

IPv6 : auto-configuration

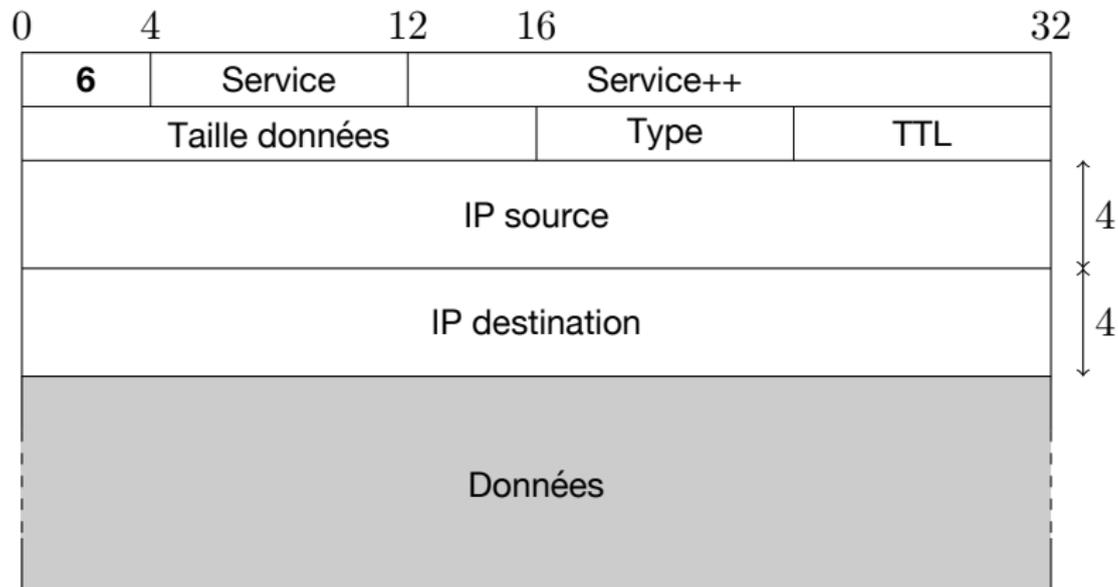
Gaétan Richard
gaetan.richard@unicaen.fr

M2 E-Secure
UMIS1E – IPv6 et nouvelles architectures

I. Paquet

Datagramme IPv6

Structure : En-tête principale de 40 octets



Fonctionnement : En-têtes supplémentaires éventuelles pour les options : proche en proche, destination, routage, fragmentation, authentification, confidentialité.

Avantage : Si première en-tête supplémentaire \neq "hop-by-hop", alors pas de traitement par les routeurs, donc analyse inutile des options supprimée.

Multicast et ethernet (rappel)



La machine utilise alors l'adresse MAC produite pour "écouter" les paquets multicast.

Prise en compte des trames (rappel)

Écoute : L'interface MAC est donc ainsi "à l'écoute" de plusieurs adresses Ethernet :

- ▶ son adresse de construction ;
- ▶ ff :ff :ff :ff :ff :ff pour les broadcasts v4 ;
- ▶ 01 :00 :5E :xx :xx :xx pour les groupes multicasts v4 ;
- ▶ 33 :33 :xx :xx :xx :xx pour les groupes multicasts v6.

Pour ces adresses, et seulement pour celles-là, la trame Ethernet est prise en compte, analysée, et son contenu envoyé au protocole IP s'il y a lieu

Adresse multicast sollicitée (rappel)

Principe : Si la machine a une ou des adresses v6, l'interface est en particulier à l'écoute sur l'adresse MAC forgée à partir de l'adresse "multicast sollicitée" obtenue par concaténation du préfixe `ff02 ::1 :ff00 :0/104` et des 24 bits de l'adresse Ipv6.

Exemple : ad. v6 = `2001 :660 :7101 :1 :20d :93ff :fe3b :91a0`
ad. multicast sollicitée : `ff02 ::1 :ff3b :91a0` ad. mac
correspondante : `33 :33 :ff :3b :91 :a0`.

Intérêt : si la machine possède plusieurs adresses v6 contenant son ad. mac en partie basse, l'ad. multicast sollicitée est la même pour toutes ces adresses.

2. Stateless auto-configuration

Adresse link-local

Adresse unique :

- ▶ Adresse MAC : xx :xx :xx :xx :xx :xx (6 octets)
- ▶ Adresse EUI-64 : xx :xx :xx :ff :fe :xx :xx :xx (8 octets)
- ▶ Adresse link-local : fe80 ::xx :xx :xx :ff :fe :xx :xx :x.

Validité : Cette adresse n'est valide que sur le réseau local.

Étape 1

Vérifier que l'adresse n'est pas utilisée :

La machine envoie un paquet **Neighbor Solicitation** à l'adresse multicast sollicitée forgée à partir de l'adresse link-local désirée. À cette étape, on utilise encore l'adresse `::` (adresse non spécifiée).

Réponse :

Toute machine qui reconnaît son adresse répond à l'adresse `ff02::1`. Si une telle réponse est reçue, on doit prendre une autre adresse (aléatoire ou manuelle).

Étape 2

Trouver un routeur : L'interface ayant une adresse lien-local, elle l'utilise (comme adresse source) pour envoyer un message de "découverte de routeurs". Ce message est envoyé à `ff02 ::2`. Tous les routeurs sont à l'écoute sur l'adresse MAC `33 :33 :00 :00 :00 :02`.

Réponse : Les routeurs répondent à la sollicitation (si programmés pour cela) en envoyant un préfixe utilisable (un/64 en général). La réponse est envoyée à tous les nœuds du lien local avec l'adresse `ff02 ::1`, afin d'avertir de la présence du routeur toutes les machines du réseau

Étape 3

Création d'adresse : Les machines qui reçoivent la réponse du routeur vont utiliser le préfixe reçu pour se forger une adresse globale :
préfixe : EUI-64.

Ultime vérification : L'adresse ainsi forgée doit toutefois être unique, il faut donc vérifier qu'elle n'est pas déjà prise sur le réseau local (même procédure que pour la première étape, non obligatoire toutefois car partie machine identique à celle de l'ad lien-local)

route : En outre, l'adresse du routeur (souvent la lien-local) sera utilisée comme route par défaut.

Précisions :

Multiple routeurs : En cas de plusieurs routeurs sur le réseau, chaque machine pourra se forger plusieurs adresses globales. Chaque routeur peut annoncer des routes précises, ainsi qu'une priorité (basse, moyenne, haute) pour l'utiliser comme route par défaut.

Données annexes : Chaque machine peut ainsi s'autoconfigurer avec une adresse globale (au moins), un masque de sous-réseau, une route par défaut. Il manque toutefois l'adresse d'un DNS, le nom du domaine,... Ceci peut être obtenu avec un DHCP, en lui demandant seulement ces paramètres (pas l'adresse, puisqu'on en a déjà une)

Problème : On peut suivre une machine avec l'unicité de l'UEI-64.

Solution : Privacy Extensions for Stateless Address Autoconfiguration in IPv6 (RFC 4941). Ajout d'une nouvelle adresse temporaire semblant aléatoire.