Migration IPv6

Etude du protocole IPv6

GRILLE DE GESTION

Type de diffusion

☐ Livrable	☐ Consultable	☒ Privé
☐ Diffusion contrôlée		Exemplaire N°

Mode d'accès

Serveur DIS : \Stages\IPv6.ML\Documents\Dossiers\Protocole.doc

Conservation

Responsable : CJ Lieu : DIS

E				
D				
C				
B				
A				
Ind.	Nom Visa	Nom Visa	Nom Visa	Date
	REDACTION	VERIFICATION	APPROBATION	

GRILLE DE REVISION

La présente Grille de révision indique l'objet et la localisation des modifications génératrices du changement d'indice.

N°	Objet	Localisation
1	Corrections mineures (orthographe, précisions, …)	-
2	Ajout des adresses IPv4-translated	Types d'adresses
3	Simplification de IPSec	IPSec
4	Reprise intégrale de QoS	QoS
5	Modification de la conclusion	Conclusion
6	Rappels sur IPv4	Protocole
7		
8		
9		
10		
11		
12		
13		
14		
15		
16		
17		
18		
19		
20		

SOMMAIRE

1 Introduction

1.1 Objet du projet

Le projet porte sur l'étude de migration des réseaux IP de la version v4 à la version v6. Cette évolution (à prévoir dans les années à venir) va poser un certain nombre de problèmes, mais va également permettre de proposer de nouvelles fonctionnalités (mobilité, routage, sécurité, …). Le but de l'étude est de proposer des méthodes pour effectuer ce basculement, ainsi qu'une étude détaillée des nouvelles fonctionnalités.

La finalité du projet est de définir un certain nombre d'offres de service à proposer à nos clients pour qu'ils puissent basculer sans problème vers IPv6.

L'étude est réalisée sous la forme d'un Projet de Fin d'Etude (PFE) entre RSI et l'INSA de Lyon. Ce PFE est effectué en entreprise à raison de 2 jours par semaine pendant 6 mois (Novembre – Avril) et à temps plein pendant 2 mois (Mai – Juin).

1.2 Objet du document

Etude technique du protocole IPv6 permettant de mieux connaître les différences avec l'ancien protocole, ainsi que ses nouvelles fonctionnalités. Il portera en particulier sur :

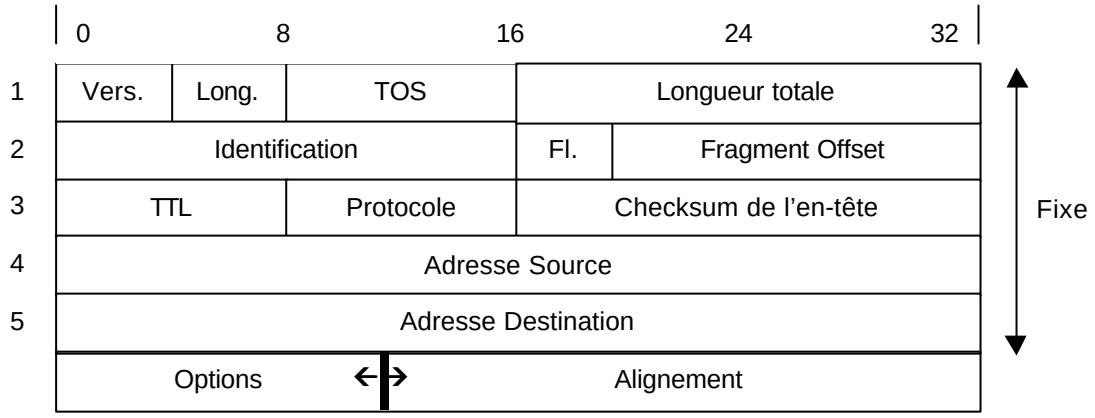
- Présentation générale
- Adressage (technique, obtention des adresses, …)
- Routage
- Sécurité (authentification, chiffrement)
- Mobilité
- Qualité de Service
- …

Note : la présentation des fonctionnalités d'IPv6 contient certains aspects ou protocoles qui ne sont pas encore standardisés et qui ne le seront peut être jamais. Ces paragraphes seront indiqués par **[WIP]** (Work In Progress).

2 Présentation du protocole IPv6

La structure de l'en-tête des trames IPv6 a été revue et simplifiée pour combler les lacunes et problèmes d'IPv4.

2.1 Rappels sur l'en-tête IPv4



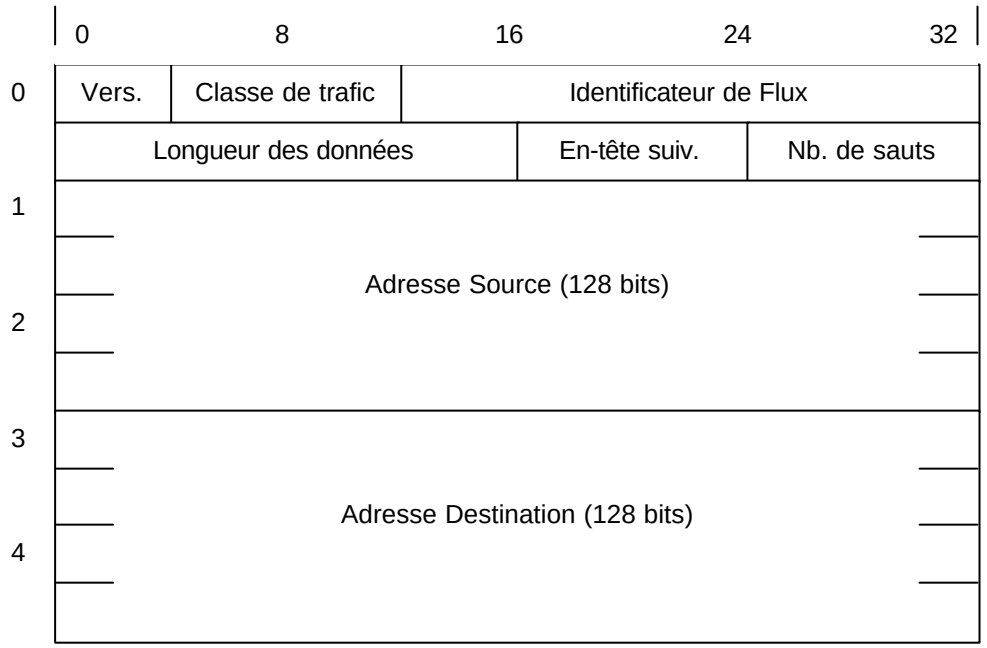
- **Version :** 4.
- **Long. :** Longueur de l'en-tête en mots de 32bits.
- **TOS :** Type of Service (Precedence + Champ TOS), utilisé pour faire de la qualité de service.
- **Longueur totale :** Longueur du paquet (en-tête + données) en octets.
- **Identification :** Numéro unique permettant de faciliter le réassemblage des paquets après l'utilisation de la fragmentation. Chaque fragment comporte le même numéro d'identification.
- **Flags :**
  - 0.
  - DF : Don't fragment (ne pas fragmenter ce paquet).
  - MF : More Fragments (1 – Ce n'est pas le dernier fragment).
- **Fragment Offset :** Emplacement du fragment (en mots de 64 bits) dans le message intégral.
- **Time To Live (TTL) :** Durée de vie (en secondes).
- **Protocole :** Protocole utilisé dans la couche supérieure (TCP, UDP, …).
- **Checksum de l'en-tête :** Somme de contrôle permettant de détecter une erreur de transmission.
- **Adresses (Source/Destination) :** Adresses IPv4 (32 bits).
- **Options :** Options facultatives (Sécurité, Routage, Horodatage, Flux, …).
- **Alignement :** Octets d'alignement pour finir le mot de 32bits.

2.2 Différences par rapport à IPv4

- Le numéro de version passe de 4 à 6.
- Les adresses passent de 32bits à 128bits (taille pouvant être considérée comme inépuisable).
- L'en-tête est simplifiée pour permettre d'en réduire la taille et d'accélérer son traitement par les routeurs.
- Des extensions sont insérées dans la trame pour ajouter des options ou traitements supplémentaires.
- Par défaut, la fragmentation n'est plus effectuée par les routeurs (pour éviter de les surcharger d'un travail que peut faire la station émettrice).
- Le *checksum* est déplacé dans les niveaux supérieurs (TCP, UDP, …), également pour alléger la charge des routeurs.

2.3 Format

L'en-tête IPv6 a une taille fixe de 40 octets (5 mots de 64 bits) auquel on peut ajouter des extensions (d'une taille multiple de 64 bits).



Version :
Sa valeur est de 6. Il permet aux équipements de connaître la version du protocole IP à utiliser (emplacement identique dans IPv4 et IPv6) pour pouvoir traiter le paquet correctement.

Classe de trafic :
Le champ classe de trafic permet de faire de la différenciation de services. Cela permettra de faire passer une classe prioritairement par rapport à une autre, de fixer une taille limite de trafic alloué à une classe, … Pour plus de détail, se reporter au § 8 – QoS.

Identificateur de flux :
Ce champ contient un numéro unique (pour une adresse source donnée), choisi par la source et permettant d'identifier le flux de manière unique. S'il est utilisé (différent de 0), les routeurs peuvent réagir plus rapidement à un paquet. L'identificateur de flux restera constant tout au long du trajet entre la source et la destination. Il n'est pas uniquement spécifique à un trajet entre deux nœuds, comme cela est le cas pour les circuits virtuels. Les routeurs peuvent ensuite garder en mémoire les traitements à effectuer sur un flux (en particulier, la route à utiliser et les filtres à appliquer). Il n'ont plus qu'à utiliser l'adresse source et l'identifiant de flux sans avoir besoin de relire toutes les options avant de router un paquet.

Longueur des données (payload) :
Ce champ contient la taille des données utiles (sans prendre en compte la longueur de l'en-tête, contrairement à IPv4) Pour des paquets de taille supérieure à 65 535 octets, ce champ vaut 0 et l'option jumbogramme est utilisée.

En-tête suivant :
Ce champ indique le type de bloc qui suit. Il peut s'agir d'un protocole de niveau supérieur (TCP, UDP, ICMP, …) ou d'un champ d'extension. Cela permet de chaîner les extensions avant le bloc TCP (ou UDP, …) que contient le paquet.

Valeur	Extension
0	Proche en proche
43	Routage
44	Fragmentation
50	Confidentialité
51	Authentification
59	Fin des en-têtes
60	Destination

Valeur	Protocole
6	TCP
17	UDP
41	IPv6
58	ICMPv6

Nombre de saut :
Ce champ est similaire au champ TTL (*Time To Live*) d'IPv4. Cependant, il ne s'agit plus de secondes mais de nombre de sauts (la durée d'un saut étant difficilement mesurable). Il est décrémenté de un à chaque nœud traversé. Lorsque sa valeur arrive à 0, il est détruit et un message d'erreur ICMPv6 est envoyé à la source (cf. § 4.1).

2.4 Extensions

Une extension commence par un champ *en-tête suivant* qui indique le type de bloc qui suivra, puis la longueur de l'extension en mots de 8 octets (la taille d'une extension doit être multiple de 64 bits).

Exemple d'insertion des extensions :

En-tête IPv6 Suivant = TCP	En-tête TCP + données

En-tête IPv6 Suivant = Routage	Routage Suivant = TCP	En-tête TCP + données

2.4.1 Proche en proche (hop-by-hop)

Cette extension est toujours située en première position et est traitée par tous les routeurs que le paquet traverse. Elle contient une suite d'options qui sont à prendre en compte par le routeur. Pour chacune, on indique le traitement à effectuer si le routeur ne connaît pas l'option (ignore, rejette, …).

Pour l'instant, seules quatre options ont été définies :
- *Pad1* : Utilisée pour introduire un octet d'alignement
- *PadN* : Utilisée pour introduire plus d'un octet d'alignement
- *Jumbogramme* : Permet la transmission de bloc de données de plus de 65 535 octets
- *Router Alert* : Demande au routeur d'examiner le contenu des données qu'il relaie. Utile pour la gestion des groupes de multicast avec ICMPv6 ou la signalisation des flux avec RSVP.

2.4.2 Destination

Cette extension est identique à l'extension *Proche en proche* mis à part qu'elle ne s'adresse qu'à l'équipement destinataire. Elle peut entre autre contenir les options d'alignement *Pad1* et *PadN*, des informations sur la mobilité, …

2.4.3 Routage

L'extension de routage permet de spécifier une suite d'équipements par lequel le paquet doit passer. Cela correspond au routage libéral de IPv4 (il n'y a plus de routage strict). Chaque routeur enverra le paquet vers le nœud suivant sur la liste, jusqu'à atteindre la machine finale. Pour cela, on indique dans le champ adresse destination le premier nœud à atteindre. Puis, chaque nœud actualisera ce champ avec la prochaine destination, jusqu'à atteindre la destination finale.

2.4.4 Fragmentation

La fragmentation est utilisée par la machine source dans le cas de programmes qui produisent des messages de grande taille. Néanmoins, il faut éviter son usage et adapter la taille des paquets à l'émission. Pour cela, on peut utiliser les techniques de découverte du MTU[1] (cf. § 5.3) pour déterminer la taille des paquets que l'on peut transmettre.

L'extension de fragmentation permet d'indiquer l'ordre des paquets pour pouvoir les réassembler par la suite.

2.4.5 Sécurité

On dispose de deux extensions de sécurité :
- Authentification/Intégrité
- Confidentialité

2.5 Checksum

Le contrôle de *checksum* a été supprimé au niveau IP, en partie parce que les supports physiques actuels sont de meilleure qualité et qu'ils possèdent souvent un moyen de détecter les erreurs (Ethernet, PPP, …). Cependant, pour se prémunir d'éventuelles erreurs, il a été décidé que tous les protocoles au-dessus d'IPv6 devaient utiliser une somme de contrôle. Le contrôle du *checksum* est donc réalisé uniquement sur la machine destination, ce qui décharge les routeurs de ce travail.

Pour le calcul du *checksum*, on doit prendre en compte à la fois les données du protocole concerné, ainsi que les adresses de source et de destination, la longueur des données et le champ en-tête suivant.

[1] Maximum Transport Unit : Taille maximale du paquet IP

3 Adressage

3.1 Taille de l'adresse IP

La taille de l'adresse IPv6 a été fixée à 128bits pour être sûr que l'on ne tomberait jamais à cours d'adresses comme cela aurait été le cas avec IPv4 si l'on n'avait pas mis en place des solutions de remplacement (CIDR[1], NAT[2]). Pour bien se rendre compte, il faut savoir qu'avec cette taille le nombre d'adresses IP est de 3.4×10^{38} et que chaque habitant de la planète pourrait ainsi avoir un Internet de la taille actuelle d'Internet.

Bien entendu, on ne peut pas affecter toutes les adresses IP (et cela est d'autant plus vrai avec IPv6), mais même avec les prévisions les plus pessimistes d'affectation, on disposerait de 1564 adresses IP par m² de surface terrestre (océan compris). La prévision la plus optimiste étant de plusieurs millions de milliards d'adresses IP par m². On peut donc considérer le pool d'adresse IPv6 comme inépuisable, même à très long terme.

3.2 Notation

La notation utilisée est la notation hexadécimale, séparée tous les 16 bits par le caractère « : ». Dans un souci de simplification, il n'est pas nécessaire d'écrire les zéros placés en tête d'un groupe et plusieurs champs consécutifs peuvent être abrégés en « :: » (utilisable qu'une seule fois).

Par exemple :
`FEDC:0000:0000:0000:0400:A987:6543:0210F` devient `FEDC::400:A987:6543:210F`

Tout comme IPv4, on peut représenter un préfixe IPv6 de la manière suivante : adresse/longueur-préfixe
Par exemple, `3EDC:BA98:765:3210::/64` ou `FE80::/10`

3.3 Plans d'adressage

Un certains nombre de plans d'adressage ont été envisagés. Parmi les plans étudiés, on a un plan d'adressage géographique (`8000::/3`) divisé en continent, pays, … et un plan d'adressage fournisseur (`4000::/3`) organisé hiérarchiquement entre les fournisseurs d'accès et les clients.

Le plan retenu est le plan d'adressage agrégé (`2000::/3`) dont les adresses sont découpées de la manière suivante :

3 bits	45 bits			16 bits	64 bits
001	Adresse Publique			Topo Site	Identifiant d'interface
	13	8	24		

La topologie publique est constituée par l'ensemble des prestataires et des points d'échange de connectivité IP. Le découpage est le suivant :

- Une unité d'agrégation haute (TLA : *Top Level Aggregator*) sur 13 bits.
- Une partie réservée sur 8 bits : elle pourra servir par la suite à agrandir les champs d'unités d'agrégation (haute ou basse) en fonction des besoin (celui qui sera plein le plus vite).

[1] CIDR : Classless Inter-Domain Routing
[2] NAT : Network Address Translation

- Des unités d'agrégation basse (NLA : *Next Level Aggregator*) dont la longueur totale est 24 bits et dont le découpage est libre.

Pour plus de détail sur les unités d'agrégation, se reporter au § 3.8.

La topologie du site (SLA : Site Level Aggregator) sur 16 bits est sous la responsabilité du responsable du site qui peut hiérarchiser son réseau comme il le souhaite.

L'identifiant d'interface devrait théoriquement être construit pour être globalement unique. Pour cela, la machine peut se servir d'adresses MAC IEEE 802, IEEE EUI-64, numéro de série, génération aléatoire, … De cette manière, il n'y a que très peu de chance de se retrouver avec deux identifiants identiques sur le même lien. De plus, en cas de conflit, il sera détecté lors de l'initialisation de l'adresse lien-local de l'interface (cf. § 5.1.1).

Certaines personnes considère que l'utilisation d'un identifiant de la machine dans l'adresse IPv6 pourrait permettre de 'pister' encore plus les machines sur Internet, ce qui soulève des polémiques sur la préservation de l'anonymat. Il est toujours possible d'utiliser des adresses IP fixes ou de se baser sur une génération aléatoire de l'identifiant, néanmoins, cela aura des conséquences sur la configuration automatique des adresses IP (cf. § 5.1.3).

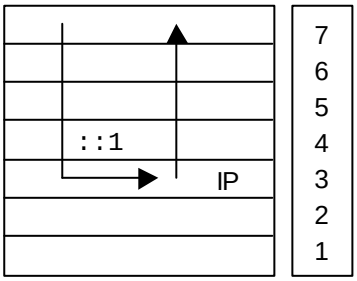
3.4 Autres types d'adresses

3.4.1 L'adresse indéterminée

L'adresse indéterminée est utilisée comme adresse source par un nœud du réseau pendant son initialisation, avant d'acquérir une adresse. Sa valeur est `0:0:0:0:0:0:0:0`, en abrégé `::`. Elle ne doit jamais être destination d'un paquet IPv6.

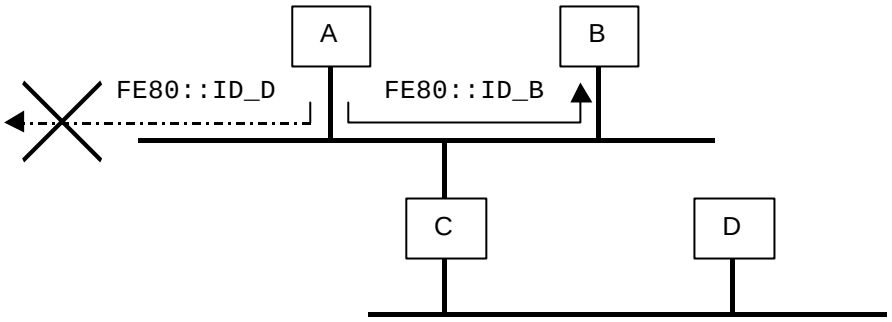
3.4.2 L'adresse de bouclage

L'adresse de bouclage vaut `::1`. C'est l'équivalent de l'adresse 127.0.0.1 d'IPv4. Elle sert à s'envoyer des paquets IPv6 sans passer par un réseau.



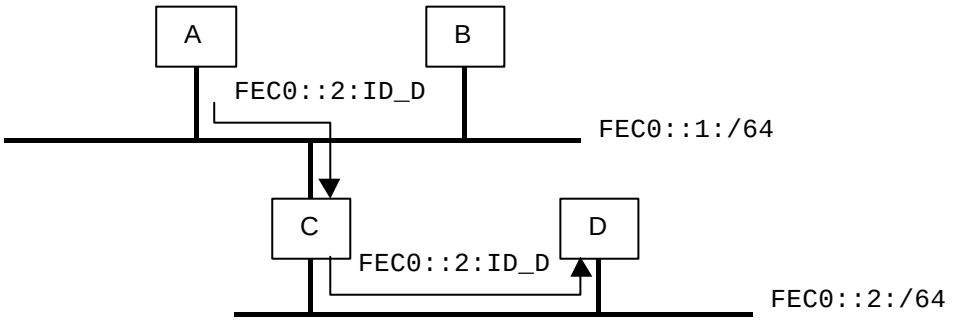
3.4.3 Les adresses lien-local

C'est une nouveauté d'IPv6. Il s'agit d'adresses qui ne sont valides que sur un lien (brin ethernet, liaison série, …). Ces adresses sont configurés automatiquement car il suffit d'ajouter l'identifiant au préfixe `FE80::/64`. Cela permet aux machines situés sur un même lien de communiquer entre elles. Ces adresses sont utilisés pour la configuration, la découverte de voisins ou de routeurs, …



3.4.4 Les adresses site-local

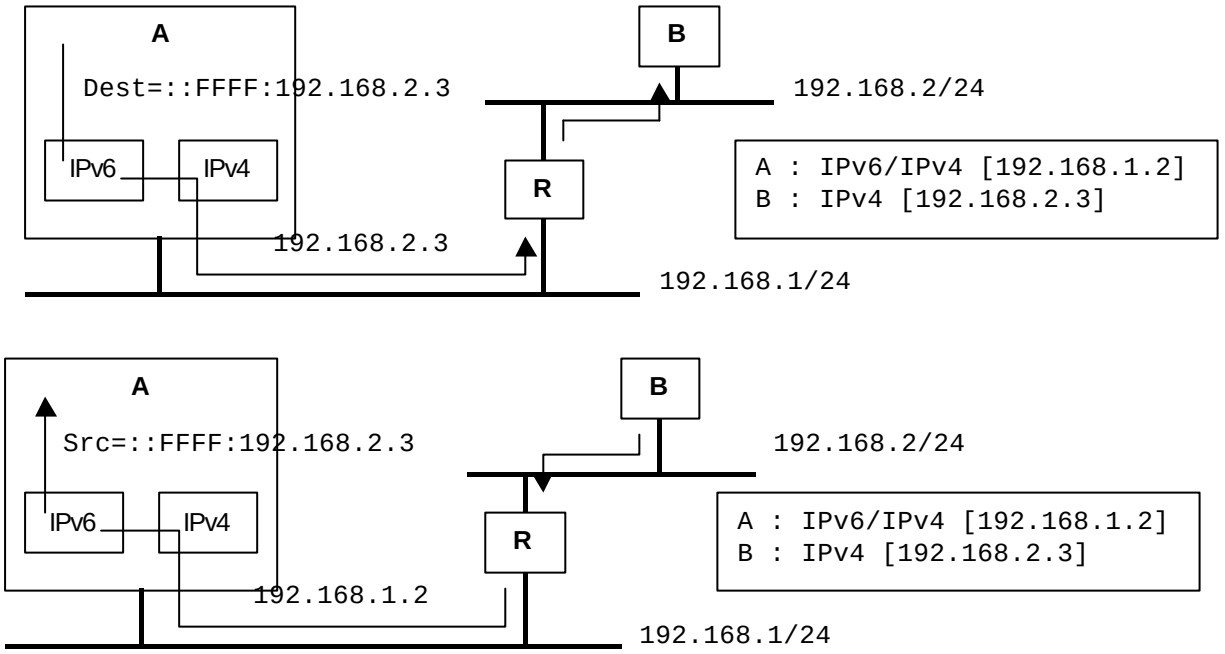
Ce sont des adresses privées qui peuvent être utilisés à l'intérieur d'un même site et qui ne seront pas routées sur Internet. Cela correspond aux adresses 10.0.0.0/8, 172.16.0.0/12 et 192.168.0.0/16 d'IPv4. Les adresses site-local seront toujours disponibles, mais on pourra également utiliser des adresses IPv6 globales si on a obtenu un préfixe auprès d'un organisme d'affectation.
Une adresse site-local est constituée du préfixe `FEC0::/48`, d'un champ de 16 bits qui permet de définir des sous-réseaux et de l'identifiant d'interface sur 64 bits.



3.4.5 Les adresses IPv4 mappées

Les adresses IPv4 mappées servent, aux logiciels utilisant des adresses IPv6, à communiquer avec des machines IPv4. Dans ce cas, il faut une double pile IP qui fera la conversion entre un paquet IPv6 et une interface IPv4 mappée (fourni par le logiciel) et un paquet IPv4 (qui sera envoyée sur le réseau). Inversement, la double pile transformera un paquet IPv4 en un paquet IPv6 pour l'envoyer au logiciel. On peut également utiliser ces adresses sur le réseau IPv6 pour que la conversion soit effectuée à distance par une machine spécialisée.

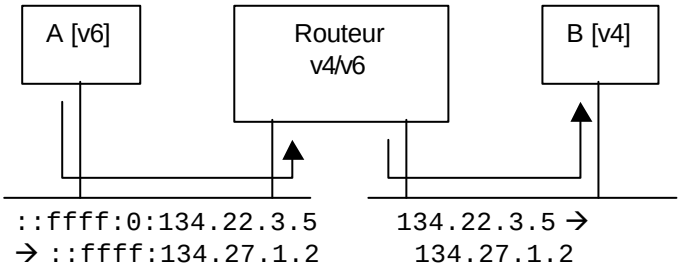
Elles sont représentées sous la forme `::FFFF:a.b.c.d` où a.b.c.d est une adresse IPv4. On peut aussi l'écrire sous la forme `::FFFF:XXXX:YYYY` où XXXXYYYY est la représentation hexadécimale de a.b.c.d.



3.4.6 Les adresses IPv4-translated

Les adresses IPv4-translated sont des adresses IPv6 particulières contenant une adresse IPv4. Dans le cas où l'on utilise un traducteur de paquets IPv4/IPv6 distant, il faut trouver un moyen de lui indiquer l'adresse IPv4 à utiliser comme source du paquet. On utilise alors une adresse IPv4-translated. Le paquet est envoyé avec une adresse source IPv4-translated et une adresse destination IPv4 mappée. On procède de la même façon dans le sens inverse.

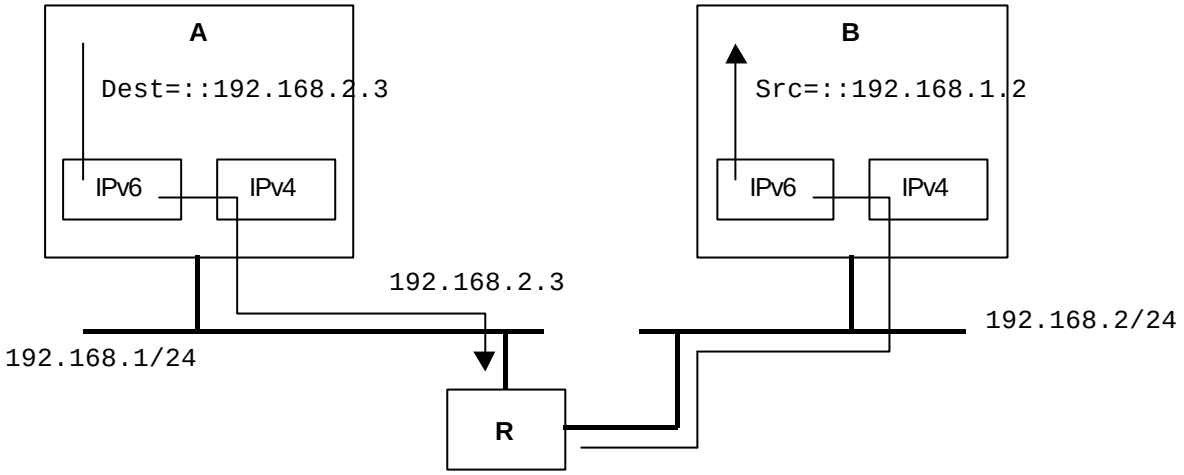
Elles sont représentées sous la forme `::FFFF:0:a.b.c.d` où a.b.c.d est une adresse IPv4. On peut aussi l'écrire sous la forme `::FFFF:0:XXXX:YYYY` où XXXXYYYY est la représentation hexadécimale de a.b.c.d.



3.4.7 Les adresses IPv4 compatibles

Les adresses IPv4 compatibles permettent à deux machines IPv6 de communiquer par l'intermédiaire d'un réseau IPv4 (les machines doivent donc avoir chacune une adresse IPv4). Les données sont encapsulées dans un paquet IPv4 et ce paquet est ensuite acheminé sur le réseau IPv4 puis désencapsulé à l'autre bout.

Elles sont représentées sous la forme `::a.b.c.d` où a.b.c.d est une adresse IPv4. On peut aussi l'écrire sous la forme `::XXXX:YYYY` où XXXXYYYY est la représentation hexadécimale de a.b.c.d.



3.4.8 Les adresses NSAP et IPX

Les adresses NSAP (*Network Service Access Point*) et IPX (Novell) sont en cours de définition. Leurs préfixes sont respectivement `200::/7` et `400::/7`.

3.4.9 Les adresses multicast

Les adresses multicast permettent, comme sous IPv4 d'accéder directement à un groupe de machines. L'envoi d'un paquet vers une adresse multicast sera reçu par toutes les machines qui appartiennent à ce groupe. Pour la gestion des groupes, il suffit d'utiliser les messages ICMPv6 (IGMP a été intégré dans ICMPv6) appropriés pour s'inscrire ou se désinscrire d'un groupe.

Le préfixe utilisé pour les adresses multicast est `FF00::/8`. Le format des adresses est le suivant :

8 bits	4 bits	4 bits	112 bits
FF00	Flags	Scope	Group Id

Le champ Flags se découpe de la manière suivante :
- 0 – réservé (=0)
- 1 – réservé (=0)
- 2 – réservé (=0)
- 3 – Validité de l'adresses (0-Permanente, 1-Temporaire)

Les adresses permanentes doivent être attribuées par une autorité compétente de l'Internet. Les adresses temporaires sont par exemple utilisées pour des visioconférences, qui ont une durée limitée dans le temps.

Le champ Scope permet de donner le niveau de diffusion de l'adresse. Les valeurs possibles sont :
- 0 – réservé
- 1 – nœud (*node-local scope*)
- 2 – lien (*link-local scope*)
- 5 – site (*site-local scope*)
- 8 – organisation (*organization-local scope*)
- E – global (*global scope*)
- F – réservé

Cela permet par exemple, de confiner des paquets 'sensibles' à l'intérieur d'un site et d'être sûr qu'ils ne se propageront pas sur Internet.

Un certain nombre de groupes standards ont été définis[1] pour permettre à certains protocoles (par exemple les protocoles de routages) de dialoguer entre eux. L'utilisation du champ Scope permettant de sélectionner le niveau de diffusion (tous les niveaux ne sont pas forcement utilisables).

- Le groupe `0x01` correspond à tous les nœuds IPv6. Cela permet par exemple, d'accéder à toutes les machines situées sur un même lien en utilisant l'adresse `FF02::1`.
- Le groupe `0x02` correspond aux routeurs IPv6. `FF05::2` correspond donc à tous les routeurs du site.
- Le groupe `0x09` correspond au protocole RIP.
- Les groupes `0x10002` à `0x10004` sont utilisé par le protocole DHCP (agents, serveurs, relais).
- Etc…

Chaque nœud IPv6 doit également construire (et adhérer à) une adresse multicast sollicité (*solicited node address*) pour chaque adresse unicast ou anycast dont il dispose. L'adresse multicast sollicité est formé en utilisant le préfixe `FF02::1:FF00:0/104` et en ajoutant les 24 derniers bits de l'adresse unicast ou anycast. Par exemple, l'adresse sollicité correspondant à l'adresse `4037::01:800:200E:8C6C` est `FF02::1:FF0E:8C6C`. Cette adresse sera utilisée entre autre lors de la découverte des voisins.

3.4.10 Les adresses broadcast

La notion de broadcast a disparu dans IPv6. On peut désormais se servir de certaines adresses multicast pour effectuer le même travail (par exemple `FF02::1` pour accéder à toutes les machines sur un même lien).

3.4.11 Les adresses anycast *[WIP]*

Les adresses anycast sont une nouveauté d'IPv6 et permettent d'envoyer un paquet à une machine parmi un groupe. Pour cela, on utilise une adresse anycast (située dans l'espace d'adressage des adresses unicast) et le système de routage va l'acheminer vers la machine du groupe la plus proche (la notion de distance correspond à celle utilisée par le protocole de routage).

Adresses anycast particulières :

- **Adresse de sous-réseau :** Elle est formée en concaténant le préfixe du sous-réseau avec le suffixe nul. Tous les paquets envoyés à cette adresse iront à l'un des routeurs du sous-réseau en question. Cela peut être utilisé par une machine pour trouver le routeur le plus proche permettant d'accéder à un sous-réseau donné.
- **Adresse anycast réservée :** Certaines adresses anycast d'un sous-réseau ont été réservées pour un usage standard. Elle sont construites de la manière suivante :
  - Si le préfixe de sous-réseau est de 64 bits, on ajoute à ce préfixe 6 bits positionné à 1, 1 bit positionné à 0, 50 bits positionnés à 1 et enfin l'identifiant réservé. Note : Le bit positionné à 0 correspond au universal/local bit du format EUI-64 qui indique que l'identifiant est local.
  - Dans le cas contraire, on ajoute au préfixe de sous-réseau, une série de bits positionnés à 1, puis l'identifiant reservé (7 bits).

  Pour l'instant, seul un identifiant anycast a été réservé :
  - 126 – Agents mères pour les mobiles

En théorie, il serait possible d'utiliser les adresses anycast avec n'importe quel groupe de nœuds IPv6 situés en tout point du réseau, mais cela reste encore expérimental. Les seules adresses anycast utilisables sont les adresses particulières définis ci-dessus.

[1] http://www.isi.edu/in-notes/iana/assignments/ipv6-multicast-addresses.txt

3.5 Espace d'adressage

Préfixe	Attribution
0::/8	Réservé
100::/8	Non attribué
200::/7	NSAP (ISO)
400::/7	IPX (Novell)
600::/7	Non attribué
800::/5	Non attribué
1000::/4	Non attribué
2000::/3	**Aggregation-Base Unicast Address**
4000::/3	Provider-Based Unicast Address (obsolète)
6000::/3	Non attribué
8000::/3	Geographic-Based Unicast Address (obsolète)
A000::/3	Non attribué
C000::/3	Non attribué
E000::/4	Non attribué
F000::/5	Non attribué
F800::/6	Non attribué
FC00::/7	Non attribué
FE00::/9	Non attribué
FE80::/10	**Link Local Use Addresses**
FEC0::/10	**Site Local Use Addresses**
FF00::/8	**Multicast Addresses**

3.6 Etat des adresses

Une machine dispose souvent de plusieurs adresses IP qui peuvent être dans des états différents. Ces états ont été définis pour faciliter la renumérotation ou la mobilité. En effet, dans ces cas précis, il faut un mécanisme permettant aux applications de passer d'une adresse à une autre sans interruption de service.

3 états ont été définis :
- Préféré : l'adresse peut être choisi pour amorcer une communication
- Déprécié : l'adresse ne doit plus être choisie pour amorcer une communication mais elle peut être utilisée dans une communication déjà en cours.
- Invalide : l'adresse ne doit plus être utilisée

Lorsque l'on doit utiliser une nouvelle adresse, on la met dans l'état préféré et on passe l'ancienne adresse dans l'état déprécié. De cette façon, les anciennes communications peuvent continuer pendant que les nouvelles utilisent la nouvelle adresse.

3.7 Renumérotation

Un des problèmes d'IPv4 a été une mauvaise gestion de l'espace d'adressage, qui a conduit à un accroissement certain des tables de routage. Cela est dû entre autre à deux phénomènes :
- Lorsqu'une entreprise change de prestataire, elle garde souvent ses adresses IP (pour éviter de tout renuméroter), et il faut donc rajouter des entrées dans les tables de routage pour continuer à router vers cette entreprise.
- Lorsqu'un prestataire fait plusieurs demandes (séparés dans le temps) pour des adresses IP, il n'obtient pas des plages d'adresses contigus et il faut donc rajouter des entrées dans les tables de routage pour que toutes ces adresses lui arrivent.

Il a donc été décidé que les adresses IPv6 n'appartenaient pas aux personnes qui les avait demandées et que l'on pouvait leur demander de les rendre. De cette manière, l'IANA s'assurera que l'espace d'adressage reste bien utilisé pour éviter le gaspillage et augmenter l'agrégation et l'efficacité des tables de routage.

Pour cela, IPv6 a été conçu pour permettre la renumérotation sans interruption de service d'un site entier. Le basculement entre l'ancienne adresse et la nouvelle est effectué grâce aux différents états que peuvent prendre les adresses (cf. § 3.6). Pour amorcer le basculement, il y a deux systèmes :
- Pour les routeurs, on peut utiliser les fonctions de renumérotation des routeurs de ICMPv6 (cf. § 4.4.1)
- Pour les nœuds terminaux, le protocole de découverte des voisins (cf. § 5.1) permet de prendre connaissance du nouveau préfixe (une fois que les routeurs sont renumérotés).

3.8 Affectation des adresses

L'IANA (*Internet Assigned Numbers Authority*) et son remplaçant l'ICANN (*Internet Corporation for Assigned Names and Numbers*) ont la charge d'affecter les nombres, mots-clés et paramètres devant être uniques sur Internet. Ils ont donc également la charge de gérer l'affectation globale des adresses IP.

Pour cela, ils s'appuie sur des organismes régionaux (*Regional Internet Registries*) qui ont à leur disposition une partie de l'espace d'adressage à affecter. Il n'y a pour l'instant que 3 *Regional Internet Registries* :
- ARIN (*American Registrery for Internet Numbers*) pour l'Amérique du Nord, du Sud, les Caraïbes, et l'Afrique sub-Saharienne.
- RIPE NCC (*Réseaux IP Européens*) pour l'Europe, le Moyen-Orient et une partie de l'Afrique.
- APNIC (*Asia Pacific Network Information Centre*) pour l'Asie et le Pacifique.

Les plages disponibles actuellement sont les suivantes :

`2001:0::/23`	IANA
`2001:200::/23`	APNIC
`2001:400::/23`	ARIN
`2001:600::/23`	RIPE NCC

Les organismes régionaux peuvent ensuite affecter des sub-TLA (*Top Level Aggregator*) à d'autres organismes, qui doivent être de gros prestataires de service. En effet, les prérequis sont les suivants :
- Avoir une connectivité avec au moins 3 autres organismes (disposant eux même d'un sub-TLA)
- Satisfaire un des deux points suivants :
  - Avoir déjà alloué au moins 40 NLA (Next Level Aggregator) à des sites clients.
  - Etre en mesure de prouver que l'organisme est capable de fournir des services IPv6 dans un délai inférieur à 12 mois.

Les organismes qui possède des sub-TLA peuvent ensuite affecter des adresses à leurs clients (NLA) qui peuvent eux-mêmes en affecter à d'autre, …

3.9 Serveur de noms

Comme pour IPv4, le serveur de nom doit pouvoir répondre au requêtes permettant de connaître l'adresse IP correspondant à un nom et inversement. Ce service de DNS est d'autant plus nécessaire que l'utilisation directe des adresses IP dans les logiciels risque de ne pas être toujours autorisé.

3.9.1 Les enregistrements AAAA

L'enregistrement AAAA indique l'adresse IPv6 correspondant à un nom.

Exemple : `pirae-v6 IN AAAA 3FFE:306:1130:1100:1:0:C0FE:EF2`

3.9.2 Les enregistrements A6

Pour faciliter la renumérotation, on préfère ne pas indiquer l'adresse entière correspondant à chaque machine mais plutôt son identificateur et le nom de son préfixe. En cas de renumérotation, il suffit de changer le préfixe et toutes les machines sont mises à jour.
Exemple :

```
pirae-v6                IN  A6  64  ::1:0:C0FE:EF2  net1.ipv6.inrialpes.fr.
net1.ip6.inrialpes.fr.  IN  A6  48  0:0:0:1100::    net.ipv6.inrialpes.fr.
net.inrialpes.fr.       IN  A6  24  0:6:1130::      net.ipv6.provider.com.
net.ip6.provider.com    IN  A6   0  3FFE:0300::
```

3.9.3 Les enregistrements PTR

Pour faire la correspondance entre l'adresse IP et le nom DNS, on utilise un enregistrement PTR dans la zone ip6.int.
Exemple :

```
2.f.e.0.e.f.0.c.0.0.0.0.1.0.0.0.0.0.1.1.0.3.1.1.6.0.3.0.e.f.f.3.ip6.int.
  IN  PTR  pirae-v6.ipv6.inrialpes.fr.
```

On peut également donner la correspondance dans une sous-zone :

```
$ORIGIN 0.3.1.1.6.0.3.0.e.f.f.3.ip6.int.
2.f.e.0.e.f.0.c.0.0.0.0.1.0.0.0.0.0.1.1  IN PTR pirae-v6.ipv6.inrialpes.fr.
```

3.9.4 Les enregistrements DNAME

Pour faciliter la renumérotation, on utilise les enregistrements DNAME pour permettre des alias sur les zones. On crée donc des zones dans ip6.int (associées à un préfixe) où on donne la relation entre le suffixe et le nom.
Exemple :

```
0.3.1.1.6.0.3.0.e.f.f.3.ip6.int  IN  DNAME  ip6.inrialpes.fr.

$ORIGIN ip6.inrialpes.fr.
2.f.e.0.e.f.0.c.0.0.0.0.1.0.0.0.0.0.1.1  IN PTR pirae-v6.ipv6.inrialpes.fr.
```

3.9.5 Mise à jour dynamique *[WIP]*

Certaines évolutions permettant de mettre à jour le DNS dynamiquement sont à l'étude et permettront au DNS d'être à jour sans avoir à rentrer toutes les adresses à la main (surtout que l'autoconfiguration automatique des machines (cf. § 5) rend ce travail quasi-impossible). Plusieurs propositions sont envisagées :

- Mise à jour dynamique où une machine envoie au serveur DNS son adresse et les noms auxquels elle veut répondre. Dans le cas où on utilise un serveur DHCP pour l'attribution des adresses, celui-ci pourra se charger de cette tâche.
- Mise à jour des serveurs secondaires. Dans le cas où le serveur primaire est remis à jour (par exemple, quand une machine a été rajoutée), il faut mettre à jour les serveurs secondaires pour qu'ils puissent propager cette information.

4 ICMPv6

Le protocole ICMP a également été revu et amélioré. En plus des fonctions déjà présentes dans IPv4 (détection d'erreur, test, configuration automatique), ICMPv6 intègre également les fonctions de gestion des groupes de multicast (effectuée par IGMP auparavant) et les fonctions du protocole ARP.

4.1 Gestion des erreurs

Les messages d'erreurs sont envoyés par un routeur ou par la machine destination lorsqu'un paquet ne peut être acheminé. Le type d'erreur a une valeur inférieure à 127 et le début du paquet fautif est envoyé avec le message.

- Destination inaccessible [Type=1]
  - Aucune route vers la destination (0)
  - La communication avec la destination est administrativement interdite (1)
  - La destination n'est pas un voisin (2)
  - L'adresse est inaccessible (3)
  - Le numéro de port est inaccessible (4)
- Paquet trop grand [Type=2]
- Temps dépassé [Type=3]
  - Limite du nombre de sauts atteinte (0)
  - Temps de réassemblage dépassé (1)
- Erreur de paramètre [Type=4]
  - Champ d'en-tête erroné
  - Champ d'en tête suivant non reconnu
  - Option non reconnue

4.2 Information

Ce sont les messages utilisés pour tester la connectivité (*ping*) et pour gérer les groupes multicast.

- Demande d'écho [Type=128]
- Réponse d'écho [Type=129]
- Demande de gestion de groupe multicast [Type=130]
- Rapport de gestion de groupe multicast [Type=131]
- Réduction d'un groupe multicast [Type=132]

4.3 Découverte de voisins

Ce sont les messages utilisés par une machine pour communiquer avec les autres. Ils permettent de trouver les routeurs, les adresses physiques des voisins (remplace ARP), et de vérifier et d'optimiser les tables de routage.

- Sollicitation d'un routeur [Type=133]
- Annonce du routeur [Type=134]
- Sollicitation d'un voisin [Type=135]
- Annonce d'un voisin [Type=136]
- Indication de redirection [Type=137]

4.3.1 Sollicitation d'un routeur

Ce message est émis par une machine désirant avoir des informations sur les routeurs présents sur le lien. Il est donc envoyé à l'adresse multicast `FF02::2` (routeurs sur le lien). Si l'équipement ne connaît pas encore son adresse source, il peut utiliser l'adresse non spécifiée.

La machine peut inclure son adresse physique en option.

4.3.2 Annonce du routeur

Ce message est émis périodiquement par les routeurs ou en réponse à un message de sollicitation. Il permet aux équipements de connaître le routeur ainsi que les paramètres de configuration à utiliser.

Paramètres pouvant être contenus dans le message :
- Nombre de saut max. à utiliser dans les paquets
- Si l'adresse d'un équipement doit être obtenue avec un protocole de configuration (DHCPv6)
- Si le routeur peut être utilisé comme agent mère pour un nœud mobile
- La durée de vie du routeur
- La durée d'accessibilité (durée pendant laquelle une information contenue dans le cache peut être considérée comme valide)
- La temporisation de retransmission (période entre deux émissions non sollicitées de l'annonce du routeur)
- L'adresse physique du routeur
- La taille du MTU à utiliser
- Le préfixe correspondant au réseau
- Si un équipement peut utiliser ce préfixe pour construire son adresse
- La durée de validité du préfixe
- etc…

4.3.3 Sollicitation d'un voisin

Ce message permet d'avoir des informations sur une machine située sur le même lien. Il est surtout utilisé pour détecter une adresse dupliquée et pour connaître l'adresse physique d'une machine (remplaçant d'ARP). Un champ adresse cible permet d'indiquer l'adresse dont on veut obtenir des informations. Le message peut être envoyé directement ou vers une adresse multicast.

4.3.3.1 Détection d'adresse dupliquée

Lorsqu'une machine veut utiliser une adresse, elle doit impérativement vérifier qu'elle n'est pas déjà utilisée. Pour cela, elle envoie un message de sollicitation vers l'adresse multicast sollicitée (adresse constituée du préfixe `FF02::1:FF00:0/104` suivi des 24 derniers bits de l'adresse unicast sollicitée) et attend une réponse. Si aucune réponse n'est reçu au bout d'une seconde (valeur par défaut), la machine peut considérer qu'aucun équipement n'utilise cette adresse et peut donc l'utiliser. Si une machine répond, on ne peut pas utiliser cette adresse, une intervention humaine sera sûrement nécessaire.

4.3.3.2 Recherche de l'adresse physique

Pour connaître l'adresse physique d'une machine située sur le même lien, une machine envoie un message de sollicitation vers l'adresse multicast sollicitée (adresse constituée du préfixe `FF02::1:FF00:0/104` suivi des 24 derniers bits de l'adresse unicast sollicitée) et attend une réponse. La réponse contiendra l'adresse physique, ce qui permettra de commencer la communication directement (sans passer par le multicast).

4.3.4 Annonce d'un voisin

Ce message est émis (le plus souvent) en réponse à une sollicitation de voisin. Il peut aussi être émis spontanément pour indiquer un changement d'adresse physique.

Les paramètres contenus dans la réponse sont :
- L'adresse physique de la source
- Si l'équipement est un routeur (peut indiquer le fait qu'un routeur redevienne une station normale)
- Si l'annonce est faite en réponse à une sollicitation
- Si cette annonce doit remplacer des informations déjà contenu dans le cache

4.3.5 Indication de redirection

Ce message est envoyé par un routeur pour indiquer à une machine qu'elle peut optimiser sa table de routage (s'il existe une route plus courte). Cela peut être le cas s'il existe un routeur plus approprié ou si la machine destination est située sur le même lien physique. Cf. § 5.2.

4.4 Autres Fonctions

Certaines nouvelles fonctionnalités sont encore expérimentales, il s'agit de :
- Renumérotation des routeurs [Type=138]
- Node Information Query [Type=139]
- Node Information Response [Type=140]

4.4.1 Renumérotation des routeurs *[WIP]*

Le protocole de renumérotation des routeurs permet d'indiquer les changements de préfixes à un routeur pour effectuer une renumérotation (une fois que le routeur sera renuméroté, les équipements terminaux se renuméroteront grâce aux messages de découverte de voisin). Cela permet de renuméroter un site en quelques messages.

Le message contient un préfixe de test (pour déterminer le ou les préfixes à remplacer), une opération (ajout, remplacement, …) et les nouveaux préfixes.

Les messages devront bien entendu utiliser l'extension d'authentification pour éviter qu'une machine ne déclenche une renumérotation sans autorisation.

4.4.2 Node Information Query / Response *[WIP]*

Ce protocole permet de demander des informations sur un nœud. Les informations pouvant être demandées sont les suivantes :
- Types d'informations supportés (donc pouvant être demandés)
- Nom DNS (avec la durée pendant laquelle le nom est valide)
- Adresse IPv6
- Adresse IPv4

5 Configuration automatique

Un des grands avantages d'IPv6 est sa capacité à automatiquement configurer les postes clients. Dans la pratique, il suffit de brancher le poste sur le réseau pour qu'il se configure automatiquement (il trouve son adresse, les routeurs, les paramètres réseaux à utiliser, …). On peut également utiliser la nouvelle version de DHCP pour avoir une configuration plus fine et transmettre d'autres paramètres (serveur de noms, …)

Note : Cela n'est valable que pour les postes clients. Les routeurs doivent bien entendu être configurés *'à la main'*.

5.1 Découverte des paramètres réseaux

5.1.1 Détermination de l'adresse lien-local

La machine commence par créer son adresse lien-local (préfixe `FE80::/64`) en utilisant l'identifiant de l'interface. Avant toute utilisation de cette adresse, elle vérifie qu'aucune machine ne l'utilise déjà en utilisant le mécanisme de détection d'adresse dupliquée (cf. § 4.3.3.1). Si un machine l'utilise, le processus de configuration s'arrête et une intervention humaine sera nécessaire pour la configuration.

5.1.2 Recherche du routeur

La machine envoie un message de sollicitation du routeur sur le lien (à l'adresse `FF02::2`). Si un routeur est présent, sa réponse contiendra la méthode à utiliser pour la configuration :

- Autoconfiguration sans état (pas de gestion de l'adressage)
- Autoconfiguration avec état (gestion de l'adressage → DHCPv6)

Si aucun routeur ne répond, la machine peut tenter une autoconfiguration avec état s'il y a un serveur DHCPv6. Dans le cas contraire, elle ne pourra communiquer qu'avec les machines situées sur le même lien en utilisant son adresse lien local.

5.1.3 Autoconfiguration sans état

Dans ce cas, la machine se sert des paramètres fournis par l'annonce du routeur pour se configurer. Elle peut récupérer le préfixe à utiliser pour créer son adresse globale, ainsi que certains paramètres (nombre de sauts max, MTU, …). Avec son adresse globale et l'adresse du routeur, la machine est désormais capable de communiquer en dehors de son lien.

5.1.4 Autoconfiguration avec état (DHCPv6)

La configuration avec état est effectué en utilisant un serveur DHCPv6 qui affecte les adresses globales à utiliser. Tout comme son prédécesseur (DHCP), il peut également renvoyer d'autres paramètres de configuration comme l'adresse du serveur de nom, du serveur WINS, etc…

Configuration DHCP :

- Sollicitation DHCP, message émis vers un serveur ou relais DHCP. Pour cela, on utilise l'adresse multicast des agents DHCP situés sur le lien (`FF02::1:2`).
- Annonce DHCP en réponse à la sollicitation. Contient l'adresse IPv6 du serveur DHCP.
- Requête DHCP pour demander les paramètres de configuration.
- Réponse DHCP contenant les paramètres de configuration.

Autre messages DHCP

- Libération DHCP émis par le client pour informer le serveur qu'il libère des ressources.

- Reconfiguration DHCP émis par le serveur pour informer le client qu'il a de nouvelles informations de configuration. Le client doit alors effectuer une requête de configuration.

Quand la machine a obtenu son adresse, elle doit vérifier que celle-ci est unique en utilisant le mécanisme de détection d'adresse dupliquée (cf. § 4.3.3.1). Si elle est unique, elle peut commencer à l'utiliser.

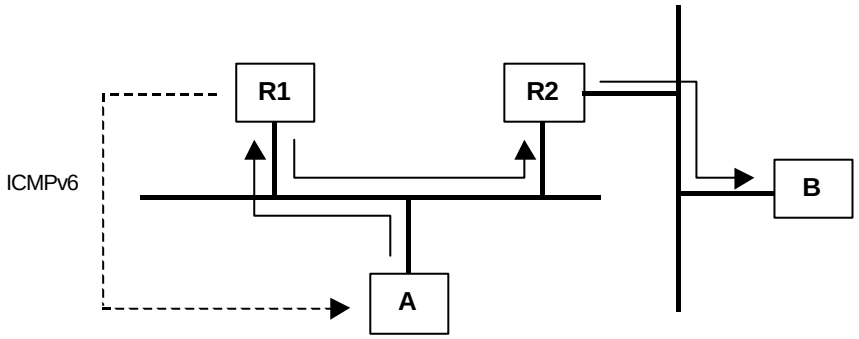
5.2 Optimisation de la table de routage

Lors de la configuration automatique, les machines utilisent le routeur qui répond à la sollicitation comme leur routeur par défaut. Toutes les communications avec une machine qui n'est pas situé sur le lien (qui n'a pas le même préfixe) sera donc dirigé vers ce routeur.

Cependant, il y a des cas où la table de routage pourrait être optimisée pour prendre en compte la topologie du réseau :
- Il y a un routeur plus approprié qui est situé sur le même lien
- La machine à joindre est située sur le même lien (même si elle a un préfixe différent)

Dans ce cas, le routeur peut envoyer un message ICMPv6 de redirection à la machine pour lui indiquer de mettre à jour ses tables de routage.

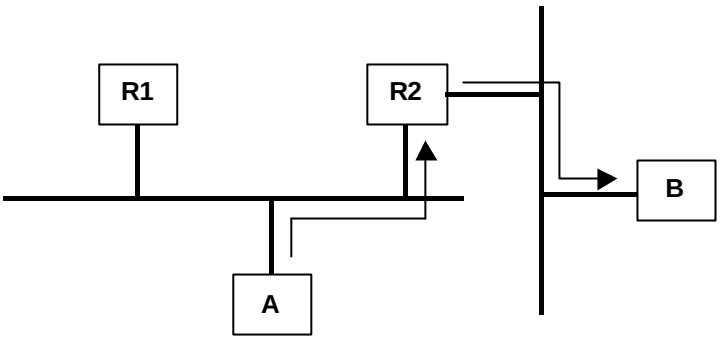
Exemple :



La machine A veut envoyer un paquet à B. Comme B n'est pas sur son réseau, elle l'envoie à son routeur par défaut : R1. R1 l'envoie alors à R2 qui est le routeur capable d'atteindre directement B. Comme R2 est sur le même lien que A, la machine A pourrait directement passer par R2 pour atteindre la machine B. Le routeur R1 envoie donc un message ICMPv6 de redirection à A.

La table de routage de A est alors la suivante :

Destination	Passerelle
Default	F0C0::1:ID_R1
F0C0::2:ID_B	F0C0::1:ID_R2



5.3 Découverte du PMTU

Le PMTU (*Path Maximum Transmission Unit*) correspond à la taille maximale à utiliser pour passer un ensemble de nœuds. Pour envoyer un message, un équipement doit donc déterminer le PMTU approprié pour que ses datagrammes soient les plus grands possibles mais également pour qu'ils puissent transiter par tous les liens (les routeurs ne font plus de fragmentation, c'est aux machines terminales de le faire).

Principe :

- Initialement, on considère que le PMTU est égal au MTU du lien sur lequel on se trouve.
- Si le paquet traverse un lien avec un MTU inférieur, le routeur détruit le paquet et envoie un message d'erreur ICMPv6 de type « message trop grand ». La taille du MTU à utiliser étant envoyé en paramètre du message d'erreur, l'équipement met à jour son PMTU.
- On recommence à envoyer jusqu'à ce que le paquet arrive à destination.
- De temps en temps, l'équipement peut envoyer un paquet plus grand pour vérifier que le PMTU n'a pas augmenté (grâce à un changement de route).

Note : La valeur minimum du PMTU est de 1280 octets.

6 Sécurité : IPSec

La plupart des logiciels voulant communiquer avec une gestion de la sécurité ont développé leurs propres mécanismes/protocoles (SSH, Secure HTTP, PGP, …). IPSec (*IP Security*) a été créé pour intégrer tous ces mécanismes directement au niveau de la couche IP. Comme IPSec sera obligatoire dans toutes les implémentations d'IPv6[1], la sécurité pourra être présente sur tous les équipements réseaux. Les services de sécurité fournis sont la confidentialité, l'authentification et l'intégrité des données, la protection contre le rejeu et le contrôle d'accès[2]. Ces services sont basés sur des mécanismes cryptographiques qui leur confèrent un niveau de sécurité élevé lorsqu'ils sont utilisés avec des algorithmes forts.

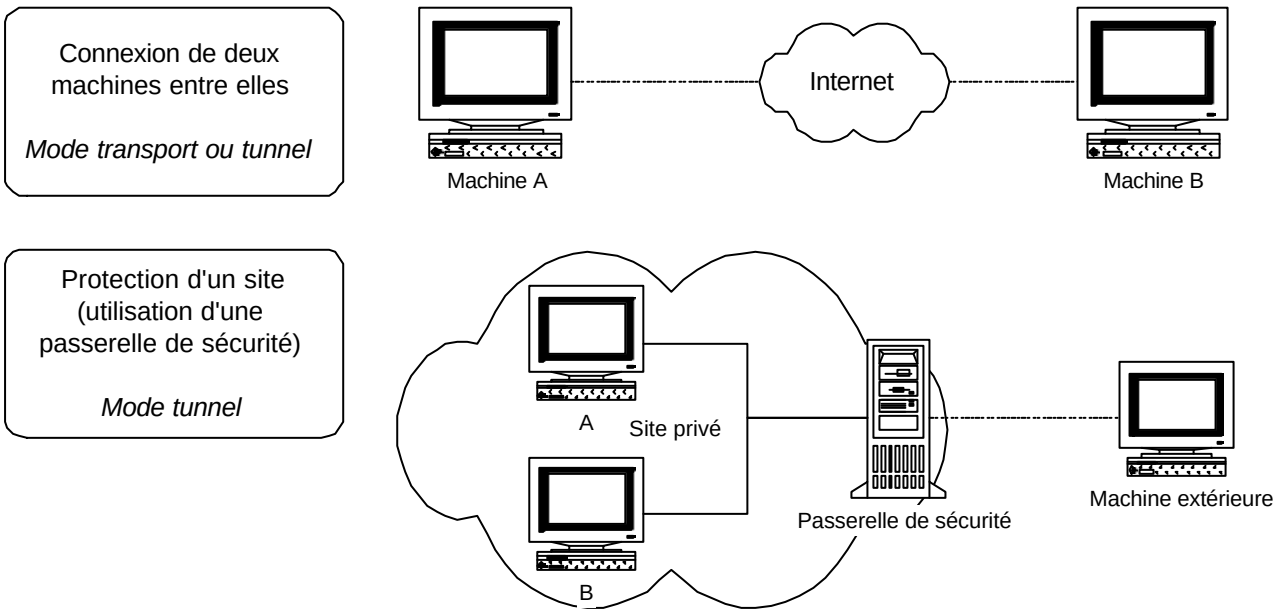
6.1 Présentation

6.1.1 Ce que fait IPSec

En offrant des services de sécurité au niveau de la couche transport, IPSec permet à n'importe quelle application d'utiliser ses services.

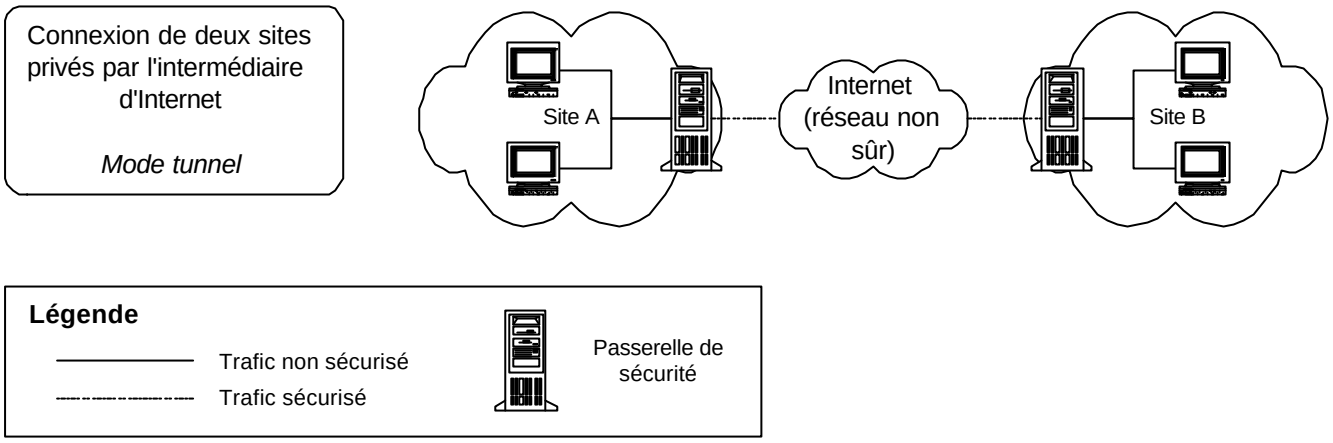
IPSec permet deux sortes de protection :

- Une protection bout en bout entre deux machines. Ce sont les machines qui gèrent IPSec (utilisé dans ce cas là en *mode transport*)
- Une protection sur un bout de segment. On utilise dans ce cas des passerelles de sécurité qui rajoutent la protection sur les paquets qui transitent par elles. On utilise dans ce cas la le *mode tunnel* où les paquets sont encapsulés dans un paquet protégé. La protection peut se faire entre deux passerelles de sécurité où entre une machine et une passerelle de sécurité



[1] On peut également l'utiliser avec IPv4.

[2] Cf. Annexe 2 pour la définition des différents services de sécurité



6.1.2 Comment fonctionne IPSec

IPSec utilise deux extensions (cf. § 2.4) du protocole IPv6 : AH (Authentification Header) et ESP (Encapsulation Security Payload). AH est utilisé pour l'intégrité et l'authentification, alors que ESP est utilisé pour la confidentialité. Ces deux services ont été séparés pour permettre d'utiliser des algorithmes différents pour chacun d'entre eux (la législation de certains pays permet par exemple d'utiliser des clés plus fortes dans le cas de l'authentification).

6.1.3 Quels sont les algorithmes utilisables par IPSec

IPSec a été conçu pour ne pas être dépendant de tel ou tel algorithme. Tous les algorithmes peuvent donc être implémentés dans IPSec, ce qui permet l'utilisation des algorithmes les plus appropriés en fonction des circonstances (législation du pays, niveau de sécurité requis, armée, …). Néanmoins, certains algorithmes seront implémentés en standard pour faciliter la communication entre les machines sur Internet : DES-CBC et 3DES-CBC pour le chiffrement et HMAC-MD5 et HMAC-SHA-1 pour l'authentification.

6.1.4 Comment est configuré IPSec

IPSec se sert du concept d'association de sécurité pour fonctionner. Une association de sécurité contient tous les paramètres à appliquer à une communication. Pour gérer ces associations, IPSec dispose de deux bases (SPD et SAD – cf. § 6.3.2) qui lui indiquent quels sont les paramètres de sécurité (type, algorithme, clés, …) à appliquer à un paquet en fonction de ses paramètres (source, destination, ports, …). Cette configuration peut être effectuée soit en statique (par l'administrateur), soit en dynamique (par les applications) dans le cas où il y a des clés générées automatiquement ou distribuées par un serveur de clés. *Note :* L'utilisation de deux bases pour gérer IPSec n'est qu'une recommandation. La manière d'implémenter ces deux bases est laissé à la charge des développeurs.

6.2 Extensions de sécurité

6.2.1 AH – Authentification Header

Le principe de l'AH est d'ajouter au paquet IP classique un identificateur permettant à la réception de vérifier l'intégrité des données contenues dans le paquet. De plus, l'intégrité de l'adresse source permet d'authentifier celle-ci et un numéro de séquence permet de détecter les tentatives de rejeu.

L'extension AH contient les données suivantes :
- SPI (*Security Parameters Index*) : Il permet (associé avec l'adresse de destination) d'identifier de manière unique l'association de sécurité[1] utilisée.
- Numéro de séquence : Il est incrémenté par la source lors de l'envoi de chaque nouveau paquet. Il permet donc de détecter les rejeux de paquet IP.
- Données d'authentification : Champ de longueur variable contenant l'identificateur (ICV – *Integrity Check Value*) calculé par la source et permettant de prouver l'intégrité du paquet.

Protection assurée en fonction du mode :
- **Mode Transport :** La protection est assurée uniquement sur les données de la couche transport et sur les champs qui ne subissent pas de modification pendant le transport.
- **Mode Tunnel :** La protection est assurée sur l'ensemble du paquet.

6.2.2 ESP – Encapsulation Security Payload

Le principe de l'ESP est de générer, à partir d'un paquet IP classique, un nouveau paquet IP dans lequel les données et éventuellement l'en-tête originale, sont chiffrés.

Note : ESP peut également assurer l'authenticité des données par ajout d'un bloc d'authentification et la protection contre le rejeu par le biais d'un numéro de séquence. Dans ce cas, l'authentification porte sur l'ensemble des données chiffrées.

L'extension ESP contient les données suivantes :
- SPI (*Security Parameters Index*) : Il permet (associé avec l'adresse de destination) d'identifier de manière unique l'association de sécurité utilisée.
- Numéro de séquence : Il est incrémenté par la source lors de l'envoi de chaque nouveau paquet. Il permet donc de détecter les rejeux de paquet IP (optionnel).
- Données chiffrées plus éventuellement des données de synchronisation (en fonction de l'algorithme utilisé)
- Octets d'alignement + longueur
- En-tête suivant
- Données d'authentification (en fonction de l'algorithme utilisé)

Protection assurée en fonction du mode :
- **Mode Transport :** La protection est assurée uniquement sur les données de la couche transport et éventuellement sur l'extension destination.
- **Mode Tunnel :** La protection est assurée sur l'ensemble du paquet. Dans le cas de deux sites reliés à l'aide de passerelles de sécurité, cela permet de chiffrer certaines données de l'en-tête pouvant être confidentielles (adresses sources et destination des machines communicantes).

6.3 Les associations de sécurité

6.3.1 Présentation

Un concept clé qui revient à la fois dans les mécanismes d'authentification et de confidentialité dans IP est l'association de sécurité. Une association de sécurité définit les paramètres de sécurité à appliquer sur une communication (on utilise une association par sens, on a donc besoin de deux associations pour une communication bidirectionnelle).

[1] Association de sécurité : Cf. § 6.3. Contient tous les paramètres de sécurité qui seront appliqués à une communication.

Une association de sécurité est définie de manière unique par une adresse de destination, un indice (SPI – *Security Parameters Index*) et l'extension de sécurité (AH ou ESP). Cela permet de retrouver les traitements à effectuer sur un paquet sans avoir accès aux autres champs (en effet, dans le cas du chiffrement, certains champs, comme les ports, ne sont pas accessibles en clair).

Une association de sécurité contient entre autres les paramètres suivants :
- Les paramètres de l'algorithme utilisé (type d'algorithme, clés de chiffrement, etc…)
- La durée de vie de l'association de sécurité
- Le mode du protocole IPsec : tunnel, transport ou wildcard (le mode sera déterminé par l'application)
- Les paramètres de protection contre le rejeu (numéro de séquence, numéro de séquence maximal, …)

6.3.2 Bases de données

Pour plus de clarté, on utilise deux bases de données, ce qui permet de séparer la sélection des paramètres de sécurité et les paramètres de sécurité en eux-mêmes.
- La base de données SPD (*Security Policy Database*) permet de trouver l'association de sécurité à utiliser sur un paquet entrant ou sortant.
- La base de données SAD (*Security Association Database*) contient l'ensemble des associations de sécurité avec leurs paramètres (algorithmes, clés, …). C'est cette base qui est utilisée pour authentifier, vérifier l'authentification, chiffrer ou déchiffrer un paquet.

6.3.2.1 SPD – Security Policy Database

Cette base contient une liste *ordonnée* d'entrée qui permettent de choisir les types d'associations à utiliser sur tel ou tel trafic. Il y a deux bases SPD pour chaque interface (une pour le trafic entrant, une pour le trafic sortant). On utilise pour cela des *selectors* :
- Adresse IP source
- Adresse IP de destination
- Port source
- Port destination
- Protocole de niveau transport (obtenu par le champ en-tête suivant)
- Identité de l'utilisateur
- Identité de l'équipement (par exemple DNS)
- Niveau de sensibilité des données (étiquettes normalisées IPSO/CIPSO[1])

Note : Certains *selectors* ne s'appliquent pas forcement sur des champs contenus dans un paquet IP. En particulier, le nom de l'utilisateur local peut être utilisé pour éviter de donner la même clé à deux utilisateurs connectés sur une même machine (ils pourraient éventuellement la trouver en analysant ce qu'ils envoient et ce qui passe sur le réseau).

Pour chacun, on peut utiliser une valeur fixe, un intervalle ou un joker.

Chaque entrée du SPD contient :
- Selectors
- Action à effectuer :
  - Discard : le paquet est jeté (il n'a pas le droit de passer).
  - Bypass IPSec : le paquet peut passer sans que IPSec ne le traite.
  - Apply IPSec : on applique une association de sécurité au paquet.
- Spécifications de Sécurité : mode (tunnel, transport, joker), type (AH, ESP, ESP+AH), algorithme (hmacdes, blowfish, …)

[1] cf. RFC1108. Options de sécurité définies par l'Armée Américaine

- Pointeur sur un groupe d'associations de sécurité (base SAD)

La liste des entrée de la SPD est parcourue jusqu'à la première entrée qui satisfait les paramètres d'un paquet. Cette entrée nous indique un groupe (zéro, une ou plusieurs) d'associations de sécurité contenus dans la base SAD. On recherche ensuite l'entrée SAD qui satisfait les paramètres du paquet et on l'utilise sur le paquet. S'il n'y a pas d'association qui correspond, on en crée une nouvelle et on la chaîne avec les autres.

Exemple : SPD Trafic Sortant

N°	Selectors						Specif. Sec.	Action	Pointeur AS
	Addr. Dst.	Addr. Src.	Protocole	Port Dst.	Port Src.	…			
1	FE80::/64	*	*	*	*		-	Bypass	Null
2	FEC0::/48	*	*	*	*		-	Bypass	Null
3	*	*	TCP	23	*		Transp – AH+ESP – hmacdes+blowfish	IPSec	3
4	*	*	*	*	*		Transp – AH – hmacdes	IPSec	1

Dans cet exemple, on n'utilise pas IPSec pour tout le trafic interne (FE80::/64 et FEC0::/48). Par contre, on utilise l'authentification en mode transport pour tous les autres trafics (algo. hmacdes). Dans le cas du telnet (port TCP 23), on ajoute également le chiffrement des données par blowfish.

6.3.2.2 SAD – Security Association Database

Cette base contient toutes les associations de sécurités, éventuellement chaînées entre elles dans le cas où elles sont associées à la même entrée de la base SPD. On accède à une entrée de la base SAD, soit par chaînage depuis la base SPD, soit avec un triplet (adresse destination, type (AH/ESP), SPI) qui identifie de manière unique l'association.

Exemple : SAD Trafic Sortant

N°	Selectors						SPI	Proto	Mode	Param. Securité*	Pointeur Suivant
	Addr. Dst.	Addr. Src.	Proto.	Port Dst.	Port Src.	…					
1	@A	@IP	TCP	110	4569		100	AH	Transport	XXXX*	2
2	@B	@IP	UDP	80	4531		200	AH	Transport	XXXX*	4
3	@B	@IP	TCP	23	4523		300	AH+ESP	Transport	XXXX*	Null
4	@C	@IP	TCP	80	4576		400	AH	Transport	XXXX*	5
5	@C	@IP	TCP	25	4521		500	AH	Transport	XXXX*	Null

* *Paramètres de sécurité* : Algorithme, clé, durée de vie, numéro de séquence, etc…

6.3.3 Traitement des paquets

6.3.3.1 Paquets sortants

- La base SPD est parcourue dans l'ordre jusqu'à trouver un élément qui satisfasse les paramètres du paquet. Si on doit appliquer IPSec sur ce paquet, on utilise le groupe d'associations de sécurité associé.
- On parcourt cette liste (base SAD) jusqu'à trouver une association qui satisfasse les paramètres du paquet.
- Si on n'en trouve pas, on la crée (avec les paramètres de la base SPD) et on l'insère dans la liste (cf. § 6.4.3).
- On applique ensuite les paramètres de l'association de sécurité sur le paquet avant de l'envoyer sur le réseau.

6.3.3.2 Paquets entrants

- On utilise l'adresse destination, type (AH/ESP) et le SPI pour rechercher l'association de sécurité à utiliser dans la base SAD.
- On applique les paramètres de cette association pour vérifier/déchiffrer le paquet.
- On recherche s'il existe bien une entrée dans la base SPD qui satisfasse les paramètres du paquet et qui contienne bien l'association qui a été utilisé. Dans le cas contraire, le paquet est refusé.

6.4 Gestion des Associations de Sécurité

6.4.1 Introduction

On a besoin d'un système de gestion des associations de sécurité pour pouvoir les créer avant de commencer une communication. Il faut également prendre en compte la gestion des clés (clés statiques, clés partagées, clés publiques/privées) pour que deux machines puissent utiliser les mécanismes de IPSec. Il est donc nécessaire, soit de pouvoir les saisir manuellement (gestion manuelle), soit d'utiliser des protocoles de gestion des associations entre les machines (gestion automatique).

6.4.2 Gestion manuelle

La gestion manuelle est la solution la plus simple pour saisir les paramètres de sécurité. C'est l'administrateur qui configure manuellement chaque équipement avec les paramètres appropriés. Si cette approche s'avère relativement pratique dans un environnement statique et de petite taille, elle ne convient plus pour un réseau de taille importante. De plus, elle implique une définition totalement statique des paramètres et un non-renouvellement des clefs. Cela peut néanmoins être utilisé pour distribuer les clés utilisées dans les passerelles de sécurité d'un réseau virtuel privé (si le nombre de sites n'est pas trop important).

6.4.3 Gestion automatique

Un système de gestion automatique des associations de sécurité et des clés associées est nécessaire pour tous les cas où la configuration manuelle n'est pas possible : génération de clés à la demande (clés pour un utilisateur, clés de session, …), distribution de clés publiques, échange de clés, … IPSec recommande d'utiliser IKE pour faire ce travail mais n'importe qu'elle autre protocole de gestion d'associations (et de clés) peut être utilisé.

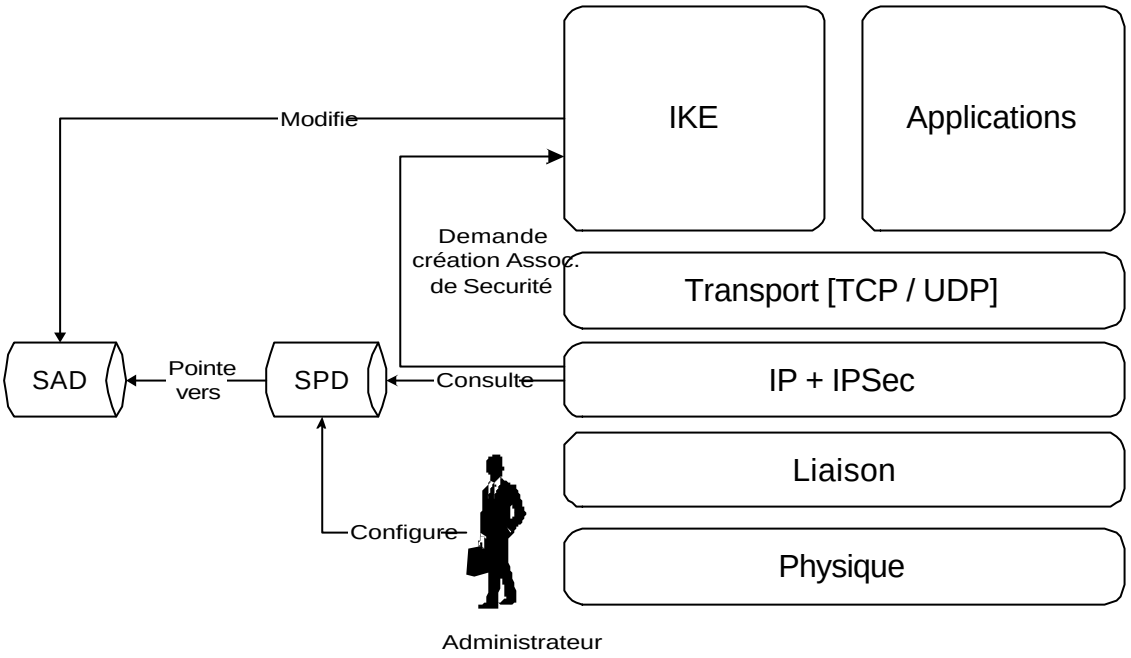
6.4.3.1 IKE

IKE (*Internet Key Exchange*) est un système développé spécifiquement pour IPsec et qui vise à fournir des mécanismes d'authentification et d'échange de clef adaptés à l'ensemble des situations qui peuvent se présenter sur l'Internet. Il s'agit d'un protocole de haut niveau (couche applicative). Il est composé de deux éléments :

- ISAKMP (*Internet Security Association and Key Management Protocol*) qui est utilisé pour la négociation, la mise à jour et la suppression des associations de sécurité.
- Oakley et SKEME qui sont utilisés pour faire de l'échange/création de clés.

Pour le moment, il n'y a pas de protocole de distribution de clés publiques dans IKE, mais plusieurs solutions sont à l'étude.

IKE est utilisé dans le cas où IPSec a déterminé qu'il fallait appliquer des mécanismes de sécurité mais qu'il n'y a pas encore d'association de sécurité correspondante. Dans ce cas IKE va établir une connexion sécurisée avec la machine distante et négocier les paramètres de sécurité. Une fois ces paramètres connus, IKE crée la nouvelle association de sécurité, qui va pouvoir être utilisée par IPSec pour envoyer son paquet.



6.4.3.2 Autres protocoles

IPSec n'oblige pas à utiliser IKE comme système de gestion de clés. On peut donc utiliser d'autres protocoles, comme :

- Kerberos
- SKIP (*Simple Key Management for Internet Protocol*)
- …

6.5 Multicast

La sécurisation du trafic multicast pose les problèmes suivants :

- Tous les membres du groupe devraient utiliser la même association de sécurité. Cela implique qu'il n'est pas possible d'authentifier la machine source de manière sûre : Si toutes les machines du groupe possèdent la clé, on ne peut pas être sûr que l'adresse source indiquée dans le paquet est la bonne. Un membre du groupe peut donc se faire passer pour un autre membre.
- Il faut utiliser des techniques de distribution de clés entre les machines du groupe. Certains protocoles sont à l'étude, mais ne sont pas encore assez matures pour être standardisés.

7 Mobilité

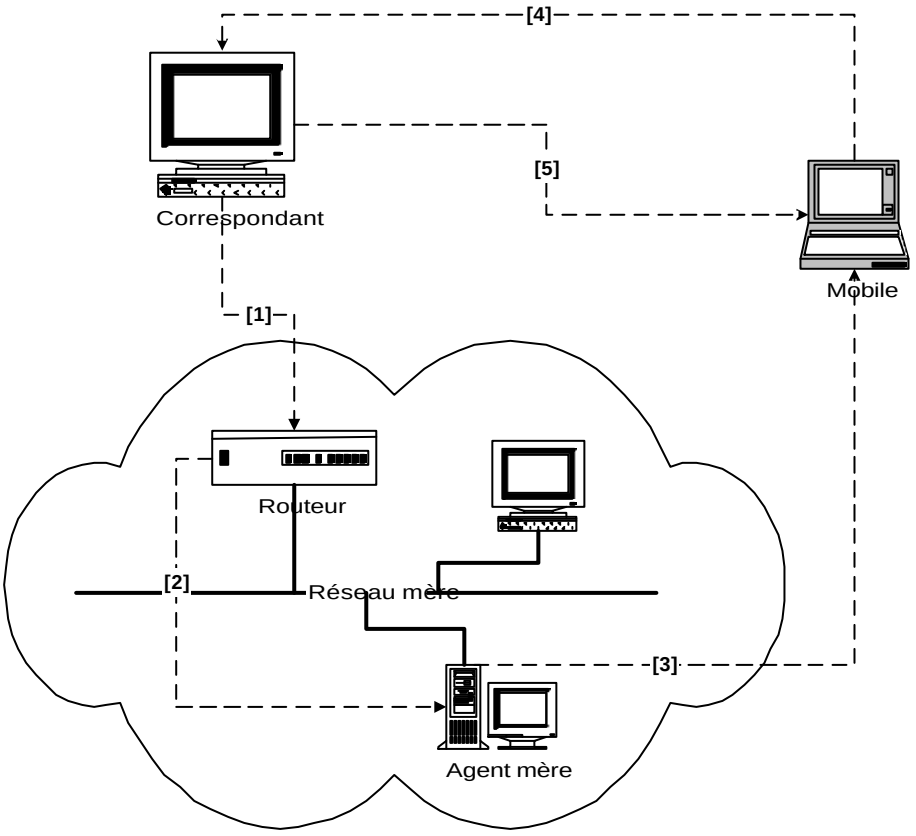
La mobilité sous IPv6 est un concept assez nouveau, il permet à un ordinateur de conserver son adresse IP quel que soit le réseau sur lequel il est relié physiquement. Le mobile peut donc être joint avec son adresse mère (*home address*) alors qu'il possède une adresse temporaire ou mobile (*care-of address*), et en cas de changement de réseau, les communications suivent automatiquement, sans interruption de service et en optimisant le routage (les paquets n'ont pas forcement besoin de passer par le réseau mère).

7.1 Introduction

Pour qu'un mobile puisse être joint par son adresse principale (ou adresse mère) quelque soit l'adresse qu'il utilise, il a besoin d'un agent mère qui se chargera de router les paquets dans le cas où les correspondants ne connaissent pas l'adresse mobile. Voici une synthèse simplifiée de l'utilisation de la mobilité :

- Le mobile cherche un agent mère (sur son réseau mère) et lui donne son adresse mobile (adresse temporaire)
- Si un correspondant veut joindre le mobile, il utilise l'adresse mère du mobile. **[1]**
- Le paquet est intercepté par l'agent mère et envoyé au mobile (tunnel IP). **[2]** et **[3]**
- Le mobile reçoit le paquet et informe le correspondant qu'il utilise une adresse mobile. **[4]**
- Le correspondant insère cette association dans son cache.
- Tant que l'association est valide, il envoie tous les paquets vers l'adresse mobile **[5]**

Grâce à ce système, une fois que le correspondant a pris connaissance de l'adresse mobile, plus rien ne passe par le réseau mère.



7.2 Options de l'extension Destination

Pour gérer la mobilité, quatre options ont été définies dans l'extension *Destination* de IPv6. Il s'agit de :

- **Mise à jour de l'association (*Binding Update*) :** Cette option est envoyée par un mobile pour envoyer à un correspondant ou à son agent mère son adresse temporaire. Il contient également un champ indiquant la durée de validité de l'association (une valeur de 0 indique que l'association n'est plus valide). Le bit *Enregistrement principal* indique que le destinataire du message est désigné comme agent mère du mobile.
- **Acquittement de l'association (*Binding Acknowledgement*) :** Acquittement du message précédent. Un champ statut indique si l'association a été acceptée ou non.
- **Demande de mise à jour de l'association (*Binding Request*) :** Cette option permet à une machine de demander l'envoi d'un message de mise à jour (pour rafraîchir le cache des associations).
- **Adresse principale :** Cette option informe un correspondant de l'adresse principale du mobile (les paquets sont envoyés avec l'adresse mobile).

Certaines sous-options peuvent être ajoutées aux messages :

- **Pad1 et Padn :** Ajout d'octets d'alignement.
- **Identifiant unique :** Utilisé pour identifier les demandes de mise à jour et les mises à jour correspondantes.
- **Liste des agents mère :** Liste d'agent mère susceptibles d'être utilisés par un mobile.
- **Autre adresse mobile :** Permet de donner une autre adresse mobile que l'adresse source pour créer une association.

Ces options peuvent être envoyées avec un paquet IP quelconque ou dans un paquet ne contenant aucune donnée.

7.3 Fonctionnement du Correspondant

7.3.1 Fonctionnalités requises

- Obligatoirement, réception et traitement de l'option *Adresse principale* contenue dans l'extension *Destination*.
- Eventuellement, être capable de traiter les options de *Mise à jour d'une association* et de les acquitter.
- Eventuellement, maintenir un cache des associations.

7.3.2 Réception de paquets en provenance d'un mobile

Si un paquet provient d'un mobile situé en dehors de son réseau mère, il devrait avoir son adresse mobile comme adresse source et son adresse principale dans l'option adresse principale. L'adresse mobile est indiquée dans l'adresse source du paquet car certains routeurs peuvent être configurés pour détruire les paquets émis avec une autre adresse que l'adresse utilisée par la machine. La couche IP du correspondant remplace ensuite l'adresse source par l'adresse principale avant de le passer aux couches supérieures. De cette manière, les applications ne savent même pas qu'il s'agit d'un mobile et que le paquet a été envoyé avec une adresse temporaire.

7.3.3 Réception d'un message de mise à jour de l'association

Si le paquet est valide, le correspondant met à jour son cache en fonction des paramètres. Il peut s'agir de :

- Nouvelle association entre une adresse principale et une adresse source.
- Mise à jour d'une association (nouvelle adresse mobile ou nouvelle durée de vie).
- Destruction de l'association.

Un message d'acquittement doit ensuite être renvoyé à la machine, en indiquant si la mise a jour a bien été prise en compte et sinon pourquoi.

7.3.4 Envoi d'une demande de mise àjour d'une association

Lorsqu'une association est retirée du cache car sa durée de vie est dépassée, toute communication en cours sera à nouveau dirigée vers le réseau mère, et le mobile enverra éventuellement une nouvelle association pour que l'on puisse à nouveau y accéder directement. Pour éviter tout ce mécanisme de recréation d'une association, le correspondant peut envoyer des demandes de mise à jour d'une association avant que la durée de vie ne soit expirée (en incluant la demande dans un n'importe quel paquet à destination du mobile). De cette manière, le mobile renverra une mise à jour de l'association avec une nouvelle durée de vie.

7.3.5 Envoi de paquets àun mobile

- Si le correspondant dispose d'une adresse temporaire valide pour le mobile, il l'utilise pour envoyer directement le paquet. L'adresse destination contient donc l'adresse temporaire, et on rajoute une en-tête de routage où l'on place l'adresse permanente. Lorsque le mobile recevra ce paquet, la couche IP échangera l'adresse destination et l'adresse contenue dans l'extension de routage. Il sera alors retransmis à la couche IP qui le fera suivre aux couches supérieures. De cette façon, les applications ne verront pas que le paquet a été envoyé à une adresse temporaire.
- Si le correspondant ne dispose d'aucune adresse temporaire, il l'envoie à l'adresse permanente. Le paquet sera intercepté par l'agent mère et envoyé au mobile (grâce à un tunnel IP).

7.4 Fonctionnement de l'Agent mère

7.4.1 Fonctionnalités requises

- Maintenir un registre des associations des mobiles gérés par l'agent.
- Interception des paquets à destination du mobile
- Capable d'encapsuler les paquets interceptés pour les envoyer à l'adresse mobile (en utilisant un tunnel IP)
- Acquitter les messages de mise à jour de l'association.
- Accepter les messages de mise à jour de l'association envoyés à l'adresse anycast des agents mère et être capable de participer à la découverte de l'adresse d'un agent mère.

7.4.2 Réception des messages d'annonce des routeurs

Dans les messages d'annonce des routeurs, il y a un champ indiquant si le routeur peut faire office d'agent mère (avec une préférence, une durée de vie, …). Chaque routeur doit garder en mémoire la liste des agents mère pour pouvoir envoyer une liste à un mobile cherchant un agent mère.

7.4.3 Découverte dynamique de l'adresse d'un agent mère

Si un mobile ne connaît pas son agent mère, il peut envoyer un message de mise à jour d'une association à l'adresse anycast des agents mères (cf. § 3.4.11). L'agent mère qui recevra cette requête devra acquitter ce message en envoyant la liste (trié par ordre de préférence) des agents mères présents sur le réseau.

7.4.4 Enregistrement de l'adresse temporaire primaire d'un mobile

Si un message de mise à jour d'une association est envoyé avec le bit d'*Enregistrement principal* positionné, le routeur est désigné pour être l'agent mère du mobile. Si le routeur ne dispose pas des fonctions agent mère ou si le mobile n'a pas les autorisations nécessaires, un message d'acquittement contenant les raisons du refus est envoyé au mobile.

Si le message est accepté, le routeur devient l'agent mère du mobile. Il place son association dans son cache comme étant une entrée principale. L'association ne pourra en aucun cas être supprimée du cache avant l'expiration de sa durée de vie. Comme l'agent mère devra intercepter tous les paquets à destination du mobile, il devra envoyer des messages *d'annonce d'un voisin* (avec son adresse MAC comme adresse MAC du mobile). De cette façon, toutes les machines du lien enverront les paquets à destination du mobile vers son agent mère.

7.4.5 Désenregistrement de l'adresse temporaire primaire d'un mobile

Lorsqu'un mobile revient dans son réseau mère, il envoie un message de mise à jour de l'association avec l'adresse mobile égale à l'adresse mère. L'agent mère doit donc arrêter d'être l'agent mère du mobile et détruit son association du cache. Il doit également envoyer un message d'*annonce d'un voisin* avec la véritable adresse MAC du mobile.

7.4.6 Interception et tunnelage des paquets à destination d'un mobile

Lorsque l'agent mère reçoit un paquet à destination d'un mobile dont il a la charge, il l'envoie à l'adresse temporaire du mobile en l'encapsulant dans un nouveau paquet IP (pour ne pas toucher à l'intégrité du paquet d'origine).

7.4.7 Renumérotation du sous-réseau mère

Pour permettre la renumérotation du sous-réseau mère lorsqu'un mobile est en dehors de son réseau, les agent mères doivent envoyer les annonce des routeurs lorsqu'un préfixe du réseau change.

7.5 Fonctionnement du Mobile

7.5.1 Fonctionnalités requises

- Capable de désencapsuler un paquet IP contenu dans un autre paquet IP.
- Capable d'envoyer les mises à jour d'association et de recevoir les acquitements.
- Pouvoir déterminer dynamiquement l'adresse de son agent mère.
- Garder la liste des toutes les machines auquel il a envoyé une mise à jour de l'association et dont la durée de vie n'a pas expirée.
- Capable de répondre aux demande de mise à jour d'association.
- Capable d'envoyer son adresse permanente dans l'option adresse permanente de l'option destination.

7.5.2 Envoi d'un paquet (mobile hors de son réseau)

Lorsqu'un mobile est en dehors de son réseau, il peut utiliser soit son adresse permanente, soit son adresse temporaire. Il utilisera son adresse temporaire pour des communications qui n'ont pas besoin d'un support de la mobilité (par exemple, une requête DNS). S'il utilise son adresse permanente, il mettra son adresse temporaire comme adresse source (pour éviter que les routeurs détruisent le paquet car il a une adresse source qui n'appartient pas au réseau) et ajoutera l'option adresse permanente de l'extension destination.

7.5.3 Réception d'un paquet (mobile hors de son réseau)

Un paquet peut arriver sous deux formes :

- Le paquet IP est encapsulé dans un autre paquet. La couche IP desencapsule le paquet et le traite normalement. On envoie également une mise à jour de l'association à l'émetteur pour qu'il sache où envoyer les paquets.

- Le paquet IP arrive à l'adresse temporaire avec l'adresse permanente incluse dans l'en-tête de routage. La couche IP échange l'adresse de destination et l'adresse contenue dans l'en-tête de routage (comme pour un routage normal). Comme la nouvelle adresse destination (adresse permanente) appartient aussi au mobile, le paquet est traité normalement.

7.5.4 Détection de mouvement

Le mobile peut envoyer des messages de *sollicitation du routeur* ou écouter les messages *d'annonce du routeur* pour détecter les changement de réseau. Lorsqu'il découvre un réseau, le mobile construit une nouvelle adresse temporaire à utiliser sur le réseau.

7.5.5 Envoi d'un message *Mise àjour de l'association* àson agent mère

Si le mobile change d'adresse temporaire primaire (par exemple, si la précédente n'est plus opérationnel), il doit en avertir son agent mère. Pour cela, il envoie un message de mise à jour de l'association avec le bit Enregistrement principal positionné et contenant son adresse permanente. Il envoie périodiquement ce message jusqu'à recevoir un acquittement.

7.5.6 Découverte dynamique de l'adresse de l'agent mère

Si un mobile ne connaît pas son agent mère, il peut envoyer un message de mise à jour d'une association à l'adresse anycast des agents mères (cf. § 3.4.11). L'agent mère qui recevra cette requête devra acquitter ce message en envoyant la liste (trié par ordre de préférence) des agents mères présents sur le réseau. Le mobile utilise ensuite cette liste pour trouver l'agent mère auquel faire sa demande.

7.5.7 Envoi de message *Mise àjour de l'association* aux correspondants

Un mobile envoie un message mise à jour de l'association quand il veut réactualiser la durée de vie de l'association ou lorsqu'il change d'adresse temporaire. Pour cela, il dispose de la liste des correspondants qui possèdent une association le concernant. Cela évite, en cas de changement d'adresse temporaire ou en cas d'expiration de la durée de vie, que les correspondant repasse par l'agent mère.

7.5.8 Demande de Forwarding par le précédent réseau temporaire

Lors d'un changement d'adresse temporaire primaire, le mobile envoie un message *de mise à jour de l'association* au précédent routeur. De cette manière, celui-ci va faire suivre tous les paquets qui lui arriveront en jouant le rôle d'agent mère le temps que la durée de vie des associations contenus dans le cache des correspondant expire.

7.5.9 Réception des acquittements de l'association

Si le message est valide, le mobile met à jour sa table de correspondants en fonction du résultat de la mise à jour :

- Si la mise à jour a été acceptée, il met à jour l'entrée du correspondant dans sa table et arrête d'envoyer des messages de mise à jour.
- Si la mise à jour a été refusée, il supprime l'entrée du correspondant de sa table.

7.5.10 Réception d'une demande de mise àjour

En cas de réception d'une demande de mise à jour, le mobile envoie un message de mise à jour pour que le correspondant puisse mettre à jour son cache (et en particulier la durée de vie). Le mobile met également à jour sa table de correspondants.

7.5.11 Utilisation de plusieurs adresses temporaires

Ce n'est pas gênant pour un mobile d'avoir plusieurs adresses temporaires. Au contraire, dans le cas de réseaux sans fils où le mobile est situé sur le chevauchement de plusieurs zones, le mobile peut accéder à plusieurs réseau. Par contre, il ne possède qu'une seule adresse temporaire primaire (enregistré auprès de son agent mère) et doit éviter la changer trop fréquemment.

7.5.12 Retour dans le sous réseau mère

Lorsque le mobile retourne dans son réseau mère, il envoie un message de *mise à jour de l'association* à son agent mère avec son adresse temporaire égale à son adresse permanente. L'agent mère va cesser d'intercepter les paquets du mobile. Le mobile envoie également des message *d'annonce du voisin* avec son adresse MAC pour que tous les paquets qui lui sont destinés lui arrivent effectivement.

7.6 Multicast

Même en dehors de son réseau, un mobile peut continuer à avoir accès à des groupes de Multicast. Pour les recevoir et envoyer des messages, il a deux possibilités :

- Il s'enregistre aux groupes de son choix avec son adresse temporaire et en utilisant le routeur local. Les envois se feront également avec son adresse temporaire.
- Il s'enregistre auprès de son agent mère et le trafic multicast passera par un tunnel entre l'agent mère et le mobile (il peut s'agir du seul moyen de recevoir des groupes privés de son site mère).

7.7 Sécurité

- Les options d'authentifications sont obligatoires pour un certains nombre de messages concernant la mobilité car il serait aussi non trop facile de court-circuiter le trafic d'une machine vers une autre. L'authentification est donc obligatoire pour les messages de mise à jour de l'association et d'acquittement.

- Dans le cas où la position du mobile dans le réseau serait confidentielle, la mise en place des mécanismes vus dans ce chapitre serait inapplicable et la seule solution resterait le tunneling de tous le trafic, sans l'utilisation des associations.

- Dans le cas d'un mobile, le trafic peut passer par n'importe quel point d'Internet, même dans le cas d'un dialogue entre deux machines du même site (mais avec le mobile en dehors du site). On pourra donc utiliser les extensions de confidentialité pour protéger le trafic.

8 Qualité de Service (QoS)

8.1 Introduction

Traditionnellement, le protocole IP ne garantit pas de qualité de service. La politique appliquée est celle du *'Best Effort'* où tous les paquets sont considérés de la même façon et où le seul but est de les faire transiter le plus vite possible. Un octet était cependant réservé dans IPv4 pour faire de la Qualité de Service (Octet TOS) mais il était assez limité (la *'precedence'* indiquait uniquement l'importance d'un paquet[1]) et n'a jamais été vraiment utilisé. Le champ *DiffServ* (*Differentiated Services*) a été défini pour permettre d'appliquer des mécanismes de Qualité de Service forts à la fois sur IPv4 et sur IPv6, tout en restant compatible avec l'ancien mécanisme (notion de *'precedence'* du champ TOS). Ce champ permet de donner un meilleur service à certains (et donc un moins bon service à d'autres) en fonction de ce qui a été défini (inégalité planifiée). La finalité principale de la Qualité de Service est de fixer par contrat les caractéristiques d'une ligne et de pouvoir traiter chaque trafic différemment.

8.2 DiffServ

8.2.1 Structure

L'octet DiffServ est utilisé dans le champ TOS de IPv4 et dans le champ Classe de trafic de IPv6. Il se présente sous la forme suivante :

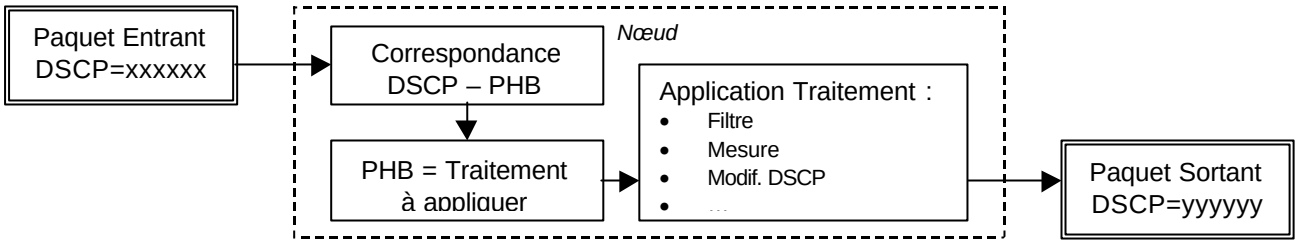
DSCP	CU
6 bits	2 bits

- Le champ CU – *Currently Unused*, n'est pas encore utilisé (comme son nom l'indique…).
- Le champ DSCP – *Differentiated Services Code Point*

Le champ DSCP permet de sélectionner le traitement à appliquer à un paquet arrivant sur un équipement (PHB – *Per-Hop Behavior*). Un équipement faisant de la Qualité de Service doit donc avoir une table de correspondance entre les DSCP et le PHB à appliquer. Cette correspondance est libre et doit être configurable. Cependant un certains nombre de correspondances *recommandées* existent et devraient être inclues dans la configuration.

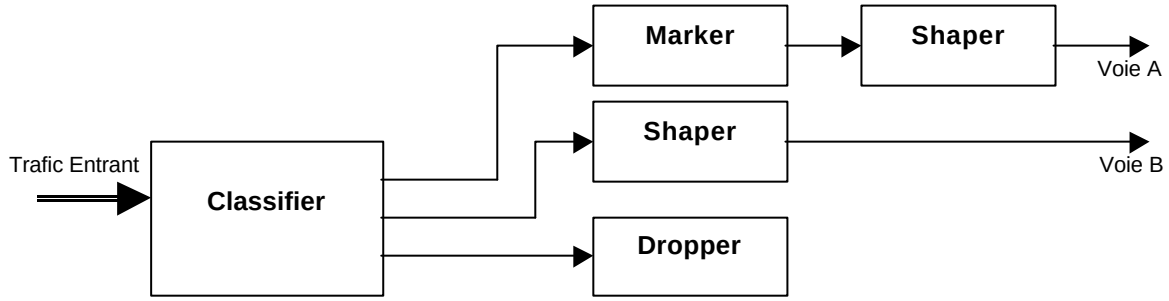
Comme la manière dont un paquet doit être traité évolue au cours du trajet, le champ DSCP peut être modifié par n'importe quel équipement en fonction de la nouvelle politique à appliquer sur un lien ou en fonction du comportement d'un flux (un flux ne respectant pas son profil prédéfini peut avoir son traitement modifié).

[1] Precedence : mesure de la nature et de l'importance d'un datagramme
- 000 : Routine
- 001 : Priority
- 010 : Immediate
- 011 : Flash
- 100 : Flash override
- 101 : Critical
- 110 : Internetwork Control
- 111 : Network Control



8.2.2 Traitements possibles

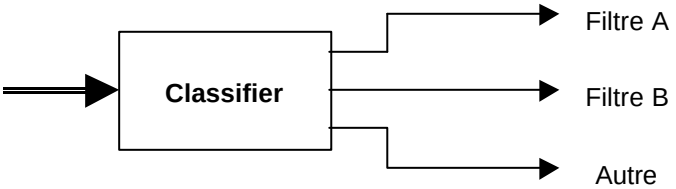
Pour décrire les traitements à effectuer, on utilise des éléments atomiques effectuant une unique opération. Ces éléments peuvent permettre de séparer le trafic, le mesurer, le réduire, … L'ensemble de ces éléments forme un TCB (Traffic Conditioning Blocks) et celui-ci définit le service à appliquer.



Exemple de TCB

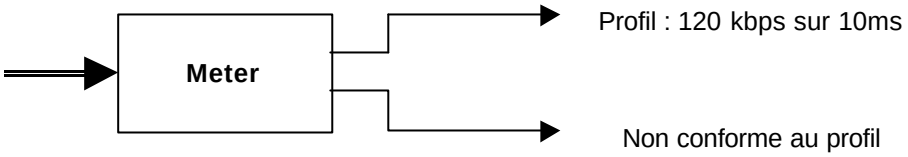
8.2.2.1 Classifier

Le Classifier sépare le flux de donnée entrant en plusieurs flux sortants en fonction de différents filtres. L'utilisation la plus courante est de séparer le trafic en fonction du champ DSCP (ou d'une partie de celui-ci) pour pouvoir ensuite appliquer les traitements fonctions de chaque classe de trafic. On peut également séparer le trafic en fonction des adresses IP ou des ports pour pouvoir ensuite le marquer avec un champ DSCP spécifique (peut être utile en sortie de site).



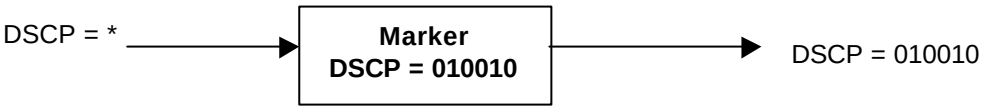
8.2.2.2 Meter

Le Meter mesure les caractéristiques d'un flux et le divise en plusieurs trafics sortants en fonction de la conformité au profil prédéfini. Le profil le plus souvent utilisé est le débit moyen que doit respecter un flux. Tous les paquets qui le respectent passent d'un côté et tous les autres passent de l'autre (ou sont détruits). On peut même avoir plus de deux sorties lorsque le choix dépend du niveau de conformité (le trafic respecte bien (vert), un peu (orange), ou pas du tout (rouge)).



8.2.2.3 Marker

Le Marker sert à marquer tous les paquets qui arrivent avec un même numéro DSCP. Cela peut servir à marquer un trafic qui n'a pas de DSCP (sortie d'un site sans QoS) ou à remarquer un trafic en fonction du lien sur lequel on va passer.

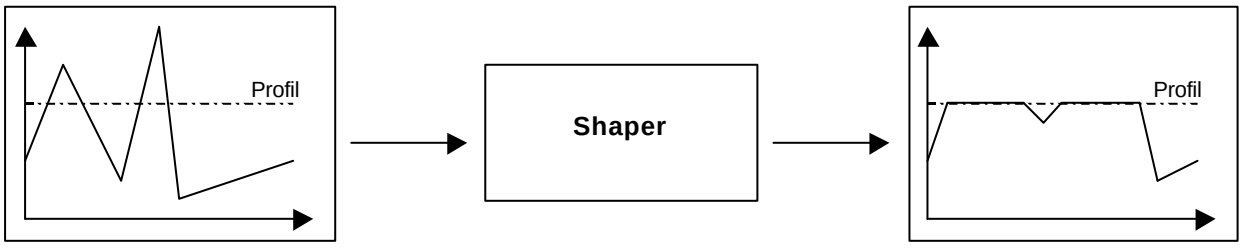


8.2.2.4 Dropper

Le Dropper détruit tous les paquets. On utilise donc les droppers après des éléments de sélection (classifier, meter) pour ne pas transmettre certains paquets.

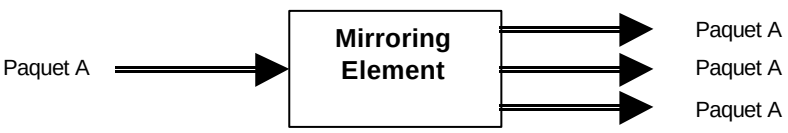
8.2.2.5 Shaper

Le Shaper est utilisé pour forcer un flux à respecter son profil. Au lieu de détourner les paquets qui ne respectent pas le profil (cf. meter), on les retarde et on les fait passer dès que possible.



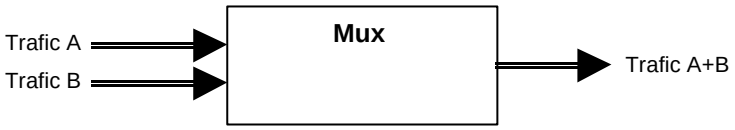
8.2.2.6 Mirroring Element

Le Mirroring Element dédouble le trafic entrant en plusieurs trafics sortants. Cela peut être utilisé pour des besoins de capture de données.



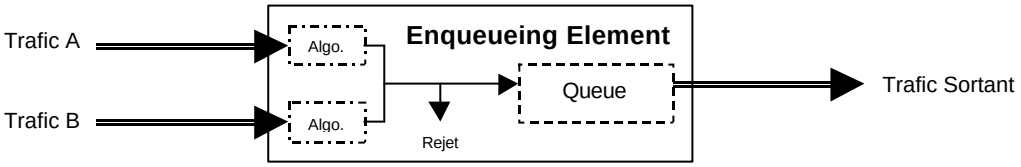
8.2.2.7 Mux

Le Mux effectue du multiplexage en regroupant plusieurs trafics entrants en un seul trafic sortant.



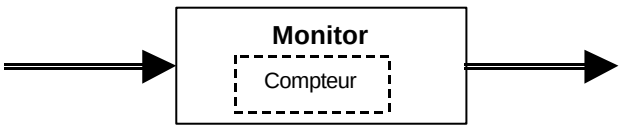
8.2.2.8 Enqueueing Element

Le Enqueueing Element insère les différents trafics entrants dans une file d'attente. Il peut utiliser plusieurs sortes d'algorithmes pour déterminer quels sont les paquets à rejeter pour ne pas faire déborder la file d'attente : *tail drop* (on rejette tous les paquets qui arrivent quand la file est pleine), utilisation de niveaux de destruction différents en fonction des paquets (cf. § 8.2.4.2), …



8.2.2.9 Monitor

Le Monitor est un élément passif qui compte le nombre d'octets qui le traversent. Cette mesure de trafic peut être ensuite utilisée pour faire des statistiques d'utilisation, établir des factures, …



8.2.3 Valeurs du champ DSCP

Les valeurs possibles que peut prendre le champ DSCP ont été divisées en trois plages :

xxxxx0	Actions standards
xxxx11	Utilisation Locale ou Expérimentale
xxxx01	Utilisation Locale ou Expérimentale (pourra éventuellement être utilisée pour des actions standards)

Parmi les actions standards, on distingue certaines valeurs particulières :

- **000000** est la valeur recommandée pour le PHB à utiliser par défaut. Ce PHB est utilisé pour tous le trafic qui n'a pas de traitement spécifique. La plupart du temps, on utilisera un traitement en FIFO et qui utilisera le débit restant. Ce PHB est également utilisé pour tous les DSCP inconnus.
- **xxx000** : Class Selector Codepoint. Les 8 valeurs possibles sont utilisées de la même façon que les 3 bits du champ *'precedence'* de IPv4 (pour rester compatible). C'est à dire que plus la valeur est élevé, plus la probabilité que le paquet soit acheminé dans les temps est grande. De plus, les deux valeurs 11x000 doivent en plus avoir une priorité plus élevée que le PHB par défaut. En effet, ces valeurs sont utilisées pour le contrôle réseau et les paquets correspondant doivent être acheminés le plus vite possible (et donc plus vite que le trafic normal).

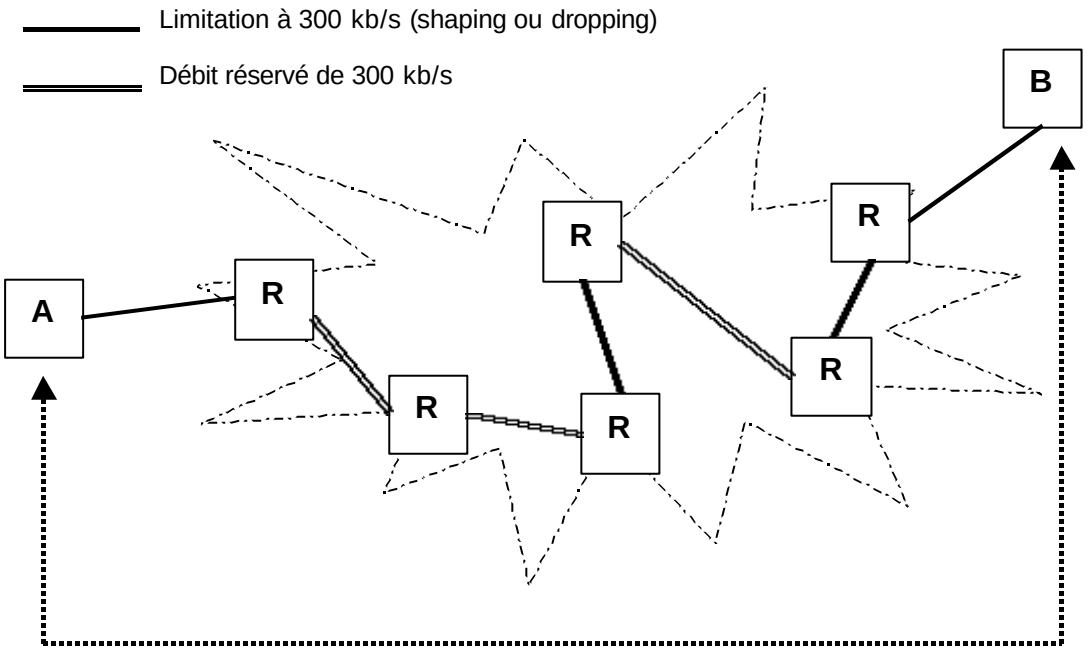
8.2.4 PHB particuliers

8.2.4.1 Expedited Forwarding PHB

Le PHB EF permet de construire une liaison avec un débit assuré[1] entre deux domaines DiffServ et avec des caractéristiques fixées par contrat. Une telle liaison peut être considérée comme une liaison point à point ou encore comme une ligne louée virtuelle. Ce service est également connu sous le nom de *Service Premium*.

Pour cela, il faut réserver le débit nécessaire sur toutes les lignes situées le long du trajet et s'assurer que le trafic aux extrémités ne dépasse pas le débit fixé. De cette manière, il n'y aura normalement aucune file d'attente car le trafic entrant pourra forcement être acheminé sans délai. On évite ainsi les pertes, temps de latence, congestion, … Le fournisseur peut donc garantir le débit et le temps de propagation sur cette LS virtuelle.

Le code DSCP recommandé pour ce service EF-PHB est 101110.



LS virtuelle de 300 kb/s

8.2.4.2 Assured Forwarding PHB

Le PHB AF est utilisé pour indiquer dans une même classe quels sont les paquets à détruire en premier en cas de congestion ou en cas de dépassement de trafic prédéfini. 12 codes DSCP sont réservé au AF-PHB, mais d'autres codes peuvent être utilisés en local. Ces 12 codes permettent l'utilisation de 4 classes comportant chacune 3 niveaux de 'destruction'.

Classe	
Classe AF 1	001xx0
Classe AF 2	010xx0

Niveau de destruction	
Low Drop	xx = 01
Medium Drop	xx = 10

[1] La définition complète est : a low loss, low latency, low jitter, assured bandwidth, end-to-end service.

Classe AF 3	011xx0	High Drop	xx = 11
Classe AF 4	100xx0		

Chaque classe est indépendante des autres, par contre à l'intérieur d'une même classe, certains paquets seront détruits en premier en cas de congestion.

Le Service Olympique utilise AF-PHB en proposant 3 classes (Or, Argent, Bronze) et où la classe en Or dispose d'une charge moins importante (et donc une probabilité d'acheminement dans les temps plus importante) que la classe en Argent. Idem entre la classe en Argent et la classe en Bronze. De plus, on dispose de 3 niveaux de destruction à l'intérieur de chacune des 3 classes.

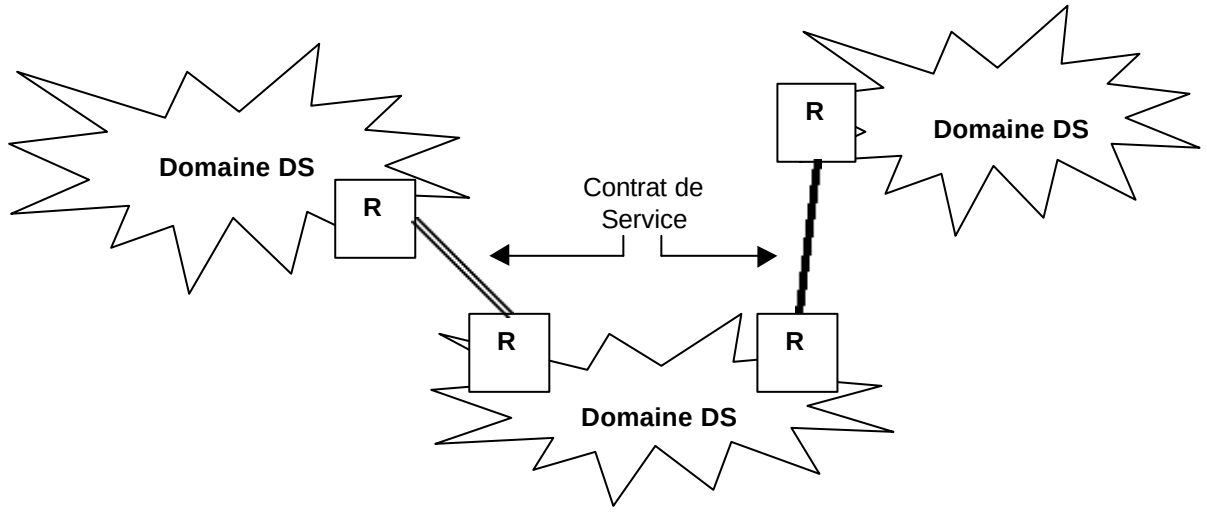
8.3 Utilisation

8.3.1 Contrat de Service

Pour pouvoir faire de la qualité de service, il faut nécessairement établir un contrat de service entre deux domaines DS[1] adjacents (le notre et celui du fournisseur d'accès). Ce contrat spécifiera les services proposés, ainsi que les caractéristiques des trafics circulants entre les deux domaines, en terme de débit, temps d'acheminement, taux de perte, … Il permettra également de spécifier les codes DSCP à utiliser.

Du côté de notre domaine DS, il faudra s'assurer (en fonction du contrat) que le trafic respecte le profil défini et il faudra éventuellement marquer celui-ci avec un code DSCP correspondant au service que l'on attend. En fonction du contrat, tous ce travail pourra être fait uniquement du côté du fournisseur.

Du côté du fournisseur d'accès, il vérifiera que le trafic respecte le profil prédéfini et appliquera des mesures restrictives (drop, changement de classe, shaping) dans le cas contraire. Il peut éventuellement remarquer le trafic avec un nouveau code DSCP en fonction de son réseau. De la même façon, il négociera un contrat avec ses propres fournisseurs pour la transmission de son trafic vers l'extérieur.



La succession des contrats de service permet d'assurer la qualité de service à travers plusieurs domaines DS. En effet, pour certains services, il faut pouvoir assurer les caractéristiques des liens entre tous les domaines DS. Si l'on passe par un domaine sans QoS, on ne peut plus assurer les caractéristiques d'un trafic. Un

[1] Domaine DS = Domaine Differentiated Service = Domaine où il y a une politique de différenciation de service qui est appliquée.

ensemble de domaines DS contigus forment une région DS, c'est à dire une région où la différentiation de service est possible.

8.3.2 Exemples d'utilisation

- Ligne louée virtuelle (Service Premium) avec des caractéristiques assurées (débit, délais, perte, …).
- Service Olympique qui définit 3 classes de trafic avec des priorités différentes ainsi que des niveaux d'importance à l'intérieur de chaque classe (pour déterminer les paquets à détruire au cas où).
- Priorité de certains paquets en fonction de :
  - adresse IP (plage)
  - protocole
  - …
- Limitation du débit de certains trafics
- Séparation du trafic pour un acheminement différent. Cela permet d'utiliser une ligne avec QoS pour un trafic X et envoyer le reste sur une ligne quelconque (et moins chère…).
- Facturation d'une ligne en fonction du volume généré par un certain trafic.
- …

9 Conclusion

Pour favoriser son déploiement, les concepteurs d'IPv6 ont dû proposer un protocole capable de résoudre tous les problèmes que l'on rencontre avec IPv4. Parmi les notions importantes d'IPv6, on peut noter :

- **Gérer les adresses plus efficacement** en gardant l'espace d'adressage le plus agrégé possible (ce qui facilite le routage) et en ayant un pool d'adresse inépuisable, capable de subvenir à tous les besoins.
- **Faciliter le déploiement de postes clients** en permettant une configuration automatique de tous les paramètres réseau.
- **Décharger les routeurs** en effectuant une partie des traitements sur les machines terminales (fragmentation, optimisation du routage, vérification des sommes de contrôle) et en simplifiant certains aspects (simplification des en-têtes, identificateur de flux, agrégation des adresses IPv6).
- **Intégrer les nouvelles technologies** qui manquent à IPv4 et qui seront essentielles au développement futur d'Internet : Sécurité, Mobilité, Qualité de Service, … L'intégration par défaut de ces nouvelles technologies permet de les utiliser à grande échelle et d'éviter l'emploi d'une multitude de mécanismes de substitution.
- **Faciliter la transition** de IPv4 vers IPv6 en définissant quelques mécanismes de cohabitation permettant une migration lente et progressive.

Du côté technique, on peut noter les fonctionnalités suivantes :

- Adresses sur 128 bits (pool inépuisable).
- Simplification des en-têtes.
- Sécurité (*IPSec*) implémentée par défaut (authentification et confidentialité).
- Renumérotation automatique.
- Pour chaque machine : présence d'une adresse globale, locale, site.
- Démocratisation des adresses Multicast et introduction des adresses Anycast.
- Configuration automatique des postes clients.
- Optimisation automatique des tables de routage des postes clients.
- Mobilité
  - Le mobile garde ses connexions même en cas de changement dynamique d'adresse.
  - Le mobile est joignable en permanence et accède à son réseau mère, comme s'il y était.
- Qualité de Service.

Toutefois, même s'il y a quelques mécanismes censés faciliter la transition, la migration de gros réseaux risque d'être délicate et va devoir nécessiter des mises à jour à tous les niveaux (équipements réseau, systèmes d'exploitation et logiciels).

10 Annexe 1 : Bibliographie

10.1 Présentations d'IPv6

[PPUREC1] *Internet Protocol version 6* – Transparents PowerPoint – B. Tuy (UREC) – Mars 1999

[PPUREC2] *Internet Protocol version 6* – Transparents PowerPoint – L. Toutain & JL. Richier & T. Noel – Présentation du G6 – Novembre 1999

10.2 Protocole

[OREIL99] *IPv6 Théorie et pratique* – Gisèle Cizault – Edition O'Reilly – Juin 1999.

[RFC2460] *Internet Protocol, Version 6 (IPv6) Specification* – S. Deering & R. Hinden – Décembre 1998 – Statut : Draft Standard.

[IANAPAR] *IANA : IPv6 Parameters* – http://www.isi.edu/in-notes/iana/assignments/ipv6-parameters.

10.3 Adressage

[OREIL99] *IPv6 Théorie et pratique* – Gisèle Cizault – Edition O'Reilly – Juin 1999.

[RFC1886] *DNS Extensions to support IP version 6* – S. Thomson & C. Huitema – Décembre 1995 – Statut : Proposed Standard.

[RFC2373] *IP Version 6 Addressing Architecture* – R. Hinden & S. Deering – Juillet 1998 – Statut : Proposed Standard.

[RFC2374] *An IPv6 Aggregatable Global Unicast Address Format* – R. Hinden & M. O'Dell & S. Deering – Juillet 1998 – Statut : Proposed Standard.

[RFC2375] *IPv6 Multicast Address Assignments* – R. Hinden & S.Deering – Juillet 1998 – Statut : Informational.

[RFC2450] *Proposed TLA and NLA Assignment Rule* – R. Hinden – Décembre 1998 – Statut : Informational.

[IETFPRIV] *Privacy Extensions for Stateless Address Autoconfiguration in IPv6* – T. Narten & R. Draves – Octobre 1999 – Work In Progress – draft-ietf-ipngwg-addrconf-privacy-01.txt.

[IETFDNS] *DNS Extensions to Support IPv6 Address Aggregation and Renumbering* – M. Crawford & C. Huitema & S. Thomson – Novembre 1999 – Work In Progress – draft-ietf-ipngwg-dns-lookups-06.txt.

[ARINASS] *Provisional IPv6 Assignment And Allocation Policy Document* – ARIN, APNIC, RIPE NCC – May 1999 – http://www.arin.net/regserv/ipv6/IPv6.txt.

10.4 ICMPv6

[OREIL99] *IPv6 Théorie et pratique* – Gisèle Cizault – Edition O'Reilly – Juin 1999.

[RFC2463] *Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6)* – A. Conta & S. Deering – Décembre 1998 – Statut : Draft Standard.

[IETFICMPNA] *IPv6 Node Information Queries* – M. Crawford – Octobre 1999 – Work In Progress - draft-ietf-ipngwg-icmp-name-lookups-05.txt.

[IETFICMPRO] *Router Renumbering for IPv6* – M. Crawford – Juin 1999 – Work In Progress - draft-ietf-ipngwg-icmp-router-renum-09.txt.

10.5 Configuration automatique

[OREIL99] *IPv6 Théorie et pratique* – Gisèle Cizault – Edition O'Reilly – Juin 1999.

[RFC2461] *Neighbor Discovery for IP Version 6 (IPv6)* – T. Narten & E. Nordmark & W. Simpson – Décembre 1998 – Statut : Draft Standard.

10.6 Sécurité

[OREIL99] *IPv6 Théorie et pratique* – Gisèle Cizault – Edition O'Reilly – Juin 1999.

[RFC2401] *Security Architecture for the Internet Protocols* – S. Kent & R. Atkinson – Novembre 1998 – Statut : Proposed Standard.

[RFC2402] *IP Authentification Header* – S. Kent & R. Atkinson – Novembre 1998 – Statut : Proposed Standard.

[RFC2406] *IP Encapsulating Security Payload (ESP)* – S. Kent & R. Atkinson – Novembre 1998 – Statut : Proposed Standard.

[RFC2409] *The Internet Key Exchange (IKE)* – D. Harkins & D. Carrel – Novembre 1998 – Statut : Proposed Standard.

[VEILLEHSC] *Veille IPSec* - Ghislaine Labouret (Hervé Schauer Consultants) – Avril/Juin 1999 – http://www.hsc.fr/ressources/veille/ipsec/index.html.fr.

10.7 Mobilité

[OREIL99] *IPv6 Théorie et pratique* – Gisèle Cizault – Edition O'Reilly – Juin 1999.

[RFC2002] *IP Mobility Support* – C. Perkins – Octobre 1996 – Statut : Proposed Standard.

[RFC2526] *Reserved IPv6 Subnet Anycast Addresses* – D. Johnson & S. Deering – Mars 1999 – Statut : Proposed Standard.

[IETFMOB] *Mobility Support in IPv6* – D. Johnson & C. Perkins – Octobre 1999 – Work in Progress – draft-ietf-mobileip-ipv6-09.txt.

10.8 Qualité de Service

[RFC2474] *Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers* – K. Nichols & S. Blake & F. Baker & D. Black – Decembre 1998 – Statut : Proposed Standard.

[RFC2475] *An Architecture for Differentiated Service* – S. Blake & D. Black & M. Carlson & E. Davies & Z. Wang & W. Weiss – December 1998 – Statut : Informational.

[RFC2597] *Assured Forwarding PHB Group* – J. Heinanen & F. Baker & W. Weiss & J. Wroclawski – Juin 1999 – Statut : Standards Track.

[RFC2598] *An Expedited Forwarding PHB* – V. Jacobson & K. Nichols & K Poduri – Juin 1999 – Statut : Standards Track.

[CISCOQOS] *Formation Technologique QoS* – Clarence Filsfils (Cisco Systems) – 1999.

[IETFDS] *A Framework for Differentiated Services* – Y. Berner & J. Blinder & S. Blake & M. Carlson & B. E. Carpenter & S Keshay&E. Daies & B. Ohlman & D. Verma & Z. Wang & W. Weiss – Février 1999 – Work in Progress – draft-ietf-diffserv-framework-02.txt.

11 Annexe 2 : Services de sécurité

• La confidentialité des données

La confidentialité des données consiste à chiffrer les données pour qu'elles ne soient pas compréhensibles par une machine ne connaissant pas les clés de chiffrement.

• La confidentialité du flux de donnée

La confidentialité du flux de donnée garantit qu'aucune information portant sur une communication (quantité d'information échangée, fréquence, identité des machines, etc…) ne peut être déduite par analyse de trafic.

• L'authentification de l'origine des données

L'authentification de l'origine des données permet de garantir que les données proviennent bien de la bonne machine.

• L'authentification mutuelle

L'authentification mutuelle permet à deux entités de se prouver mutuellement leur identité.

• L'intégrité des données

L'intégrité des données permet de garantir que les données reçues n'ont pas été modifiées pendant leur parcours sur le réseau.

• La prévention contre le rejeu des données

La prévention contre le rejeu des données permet de garantir que les données reçues n'ont pas été déjà envoyées.

• La non répudiation des données

La non répudiation des données permet de prouver, en cas de litige, que les données ont bien été émises ou reçues par les entités.