MEMOIRE
IPV6
3CMR7

Référence MEMOIRE/3CMR7

Objet de ce document

Ce document presente les Caractéristiques générales du protocoles IPV6.

Date de création :	fevirer 28, 2001
Dernière modification :	mars 23, 2002
Groupe:	3CMR7
Auteurs:	Thomas GUENNEGUEZ
	Pierre JOFFRE
	Arnaud TANGUY

Table des matières

Chapitre 1 INTRODUCTION

Chapitre 2 L'adressage

2.1 Type des adresses IPv6 2–1
2.2 Représentation des adresses et des préfixes 2–1
2.3 Format des adresses 2–2
2.3.1 Allocation des adresses 2–2
2.3.2 Adresses unicast 2–3
2.3.2.1 Identificateur d'interface 2–3
2.3.2.2 Adresses à plan d'adressage agrégé 2–3
2.3.2.2.1 Identifiant d'unité d'agrégation haute 2–4
2.3.2.2.2 Identifiant d'unité d'agrégation basse 2–5
2.3.2.2.3 Identifiant d'agrégation de site 2–5
2.3.2.2.4 Identificateur d'interface 2–6
2.3.2.3 Adresses NSAP 2–6
2.3.2.4 Adresses IPX 2–6
2.3.2.5 Adresses à usage local 2–6
2.3.2.5.1 Adresses lien-local (link-local addresses) 2–6
2.3.2.5.2 Adresses site-local 2–6
2.3.2.6 Adresses supportant les extensions IPv4 2–7
2.3.2.6.1 Adresses IPv6 compatibles IPv4 2–7
2.3.2.6.2 IPv4 mappées 2–7
2.3.2.7 Adresses particulières d'unicast 2–7
2.3.2.7.1 Adresses indéterminées ou non-spécifiées (unspecified address) 2–7
2.3.2.7.2 Adresse de bouclage (Loopback address) 2–7
2.3.3 Adresses multicast 2–8
2.3.4 Adresse anycast 2–8

Chapitre 3 Format des en-têtes IPv6

3.1 Les champs de l'en-tête 3–1
3.1.1 Identificateur de flux (Flow labels) 3–2
3.2 Extension en-têtes 3–2
3.2.1 Ordre des extensions 3–2
3.2.2 Options 3–3
3.2.2.1 En-tête Proche-en-Proche (Hop by hop) 3–3
3.2.2.2 En-tête d'option de destination 3–3
3.2.2.3 En-tête de Routage 3–3
3.2.3 En-tête de fragmentation (Fragment) 3–4
3.2.3.1 MTU 3–4

Chapitre 4 Automatisation de la configuration sous IPv6

4.1 ICMPv6 4–1
4.2 Le protocole de découverte des voisins (Neighbor Discovery Protocol, NDP) 4–1
4.2.1 Détection d'inaccessibilité des voisins (Neighbor Unreachability Detection, NUD) 4–2
4.2.2 Détection des adresses dupliquées (Duplicate Address Detection, DAD) 4–2
4.2.3 Redirection 4–2
4.2.4 Types de paquets ICMPv6 utilisés par NDP 4–2
4.3 Autoconfiguration 4–2
4.3.1 Autoconfiguration à mémoire d'état 4–3
4.3.2 Autoconfiguration sans état 4–3
4.4 Mobilité 4–4

Chapitre 5 Sécurité du protocole IPv6

5.1 Confidentialité des données 5–1
5.2 Authentification et intégrité des données 5–2

Chapitre 6 CONCLUSION

Chapitre 7 Bibliographie

7.1 Les sites 7–1
7.2 Les livres 7–1
7.3 Les RFC 7–1
7.4 Les mailing listes 7–1

Glossaire

Index

Exemples

2–1 Adresse IPv6 2–1
2–2 Adresse IPv6 contenant des champs nuls 2–2
2–3 Préfixe IPv6 2–2
2–4 Combinaison adresse IPv6 avec préfixe 2–2

Tableaux

2–1 Allocation des préfixes 2–2
2–2 Portée des adresses 2–8

Chapitre 1
INTRODUCTION

La création du réseau actuel tel que nous le connaissons aujourd'hui a été basée sur le protocole TCP/IP.

Le protocole IPv4 est un protocole de niveau 3 dans les couches ISO, il sert à l'acheminement des données. Il permet d'identifier une interface connectée à un réseaux par l'attribution d'une adresse unique.

Hors, du fait de la croissance exponentielle de l'Internet (il double de taille tous les 18 mois), les adresses codées sur 32 bits viennent à s'épuiser.

A cela s'ajoutent quelques propriétés qui font défaut au protocole IPv4 : il ne prend pas en compte de notions de sécurité telles que l'authentification et le chiffrement, de plus, ce système d'attribution des adresses a tendances à générer des tables de routage gigantesques, enfin ce protocole n'est plus adapté face aux nouveaux besoins qui naissent sur l'Internet comme la qualité de service sur des communications à haut-débit, ou la mobilité des équipements.

Des améliorations ont été developpées pour faire face à ces carences mais la mise en oeuvre de ces patchs hétéroclites peut poser des problèmes de compatibilité. La nouvelle version d'IP : IPv6 (ancien IP nouvelle génération), a été mis au point afin de corriger tous les défauts de IPv4 de façon native et de simplifier le protocole.

Nous allons détailler les caractéristiques techniques d'IPv6 et voir dans quelles mesures cette norme va résoudre bon nombre des problèmes précedemment abordés.

La première partie de cet exposé traitera de l'adressage en IPv6, de quelle facon est distribué l'impressionnant nombre d'adresses disponibles, puis il sera question de l'architecture des en-têtes des paquets IPv6, enfin seront abordées deux grandes nouvautés du protocole IPv6 que sont la mise en place d'une politique de sécurisation des communications et la simplification de configuration des équipements se connectant à un réseau.

Chapitre 2

L’adressage

Comme nous allons le voir dans ce chapitre, IPv6 répond aux deux problèmes majeurs pour l’Internet que sont la saturation du nombre d’adresses et l’explosion de la taille des tables de routage Glossaire des routeurs.

2.1 Type des adresses IPv6

Les adresses IPv6 sont codées sur 128 bits et permettent d’identifier des interfaces Glossaire ou des jeux d’interfaces sur les réseaux.

Elles peuvent être de trois types différents :

Le type unicast Glossaire fait correspondre à une adresse une interface unique. Dans ce cas tout paquet envoyé à cette adresse sera délivré à cette interface.

Le type multicast Glossaire fait correspondre à une adresse un groupe d’interfaces qui peuvent appartenir à différents équipements. Tout paquet émis vers une adresse multicast sera transmis à toutes les interfaces du groupe et cela n’importe où sur l’Internet.

Enfin, l’innovation d’IPv6 en matière de type d’adresse est l’adresse de type anycast Glossaire. Comme dans le cas du multicast une adresse anycast correspond à un jeu d’interfaces mais lorsqu’un paquet Glossaire est émis vers cette adresse, il est alors redirigé vers l’interface appartenant au groupe le plus proche (au moyen du protocole de mesure de distance).

Il est à noter qu’il n’existe pas dans le protocole IPv6 d’adresses de type broadcast Glossaire. Les adresses de ce type ralentissent les réseaux en occupant de la bande passante Glossaire par l’envoi de paquets à tous et agrandissent les tables de routage.

La fonction multicast Glossaire permet de remplacer plus efficacement le broadcast.

2.2 Représentation des adresses et des préfixes

Une adresse IPv6 est codée par un mot de 128 bits Glossaire. Elle peut être représentée par l’une des trois formes suivantes :
Chaque mot est découpé en un ensemble de 8 mots Glossaire (sous forme hexadécimale Glossaire). de 16 bits séparés par " : "

Exemple 2–1: Adresse IPv6

FEDC:BA98:7654:3210:FEDC:BA98:7654:3210

En raison de certaines méthodes d’allocation des adresses IPv6, il ne sera pas peu fréquent pour de nombreuses adresses de contenir plusieurs champs nuls.

Aussi, par soucis de simplification il est possible de réduire l’écriture de l’adresse dans le cas ou elle possède plusieurs champs nuls d’affilée par " : ".

Exemple 2–2: Adresse IPv6 contenant des champs nuls

L'adresse 1080:0:0:0:8:800:200C:417A deviendra 1080::8:800:200C:417A

Cette abréviation " :: " ne peut être contenue qu'une fois dans chaque adresse.

La représentation des préfixes est similaire à la notation des préfixes des adresses IPv4 sous CIDR Glossaire.

Elle est de la forme : adresse IPv6 / longueur du préfixe où " adresse IP " est représenté sous la forme vue précédemment et " longueur du préfixe " spécifie le nombre de bits contigus à partir de la gauche de l'adresse formant le préfixe.

Exemple 2–3: Préfixe IPv6

L'adresse 12AB:0000:0000:CD30:0000:0000:0000:0000/60 deviendra 12AB:0:0:CD30::/60

Enfin on peut combiner une adresse et son préfixe réseau en une seule représentation :

Exemple 2–4: Combinaison adresse IPv6 avec préfixe

12AB:0:0:CD30:C543:0300:02A0:801A et 12AB:0:0:CD30::/60 peuvent être liés en : 12AB:0000:0000:CD30:C543:0300

2.3 Format des adresses

2.3.1 Allocation des adresses

En tête de chaque adresse IPv6 se trouve une série de bits Glossaire, qui compose le préfixe et qui permet d'identifier le type de l'adresses.

L'allocation actuelle des adresses IPv6 selon le préfixe se compose de la manière suivante :

Tableau 2–1: Allocation des préfixes

Allocation	Préfixe (binaire)	Préfixe (hexa)	Fraction de l'espace d'adresse
Réservées	0000 0000		1/256
Réservées pour l'allocation NSAP	0000 001		1/128
Réservées pour l'allocation IPX	0000 010		1/128
Adresses à plan d'adressage agrégé	001		1/8
Adresses unicast lien-local	1111 1110 10	FE80	1/1024
Adresses unicast Site-local	1111 1110 11	FEC0	1/1024
Adresses multicast	1111 1111		1/256

Les adresses dont les préfixes (en binaire) sont 010, 011, 100, 101, 110, 1110, 1111 0, 1111 10, 1111 110, 1111 1110 0 ne sont pas allouées pour le moment. Elles sont destinées soit à une expansion du nombre d'adresses d'un groupe (adresses NSAP Glossaire par exemple) soit à la création de nouveaux modes d'utilisation. Initialement 15% des adresses ont été allouées, le reste des adresses (soit 85%) forme une réserve qui sera utilisée dans le futur.

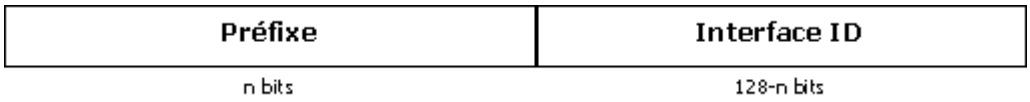
Pour avoir un identifiant d'interface de 64 bits il faut utiliser les préfixes de 001 à 111 (mis à part le préfixe multicast 1111 1111)

La distinction des adresses multicast et unicast se fait sur le premier octet de l'adresse. Si cette valeur est égale à FF en hexadécimal Glossaire, alors, il s'agit d'une adresse multicast, et toute autre adresse identifie une adresse unicast. Il est à noter que les adresses anycast sont extraites des adresses unicast et donc ne sont pas distinguables syntaxiquement de celles-ci.

2.3.2 Adresses unicast

L'architecture des adresses unicast de IPv6 est basée sur l'agrégation Glossaire de la même façon que le CIDR Glossaire.

Il existe actuellement 6 formes d'adresses unicast qui sont : les adresses unicast à plan d'adressage agrégé que nous aborderons dans une partie dédiée, l es adresses NSAP, les adresses IPX Glossaire, les adresses à usage local (adresses lien-local et site-local) et les adresses IPv6 compatibles avec IPv4. En complément de ces types d'adresses d'autres pourront être créés à l'avenir.



2.3.2.1 Identificateur d'interface

L'identificateur d'interface est utilisé pour identifier une interface sur un lien.

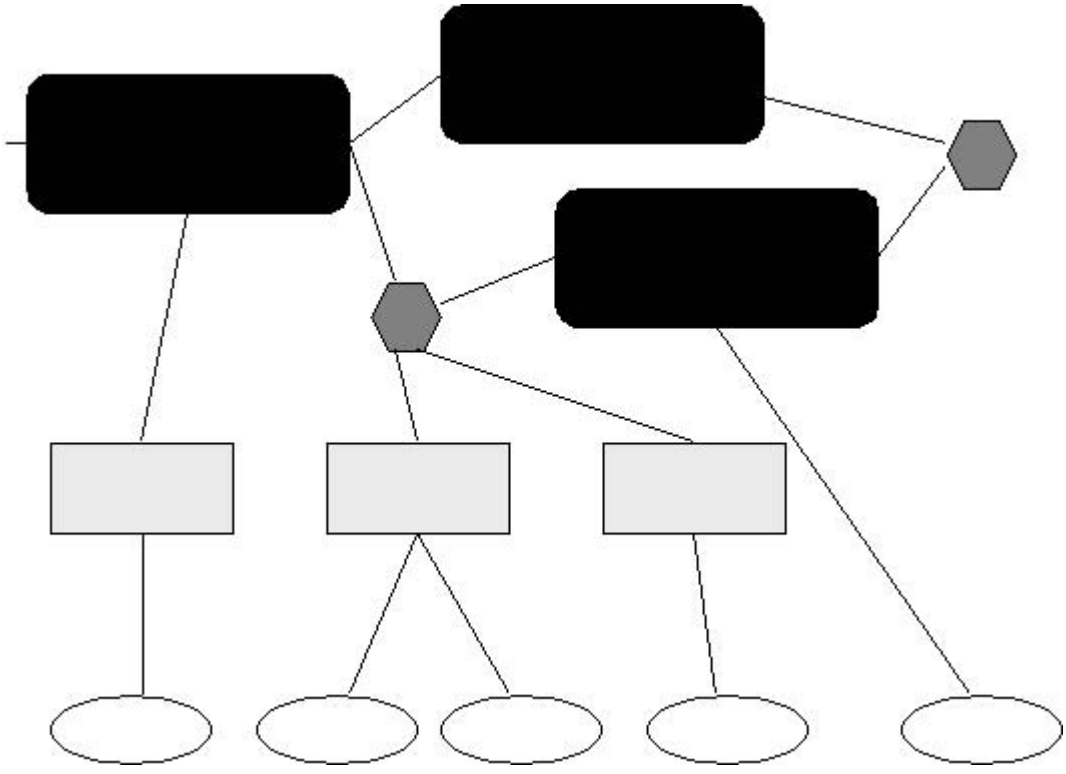
Il nécessite d'être unique sur ce lien, voire sur un groupe d'interface plus large. Cet identifiant a une portée locale lorsque qu'un signe d'unicité est disponible (adresse MAC Glossaire par exemple) sa mise en poeuvre a été normalisée p.

2.3.2.2 Adresses à plan d'adressage agrégé

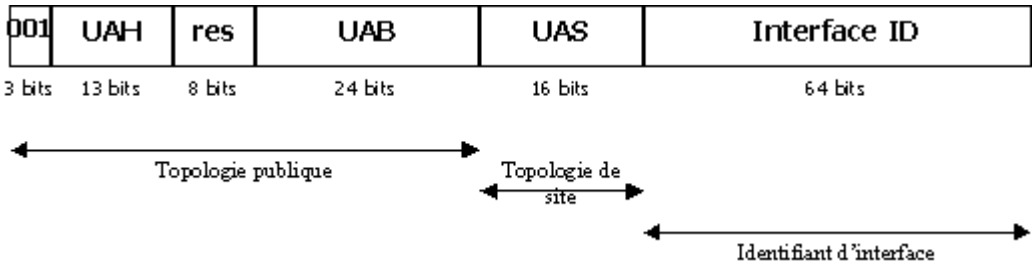
Le principe d'agrégation a été mis en place pour faciliter le routage et limiter la taille des tables de routage.

Sur la figure XXX sont représentés les niveaux d'architecture de l'Internet, d epuis les prestataires de haut niveau (ici en noir), les équipements d'interconnexions (gris), les prestataires de niveaux inférieurs (gris clair) et les abonnés.

Nous allons voir que, depuis les équipements de haut niveau jusqu'à l'abonné, la notion d'adresse par agrégation permet l'attribution naturelle d'adresse à chaque interface.



Le format des adresses à plan d'adressage agrégable est le suivant :



Le premier champ de 3 bits égal à "001" indique le type de l'adresse : adresse unicast à plan d'adressage agrégé.

Le champ UAH Glossaire correspond à l'identifiant d'unité d'agrégation haute (Top Level Aggregator).

Le champ res Glossaire est initialisé à 0. Il est prévu pour un usage futur.

Le champ UAB Glossaire est l'identifiant d'unité d'agrégation basse (Next Level Aggregator).

Enfin le champ UAS Glossaire est l'identifiant d'unité d'agrégation du site (Site Level Aggregator).

Les adresses à plan d'adressage agrégé sont organisées hiérarchiquement selon trois niveaux :

1. La topologie publique codée sur 48 bits.
2. La topologie de site sur 16 bits.
3. L'identifiant d'interface sur 64 bits.

La topologie publique dépend des différents fournisseurs d'accès et des différents prestataires de services de transit.

La topologie publique est formatée selon les champs suivants :

- le champ de préfixe "001" qui désigne une adresse de type unicast agrégée
- le champ res
- les champ UAH et UAB dont nous étudierons les découpages particuliers.

La topologie de site dépend de l'organisation interne de chaque site et est identifiée par le champ UAS.

2.3.2.2.1 Identifiant d'unité d'agrégation haute

Les identifiants d'unité d'agrégation haute(UAH ID) désignent la couche la plus haute de la hiérarchie des adresses IPv6. Ils sont distribués à des organisations ou des prestataires d'allocation de domaines de niveau mondial représentés en noir sur la figure XXX.

Les identifiants d'unité d'agrégation haute sont les premiers dans la hiérachie de routage. Les routeurs contiennent dans leur table de routage une entrée pour chaque UAH ID actif. Ils contiennent de plus des informations relatives au routage au sein de l'unité d'agrégation haute à laquelle ils appartiennent.

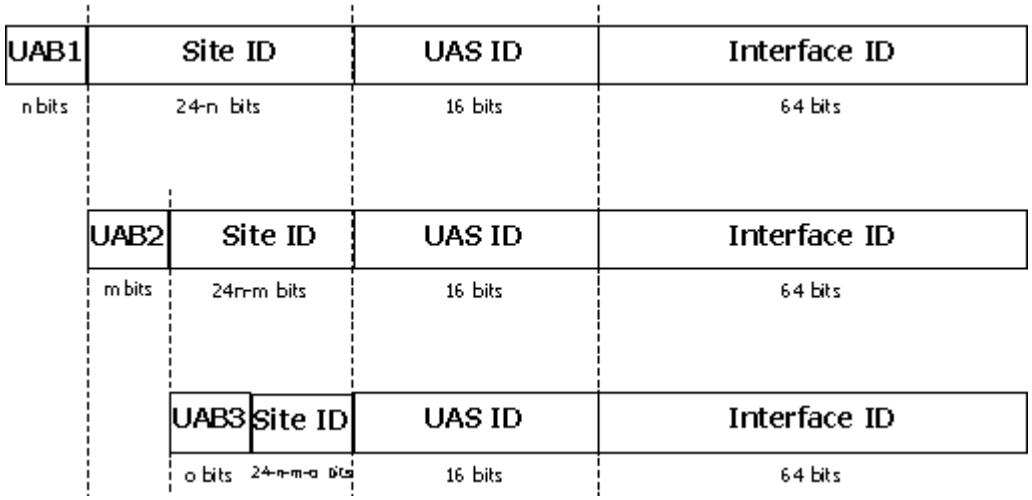
Les routeurs peuvent contenir d'autres informations relatives au routage de leur topologie, mais de façon à ne pas surcharger les tables de routage, il faut les minimiser quel que soit le niveau de topologie.

Pour l'instant 2^13 (8192) identifiants d'UAH sont en service.

2.3.2.2.2 Identifiant d'unité d'agrégation basse

Chaque prestataire en charge d'un identifiant d'unité d'agrégation haute détermine un découpage en différents sous-réseaux désignés par des identifiants d'unité d'agrégation basse (ID UAB). Chaque ID UAB est attribué à un prestataire, représenté en gris clair sur la figure XXX, qui peut de même allouer d'autres ID UAB dans le champ site ID lui " appartenant ".

Cela fonctionne selon le modèle suivant :



Le découpage ID UABn/site ID, où n, d'après la figure, représente le niveau de l'unité, dépend du prestataire de niveau n-1.

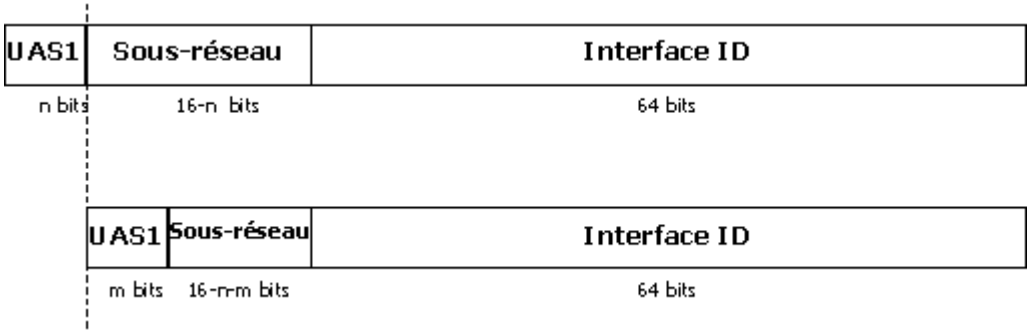
Le design du plan d'adressage UAB doit être un compromis entre une agrégation efficace et une certaine flexibilité.

La création d'une hiérachie augmente le nombre d'agrégations et réduit la taille des tables de routage.

Une unité d'agrégation basse sans hiérarchie permet une meilleure flexibilité dans l'attribution des adresses mais cause une augmentation de la taille des tables de routage.

2.3.2.2.3 Identifiant d'agrégation de site

L'identifiant d'agrégation de site (ID UAS) permet à une organisation individuelle de créer sur un site local sa propre hiérarchie de sous-réseaux.



On retrouve ici le principe des sous-réseaux IPv4, cependant il faut noter que le nombre de sous-réseaux pouvant être supportés par un ID UAS est de 65 535.

Tout comme pour les unités d'agrégation basse la création de un ou plusieurs sous-réseaux est à la discrétion de l'organisation qui possède cet identifiant d'UAS.

2.3.2.2.4 Identificateur d'interface

Dans le cas des adresses à plan d'adressage agrégé les identifiants d'interface doivent être codés sur 64 bits.

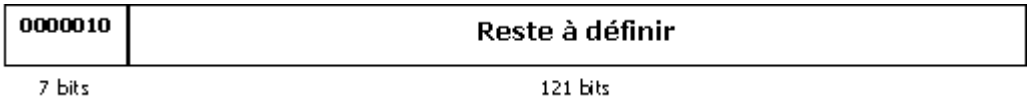
2.3.2.3 Adresses NSAP

NSAP est un système d'adresses hierarchique utilisé pour mettre en place un système d'adressage d'interconnexion. C'est le point logique entre la couche réseau et la couche transport. Le protocole IPv6 spécifie l'allocation d'adresses NSAP.

2.3.2.4 Adresses IPX

Le Protocole IPX est spécifique au logiciel d'exploitation de réseau Netware de Novell Glossaire. Il assure la transmission des paquets sur les réseaux Netware.

Les adresses IPX sont définis dans IPv6 selon l'architecture suivante :



Le préfixe composé de sept bits qui sont 0000010, le reste du contenu de l'adresse est en cours d'élaboration.

2.3.2.5 Adresses à usage local

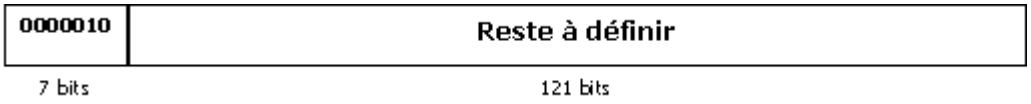
Il existe deux types d'adresses unicast à usage local, les adresses lien-local et les adresses site-local.

2.3.2.5.1 Adresses lien-local (link-local addresses)

Le concept d'adresse lien-local sert à connecter deux interfaces directement sans périphérique de routage, par exemple les deux extrémités d'une connexion effectuant un tunneling Glossaire ou bien une connexion PPP (Point-to-Point Protocol).

L'attribution des adresses aux interfaces s'effectue automatiquement à la connexion autour du lien.

Ces adresses sont de la forme :

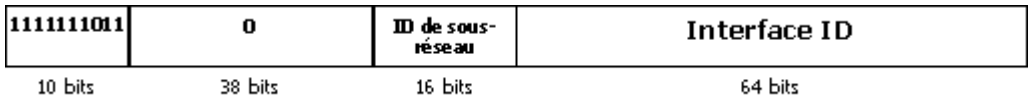


Le préfixe FE80::/64 est associé aux adresses lien local IPv6.

2.3.2.5.2 Adresses site-local

Les adresses de type site-local servent à identifier des interfaces sur un réseau à usage local uniquement et sans requérir l'usage d'un préfixe global.

La syntaxe des adresses de type site-local est la suivante :



Le préfixe FECO::/48 est associé à un champ de 16 bits permettant de définir différents sous-réseaux, et à l'identifiant de l'adresse codé sur 64 bits.

Tout équipement de routage ne doit pas pouvoir transmettre une adresse à usage local.

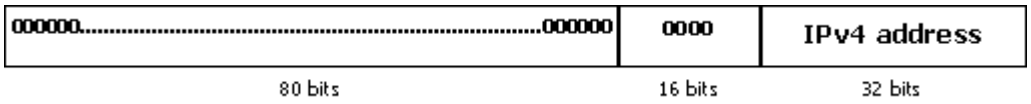
2.3.2.6 Adresses supportant les extensions IPv4

2.3.2.6.1 Adresses IPv6 compatibles IPv4

Le mécanisme de transition de IPv4 vers IPv6 nommé Simple Internet Transition (SIT) permet de faire circuler des paquets IPv6 au travers d'infrastructures de routage supportant IPv4 via un tunnel.

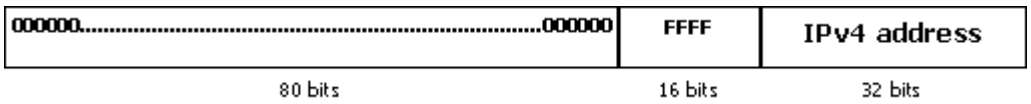
Les équipements IPv6 utilisent des adresses IPv6 qui contiennent une adresse IPv4 dans leurs 32 derniers bits.

La forme de cette adresse est la suivante :



2.3.2.6.2 IPv4 mappées

Il s'agit d'un second type d'adresses IPv6 compatible avec les adresses IPv4. Il désigne les adresses des équipements IPv4 (ne supportant pas IPv6), comme étant des adresses IPv6.
Elles possèdent le format suivant :



2.3.2.7 Adresses particulières d'unicast

2.3.2.7.1 Adresses indéterminées ou non-spécifiées (unspecified address)

L'adresse 0:0:0:0:0:0:0:0 ou :: en abrégé, nommée adresse non-spécifiée ("unspecified address") ne doit jamais être associée à un équipement. Elle est utilisée durant la phase d'attribution d'une adresse. L'hôte ne connaissant pas encore son adresse envoie cette adresse en tant qu'adresse source.

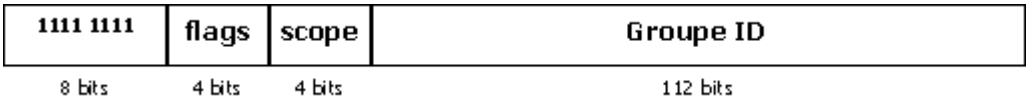
2.3.2.7.2 Adresse de bouclage (Loopback address)

L'adresse unicast 0:0:0:0:0:0:0:1 ou ::1 en abrégé est nommée adresse de bouclage (loopback adress) Elle permet à un équipement de s'adresser des paquets à lui-même (comme le fait l'adresse 127.0.0.1 en IPv4).

Elle peut être considérée dans le cas d'une connexion à une interface (localhost interface).

2.3.3 Adresses multicast

Une adresse de type multicast permet d'attribuer à un groupe d'interfaces un identifiant unique. Tout paquet envoyé à destination de cette adresse est transmis à toutes les interfaces du groupe. Une interface peut s'intégrer à un ou plusieurs groupes et en sortir à tout moment, un groupe existe tant qu'une interface en fait partie. Le format de ce type d'adresse est le suivant :



Le préfixe des adresses multicast est FF::/8 en hexadécimal.

Le champ flags Glossaire (drapeaux) est codé sur 4 bits. Les trois premiers sont initialisés à 0. Le quatrième bit différencie les adresses assignées de manière permanente (well-known addresses) et les adresses assignées de manière provisoire (transcient adresses).

- 0000 : adresse permanentes
- 0001 :adresses provisoires

Le champ scope Glossaire (portée), codé sur 4 bits, définit l'étendue d'un groupe multicast.

La normalisation actuelle des valeurs répartit les adresses multicast selon le tableau ci-dessous.

Tableau 2–2: Portée des adresses

Scope	Type d'adresse
0	Adresses réservées
1	Portée de niveau équipement (node-local)
2	Portée au niveau du lien (link-local)
5	Portée au niveau du site (site-local)
E	Portée de niveau global
F	Adresses réservées

La notion de portée permet de bien cloisonner les groupes multicast pour éviter des transmissions en dehors de zones non autorisées.

Enfin le groupe ID identifie un groupe multicast au sein d'un niveau de distribution

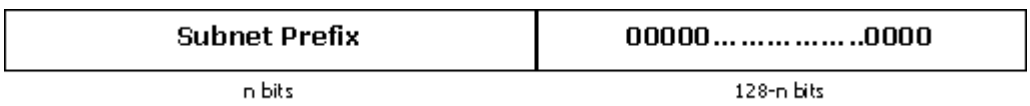
La validité des adresses multicast permanentes est indépendante du niveau de portée alors que les adresses multicast transitoires ne sont valables que dans leur niveau de portée.

2.3.4 Adresse anycast

Les adresses anycast tout comme les adresses multicast identifient plusieurs interfaces.

Lors de l'envoi d'un paquet à destination, il est dirigé vers l'interface la plus proche.

Actuellement seule l'adresse de "subnet prefix" Glossaire est définie. Elle est formalisée de la façon suivante :



Cette adresse est syntaxiquement la même qu'une adresse unicast dont l'identifiant d'interface serait mis à 0000.

Tout paquet émis en direction du sous-réseau (subnet) identifié par le " subnet prefix " sera délivré à un routeur de ce sous-réseau. Tous les routeurs doivent pouvoir supporter un préfixe de sous-réseau correspondant à un sous-réseau qui contient au moins une de ses interfaces identifiées par ce préfixe.

Les adresses anycast de routeur de sous-réseau sont utilisées pour des applications pour lesquelles un équipement d'un réseau cherche à communiquer avec un ou plusieurs groupes de routeurs d'un sous-réseau distant. A titre d'exemple, on peut citer le cas d'un hôte mobile qui a besoin de communiquer avec un des agents mobiles de son propre sous-réseau.

Chapitre 3

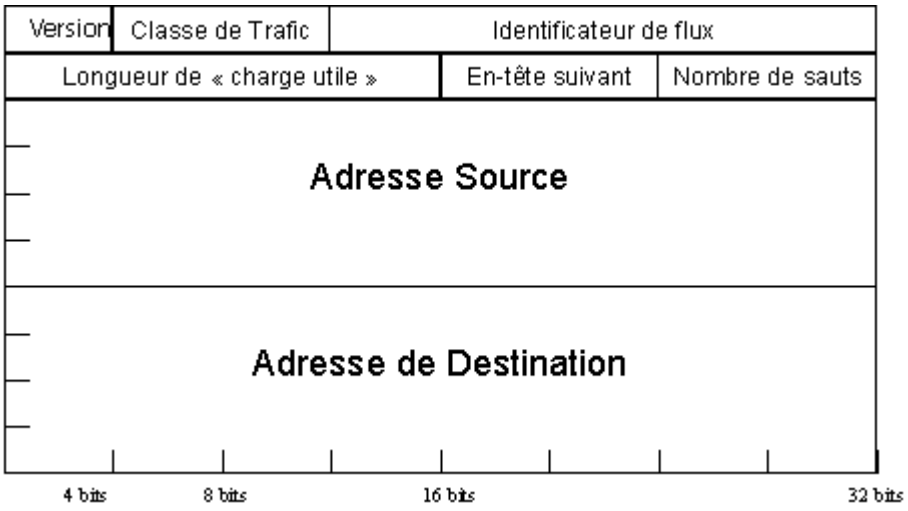
Format des en-têtes IPv6

Le format des en-têtes IPv6 a été élaboré en profitant de l'expérience tirée de IPv4. Il a été simplifié passant de 14 champs à 8 champs ce qui facilite le traitement des routeurs intermédiaires et donc accélère le transit des paquets sur les réseaux.

Il possède une taille fixe.

3.1 Les champs de l'en-tête

Le format des en-têtes est le suivant :



Les différents champs de l'en-tête sont explicités ci-dessous :

- Le champ "version" (codé sur 4 bit) est le numéro de version du protocole pour IPv6 ; il est donc égal à 6 ou 0110 en binaire.
- Le champ " Classe de Trafic " (Traffic class - 8 bits) pourra à l'avenir contenir une variable de priorité ou de classe de paquet.
- Identificateur de flux (Flow Label - 20 bits) désigne une méthode de traitement pour certains paquets utilisés par des applications particulières (communication temps réel par exemple).
- Longueur de " charge utile Glossaire " (Payload length -16 bits) désigne la longueur du reste du paquet qui suit cet en-tête.
- En-tête suivant (Next Header - 8 bits) désigne l'en-tête suivant immédiatement (protocole de niveau supérieur ou extension).
- Nombre de sauts (Hop Limit - 8 bits) est un nombre entier décrémenté de 1 à chaque traversée de routeur par le paquet. Le paquet est détruit dès que ce nombre devient égal à 0. Etant codé sur 8 bits un paquet IPv6 ne peut traverser qu'au maximum 255 routeurs.
- Adresse Source (Source Address - 128 bits) contient l'adresse de l'émetteur du paquet.

- Adresse de Destination (Source destination - 128 bits) contient l'adresse du destinataire. Cette adresse peut ne pas être le destinataire final si un en-tête de routage est présent.

Le champ " checksum Glossaire" d'IPv4 n'existe plus, la vérification du trafic se fait maintenant au niveau du protocole supérieur.

3.1.1 Identificateur de flux (Flow labels)

Il est intéressant de se pencher sur l'utilisation du champ " identificateur de flux " car il est très représentatif de l'orientation d'IPv6 en terme de qualité de service Glossaire. En effet ce champ permet de demander aux routeurs un traitement spécial du flux de paquet qui les traverse. Ce traitement peut être adopté pour des raisons de qualité de service ou bien pour des contraintes de flux temps réel.

Les hôtes et routeurs ne supportant pas le " Flow label " initialise le champ à 0 lorsqu'il sont les émetteurs du paquet, le transmettent sans le modifier en cas de transfert et l'ignorent lorsqu'ils en sont destinataires.

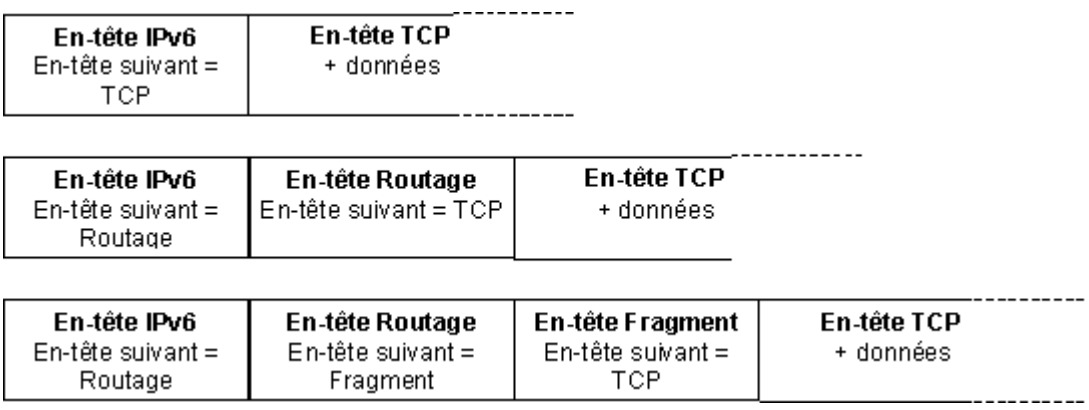
3.2 Extension en-têtes

Les extensions d'en-tête IPv6 sont codées dans des en-têtes séparés placés entre l'en-tête IPv6 et les en-tête du protocole de niveau supérieur (TCP Glossaire, UDP Glossaire, ICMP Glossaire).

Les extensions se trouvent donc dans l'espace mesuré par le champ "longueur de charge utile".

La particularité de ces en-têtes est que chacun d'entre eux contient un champ "En-tête suivant" qui pointe sur l'en-tête suivant à parcourir.

La figure suivante donne un exemple de ce principe :



Les routeurs sur lesquels transitent les paquets ne tiennent pas compte des extensions hormis dans le cas de l'extension " Proche-en-Proche " (hope by hope). C'est seulement lorsque le paquet atteint l'équipement de destination que les extensions sont décodés. C'est pourquoi un ordre doit être respecté aussi bien au moment de l'encodage que du décodage.

3.2.1 Ordre des extensions

L'en-tête "Proche-en-Proche", du fait qu'il puisse être lu par des routeurs intermédiaires, doit se situer directement après l'en-tête. La présence ou non de ce type d'extension est indiquée dans l'en-tête IPv6 par l'initialisation à la valeur 0 du champ "En-tête suivant".

Une implémentation complète de IPv6 comprend tous ces en-têtes d'extensions placés dans cet ordre précis :

- En-tête IPv6
- En-tête d'option Proche-en-Proche (Hop-by-Hop)
- En-tête d'option de destination

- En-tête " Routage "
- En-tête Fragment Glossaire
- En-tête Authentification
- En-tête Chiffrement (Encapsulating Security Payload Glossaire)
- En-tête Destination Options
- En-tête du protocole de niveau supérieur

3.2.2 Options

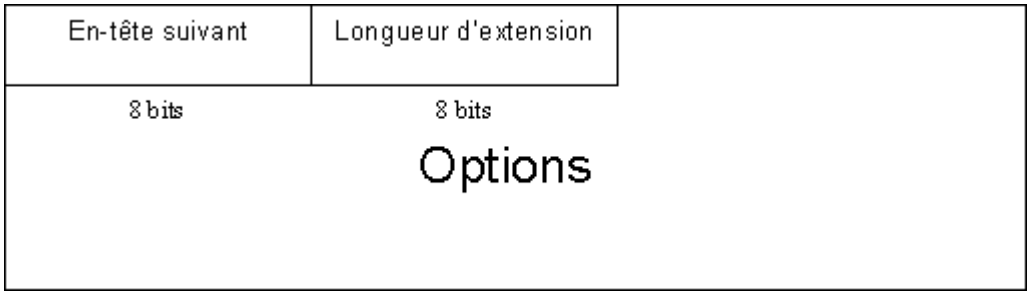
3.2.2.1 En-tête Proche-en-Proche (Hop by hop)

L'en-tête "Hop by Hop" est utilisé pour contenir des informations qui pourront être examinées par chaque équipement traversé par le paquet.

Cet en-tête est déclaré par la valeur "0" du champ "en-tête suivant" de l'en-tête IPv6.

Il se situe en première position après l'en-tête IPv6.

La figure ci-dessous montre le schéma de cet en-tête :



Le champ longueur d'extension contient un entier de 8 bits déterminant la longueur de l'en-tête moins les 8 premiers octets.

Le champ option contient des options à traiter par chaque équipement traversé.

3.2.2.2 En-tête d'option de destination

Cet en-tête possède le même format que l'en-tête "Proche-en-Proche".

Il contient des informations qui doivent être examinées par le destinataire des paquets.

Cet en-tête est déclaré par la valeur "60" du champ " en-tête suivant " de l'en-tête le précédant immédiatement.

Il y a deux manières d'encoder une option de destination, soit la contenir dans l'en-tête d'option de destination soit dans un deuxième en-tête d'extension.

Le choix entre ces deux stratégies dépend de l'action que désire effectuer l'équipement de destination du paquet.

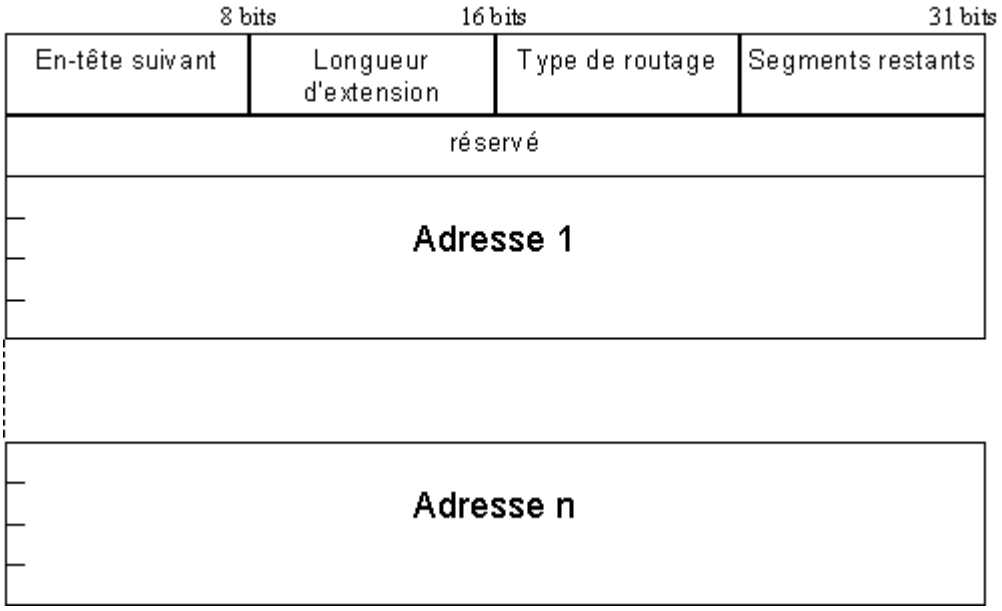
Options Bourrage Mobilité

3.2.2.3 En-tête de Routage

L'en-tête de Routage permet de lister un ou plusieurs routeurs à emprunter afin d'imposer une route pour atteindre la destination finale du paquet.

L'en-tête de routage est déclaré par la valeur "43" dans le champ "en-tête suivant" de l'en-tête le précédant immédiatement.

Il possède le format suivant :



Les champs "en-tête suivant" et "Longueur d'extension" sont les mêmes que dans le cas des en-têtes d'extensions précédents.

Le champ "Segments restants" contient un entier codé sur 8 bits qui détermine le nombre de segments qu'il reste à parcourir, c'est-à-dire le nombre d'équipements listés explicitement par lesquels le paquet doit passer avant d'atteindre la destination finale.

Or nous avons vu précédemment que seuls les en-têtes d'extensions de " Proche en Proche " étaient auscultés par les routeurs traversés.

3.2.3 En-tête de fragmentation (Fragment)

3.2.3.1 MTU

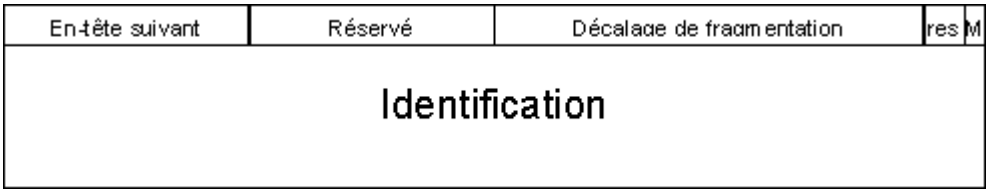
La MTU est l'unité de transmission maximum pouvant être transmise sur un lien. Dans le cas de IPv6 la MTU Glossaire (index) est la taille maximum d'un paquet IPv6 et sa valeur est 1280 octets.

On appelle "MTU path" Glossaire (index) la MTU minimum sur un trajet utilisant plusieurs tronçons de MTU propres différentes.

Pour pouvoir envoyer un paquet plus large que le " MTU path " à destination, il est nécessaire de le découper en tronçons pouvant respecter ce MTU path.

C'est le routeur Glossaire source qui décide et effectue la fragmentation pour un paquet contrairement à IPv4 où ce sont les routeurs intermédiaires qui le font.

L'en-tête de fragmentation utilisé dans ce cas est déclaré par la valeur "44" dans le champ "en-tête suivant" de l'en-tête le précédant immédiatement et possède le format suivant :



Le champ "décalage de fragmentation" est un entier de 13 bits représente le décalage des données après cet en-tête. Il est exprimé par le nombre de mots de 8 bits depuis le début de la partie fragmentable.

Le champ "réservé" est réservé pour un usage futur.

Dans le cas d'une fragmentation, le noeud Glossaire source est amené à diviser le paquet en fragments et à les envoyer en tant que paquets distincts.

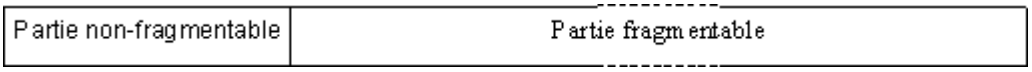
Afin que le destinataire puisse les réassembler, la source les identifie au moyen d'un entier de 32 bits contenu dans le champ "Identification".

Le paquet initial se compose d'une partie non-fragmentable et d'une partie fragmentable.

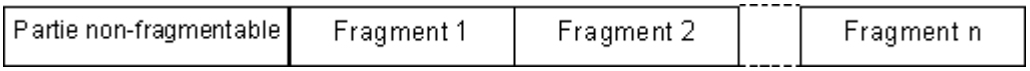
La partie non-fragmentable est constituée de l'en-tête IPv6 et tous les en-tête d'extensions pouvant être traités par les noeuds intermédiaires ("Routage" et "Proche-en-Proche") s'ils existent.

Le reste du paquet constitue la partie fragmentable.

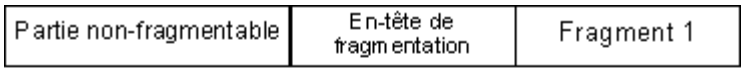
La fragmentation s'exécute selon le modèle suivant :

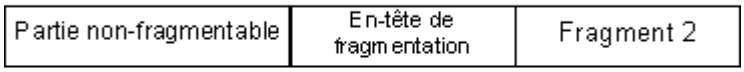


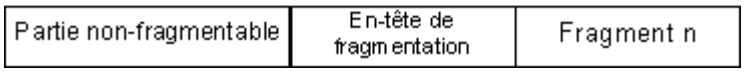
On définit des fragments dans la partie fragmentable.



La fragmentation donne ceci :







Chapitre 4

Automatisation de la configuration sous IPv6

IPv6 met aussi en oeuvre des fonctionnalités ayant pou but d'automatiser la configuration d'une nouvelle connexion à un réseau.

4.1 ICMPv6

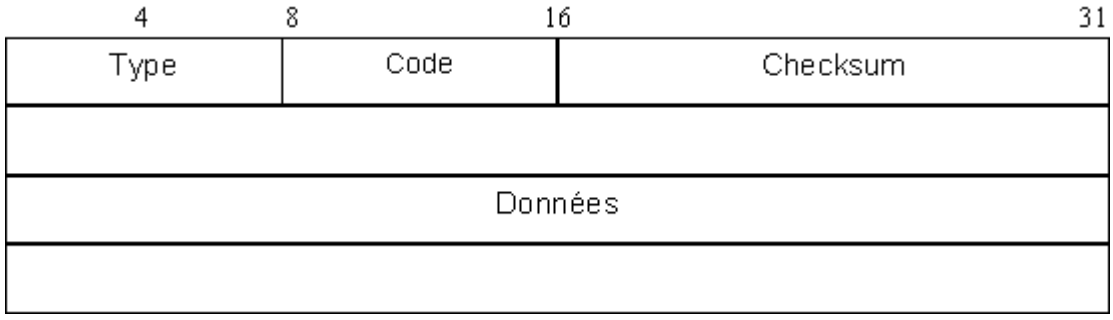
Le protocole ICMPv6 (Internet Control Message Protocol) est le protocole de contrôle de IPv6.

Il est utilisé par les équipements IPv6 afin de détecter les erreurs de traitement des paquets, d'effectuer des tests (pingGlossaire), et la découverte des voisins (NDPGlossaire).

ICMPv6 doit être supporté par tous les équipements IPv6.

Le protocole Multicast Listener Discovery (MLDGlossaire) intégré à ICMPv6 permet la gestion des groupes multicast. Le protocole contient des fonctionnalités qui remplacent le protocole ARP Glossaireutilisé avec ICMPv4.

Le format des paquets ICMPv6 est le suivant :



La nature du message ICMPv6 est contenue dans le champ. Elle est codée sous la forme d'un entier de 8 bits : les nombres inférieurs à 127 codent des messages d'erreur, les autres codent des messages d'information (utilité pour le protocole de découverte des voisins).

Le champ "code" identifie la cause d'envoi du paquet.

Dans le cas où l'on ait affaire à un message d'erreur, le compte-rendu ainsi que le paquet IPv6 erroné sont contenus dans le champ "données".

4.2 Le protocole de découverte des voisins (Neighbor Discovery Protocol, NDP)

Le protocole de découverte des voisins est utilisé par des équipements IPv6 partageant le même lien pour se découvrir mutuellement, déterminer les adresses de niveau 2 des voisins (ancien ARP), déterminer l'accessibilité ou la non-accessibilité des voisins(NUD Glossaire) et localiser les routeurs Glossaire.

Il permet donc à un équipement de s'intégrer sur un lien en ne découvrant que ses interlocuteurs directs.

Le protocole NDP est appelé protocole " plug and play " du fait des fonctionnalités de connexion qui automatisent la configuration d'un équipement.

Il intègre par défaut la fonction de découverte des routeurs qui détermine les routeurs présent sur le lien et la fonction de découverte des préfixes qui apprend à l'équipement les préfixes du réseau et lui permet ainsi d'extrapoler sa propre adresse IPv6 en y associant son identificateur d'interface.

4.2.1 Détection d'inaccessibilité des voisins (Neighbor Unreachability Detection, NUD)

Cette fonctionnalité permet à un équipement de tester les adresses de ses voisins sur le lien et, le cas échéant, d'effacer du cache les adresses non-valides. Il permet de déterminer, en cas de disparition d'un routeur, un nouveau chemin dans la table de routage.

4.2.2 Détection des adresses dupliquées (Duplicate Address Detection, DAD)

La génération automatique d'adresse risquant d'attribuer une même adresse à plusieurs équipements, la DAD permet de vérifier l'unicité de l'adresse d'un équipement.

4.2.3 Redirection

La fonction de redirection (index) est utilisée par un routeur pour déterminer une route meilleure en nombre de sauts que celle définie dans les tables de routage.

4.2.4 Types de paquets ICMPv6 utilisés par NDP

Le protocole NDP utilise cinq types de messages ICMP :

- **Router Advertisement** (RA Glossaire) : il s'agit d'une émission de confirmation de la présence d'un routeur. Il se compose de la liste des préfixes utilisés sur le lien local, le nombre de sauts maximum (Max Hop Limit) et la valeur du MTU.
- **Router Solicitation** (RS Glossaire) : il s'agit d'une requête d'un équipement pour recevoir un RA.
- **Neighbor Solicitation** (NS Glossaire) : Une sollicitation de voisinage est demandée pour obtenir l'adresse de niveau 2 d'un voisin sur le lien, déterminer son accessibilité, il demande en réponse un NA.
- **Neighbor Advertisement**(NA Glossaire): message émis en réponse à un NS ou pour signifier un changement d'adresse.
- **Redirect** : indique le meilleur chemin. Redirect est utilisé dans la fonction de redirection.

4.3 Autoconfiguration

La configuration de l'interface d'une machine sous IPv4 est une tâche longue à effectuer puisque manuelle. Le protocole IPv6 permet d'automatiser cette configuration (configuration " plug and paly "). L'autoconfiguration signifie qu'automatiquement soient mis à disposition de la machine les paramètres à la création d'une adresse sur un réseau, le but étant que n'importe quel utilisateur, quelles que soient ses connaissances en réseau, puisse brancher une machine sur un réseau local et y accéder de manière automatique.

Le déroulement du processus d'autoconfiguration comporte la création d'une adresse de type lien-local, la vérification de l'unicité de cette adresse sur le réseau, la détermination de son adresse unicast globale.

Deux méthodes d'autoconfiguration sont possibles avec IPv6 : l'autoconfiguration à mémoire d'état et l'autoconfiguration sans état.

La première étape est commune aux deux méthodes : il s'agit de la création de l'adresse lien-local et de la vérification de son unicité.

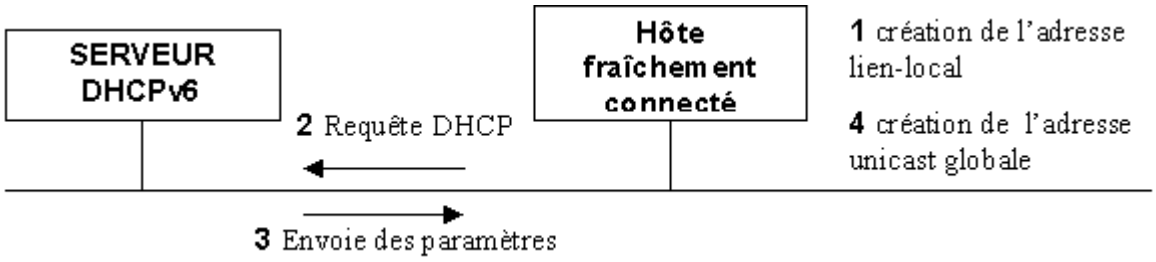
Lors de l'initialisation de l'interface la machine détermine un identificateur d'interface qui doit nécessairement être unique sur le lien. Pour des raisons de respect de la vie privée l'idée d'utiliser l'adresse MAC a été annulée et remplacée par l'emploi du format d'identificateur EUI-64.

Munie de cet identificateur, la machine crée son adresse lien local en le concaténant avec le préfixe FE80 ::/64. Au moyen de la fonction DAD du protocole NDP, on vérifie l'unicité de l'adresse. Dans le cas où l'adresse lien-local créée n'est pas unique, le processus se bloque et il est nécessaire de configurer manuellement la connexion. Dans le cas où l'adresse est unique, elle est validée et peut être utilisée sur le réseau.

4.3.1 Autoconfiguration à mémoire d'état

L'autoconfiguration à mémoire d'état est mise en place dans le cadre d'une gestion centralisée de l'attribution des adresses d'un réseau.
Elle permet à une machine qui se connecte à un réseau d'obtenir les paramètres de connexions par un serveur. Toutes les transactions de configuration sont donc basées sur le modèle client-serveur. Le protocole utilisé pour les échanges est le protocole DHCPv6 (Dynamic Host Configuration Protocol).

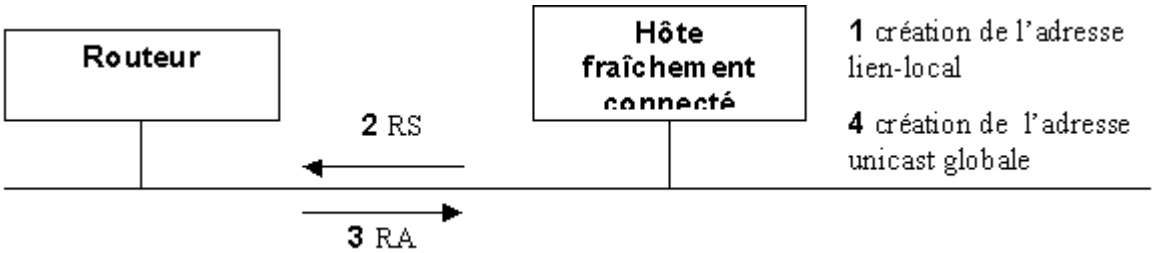
Le client envoie des requêtes au serveur DHCPv6 Glossaire lui communiquant son adresse lien-local. Le serveur lui communique en réponse une adresse unicast ainsi que les différents paramètres du réseau (MTU, nombre de sauts maximum)



4.3.2 Autoconfiguration sans état

L'autoconfiguration sans état est utilisée lorsqu'un réseau n'impose pas de contrôle particulier sur l'attribution des adresses. Ainsi chaque machine du site doit elle-même créer sa propre adresse unicast globale.

Cette autoconfiguration ne nécessite pas de serveur, la machine se construisant elle-même sa propre adresse. Elle se base sur le protocole ICMPv6. L'équipement qui se connecte va émettre une requête RS en direction d'un routeur. Le routeur lui renvoie les préfixes et les paramètres du réseau. En combinant le préfixe et son identifiant d'interface l'équipement détermine son adresse. Il peut ensuite vérifier l'unicité de son adresse au moyen de la fonctionnalité DAD du protocole NDP.



4.4 Mobilité

L'accroissement de la taille de l'Internet s'accompagne d'un grand besoin de simplification de la configuration des machines mobiles. De plus en plus de terminaux mobile (téléphonie cellulaire, ordinateur portables) vont nécessiter de pouvoir se connecter à un réseau de s'authentifier facilement en gardant une adresse unique.

MIP Glossaire (Mobile Internet Protocole) a été mis en uvre dans ce sens. Il permet à une machine mobile de se connecter en dehors de son réseau mère et d'être toujours joignable avec son adresse mère.

Considérons le réseau mère du mobile, auquel appartient le "Host Agent" (HA), et le réseau distant sur lequel est branché le poste mobile et auquel appartient un "Mobility Agent" (MA).

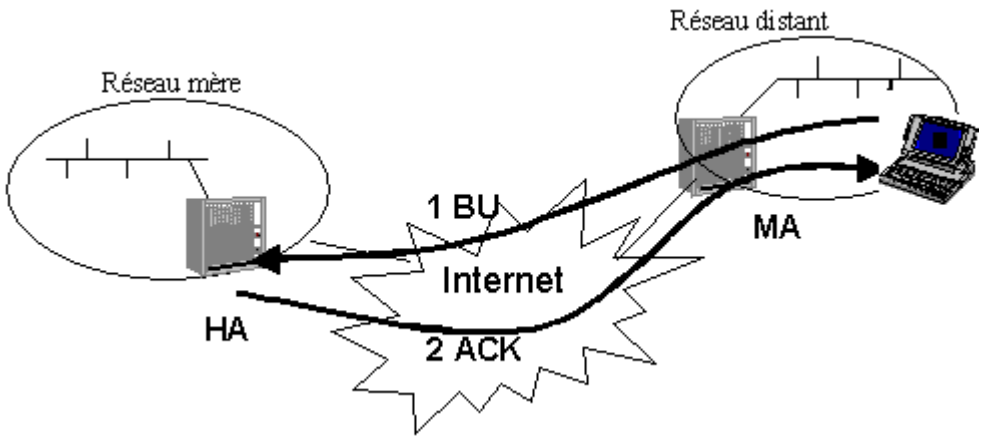
Le Host Agent a pour rôle de faire la correspondance entre une adresse mère (appartenant au réseau mère) et l'adresse actuelle du poste mobile.

Le Mobility Agent attend, lui, des connexions d'hôtes mobiles sur son réseau et se charge de rapatrier son adresse temporaire au MA.

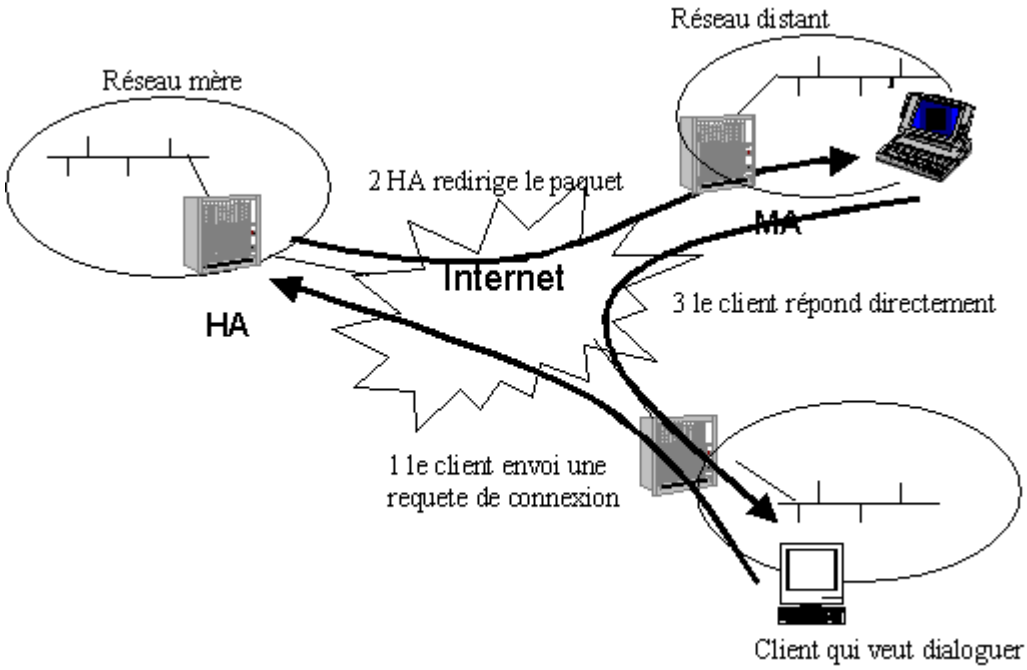
Le poste mobile en se connectant va tout d'abord se créer une adresse IPv6 en concaténant son identificateur d'interface avec le préfixe qui lui aura été alloué soit par autoconfiguration avec soit par autoconfiguration.

A chaque déplacement, un mobile envoie une mise à jour de son adresse temporaire, le Binding Update (BU).

Il transmet une requête BU à son HA en passant par le MA du réseau sur lequel il se trouve afin de mettre à jour les tables de correspondances du HA. Le HA lui renvoie un ACK.



Dès cet instant, il sera identifié par son adresse unique. Lorsqu'un client veut communiquer avec lui, c'est le Home Agent qui se charge de transmettre les paquets vers l'adresse temporaire, la réponse étant envoyée directement du poste vers le client sans repasser par le Home Agent.


Réseau distant
Réseau mère
2 HA redirige le paquet
MA
Internet
3 le client répond directement
HA
1 le client envoi une
requete de connexion
Client qui veut dialoguer

Chapitre 5

Sécurité du protocole IPv6

Le protocole IPv6 intègre des fonctionnalités de sécurité.

Ces fonctionnalités sont optionnelles ; elles assurent l'authentification, l'intégrité et la confidentialité des données escortées. Elles peuvent être sélectionnées de manière individuelle mais dans le cadre d'une politique de sécurité cohérente, la confidentialité gérée par l'ESP Glossaire (Sécurité par chiffrement des données utiles), l'authentification et l'intégrité gérées par l'AH Glossaire (En-tête d'authentification) doivent être mises en oeuvre simultanément.

Toute connexion sécurisée en IPv6 fait appel à une association de sécurité (AS Glossaire). Il s'agit d'une structure de données définissant l'ensemble des paramètres de sécurité dans le cadre de cette connexion.

Chaque AS est identifiée à l'aide de l'adresse destination des paquets, de l'identifiant de l'en-tête de sécurité, et de l'index des paramètres de sécurité (SPI).

Il n'existe pas de protection contre l'analyse de trafic.

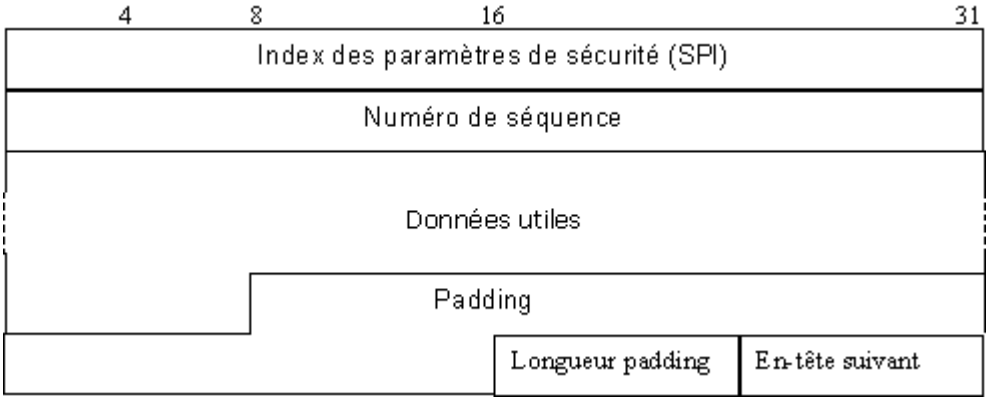
5.1 Confidentialité des données

La confidentialité des données est assurée par l'en-tête d'extension de " chiffrement des données utiles ", Encapsulating Security Payload header (ESP).

L'ESPGlossaire effectue un chiffrement du paquet et l'encapsule entre des en-têtes ESP. Comme tous les en-têtes d'extensions, l'ESP se situe entre l'en-tête le précédant (IPv6 ou extension) et le reste du paquet.

L'ESP assure la confidentialité en effectuant un chiffrement des données qu'IPv6 transporte.

L'en-tête ESP a le format suivant :



Le champ "SPI" contient une valeur codée sur 32 bits qui permet de définir le niveau de sécurité associé à l'association de sécurité.

Le champ de 32 bits intitulé "numéro de séquence" est un compteur initialisé à 0 en début d'AS par l'émetteur et mis à disposition du receveur pour valider les octets qui lui arrivent.

Les champs "padding" et "longueur padding" contiennent respectivement des instructions afin de remplir le champ données utiles afin qu'il puisse être chiffrable et la taille des instructions de remplissage.

Les données utiles contenues dans le paquet sont chiffrées.

La mise en oeuvre de l'ESP dans une connexion peut se dérouler selon deux méthodes, la méthode transport et la méthode tunnel.

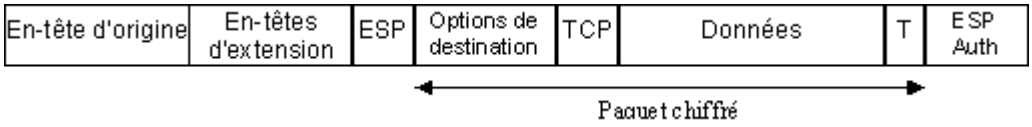
En premier lieu, considérons le paquet IPv6 englobant une trame TCP :

La méthode transport exécutée par l'ESP consiste en un chiffrage des données puis à l'ajout de l'extension ESP.

Dans le cas de cette méthode, l'en-tête ESP est placé entre l'en-tête IPv6 et l'en-tête de niveau supérieur.

Elle est utilisée entre deux équipements ne nécessitant pas la compréhension de l'ESP.

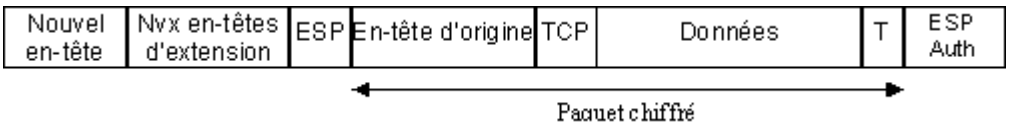
Le champ T contient les informations de padding et de contrôle ainsi que les informations concernant le protocole de niveau supérieur.



La méthode d'ESP par tunnelGlossaire s'applique dans le cas où l'ESP est implémenté sur des routeurs ou des infrastructures de transport. On peut effectuer un tunnelling du flux en encapsulant données et en-tête chiffrés entre de nouveaux en-têtes.

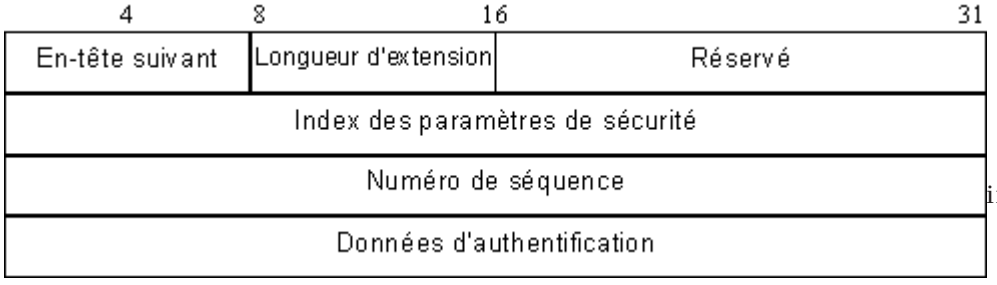
Dans le cas d'un tunnel, l'en-tête IPv6 interne contient les données relatives au destinataire final et le nouvel en-tête externe contient des adresses de destinataires intermédiaires.

Si des extensions suivent l'en-tête et qu'ils doivent être pris en compte durant le parcours ("Proche-en-Proche", "Routage"), des nouveaux en-têtes d'extensions sont également ajoutés durant l'encapsulation.



5.2 Authentification et intégrité des données

L'en-tête d'authentification, Authentification Header (AH Glossaire), fournit une authentification et l'intégrité des paquets IPv6. Cette option peut être choisie par le destinataire lorsqu'une connexion "association de sécurité" est active.



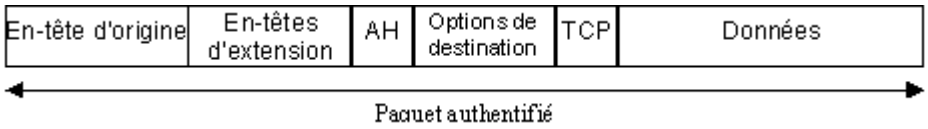
intégrité du paquet.

Tout comme pour l'ESP, l'authentification supporte deux modes : le mode transport et le mode tunnel. Dans le cas du mode transport, l'en-tête d'extension AH est inséré entre l'en-tête IPv6 et l'en-tête du protocole supérieur (TCP,

Le diagramme suivant explicite le mode transport de AH.

Considérons un paquet IPv6 englobant une trame TCP possédant cette forme avant l'application de AH :

Après l'application de AH, on obtient un paquet de la forme suivante:

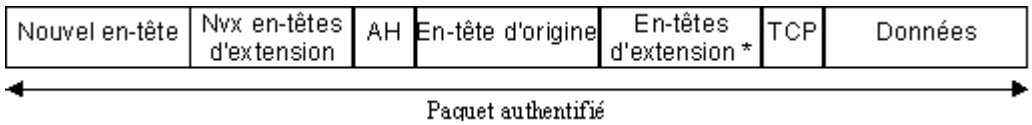


Le mode tunnel peut être utilisé dans le cas d'hôtes et de passerelles sécurisés. Dans le cas où AH est implémenté sur des équipements de connexion, alors le mode tunnel doit être utilisé.

L'en-tête d'origine conserve les données relatives au destinataire final tandis que le nouvel en-tête peut contenir différents points de passages sécurisés.

Dans le mode tunnel, AH protège la totalité du paquet IPv6 d'origine. Les extensions éventuelles du paquet initial sont protégées et remplacées par de nouvelles.

La figure suivante illustre la mise en place de AH en mode tunnel :



L'algorithme d'authentification est spécifié par l'association de sécurité. On utilise des algorithmes de cryptage symétrique dans le cas de connexions point à point et un cryptage à signature asymétrique dans le cas de connexions multicast.

Les en-têtes AH et ESP peuvent être indifféremment combinés.

Chapitre 6

CONCLUSION

Le nouveau protocole IPv6 permet d'intégrer nativement les améliorations apportées à IPv4 afin de le rendre compatible avec les nouveaux usages de l'Internet.

Les améliorations successives rajoutées IPv4 compliquaient le protocole et nécessitait des démarches lourdes de compatibilité.

Il prend en compte la sécurité (authentification et intégrité des données), la qualité de service (notamment pour les communications temps réel), la mobilité et une simplification de la configuration des équipements.

Il était devenu urgent de procéder à la mise en oeuvre de IPv6 car la date estimée d'épuisement des adresses IPv4 est en 2008.

Le processus de transition de IPv4 à IPv6 ne s'effectuera pas en une seule fois mais par cohabitation des deux protocoles, on estime à 2010 l'année où les équipements IPv4 seront minoritaires face à IPv6.

Au niveau mondial, IPv6 est testé est mis en oeuvre par le 6bone sous l'égide de IETF.

On dénombre près de 53 pays dans lequel IPv6 est expérimenté, il utilisé sur près de 800 sites.

En France, les précurseurs était un groupement d'universitaires et d'industriels réunis sous le nom de G6. Il regroupe entre autre le CNRS, ENST, INRIA, IMAG, Bull, Dassault...

Il a developpé une architecture de test et d'interconnexion des sites français appelé G6bone.

D'autres sites pilotes sont reliés au G6bone, comme celui du CNET, de Renater ou de l'INRIA.

Chapitre 7

Bibliographie

7.1 Les sites

http://www.ntdios.org/winsock/ipv6.htm
http://minimum.inria.fr/
http://www.rennes.enst-bretagne.fr/Rapports/IPngMM
http://www.urec.fr/IPv6/
http://www.ipv6.imag.fr
http://playground.sun.com/pub/ipng/
http://www.ipv6forum.com
http://www.g6.asso.fr
http://www.ipv6.org
http://www.renater.fr/Reseau/IPv6/

7.2 Les livres

IPv6, Theorie et Pratique. Gisèle Cizault. O ´Reilly ed. (03/2002)
IPv6 Clearly Explained. Peter Loshin. Morgan Kaufmann Publishers. (09/1999)

7.3 Les RFC

RFC 2460
RFC 2406
RFC 2402
RFC 2373
RFC 2374
RFC 2375
RFC 2378

7.4 Les mailing listes

ipv6@imag.fr
ipng@urec.fr

Glossaire

Adresse MAC
Adresse matérielle d'un équipement.

AH Authentification Header
En-tête controlant le processus d'authentification en IPv6.

Anycast
Principe qui permet d'identifier plusieurs interface par un même adresse IPv6 et de router un paquet à destination de cette adresse vers l'interface la plus proche.

ARP
Protocole de résolution d'adresses qui fait correspondre les adresses locales aux adresses réseau.

AS Association de sécurité
Structure de donnée définissant l'ensemble des paramètres de sécurité dans le cadre d'une connexion sécurisé.

Authentification
Mécanisme de vérifiation de l'identité d'un processus.

Bande passante
Capacité de transmission d'un médium de communication.

Bit
Unité d'information de base en communication 0 ou 1.

Broadcast
Message transmis à destination de tous les équipements.

BU Binding update
Mise à jour envoyé par un mobile en direction de son HA a chaque deplacement.

Checksum
Donnée permettant de vérifier l'intégrité des données transportées.

CIDR Classless Inter Domain Routing
CIDR permet d'assigner des adresses IPv4 sans faire appel aux classes A, B, C.

Confidentialité
Prévention d'une divulgation non autorisée de l'information.

DAD Duplicate Address Detection
Protocole qui permet de détecter si deux une adresse IPv6 est déja attribuée.

Datagramme

Nom donné à un paquert qui circule sur un réseau avec un protocole non connecté (UDP par exemple).

DHCPv6 Dynamic Host Configuration Protocol

Protocole qui distribue les adresses IP aux équipement d'un réseau.

En-tête

Conteneur de donnée placé en debut de paquet.

ESP Encryption Security Protocole

En tête qui assure la fonction d'encryption des données dans IPv6.

Flag

Mot d'information d'état.

Hop by Hop

L'en-tête Hop by Hop est utilisé pour contenir des informations qui pourront être examinées par chaque équipement traversé par le paquet.

ICMP Internet Control Message Protocol

Protocole de control de IP, fonctionne au moyen de messages émis en cas d'erreur.

Interface

Frontière à travers lesquels deux systèmes communiquent.

IPv6

Version 6 du protocole Internet.

IPX

Protocole assurant la transmission de paquet sur un réseau Netware.

MIP Mobile Internet Protocole

Protocole implemantant les fonctionnalités de mobilité pour IPv6.

MLD Multicast Listener Discovery

Protocole intégré à IPv6 qui permet la gestion des groupes multicast.

mot

Association de bits ayant une signification.

MTU

La MTU est l'unité de transmission maximum pouvant être transmise sur un lien.

MTU path

La MTU minimum sur un trajet utilisant plusieurs tronçons de MTU propres différentes.

Multicast

Adresse IP désignant plusieurs interface, lorsqu'un paquet est transmis à cette adresse alors il est envoyé à toutes les interfaces.

NA Neighbor Advertisement

Message ICMP émit en réponse à un NS ou pour signifier un changement d'adresse.

NDP Neighbor Discovery Protocol

Protocole qui permet la découverte mutuelle des voisins lors de l'installation d'une machine sur un réseau.

NS Neighbor Solicitation

Message ICMP permettant d'obtenir l'adresse de niveau 2 d'un voisin sur le lien.

NSAP

Système d'adresses hierarchique utilisé pour mettre en place un système d'adressage d'interconnexion. C'est le point logique entre la couche réseau et la couche transport.

NUD Neighbor Unreachability Detection

Fonctionnalité de NDP permettant de déterminer un voisin dont l'adresse est stockée sur la table de routage est toujours accessible.

Paquet

Unité de donnée correspondant à une couche réseau.

Payload

Données utiles transportés dans un paquet.

Ping

Requete ICMP qui a pour but de savoir si une destination peut-être atteinte.

RA Router Advertisement

Message ICMP de confirmation de la présence d'un routeur.

Routeur

Equipement d'acheminement sur un réseau.

RS Router Solicitation

Message ICMP émis pour recevoir un RA en réponse.

SPI

Champ des en-têtes ESP et AH déterminant le niveau de sécurité associé à une "association de sécurité".

Table de routage

Table utilisée par les routeurs pour diriger les paquets vers leur destination par le chemin optimal.

Tunnel

Procédé d'encapsulation qui permet l'acheminement de données de façon protégée entre deux points.

UAB unité d'agregation basse

Niveau d'attribution des adresses IPv6 correspondant aux fournisseurs de moyenne portée.

UAH Unité d'agrégation haute

Niveau d'attribution des adresses IPv6 correspondant aux fournisseurs de portée mondiale.

UAS Unité d'agrégation de site

Niveau d'attribution des adresses IPv6 correspondant à un site local.

Unicast

Désigne une adresse désignant une unique interface.

Index

A

Abréviation, 2–2
Adresse de Destination, 3–2
Adresse Source, 3–1
AH, 5–2
ARP, 4–1
AS, 5–1

B

Bande passante, 2–1
Broadcast, 2–1

C

Checksum, 3–2
Classe de Trafic, 3–1

D

DAD, 4–2
DCPHv6, 4–3

E

ESP, 5–1

F

Flags, 2–8
Flow label, 3–1

H

Hop limit, 3–1

I

Interface, 2–1

M

MIP, 4–4
MLD, 4–1
Multicast, 2–1

N

NDP, 4–1
Noeud, 3–5
NUD, 4–2

P

Payload length, 3–1

S

Scope, 2–8
SPI, 5–1
Subnet, 2–8

U

UAB, 2–4
UAH, 2–4
UAS, 2–4
Unicast, 2–1, 2–3