Adressage IP version 6

Introduction

Au delà du simple épuisement des adresses IPv4 annoncé pour les années futures du fait de l'émergence des nouveaux terminaux (téléphonie mobile, domotique, etc), l'ancienne mouture du protocole d'interconnexion de réseau présente de nombreux défauts qui ont été complétés ou corrigés au fur et à mesure sans jamais être parfaitement intégrés :

- NAT : cette technique est devenue obligatoire pour assurer l'existence de réseaux internes connectés sans monopoliser les adresses utilisables. Elle pose des problèmes pour l'application d'éléments de sécurité (VPN notamment) ou d'un point de vue juridique (qui est l'émetteur réel d'un flux adressé au nom du routeur).
- Agrégation des adresses (disposer d'adresses contiguës pour pouvoir les adresser en une seule fois) : les routeurs et les tables de routage doivent effectuer un travail lourd de recherche parmi plusieurs dizaines de milliers de lignes de routage. L'organisation ***CIDR (Classeless InterDomain Routing)*** permet de fonctionner par adresses agrégées, mais elle n'a pas été généralisée du fait d'une distribution aléatoire des adresses au démarrage.
- Routage : les protocoles de routage sont basiques et reposent sur des informations arbitraires (débit, nombre de sauts ou champ TTL)
- Agrégation des communications : le ***multicast*** (un seul flux pour plusieurs destinataires) n'est pas encore intégré à tous les routeurs.
- Sécurité : IPSec a été ajouté pour assurer les fonctions de sécurité indispensables à un usage sur un réseau public (authentification, signature, confidentialité et intégrité).
- Prioritarisation (ou priorisation) des flux : le protocole RSVP (Resource Reservation Protocol) va permettre de donner un niveau de priorité à certains flux (payés en conséquence) pour un acheminement plus rapide.
- Qualité de service : (garantie de débit, de sécurité, de disponibilité, de rétablissement, etc). Elle est assurée par un travail sur le contenu de tout le paquet (niveaux 3, 4, 5 et 7) qui demande de la puissance de calcul sur les routeurs.

Toutes les évolutions d'IPv4 sont le fruit d'ajouts ou de compléments qui nécessitent une adaptation des matériels d'extrémité et de cœur de réseau. Leur déploiement prend du temps et ne suit pas l'évolution des besoins en temps réel. Pour prendre en compte ces nouvelles exigences, les concepteurs d'IPv6 ont décidé d'entreprendre un travail de mise à plat des améliorations apportées en les intégrant directement dans la nouvelle version, effaçant de fait les incompatibilités existant entre des protocoles apparus simultanément. En outre, l'organisation d'IPv6 permet l'intégration de nouveautés sans remise en cause de la structure, rendant l'évolutivité future plus simple. Mais la première action d'IPv6 est de reprendre la structure de l'adressage.

I L'adressage

IPv6 repose, en premier lieu, sur un adressage largement étendu par rapport à IPv4 : alors qu'on ne disposait que de 32 bits (4 octets) pour les adresses, les valeurs actuelles sont définies sur 128 bits (16 octets), portant le nombre d'adresses possibles à 3x 1038.

La taille de l'adressage a été revue, et, partant, la notation itou.

À présent, une adresse aura la forme —-:—-:—-:—-:—-:—-:—-:—-/xx

- la première moitié (4 mots de 16 bits) constitue l'adresse de réseau,
- les 64 bits suivants indiquent l'adresse de la machine
- la dernière partie nommée le ***préfixe*** (/xx) fournit l'équivalent du masque de réseau, permettant de distinguer des agrégats (préfixe <64) ou des sous-réseaux (préfixes > 64).

Pour ce qui est de la notation, une adresse aura donc la forme :

```
FEDC:123D:19A3:9453:FFE3:34E1:6543:9100
```

On notera que la séparation est représentée par « : » et non plus le point « . ».

Des simplifications existent pour éviter les écritures trop longues. Ainsi, dans un réseau FEDC:123D:9341:0000/64

```
La machine portant le numéro 0000:E234:05DC:1200
Pourra être représentée comme suit :
FEDC:123D:9341:0000:0000:E234:05DC:1200
Ou, dans une version simplifiée :
FEDC:123D:9341__::__E234:5DC:1200
```

Les suites de zéro consécutives seront compactées dans le double « :: ». Ce signe ne pourra cependant apparaître qu'une seule fois. Tous les zéros en début de partie de mot (4 valeurs hexadécimales) pourront aussi être supprimés.

L'adresse de la route par défaut (0.0.0.0 Masque 0.0.0.0 en IPv4) peut ainsi être résumée par ::/0 en IPv6.

Mais le plus important n'est pas cette notation, c'est la possibilité d'agréger des adresses pour simplifier le routage

Plan agrégé

Trois niveaux peuvent être retenus, chacun pouvant être hiérarchisé par le biais du préfixe (qui joue le rôle du masque de sous/sur réseau) :

- grands transporteurs (opérateurs télécom nationaux et internationaux) : on leur donnera un adressage avec un préfixe sur 28 bits (c'est à dire que les 28 bits de poids fort sont fixés pour chacun d'entre eux). Ils pourront ensuite répartir leurs adresses réseau (il reste 36 bits) à un niveau inférieur, soit pour un usage personnel, soit en revendant des blocs d'adresses de manière agrégée
- fournisseurs d'accès (opérateurs nationaux ou régionaux, FAI, etc) : on leur attribuera une adresse ::/32 ou ::/36 par exemple. Il reste 16 ou 12 bits pour répartir leur plage auprès de leurs clients.
- Site : il s'agit des entreprises utilisatrices finales ou des FAI locaux. Les 16 bits de poids faible de la partie réseau sont affectés à cet usage. Selon la taille de l'entreprise (et l'achat réalisé auprès d'un organisme), elles pourront se voir fixer plus ou moins de valeurs (bits de poids fort

de ces 16 bits), charge à elle de répartir le reste entre ses propres services.

Ce plan agrégé comportera deux parties sur les 64 bits de réseau :

- Les 48 bits de poids fort constituent une topologie publique, attribuée par les organismes de l'internet. Ils sont découpés selon la structure suivante
  - si une adresse relève d'un plan agrégé, elle commencera par la représentation 2000::/3
  - suivront 13 bits attribués par le NIC à un transporteur/opérateur : on parle d'une unité TLA (Top Level Aggregator)
  - le reste (24 bits), ou unité NLA (Next LA), est attribué par l'opérateur à un FAI
- les 16 bits de poids faible de la partie réseau définissent une topologie de site SLA (Site LA), attribuée par le FAI à d'autres FAI ou à des entreprises

3 bits			**13 bits**	**8 bits**	**24 bits**	**16 bits**	**64 bits**
0	0	1	TLA	Réservé	NLA	SLA	ID Hôte
Exemple pour un Grand transporteur : 3F4E::/24							
3F4E:				00	00:0000	0000	
Exemple pour un FAI alloué par ce transporteur : 3F4E:003B:C000::/40							
3F4E:				00	3B:C000	0000	
Exemple pour un gros client de ce FAI : 3F4E:003B:C0FF:1F00::/56							
3FE4:				00	3B:C0FF	1F00	
Exemple pour un petit client de ce FAI : 3F4E:003B:C040:0003::/64							
3FE4:				00	3B:C040:	0003	

Cela va simplifier les lignes de routage car l'on pourra faire du transport de FAI en Gros transporteur du fait que les routeurs sont capables de prendre en compte les adressages de réseau avec le préfixe (et non plus, comme en IPv4, seulement avec la notion de classe). C'est ce qui avait été implémenté avec VLSM (Variable Length Subnet Mask) et son évolution CIDR (Classeless Inter-Domain Routing) qui abandonnaient la notion de classe d'adresse au profit d'un masque variable. Toutes les adresses ne sont cependant pas agrégées et l'on peut aussi utiliser une adresse /64 pour une entreprise standard. Des valeurs sont réservées aussi à des usages spécifiques.

Autres adresses

Elles reprennent en partie ce qui existait et le complètent.

Loopback

L'usage est le même que celui du 127.0.0.1. L'adresse de loopback en IPv6 se note ::1.

Indéterminée

C'est l'adresse présente sur un client DHCP avant qu'il ne reçoive une proposition d'adresse par le serveur. Le 0.0.0.0 d'IPv4 devient ::/0 en IPv6.

Adressage privé

L'adressage privé d'IPv4 aux valeurs 10.0.0.0, 172.16.0.0 à 172.31.0.0 et 192.168.x.0 est remplacé par la notion de site local. Les 48 bits de poids fort sont fixés à la configuration FEC0::/48, les 16 bits suivants (SLA) sont disponibles pour opérer une segmentation.

Lien local

La notion de lien local, nouvelle en IPv6, correspond à un adressage standard permettant à des machines présentes sur un même lien physique (réseau Ethernet, lien PPP, extrémités d'un tunnel IPSec) de se trouver sur le même réseau sans avoir besoin d'utiliser des adresses publiques. La partie réseau (sur 64 bits) est imposée au format FE80::/64, la partie machine est libre. Cet adressage permet par exemple l'initialisation des communications DHCP, la découverte d'adressage réseau auprès des routeurs, etc. Il coexiste avec l'adressage public.

Adresse IPv4

Pour garder la compatibilité avec IPv4, les adresses en w.x.y.z seront notées 0:0:0:0:0:0:w.x.y.z. On observera la notation pointée et pas avec ":", et l'absence d'identification réseau.

Multicast

L'adressage ***multicast*** permet d'adresser, en une seule opération, un même message à plusieurs destinataires abonnés à un groupe. En IPv6, il remplace l'adressage ***broadcast*** (des 1 sur la partie machine) trop lourd d'IPv4 et corrige les éléments du ***multicast*** (adresses 224.0.0.0) très peu utilisés.

La forme d'une adresse ***multicast*** est ***FF::/8***.

8 bits	**4 bits**	**4 bits**	**112 bits**
FF	Drapeau	Portée	Numéro de groupe multicast

On précisera la portée de la diffusion selon les valeurs ci-contre.

Portée	
0	réservé
1	équipement
2	lien
5	site
8	organisation
E	global (équivalent au *broadcast*)
F	réservé

Le drapeau vaudra 0 si le groupe est une valeur permanente définie par un organisme d'internet, et 1 s'il s'agit d'un groupe temporaire.

Parmi les valeurs significatives, on trouvera notamment le groupe ***All-Nodes-Group*** identifié par **FF02::1/128**, équivalent d'un ***broadcast*** sur le lien physique où se situe une machine. Ainsi, toute machine doit être abonnée à ce groupe ***multicast***.

Autre groupe obligatoire, il s'agit du ***multicast*** sollicité qui va servir aux machines à dialoguer au sein d'un réseau physique (voir plus loin).

Outre l'adressage, d'autres éléments ont été revus en IPv6, qui entraînent un changement du format de l'entête. ***Tentative Address*** (Adresse temporaire)

Lors de la configuration autonome, un poste doit se constituer une adresse de machine en essayant de ne pas être en conflit avec une adresse déjà présente sur le réseau. Deux possibilités permettent de déterminer cette adresse.

Adresse Universelle d'interface (EUI-64)

Elle est constituée à partir de l'adresse MAC (sur 6 octets, présentés ci-dessous de MAC6 à MAC1) de la manière suivante :

MAC6*	MAC5	MAC4	FFFE	MAC3	MAC2	MAC1

*le 7ème bit de poids fort de MAC6 est positionné à 1 pour préciser qu'il s'agit d'une adresse universelle unique

Adresse calculée

Pour garder la confidentialité des utilisateurs et ne pas autoriser l'espionnage (une adresse MAC est unique !), l'adresse de démarrage peut être calculée de manière pseudo aléatoire en utilisant des fonctions de hachage appliquées sur l'adresse MAC et l'horloge système.

II Entête IPv6

Au delà de cet aspect visible, l'évolution d'IPv6 vise à améliorer le transfert des datagrammes sur le réseau grâce à un entête fondamentalement revu :

- disparition du checksum (contrôle d'intégrité sur les entêtes de niveau 3) qui devait être recalculé à chaque passage par un routeur. Cela permet d'augmenter la rapidité de transfert, et supprime un contrôle déjà opéré au niveau 2 et 4.
- une taille d'entête fixe de manière à simplifier l'accès à la partie données et l'extraction des informations à traiter par chaque intermédiaire. On pourra notamment utiliser des circuits électroniques en lieu et place de calculs logiques.
- retrait des options remplacées par des extensions : on ne les traite qu'au moment opportun

L'entête prend alors la forme suivante : **champ non modifié** *champ modifié* élément nouveau

0			**4**			**8**			**12**			**16**			**20**			**24**						**31**
Version			**Classe de trafic**			identificateur de flux																		
longueur des données												*entête suivant*			**nb de sauts**									
adresse source																								
adresse destination																								

Champs non modifiés

- Version : La notion de version permet de conserver la compatibilité avec IPv4. Elle vaudra 6.
- Classe de trafic : Anciennement nommé Type de service, ce champ garde la même fonction mais sera mieux utilisé. On l'appèle aussi priorité ou DiffServ (Differenciated Service) en IPv4. Il s'agit d'assurer la qualité de service en précisant si un paquet doit être traité prioritairement. Il s'agit d'une information ajoutée par l'émetteur conformément à un accord passé avec le fournisseur du réseau de transport.
- Nombre de sauts : Correspondant au TTL (Time To Live), il n'apporte d'autre innovation que de ne plus être lié à la notion de temps.

Champs modifiés

- Longueur des données :Elle ne porte plus que sur la partie utile (payload) sans l'entête.
- Entête suivant : Anciennement nommé Protocole, dans la nouvelle version, il désigne soit un protocole de niveau 4 comme en IPv4, soit un numéro d'extension (expliqué plus loin)

Élément nouveau

- Identificateur de flux :Il va permettre de réaliser la qualité de service en produisant un numéro spécifique pour certains échanges (à la manière du numéro de session) qui pourra être repéré par les routeurs. C'est le point le plus important du nouveau protocole. Il va permettre :
  - une accélération du transfert de données en généralisant la notion de contexte (information ajoutée pour faciliter l'acheminement sans parcourir à nouveau la table de routage) déjà en cours dans la version 4
  - une meilleure qualité de service à la façon du protocole RSVP (Resource reSerVation setup Protocol)

Éléments supprimés

De nombreuses parties de l'entête IPv4 ont été supprimées de manière à rendre le routage beaucoup plus rapide. D'abord, les options ont été reléguées dans la partie extension qui permet de ne faire apparaître dans l'entête que les parties réellement utile et de repousser les informations optionnelles dans une partie annexe. Nous avons aussi vu que le champ de contrôle des entête (checksum) a disparu. Il en va de même des drapeaux (qui indiquaient un message urgent, un paquet d'accusé de réception, etc et qu'on trouvera maintenant dans les extensions ICMP.), de la notion de fragment (redécoupage d'un paquet TCP/UDP, repoussé dans les extensions) ainsi que de la longueur de l'entête (fixé à 40 octets à présent).

Les extensions

Les extensions sont une manière de sortir de l'entête des informations qui ne seront traitées que de bout en bout ou par certains intermédiaires. L'intérêt est à la fois de diminuer les traitements intermédiaires et d'enrichir les possibilités d'IPv6 en permettant une encapsulation dès la conception de l'entête. Le champ prochain entête indique ainsi le type d'option à suivre. Parmi les valeurs possibles, on trouve :

	Extensions	N°	Protocole
0	proche en proche : étudié par tous les nœuds traversé	6	TCP
43	Routage : définit la route (les adresses de routeur) à suivre	17	UDP
44	Fragmentation : découpage et numérotation réalisés par l’émetteur pour diviser un paquet conformément à ce qui est supporté par le réseau	41	IPv6
46	RSVP : réservation de bande passante sur un réseau	58	ICMPv6
50	Confidentialité : ESP		
51	Authentification : AH		
59	Fin des entêtes		
60	Destination (ou end-to-end) : les données ne sont lues que par l’émetteur et le destinataire final		

Plusieurs options peuvent être utilisées comme suit :

<table>
<tr><td>Entête1</td><td>Prochain entête=XX</td><td>…</td><td>Entête option 1</td><td>Prochain entête=YY</td><td>…</td><td>Entête option N</td><td>Prochain entête = 59</td></tr>
<tr><td></td><td colspan="3">__ _ _ _ _ _ _ _ _ _ _ _ _ _ _ /|||\ _ _ _ _ _ _ _ _ _ _ _ _ _ _ __/</td><td></td><td></td><td></td><td></td></tr>
</table>

Un message n’ayant pas d’option portera le numéro de protocole de couche 4 dans le champ prochain entête.

III Fonctionnement des communications

Il repose essentiellement sur l’amélioration du protocole ***ICMP*** (Internet Control Message Protocol) et sur un fonctionnement de voisinage renouvelé. Cela va permettre d’inclure en un seul protocole toutes les fonctions d’échange de messages qui autorisent la configuration des postes et des routeurs.

ICMPv6 et la découverte de voisinage

La nouvelle version incorpore un ensemble de fonctions définies auparavant dans plusieurs protocoles :

Protocole (version 4)	Équivalent (version 6)	Fonction
ARP (Address Resolution Protocol)	Résolution d’adresse	Recherche l’adresse MAC associée à une adresse IP
ARP Gratuit	DAD (Duplicate Address Detection)	Lancé à l’initialisation, il permet de savoir si l’adresse IP de l’équipement est déjà attribuée.
ICMP Router Discovery	Découverte des routeurs	Permet à l’équipement de détecter les routeurs sur leur lien physique
IGMP (Internet Group Management Protocol)	Gestion de groupes multicast Remplacé par MLD (Multicast Listener Discovery)	Permet la communication multicast

Protocole (version 4)	Équivalent (version 6)	Fonction
Indication de redirection	Idem	permet l'optimisation de la circulation en cherchant un chemin moins coûteux en terme de sauts

De nouvelles fonctions ont été ajoutées :

- NUD (Neighbor Unreachability Detection), qui efface les adresses qui n'ont plus cours
- Découverte des préfixes, pour qu'un équipement construise son adressage à partir d'un dialogue avec le routeur
- Découverte des paramètres pour se caler sur les spécifications du réseau physique (taille des paquets) à partir de l'analyse des paquets d'échange

Un paquet ICMPv6 correspond à une extension dans un paquet IPv6 où le champ prochain entête est positionné à 58. Il est structuré comme suit :

8 bits	8 bits	16 bits	Variable
Type	Code (numéro pour différencier les types)	Checksum sur entête ICMP	Message ICMP

Le Type sera une valeur commençant par

- 0 sur le bit de poids fort s'il s'agit d'un message d'erreur
- 1 sur ce bit de poids fort s'il s'agit d'un message informationnel.

Les messages d'erreur

Avec ICMPv6, le protocole va fournir toutes les informations nécessaires pour faciliter le paramétrage des postes et la configuration des routeurs.

Mais pour ne pas saturer le réseau de messages d'erreur, on limitera leur envoi dans un taux contraint : toutes les 1000 ms ou en n'utilisant pas plus de 2% de la bande passante par exemple.

Destination inatteignable (Destination Unreachable) Type 1- Code 0-4

Autrefois, il fallait un ping pour repérer ce genre d'erreur. Maintenant, les messages ICMPv6 vont enrichir la notion en offrant plus de détail.

Le code pourra prendre les valeurs pages suivantes.

Code	Description
0	Aucune ligne de routage n'a été trouvée concernant la destination.
1	La communication avec le destinataire a été rejetée pour des question de stratégie. C'est typiquement le type d'envoi lorsqu'un paquet a été rejeté par un firewall.
2	L'adresse est au-delà de l'étendue de l'adresse source
3	Hôte inconnu. C'est le message de réponse lorsque la résolution d'adresse MAC n'a pu être opérée
4	Port de destination inatteignable. Fonctionne avec UDP, lorsque aucun service n'est en écoute sur le port demandé.

Paquet trop gros (Packet too big) Type 2 – Code 0

Lorsque l'on véhicule IPv6 sur un réseau, le paquet doit être dimensionné selon la taille supportée par l'infrastructure de niveau 1/2. Cependant, en passant au travers de réseaux multiples, la dimension tolérable (MTU : Maximum Transport Unit) n'est pas la même et il est nécessaire de prévenir l'émetteur d'adapter la taille de ces paquets pour éviter un redécoupage ou un rejet systématique.

Délai de la demande dépassé (Time Exceeded) Type 3 – Code 0 ou 1

Apparaît lorsque la valeur nombre de sauts (anciennement TTL) arrive à 0, suite à une boucle dans le routage ou à un nombre d'équipements à traverser trop important. Le code vaudra alors 0. une autre possibilité de dépassement est lorsque le ré-assemblage des divers paquets d'un même message est trop long. Le code vaudra alors 1.

Problème de paramétrage (Parameter Problem) Type 4 – code 0-2

Il s'agit d'erreurs dans les numéros de prochain entête ou dans la structure d'un paquet.

Les messages informationnels

Ils vont permettre aux machines de se tenir au courant de leur état de manière à détecter la présence ou la rupture de communication entre équipements.

Requête d'echo (Echo Request) Type 128 – Code 0

C'est l'équivalent du ping, permettant d'envoyer une sollicitation et de recevoir une réponse.

Réponse à echo (Echo Reply) Type 129 – Code 0

Il s'agit de la réponse à une sollicitation.

L'automatisation de la configuration

En plus de ces nouveautés, IPv6 apporte des fonctions complémentaires d'autoconfiguration, notamment pour l'apprentissage de l'adresse de l'équipement de manière autonome (Stateless Address Autoconfiguration, utilisant l'adresse Tentative Address décrite plus haut) ou avec le DHCPv6 (Stateful Autoconfiguration).

IV Conclusion

La généralisation d'IPv6 était prévue pour 2010. Elles est déjà partiellement opérationnelle et, ce qui est important, est compatible avec la version 4. Et, contrairement à cette dernière, elle anticipe largement les évolutions futures du réseau. Le site www.comprendre-ipv6.net donne des éléments de compréhension sur l'apparition et l'expansion d'IPv6 (raison, enjeux, technologie, etc).

From:
https://wiki.sio.bts/ - **WIKI SIO : DEPUIS 2017**

Permanent link:
https://wiki.sio.bts/doku.php?id=ipv6&rev=1595780829

Last update: **2020/07/26 16:27**