traducteur maintient la correspondance qu'il a effectué entre les 2 versions du protocole. Cela nécessite une table des correspondances en mémoire. Cette solution est utilisée lorsque le paquet Ipv4 contient trop d'informations (TTL/Hop limit, DiffServ, Payload Length).

Lorsque qu'il n'y a pas de relation1/1, la mise en correspondance d'une adresse IPv6 avec une adresse IPv4 demande une traduction d'adresse avec état. La mise en correspondance est dynamique, NAT utilise une adresse IPv4 libre, sélectionnée dans un pool d'adresses qui lui a été fourni.

Comme pour le NAT44, il n'y a pas assez d'adresses IPv4, on utilise le numéro de port de la couche de transport pour reconnaitre les nœuds IPv6.

Création de l'adresse

Le RFC définit le préfixe réservé **64:ff9b::/96** ainsi que les règles pour embarquer une adresse IPv4 dans des préfixes IPv6 de 32, 40, 48, 56, 64 ou 96 bits.

Les 8 bits aux positions 64 à 71 sont réservés et doivent être nuls. Cela implique que pour les préfixes de longueur 40, 48 et 56 l'adresse IPv4 est scindée en 2 parties.

La méthode consiste à inclure les 32 bits l'adresse IPv4 à la suite du préfixe IPv6. Le mécanisme d'inclusion de l'adresse IPv4 est diffèrent en fonction de la longueur du préfixe.

Une adresse IPv6 incorporant une adresse IPv4 est **traduisible** en IPv4 si elle est unique et routable. Elle est **convertible** si elle ne fait que représenter un nœud IPv4 dans l'espace d'adressage IPv6 interne.

Le préfixe 64:ff9b::/96 est donc réservé aux adresses traduisible.

DNS64

Les clients IPv6 ne pouvant pas communiquer avec des serveurs IPv4, il est nécessaire de les tromper en fabriquant dynamiquement des adresses IPv6.

Cette fabrication est effectuée par le relais DNS auxiliaire (DNS Application Layer Gateway : DNS-ALG).

Celui-ci convertit l'adresse IPv4 en une adresse IPv6 avant de répondre au client par un enregistrement de type AAAA

1. Un client IPv6 formule une requête de type AAAA pour résoudre le nom d'un serveur, le DNS64 la transfère au serveur DNS en charge du nom de domaine du serveur.
2. Si la réponse est vide, le DNS64 renvoie une requête de type A pour le même nom au serveur DNS.
3. Le DNS64 reçoit alors une réponse de type A.
4. Le DNS64 traduit l'adresse IPv4 obtenue en adresse IPv6, Il combine le préfixe IPv6 aux 32 bits de chacune des adresses obtenues comme résultats.

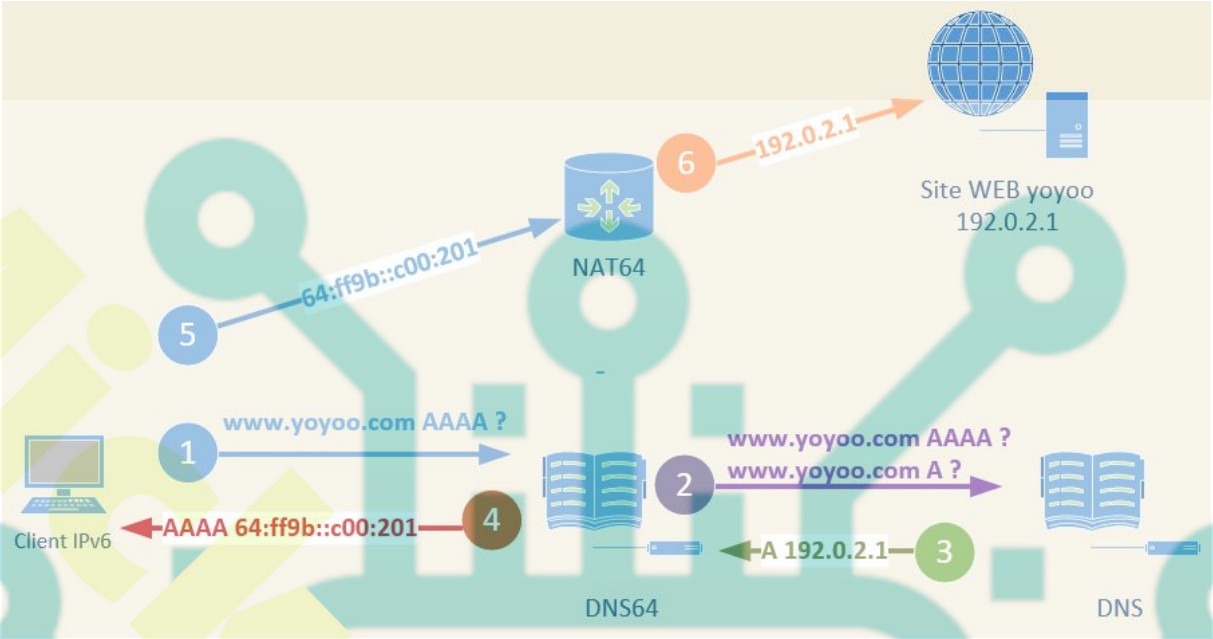
5. L'adresse IPv6 résultante est transmise au client sous la forme AAAA.

Mécanisme de transition NAT64/DNS64

L'interopérabilité avec les services IPv4 peut être réalisée en traduisant les paquets IPv6 en paquets IPv4 à travers un dispositif NAT64, couplé a un relais traducteur DNS64.

Sur l'équipement client, il suffit de déclarer le DNS64 comme serveur de résolution de nom. L'interrogation du client concerne les enregistrements AAAA car ceux-ci sont les seuls qui sont utilisables pour le client.

- Si un nom de domaine possède une résolution en IPv6, le serveur DNS64 se comporte alors comme un "resolveur" de noms normal et il répond à la demande du client.
- Si un nom de domaine n'a pas de connectivité IPv6, le DNS64 interroge le service DNS sur les différentes adresses disponibles.
- Comme le DNS64 n'obtient que des réponses de type A, il va devoir transformer les adresses IPv4 obtenues du service, en adresses IPv6 afin de satisfaire la demande du client.
- Le DNS64 complète le préfixe 64:ff9b::/96 avec l'adresse IPv4 obtenue.
- Le client utilise cette adresse IPv6 comme destinataire de la communication
- Ce préfixe est routé vers le dispositif NAT64.
- Les paquets sont reçus par le NAT64 avec comme adresse source IPv6 celle du client et comme adresse de destination l'adresse transformée par le DNS64.
- Le NAT64 doit maintenant traduire ces paquets IPv6 vers IPv4. Il crée alors un en-tête IPv4 à partir des champs de l'en-tête IPv6.
- Pour l'adresse destination du paquet IPv4, le traducteur applique la transformation inverse de celle appliquée par le DNS64, il extrait l'adresse IPv4 en extrayant de l'adresse destination du paquet IPv6 le préfixe utilise pour la traduction d'adresse, en l'occurrence 64:ff9b::/96
- Le NAT choisit, comme adresse "source", une adresse IPv4 de son pool d'adresses réservées à cet usage.
- Pour le retour, comme l'adresse IPv4 est partagée entre les clients IPv6, le traducteur va aussi utiliser le numéro de de port "source" du côté du réseau IPv4 pour identifier la source sur le nœud IPv6.
- Puis, les informations de la connexion, vont être conservées en mémoire, de cette correspondance entre l'adresse de transport IPv6 du client et l'adresse de transport IPv4 choisie.



Shéma DNS64/NAT64 simplifié

Tunnel Broker

Un serveur de tunnels (IPv6 dans IPv4) permet de connecter à l'Internet v6 une machine double pile isolée dans l'Internet v4. La configuration du tunnel entre le serveur et la machine cliente est automatique et repose sur le protocole TSP. La demande de connexion au serveur est réalisée par une page HTML dont l'URL est connue à l'avance.

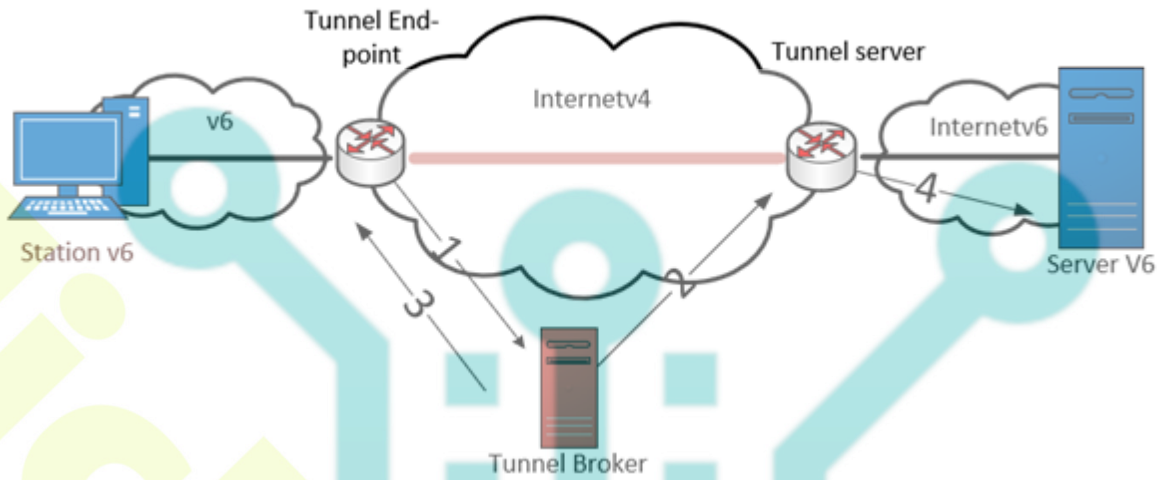
Cette connectivité est fournie à titre provisoire, et permet à un FAI d'assurer la connectivité IPv6 à ses clients.

- Côté client l'installation d'un simple service permet de faire la demande de tunnels au serveur.
- Coté FAI, il faut mettre en œuvre un serveur qui possède une interface HTML pour accueillir les demandes de tunnels des usagers, et le configurateur de tunnels qui gère les extrémités du tunnel.

TSP : tunnel setup protocol

Le tunnel setup protocol a été défini en complément du Tunnel Broker afin de permettre une négociation automatisée des différents paramètres entrant en jeu lors de l'établissement d'un tunnel.

La création d'un tunnel à l'aide d'un *Tunnel Broker* + *TSP* fonctionne comme suit :

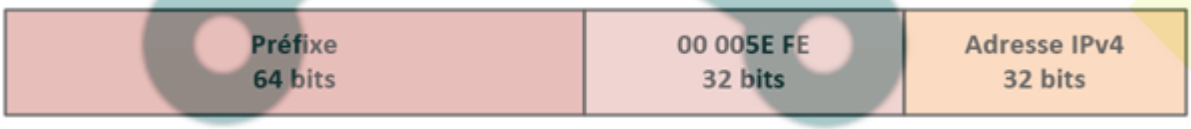


1. Le routeur double pile du réseau IPv6 s'authentifie auprès du *Tunnel Broker* pour obtenir les informations de configuration du tunnel ainsiqu'un préfixe délégué.
2. Le *Tunnel Broker* configure le serveur de tunnel.
3. Le *Tunnel Broker* envoie le script de configuration à la machine "double pile" coté utilisateur.
4. Cette dernière, en exécutant le script reçu, crée le tunnel et encapsule ses paquets IPv6 dans des paquets IPv4 à destination du serveur de tunnels (routeur). La communication en IPv6 peut s'effectuer entre des nœuds d'un réseau IPv6 isolé avec des nœuds de l'Internet v6.

ISATAP

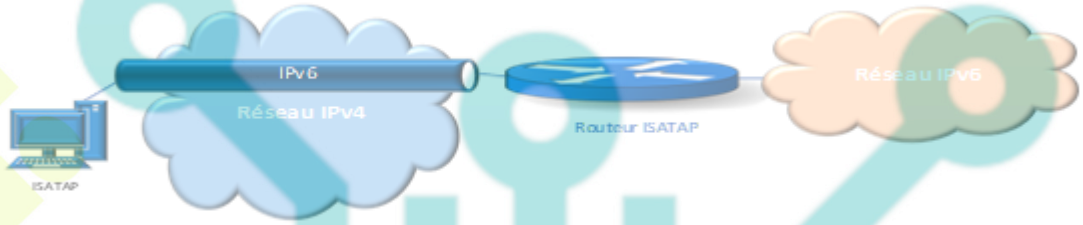
Ce protocole est un peu le 6to4 adapté à un réseau local. Cependant, si ISATAP (*Intra-Site Automatic Tunnel Addressing Protocol*) permet de connecter des équipements IPv6 isolés dans un réseau IPv4, cette technique s'applique seulement à l'intérieur d'un domaine.

ISATAP s'appuie sur un format d'adresse qui intègre dans la partie identifiant de l'équipement l'adresse IPv4 du terminal. L'identifiant d'interface est construit à partir d'une adresse MAC en ajoutant la valeur 00-00-5E. et un type indiquant l'adresse incorporée (FE)



Quand un routeur reçoit un paquet IPv6 dont l'identifiant d'interface commence par la valeur 00-00-5E-FE, il sait que le paquet est destiné à une machine isolée et il procède à

l'encapsulation du paquet IPv6 dans un paquet IPv4 avec comme adresse de destination celle contenue dans la partie identifiant d'interface.



Procédure de configuration

1. L'équipement cherche l'adresse IPv4 du routeur ISATAP par le biais du DNS ou d'une adresse anycast.
2. La machine envoie un message IPv6 Router Sollicitation au routeur en utilisant comme adresse de la source, son adresse lien-local (fe80::5e:fe:IPv4) et comme adresse de destination l'adresse de multicast des routeurs (FF02::02).
3. Ce message est encapsulé dans un paquet IPv4 dont l'adresse destination est l'adresse IPv4 du routeur.
4. Le routeur répond au message IPv6 Router Sollicitation en renvoyant la liste des préfixes IPv6 utilisés pour joindre les équipements isolés (Router Advertisement) dans un message encapsulé dans un paquet IPv4,

ISATAP est compatible avec 6to4. Le préfixe global peut contenir l'adresse IPv4 du routeur d'accès et la partie identifiant d'interface l'adresse IPv4 privée de l'équipement. Deux tunnels seront nécessaires (le premier entre le routeur 6to4 de la source et le routeur d'accès du site et le second entre le routeur d'accès et le destinataire). Un équipement, possédant une adresse privée en IPv4, peut de cette manière disposer une adresse IPv6 globale.

TEREDO

L'objectif de Teredo (RFC 4380) est de fournir une connectivité IPv6 à un équipement situé derrière un NAT et ne disposant pas d'une adresse IPv4 publique. Cela implique la mise en œuvre d'une encapsulation UDP.

Teredo utilise un format d'adresse IPv6 spécifique qui ne requiert aucune allocation de la part des organismes officiels. Il construit l'adresse en intégrant : dans la partie préfixe,

l'adresse IPv4 du serveur Teredo et dans la partie identifiant les adresses et numéros de port (en sortie de NAT) du terminal client Teredo.

Cette dernière information est brouillée avec un XOR afin de ne pas être modifiée par certains NAT qui modifient les séquences binaires ressemblant à une adresse.

Le préfixe Teredo de longueur 64 bits inclus l'adresse du serveur Teredo auquel le terminal est rattaché. Actuellement le préfixe **3FFE:831F::/32** mais l'IANA pourrait assigner une valeur définitive.

La phase d'initialisation d'un client Teredo a en particulier pour but de déterminer le type de NAT derrière lequel il se trouve.

Relais applicatifs

Les relais applicatifs ou ALG (*Application Level Gateway*) est le plus simple car il suffit d'un équipement à double pile qui reçoit une requête en v6 et qui la retransmet en v4.

Les relais peuvent être installés en fonction des services et applications disponibles sur le réseau (messagerie, relais http, …) et les machines clientes sont configurées pour envoyer les requêtes applicatives à ces derniers.

Dans ce mécanisme, on peut positionner les proxy, serveur mail, spooler d'impression, serveur DNS…

SOCKS

Cette technique reprend les systèmes existants en v4 permettant de passer d'un adressage privé à un adressage public. SOCKS permet d'utiliser à la fois les communications entrantes et sortantes.

Une des difficultés de ce système est la gestion des adresses et des noms DNS. Si l'application v4 utilise un FQDN, SOCKS va devoir capturer la demande de résolution et retourner à l'application une fausse adresse IP prise dans un pool. Quand l'application va ouvrir la connexion avec cette adresse, il faut que le nom de la machine distante puisse

être retrouvé et envoyé au relais SOCKS qui pourra retourner un enregistrement AAAA, et ouvrir la connexion en utilisant la v6.

DSTM

La tâche de DSTM (*Dual Stack Transition Mechanism*) est de fournir une connectivité IPv4 temporaire à un équipement double pile connecté à un réseau uniquement v6. La connectivité IPv4 n'est disponible que durant le temps d'une communication avec une station distante ne possédant que la v4.

DSTM fonctionne à l'inverse du Tunnel Broker.

DSTM est utilisé quand la majorité du réseau est passée en IPv6, mais qu'il existe encore des applications n'utilisant qu'IPv4.

DSTM utilise une interface réseau spéciale DTI (*Dynamic Tunneling Interface*) qui permet l'encapsulation des paquets IPv4 dans des paquets IPv6.

Un routeur particulier appelé TEP (*Tunnel End Point*) possédant la connectivité entre le monde IPv4 et le monde IPv6 effectue l'encapsulation et la désencapsulation des messages.

Avec cette technique, on ne configure que la pile IPv6 d'un équipement. La pile IPv4 est configurée à la demande en fonction des besoins applicatifs.

L'utilisation de tunnels facilite la gestion car les adresses IPv4, perdent leur fonction de localisation, on doit juste leur garantir la propriété d'unicité.

La sécurité dans IPv6

Avec la conception protocole d'IPv6, l'IAB a mis l'accent sur la nécessité d'intégrer des services de sécurité en vue de protéger le trafic IP et d'offrir ainsi un moyen de protection solide pour l'interconnexion des réseaux de sites à sites et la gestion des appareils nomades.

Toutes les implémentations IPv6 doivent obligatoirement intégrer IPsec pour être conformes. La sécurité d'IPv6 met en œuvre un protocole d'échange de clé.

Le choix de l'IETF

Dans le cahier des charges, L'IETF a indiqué que la sécurité devait permettre de se prémunir des attaques de types IP spoofing et IP sniffing par des procédures de confidentialité, d'intégrité et d'authentification de l'origine des données.

L'IETF s'est appuyée sur le fait que la législation appliquée pour le service de confidentialité est plus stricte que celle appliquée pour les services d'intégrité/authentification. En effet, l'utilisation de la cryptographie est différente selon les pays.

Du fait les deux extensions proposées (AH et ESP), si un utilisateur n'est pas autorisé par sa législation à utiliser l'extension ESP, il pourra utiliser l'extension AH.

SEND

La configuration automatique présente un certain nombre d'avantage, mais peut rencontrer un problème si un équipement non autorisé répond aux Sollicitations de Routeurs (RS) émis par les équipements d'un lien.

Le groupe SEND (SEcure Neighbor Discovery) propose une solution à base de certificats pour authentifier les deux équipements (celui qui fait la demande et le routeur qui y répond).

DNSSEC (Domain Name System Security)

DNSSEC (RFC 2535) est un standard définissant des extensions de sécurité pour le DNS. Il assure l'intégrité et l'authenticité des enregistrements DNS (RR : Registration Record) par l'intermédiaire des signatures électroniques (RRSIG RR).

Chaque zone possède deux paires de clés RSA appelées **Key Signing Key** (KSK) et **Zone Signing Key** (ZSK).
La clé publique de KSK permet à la zone parent d'authentifier sa zone fille. Les clés ZSK permettent de signer les enregistrements gérés par la zone elle-même.

Chaque zone DNSSEC peut jouer le rôle d'une autorité de certification. Il lui suffit de certifier la clé publique de sa zone fille en signant le haché de cette clé et en publiant ce haché dans l'enregistrement DS RR (Delegation Signer) (RFC 3658).

Les « systèmes de détection d'intrusions » (IDS)

Ils se mettent progressivement à IPv6. L'usage d'IPsec va aussi compliquer la tâche des sondes surveillant le trafic du réseau. Si les paquets sont chiffrés, il sera plus difficile d'y voir des indications de code malveillant.