Master – Adressage IPv6

Les mécanismes d'adressage

Configuration manuelle

L'administrateur fixe l'adresse. Les adresses constituées entièrement de 0 ou de 1 ne jouent pas de rôle particulier dans IPv6.

Configuration automatique

La configuration automatique peut utiliser 3 méthodes :

Auto configuration sans état basée sur l'adresse MAC
Auto configuration DHCPv6 avec état
Auto configuration DHCPv6 sans état

Auto configuration sans état basée sur l'adresse MAC

L'autoconfiguration sans état, **SLAAC** (Stateless Automatic Auto Configuration) est une méthode par défaut de configuration IPv6 dans un environnement routé pour les routeurs **RADVD** (Router Advertisement Daemon) et les nœuds.

- Le routeur (RA-Router Advertisement) envoie les paramètres préfixe(s) avec le Flag A activé, MTU, préférence, passerelle, Flags M et O
- L'interface construit elle-même son identifiant d'interface selon différentes méthodes MAC EUI 64 ou de manière aléatoire.

Cette méthode est utilisée pour configurer des adresses lien-local en échangeant des messages (sollicitation et annonce) avec les routeurs de voisinage.

Configuration automatique des adresses avec état basée sur DHCP

Utilisé pour configurer les adresses lien-local à l'aide d'un protocole de configuration tel que DHCP.

Ce mode est appelé DHCPv6 Stateful. Il est similaire à ce que DHCP IPv4. Le serveur assigne l'adresse complète et des paramètres optionnels
RA Flags activés M=1 et O=1.

Configuration automatique des adresses sans état basée sur DHCP

Dans un adressage sans états, le serveur DHCP ne fournit que des informations optionnelles : serveur DNS, NTP, SIP, etc. Il ne donne aucune adresse, elles sont alors générées par SLAAC. Il ne maintient aucun état dynamique des clients qui le sollicitent.
Le RA flags M=0/1 et O=1 selon le déploiement choisi.

Les flags

Ces quatre méthodes peuvent se combiner au choix et servir à la gestion de l'adressage IPv6 ainsi qu'à la re-numérotation IPv6. Elles sont indiquées dans le champ Flags :

Configuration	Flag M	Flag O
Configuration statique ou nulle seul	0	0
Stateless Automatic Autoconfiguration źSLAACž	0	0
DHCPv6 źStateful) avec ou sans SLAAC	1	1
DHCPv6 Stateless avec SLAAC	0	1

Affectation des flags pour l'adressage

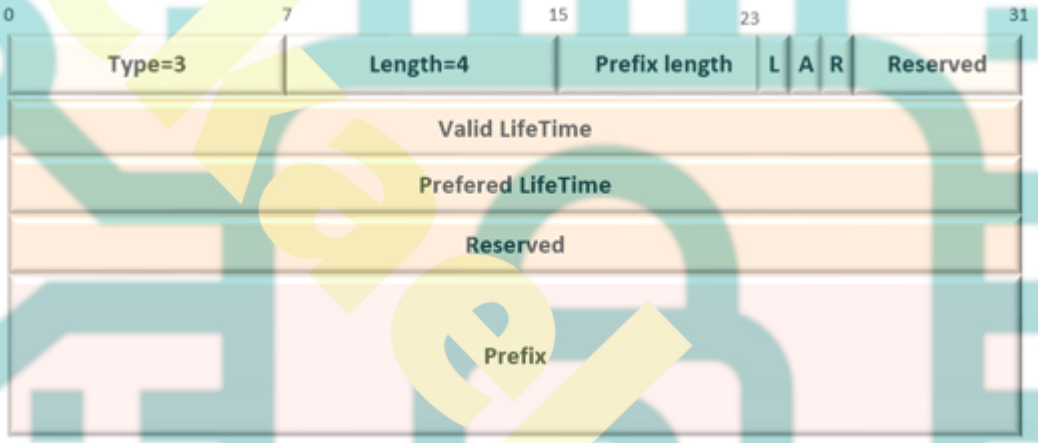
- Le bit **M** (*Managed address configuration*) mis à 1 indique que l'équipement ne doit pas construire lui-même l'adresse à partir de son identifiant d'interface et des préfixes reçus, mais doit demander une adresse auprès d'un serveur d'adresses.

- Le bit **O** (*Other stateful configuration*) indique que l'équipement doit interroger le serveur de configuration pour obtenir des paramètres autre que l'adresse.

Les annonces de préfixes de routeur

Le routeur communique au nœud les informations sur le préfixe utilisé sur son lien au moyen d'une option incluse dans le message ICMPv6 d'annonce de routeur.

Informations sur le préfixe envoyée par le routeur



Cette option contient les informations sur le préfixe pour permettre une configuration automatique des équipements.

> Le champ type vaut 3 et le champ longueur vaut 4.

- Le champ **Prefix Length** indique combien de bits sont significatifs pour le préfixe annoncé dans un champ suivant.
- Le bit **L à 1**, permet d'indiquer que tous les autres équipements partageant le même préfixe sont sur le même lien. L'émetteur peut donc directement les joindre. Dans le cas contraire, l'équipement émet le paquet vers le routeur. Si ce dernier sait que l'équipement émetteur peut joindre directement le destinataire, il émettra un message ICMPv6 d'indication de redirection.
- Le bit **A à 1**, signifie que le préfixe annoncé peut être utilisé pour construire l'adresse de l'équipement.
- Le bit **R à 1**, indique que le champ préfixe contient l'adresse globale d'un routeur «agent mère». Les bits de poids fort peuvent toujours être utilisés pour construire un

préfixe.

- Le champ **durée** de validité indique en secondes la durée pendant laquelle le préfixe est valide.
- Le champ **durée préférable** désigne la durée en secondes pendant laquelle une adresse construite avec le protocole de configuration sans état demeure « préférable »

Pour ces deux champs, une valeur de 0xffffffff représente une durée infinie. Ces champs peuvent servir dans la phase de passage d'un fournisseur d'accès à un autre ; c'est-à-dire d'un préfixe à un autre.

Communication entre équipements

Détection d'inaccessibilité des voisins ou NUD (Neighbor Unreachability Detection) Cette fonction n'existe pas en IPv4. Elle permet d'effacer des tables de configuration d'un équipement, les voisins qui sont devenus inaccessibles (panne, changement d'adresse…) Si un routeur devient inaccessible, la table de routage peut être modifiée pour prendre en compte une autre route.

Découverte des routeurs. Ce protocole permet aux équipements de déterminer les routeurs qui sont sur leur lien physique. Dans IPv4, ces fonctionnalités sont assurées par le protocole ICMP Router Discovery.

Découverte des paramètres. Ce protocole permet aux équipements d'apprendre les différents paramètres du lien physique, par exemple, la taille du MTU, le nombre de sauts maximal autorisé, si la configuration automatique avec état (comme DHCPv6) est active… Il n'existe pas d'équivalent en IPv4.

Indication de redirection. Ce message est utilisé quand un routeur connaît une route meilleure (en nombre de sauts) pour aller à une destination.

Le rôle du routeur est important dans l'auto-configuration. Il indique à la machine via un message d'annonce de routeurs, la méthode à retenir et fournit éventuellement les informations nécessaires à sa configuration.

Cycle de vie d'une adresse

Avec les besoins de renumérotation, l'attribution d'une adresse à une interface est faite temporairement, les adresses IPv6 ne sont pas données mais prêtées.

Une adresse IP passe par différents états logiques qui permettent savoir si elle est ou non utilisable pour les communications

- **Test unicité (DAD – Duplicate Address Detection)** vérifie si l'adresse est déjà utilisée (comme ARP gratuit d'IPv4)
- **Préféré** – l'utilisation ne subit pas de restriction.
- **Déprécié** – l'utilisation de l'adresse est déconseillée, mais pas interdite. L'adresse dépréciée ne doit plus être utilisée comme adresse de source pour les nouvelles communications mais elle peut encore servir d'adresse de source dans le cas des communications existantes. Les paquets reçus à une adresse dépréciée continuent à être remis normalement.
- **Invalide** – Une adresse invalide (durée de vie de l'adresse préférée terminée) ne doit jamais être utilisée comme adresse dans des communications. La valeur par défaut de la durée de vie d'une adresse est de 30 jours, mais cette durée peut être prolongée, ou portée à l'infini.
  L'adresse lien-local a une durée de vie illimitée.

Quand la durée de vie est arrivée à terme, l'adresse devient invalide, elle est supprimée de l'interface et devient potentiellement assignable à une autre interface. Pour faciliter la renumérotation d'une interface, il faut le faire en douceur pour ne pas risquer la perte des communications TCP.

Découverte de voisins

Processus d'auto configuration

> L'algorithme de la procédure d'auto configuration d'adresse se décompose de la manière suivante :

- Création de l'adresse lien-local.

- L'attachement aux groupes de multicast sollicités
- Vérification de l'unicité.
- Acquisition d'un message d'annonce du routeur pour déterminer la méthode d'obtention de l'adresse unicast globale.

> S'il existe un routeur sur le lien, la machine doit appliquer la méthode indiquée par le message d'annonce de routeurs :

- L'auto configuration sans état,
- L'auto configuration avec état.

> Si aucun routeur n'existe sur le lien, la machine doit essayer d'acquérir l'adresse unicast globale par la méthode d'auto configuration avec état.

Création de l'adresse lien-local

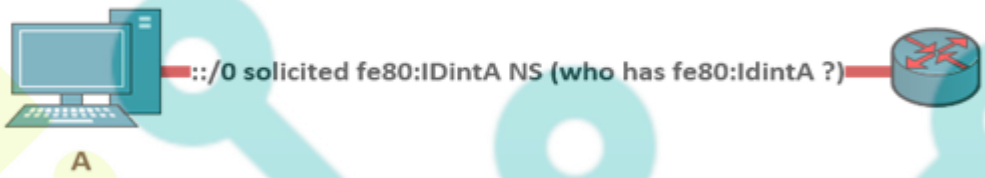
À l'initialisation de l'interface, l'équipement construit un identifiant pour l'interface qui doit être unique au lien.

Cet identifiant utilise l'adresse EUI-64, on additionne le préfixe avec l'identifiant. Dans le cas de l'adresse de lien local c'est le préfixe **FE80::/64** qui est alloué. L'adresse possède un état provisoire et l'adresse ne peut pas être utilisée avant d'avoir vérifiée sont unicité.

Création de l'adresse lien-local

> Comme dans le cadre de la création de l'adresse lien-local, **l'adresse unicast globale** est obtenue en concaténant le préfixe avec l'identifiant de l'interface.
> Le préfixe est fourni via un message d'annonce de routeurs.

Détection d'adresse dupliquée (DAD)



Pour vérifier l'unicité des adresses lien-local ou unicast, les machines doivent exécuter un algorithme de Détection d'Adresse Dupliquée (DAD) avant de les utiliser.

L'algorithme utilise les messages ICMPv6 sollicitation d'un voisin et annonce d'un voisin. Une adresse est qualifiée de "provisoire" pendant l'exécution de l'algorithme DAD et ce jusqu'à la confirmation de son unicité.

Une adresse provisoire est assignée à une interface uniquement pour recevoir les messages de sollicitation et d'annonce d'un voisin. Les autres messages reçus sont ignorés. L'algorithme DAD utilise un message de sollicitation d'un voisin avec dans le champ adresse cible l'adresse provisoire.

Afin de différencier l'algorithme DAD de celui de découverte des voisins, le paquet IPv6 DAD de message de sollicitation d'un voisin a comme adresse de source l'adresse indéterminée.

- **Si un message annonce d'un voisin est reçu** l'adresse provisoire est déjà utilisée comme adresse valide par une autre machine. L'adresse n'est pas retenue.
- **Si un message de sollicitation d'un voisin est reçu** lors de la procédure DAD l'adresse provisoire est également sollicitée pour une autre machine. L'adresse provisoire ne peut être utilisée par aucune des machines.
- **Si rien n'est reçu au bout d'une seconde**, l'adresse provisoire est unique, elle passe de l'état de provisoire à celle de valide et est assignée à l'interface.

L'adresse unicast obtenue par auto configuration sans état ne nécessite pas la procédure DAD car l'unicité de l'identifiant de l'interface a déjà été contrôlé dans l'étape de création de l'adresse lien-local.

Si l'adresse lien-local n'est pas unique, l'auto configuration s'arrête et une intervention manuelle est nécessaire.

Si l'adresse lien-local est unique alors, l'adresse provisoire devient une adresse utilisable pour l'interface. La première phase de l'auto configuration est achevée.

Les réseaux NBMA

Les réseaux NBMA (*Non Broadcast Multiple Access*) ne peuvent pas utiliser la diffusion, c'est pourquoi, le protocole de découverte de voisins possède un mode NBMA appelé OffLink qui n'autorise le dialogue qu'avec un routeur.

L'équipement arrivant dans le réseau, émet un message Router Sollicitation en utilisant l'adresse de destination **ff02::2** (tous les routeurs du lien) et le réseau NBMA relai ce message vers un routeur.

Le routeur répond en positionnant le bit **L** (OffLink) à 1 dans l'option Information sur le préfixe, indiquant que tous les échanges devront passer par lui.

- L'équipement construit son adresse globale en concaténant le préfixe à son identifiant d'interface.
- L'équipement envoie systématiquement tous les paquets à l'adresse physique du routeur et celui-ci les réémet vers le bon destinataire. Cependant, le routeur peut également émettre un message **ICMP Redirect** pour informer l'équipement de la véritable adresse du destinataire et les paquets suivants ne transiteront plus par le routeur central.

Les réseaux Mobiles

Le processus DAD peut être relativement long. Dans ce cas, un équipement peut tenter plusieurs fois de résoudre sa propre adresse avant de la garantir unique.

Dans le cadre de la mobilité, ce délai qui s'ajoute à ceux propre à la téléphonie pourrait poser des problèmes. L'astuce choisie fait intervenir le concept appelé DAD optimiste (*optimistic DAD*).

L'état de recherche d'unicité est remplacé par l'état optimiste qui permet l'utilisation de cette adresse. Cependant, le processus classique continue parallèle.

Les messages **NS** (Neighbor sollicitation) sont émis avec le bit **O** (Override) à 0 pour que les caches **ND** (Neighbor Discovery) ne soit pas mis à jour au cas où cette adresse serait déjà utilisée sur le réseau.

DHCPv6

DHCPv6 utilise des messages de protocole UDP.

- Les clients DHCPv6 écoutent les messages DHCP sur le port UDP 546.
- DHCPv6 et les agents de relais écoutent les messages DHCPv6 sur le port UDP 547.

> f1bb74f1bb74Il n'y a aucune adresse de diffusion définie pour IPv6. Par conséquent, l'utilisation de l'adresse de diffusion limitée pour certains messages DHCPv4 a été remplacée par l'utilisation de l'adresse **All_DHCP_Relay_Agents_and_Servers (FF02::1)**

L'adressage sans état n'est pas stable (changement de carte, changement dans le temps) et les adresses peuvent être choisies aléatoirement ou construites avec l'adresse MAC.

Dans le cadre d'une configuration avec état, l'adresse est stable et convient aux éléments réseau qui ne doivent pas varier dans le temps (serveur, tunnel…) Cette configuration permet de fournir au préalable les adresses à assigner, de centraliser les configurations et d'automatiser le mécanisme d'assignement.

L'architecture

- Client : équipement ayant besoin d'une adresse
- Serveur : élément fournissant les adresses
- Relais : élément qui transmet les requêtes au serveur
- Requestor : élément de supervision et d'administration du serveur

Un client DHCPv6 utilise le message DHCPv6 SOLICIT pour découvrir les serveurs configurés pour lui fournir des adresses IPv6 ou des paramètres de configuration du réseau. Le client DHCPv6 envoie ce message à l'adresse multicast FF02::1:2 qui identifie le groupe des serveurs et relais (ALL_DHCP_Relay_Agents_And_Servers).

L'adresse de destination est une adresse de diffusion sélective. L'adresse IPv6 "source" utilisée est l'adresse locale au lien de cette interface.

DHCPv6 sans état

Pour un réseau IPv6 disposant de routeurs configurés pour attribuer des préfixes d'adresses sans état pour les hôtes IPv6, le DHCPv6 peut indiquer des paramètres DNS (serveur, nom de domaine) et les autres paramètres de configuration qui ne sont pas inclus dans le message d'annonce de routeur.

DHCPv6 avec état

Dans le cadre d'une configuration DHC, les messages sont les suivants :

- **Découverte du serveur** – SOLICIT, ADVERTISEE
- **Informations de configuration** – REQUEST, REPLY
- **Gestion des ressources allouées au client** – RENEW, RELEASE
- **Relayage des messages** – RELAY-FWD, RELAY-REPLY

Les différents messages

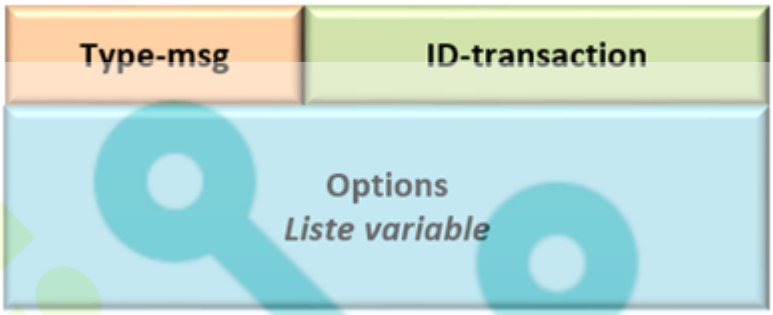
Code	Message	Utilisation	Equivalence v4
1	SOLICIT (client)	Localise les serveurs DHCP	Discover
2	ADVERTISE (serveur)	Annonce la disponibilité du serveur DHCPv6.	Offer
3	REQUEST (client)	Demande des adresses et/ou des paramètres de configuration au serveur choisi.	Request
4	CONFIRM (client)	Indique au serveur qui a alloué les adresses et les paramètres que ces derniers sont adaptés au lien auquel le client est raccordé.	Request
5	RENEW (client)	Prolonge le bail et actualise les paramètres de configuration auprès du serveur qui les a alloués.	Request
6	REBIND (client)	Obtient un bail et actualise les paramètres de configuration auprès de tout serveur en cas de non réponse au message RENEW	Request
7	REPLY (serveur)	Réponse à un message SOLICIT, REQUEST, REBIND, RELEASE reçu d'un client.	Ack
8	RELEASE (client)	Indique au serveur que le client n'utilise plus d'adresses IPv6.	Release
9	DECLINE (client)	Signale au serveur qu'une ou des adresses allouées par le serveur sont déjà utilisées sur le lien du client.	Decline
10	RECONFIGURE (serveur)	Signale au client que le serveur a de nouveaux paramètres ou les a actualisés.	N/A
11	INFORMATION-REQUEST (client)	Demande des paramètres de configuration au serveur, sans lui demander d'adresse.	Inform
12	RELAY-FORWARD (relais)	Relaye des messages vers un serveur DHCPv6. Le message relayé (celui du client DHCPv6 ou du relais précédent) est placé dans l'option RELAY-FORW de ce message.	N/A
13	RELAY-REPLY (serveur)	Envoie un message à un client via un relais. Le relais extrait le message destiné au client ou au relais suivant contenu dans l'option "message relayé» afin de lui remettre.	N/A

Message DHCP

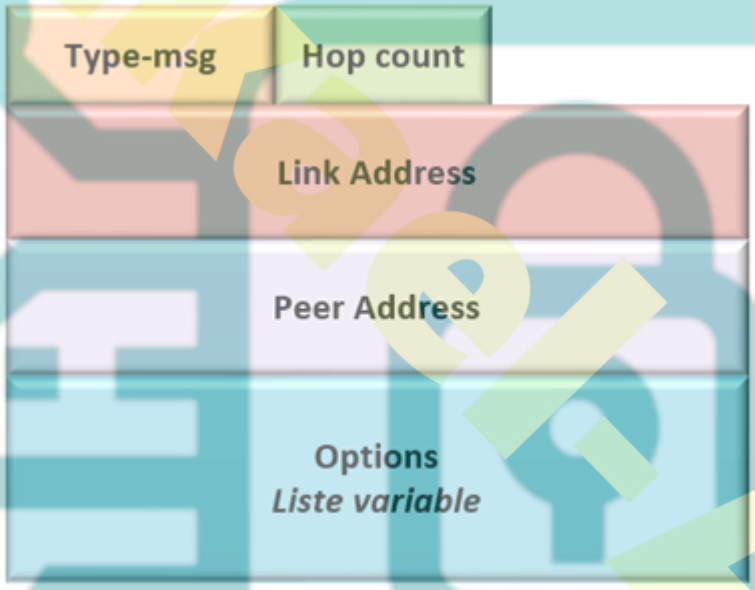
Le champ **type de message** identifie la nature du message DHCPv6. Il est codé sur un octet.

Le champ **ID** identifie une transaction (question/réponse). Il permet d'associer les réponses aux requêtes correspondantes (pallie le fait qu'UDP ne gère pas le séquencement des réponses si plusieurs demandes arrivent simultanément). Il est codé sur 3 octets.

Le champ **OPTIONS** transporte, soit les adresses IPv6, soit les paramètres de configuration du réseau (hors adresse IPv6) nécessaires au fonctionnement du réseau.



MESSAGE DHCPV6 RELAY-FORWARD (RELAIS VERS SERVEUR)



- **Type-msg** = 12.
- **Hop-count** – indique le nombre de relais traversés par ce message pour atteindre le serveur.
- **Link-address** – adresse unicast (globale ou locale) qui sera utilisée par le serveur pour identifier le lien sur lequel est localisé le client. C'est l'adresse unicast (globale ou locale) du relais côté du client.
- **Peer-address** – adresse du client ou du relais depuis laquelle le message à relayer a été reçu (elle est extraite de l'adresse source du paquet du message reçu). Elle permet d'identifier l'interface du relais derrière laquelle se trouve le client, (elle sera utilisée comme adresse de destination du paquet contenant le message RELAY-REPLY).
- **Option list** – contient (Relay Message Option) et éventuellement d'autres options ajoutées par le relais.

MESSAGE DHCPV6 RELAY-REPLY (SERVEUR VERS RELAIS)

- **Type-msg** = 13
- **Hop-count** – indique le nombre de relais que ce message traversera pour atteindre le client.
- **Link-address et Peer-address** – les adresses du lien et du pair sont recopiées à partir du message RELAY-FORWARD précédent.
- **Option list** – réponse du serveur DHCPv6 destinée au client DHCPv6.

Authentification des messages

L'authentification de la source et l'intégrité du contenu des messages DHCP permet de se protéger de certaines attaques.

DHCPv6 Unique IDentifier

Afin de connaître l'état des ressources gérées, le serveur DHCP crée une liste d'associations entre le paramètre attribué et le client.

Le serveur référence le client par un identifiant unique, le DUID (DHCP Unique Identifier).

Une station peut, générer un DUID à partir de l'adresse MAC d'une de ses cartes réseau. Elle le conservera alors comme identifiant, même lors du changement de carte.

Les clients utilisent les DUID pour identifier le serveur qui leur a alloué des adresses IPv6 et/ou des paramètres de configuration du réseau.

CRÉATION D'UN DUID

1. **DUID-LLT** (Link-Layer address plus Time) combinaison d'une adresse physique et d'une horodate.
2. **DUID-EN** (Vendor-assigned unique ID based on Enterprise Number) dérivé d'un numéro de constructeur ou d'un numéro unique affecté par un constructeur.
3. **DUID-LL** (Link-Layer address) dérivé de l'adresse MAC d'une interface de réseau.

Association d'identité

Une Association d'identité (IA) est une construction à travers laquelle un serveur et un client peuvent s'identifier, grouper et gérer un ensemble adresses d'IPv6.

Un client doit associer au moins une IA distincte à chacune de ses interfaces réseau pour lesquelles il a demandé l'attribution adresses d'IPv6 à un serveur DHCP. Le client utilise les IA assignées à un interface pour obtenir des informations de configuration à partir d'un serveur.

Types d'adresses

Un serveur DHCPv6 peut allouer des adresses non temporaires et des adresses temporaires.

Allocation des adresses non temporaires

Le serveur choisit les adresses d'un client en fonction du lien du client, du DUID du client, des options fournies par le client, et des informations fournies par le relais DHCPv6.

Les adresses allouées font l'objet d'une écriture dans le fichier des baux.

Allocation des adresses temporaires

Une **adresse temporaire** IPv6 contient un numéro de 64 bits généré de manière aléatoire en tant qu'ID d'interface, plutôt que l'adresse MAC d'une interface.

Options du protocole DHCPv6

Chaque option est codée en format : type, longueur, valeur

Code	Options	Utilisation
1	OPTION_CLIENTID	Identification du client
2	OPTION_SERVERID	Identification du serveur
3	OPTION_IA_NA	Association d'identités pour les options d'adresse non temporaire
4	OPTION_IA_TA	Association d'identités pour les options d'adresse temporaire
5	OPTION_IAADDR	Adresse associée à IA_NA ou IA_TA
6	OPTION_ORO	Identifie une liste d'options dans les messages échangés entre un client
7	OPTION_PREFERENCE	Annonce au client la priorité du serveur DHCPv6 et comment gérer cette priorité.
8	OPTION_ELAPSED_TIME	Temps écoulé depuis le démarrage d'un échange pour la machine qui tente d'achever sa configuration.
9	OPTION_RELAY_MSG	Transporte un message DHCPv6 relayé dans des messages relay-forward ou relay-reply.
11	OPTION_AUTH	Transporte les informations d'authentification de l'identité et du contenu des messages DHCPv6.
12	OPTION_UNICAST	Permet au serveur d'indiquer au client qu'il peut utiliser l'adresse individuelle (unicast) du serveur pour échanger avec lui.
13	OPTION_STATUS_CODE	Indique le statut du message DHCPv6 qui transporte cette option.
14	OPTION_RAPID_COMMIT	Permet, dans un message SOLICIT, à un client, de demander ce mode de fonctionnement pour réaliser des échanges en deux temps au lieu de quatre. Le serveur doit inclure cette option dans la réponse correspondante (Solicit reply).
15	OPTION_USER_CLASS	Définit la classe d'utilisateur associée à un utilisateur ou à une application.
16	OPTION_VENDOR_CLASS	Identifie le constructeur du matériel utilisé par le client.
17	OPTION_VENDOR_OPTS	Permet que le client et le serveur échangent des informations spécifiques d'un constructeur.
18	OPTION_INTERFACE_ID	Identifie l'interface de réception du message du client DHCPv6.
19	OPTION_RECONF_MSG	Indique, dans un message reconfiguration, si le client doit répondre par un message renew ou information-request.
20	OPTION_RECONF_ACCEPT	Indique à un serveur si le client accepte ou refuse les messages reconfigure ou annonce à un client qu'il peut ou non accepter les messages reconfigure.

Il existe également des options pour les serveurs SIP, DNS, NIS, NTP, MIP6, KERBEROS, RADIUS

Renumérotation des réseaux

La renumérotation peut utiliser 2 méthodes : passive ou active.

Renumérotation passive

Dans la renumérotation passive, chaque machine du réseau dispose de deux adresses IPv6, une ancienne et une nouvelle. L'ancienne adresse est utilisée par les communications en cours.

Ces communications sont préservées aussi longtemps que nécessaire. Cependant, les nouvelles communications sont établies à l'aide de la nouvelle adresse. La renumérotation est terminée lorsque la dernière machine du réseau cesse d'utiliser son ancienne adresse.

Renumérotation active

Le serveur DHCPv6 force les clients à cesser d'utiliser leur ancienne adresse à une date donnée. Le serveur réduit la durée de vie des anciennes adresses en fonction de la date d'échéance cible.

Dès la date d'échéance, aucune utilisation d'ancienne adresse n'est possible. Toutes les communications utilisant les anciennes adresses sont arrêtées.

Avenir de DHCPv6

DHCP est un service très lié à IPv4, dans IPv6, la notion d'adresses temporaires (baux DHCP) a peu de sens en IPv6 car le mécanisme de gestion des adresses et déjà présent et le nombre d'adresses disponibles est quasiment illimité.

Alternative à DHCP

La mise en œuvre de DHCP impose la gestion de deux protocoles, Neighbor Discovery pour la configuration sans état de l'adresse IPv6 et DHCPv6.

Le RFC 5006 propose de manière expérimentale, la possibilité d'utiliser une option supplémentaire dans les messages RA pour permettre de réduire les temps de configuration d'un équipement ce qui est intéressant dans le cas de la mobilité.

L'option peut contenir plusieurs adresses de serveur DNS récursifs, mais il en faut obligatoirement 1 au minimum.
Elle contient un champ **durée de vie** (Lifetime) qui permet d'indiquer le temps maximum (en secondes) pendant lequel ces informations peuvent être prises en considération. La valeur doit être supérieure à la période d'émission des RA. La valeur **0xFFFFFFFF**

indique une durée infinie et la valeur **0** informe que des paramètres précédemment annoncés ne doivent plus être pris en compte.

> Plusieurs pistes alternatives à DHCPv6 sont envisagées comme l'utilisation d'adresses anycast pour découvrir le « bon » routeur.

Adresses Multicast

Cette adresse spécifie un groupe d'interfaces appartenant au groupe de diffusion. Elle peut être permanente ou temporaire.

Typiquement, une vidéo-conférence est temporaire. L'étendue de la diffusion peut être indiquée, ce qui permet d'indiquer si la demande doit être confinée au lien local, au site, ou au-delà.

Le préfixe vaudra ff00::/8

Les bits du flag sont utilisés pour indiquer des cas particuliers (adresse dynamique ou permanente par exemple).

- **Si le bit T=0** il pourra être distribué aux chaines de TV sur internet par exemple. **Si le bit T=1**, c'est une adresse temporaire.
- Le bit O est réservé à une utilisation future
- **Le bit P=1** est dérivé de l'adresse unicast, le **bit P=0**, est pour les points de rendez-vous (nœud central d'un arbre multicast).

La portée des messages

Le scope est utilisé pour indiquer si la portée du message est globale, site ou locale.

Tableau des scopes

Etendue (en hexa)	Etendue
0	Reserved
1	Interface Local Scope
2	Link Local Scope
3	Realm Local Scope
4	Admin Local Scope
5	Site Local Scope
8	Organization Local Scope
E	Global Scope
F	Reserved
Identifiants du groupe	
Valeur 0	Reserved de ff00:: à ff0f::
Valeur 1	
ff01::1	Toutes les interfaces du nœud
ff02::1	Tous les nœuds du lien
Valeur 2	
ff01::1	Tous les routeurs du nœud
ff01::1	Tous les routeurs du lien
ff01::1	Tous les routeurs du site

Ces adresses n'ont pas de portée sur internet par exemple, elles ne sont valables que pour le multicast au sein d'un site.

Exemple d'adresses permanentes avec une portée pour les serveurs NTP (RFC 3307)

- ff01::101 = tous les serveurs sur la même interface
- ff02::101 = tous les serveurs sur le même lien
- ff05::101 = tous les serveurs sur le même site
- ff0e::101 = tous les serveurs de l'internet

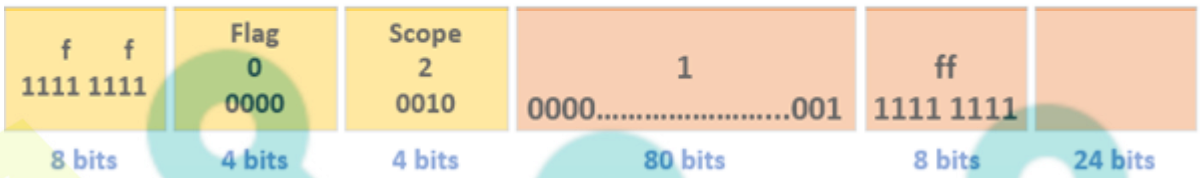
Adresse multicast sollicitée

C'est un type @multicast prédéfini.

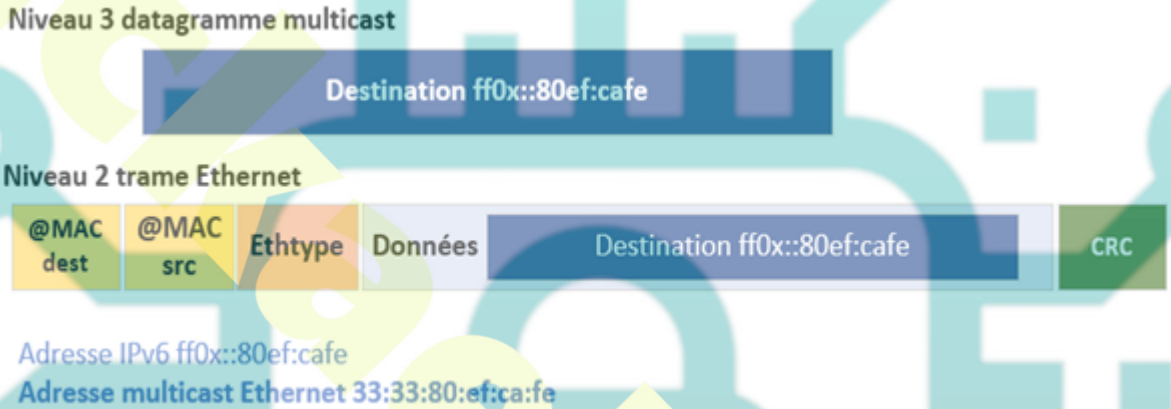
Comme Ipv6 interdit le broadcast, les protocoles comme la découverte de voisins (équivalent de l'ARPv4) doivent utiliser une adresse de multicast.

Pour être plus efficaces, au lieu d'utiliser l'@ff02::1 qui correspond à l'@ de tous les équipements, elle se construit à partir d'une adresse unicast en concaténant le préfixe réservé **ff02::1:ff00:0/104** aux 24 bits de poids faible de l'adresse unicast ou anycast.

ff02::1::ff00:0/104 + 24 bits de poids faible de l'adresse unicast/anycast



Correspondance @multicast niveau 3 et niveau 2



Les 4 derniers octets de l'adresse IPv6 sont concaténés avec l'adresse MAC multicast 33fb33 (par exemple avec cafe)

Adresse temporaire

Les adresses temporaires sont des adresses multicast IPv6 dont le bit T est positionné à 1

Il existe plusieurs types d'adresses temporaires :

- Celles qui sont générales,
- Celles dérivées d'un préfixe unicast,
- Les adresses multicast "Embedded-RP"
- Les adresse SSM.

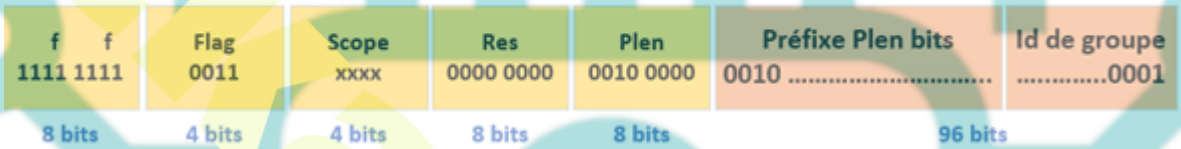
Une @ temporaire n'est valable que dans la portée donnée ainsi une adresse site local ff15::999 sur un site 1 n'a aucune relation avec la même @temp sur un site 2.

Ces adresses peuvent être utilisable pour une utilisation lors d'une Visio conférence ponctuelle par exemple.

ADRESSES MULTICAST DÉRIVÉES D'UN PRÉFIXE UNICAST

- Les drapeaux RP ont un bit 01,
- Le champ réservé ne contient que des bits à 0
- Le champ préfixe longueur (PLEN) contient la longueur du préfixe unicast permettant de dériver le préfixe multicast
- le champ préfixe contient la valeur effective du préfixe.
- Le champ identifiant de groupe à une taille de 32 bits.

ff3x20:2001:660::/32 (renater)
ff3x20:2001:660:cafe:deca

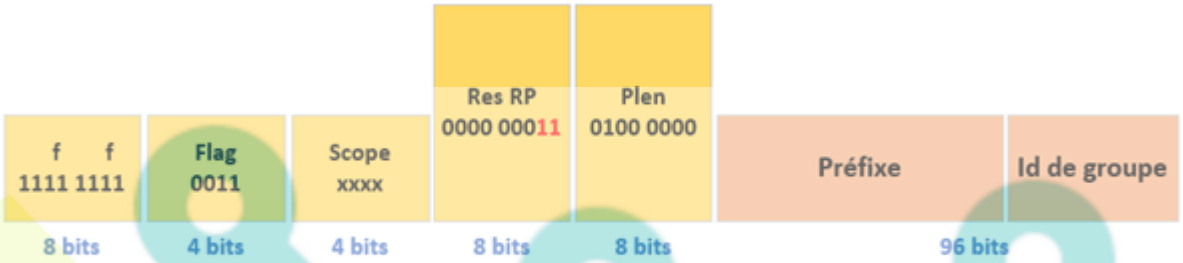


ADRESSE MULTICAST EMBARQUANT UN POINT DE RENDEZ-VOUS

Elle sert à inclure l'adresse du RP (Point de Rendez-Vous qui sert à la construction de l'arbre multicast dans l'adresse multicast IPv6.

- Embedded RP et Bit RT à 1
- Le champ RP prend les 4 derniers bits du point de rendez-vous

Dans l'exemple suivant, on prend la valeur 3 (11)



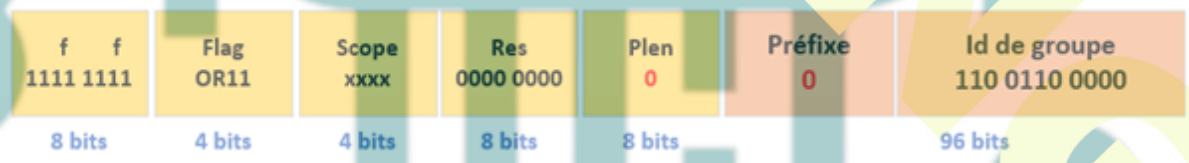
Point de rendez-vous d'adresse unicast 2001:660:3307:125:3/64
Adresse multicast embarquant ce point de RDV = ff7x:340:2001:660:3307:125:deca:cafe

Le champ LEN prend la longueur du préfixe de point de rdv 40 (0100 0000)

Point de rendez-vous d'adresse unicast 2001:660:3307:125:3/64
Adresse multicast embarquant ce point de RDV = ff7x:340:2001:660:3307:125:deca:cafe

Adresse multicast à source spécifique (SSM)

C'est une adresse dans laquelle les seuls paquets qui sont délivrés à un récepteur sont ceux qui proviennent d'une adresse de source spécifique demandée par le récepteur (permet de réduire les demandes sur le réseau et permet d'améliorer la sécurité).



Seules les adresses dérivées du préfixe ff3x::/96 sont utilisables pour l'instant

Gestion des abonnements sur le lien-local : MLD

Pour offrir un service de distribution multicast, deux composants sont nécessaires : **un protocole de gestion de groupe multicast** et **un protocole de construction d'arbre multicast**. En IPv6, ce protocole est **MLD** (*Multicast Listener Discovery*). Il est utilisé par un

routeur de bordure IPv6 pour découvrir la présence de récepteurs multicast sur ses liens directement attachés, ainsi que les adresses multicast concernées.

MLD est un sous-protocole d'ICMPv6, les messages MLD sont des messages ICMPv6 particuliers. Ils sont envoyés avec :

- une adresse source IPv6 lien-local ;
- le champ "nombre de sauts" fixé à 1 ;
- l'option "IPv6 Router Alert" activée.

Construction de l'arbre multicast : PIM

PIM est le protocole qui permet de construire l'arborescence de distribution de multidiffusion dans un environnement de routage global IPv4 ou IPv6 (pas MPLS) à partir d'une source de flux et d'un ensemble d' abonnés de multidiffusion.

Un flux de multidiffusion est identifié de manière unique par quelques adresses nommées (S; G) :

- L'adresse IP de la source: une adresse IPv6 unicast
- L'adresse IP de multidiffusion d'un groupe de multidiffusion: une IP IPv4 (plage 224/8) ou IPv6 (plage FF00 :: / 8)

Habituellement, les abonnés finaux ne connaissent pas la ou les sources d'un flux de multidiffusion donné, mais uniquement l'adresse de groupe de celui-ci. Ils ont utilisé un protocole comme IGMPv2 ou MLDv1 qui fournit simplement des interfaces pour «rejoindre» ou «quitter» un groupe de multidiffusion G. donné.

> NB: Les protocoles améliorés comme IGMPv3 ou MLDv2 offrent la possibilité de transmettre également la source associée S d'un groupe G donné.

les informations SSM (Source Specific Information) se réfèrent à un flux spécifique (S; G).

RP: ROUTEUR RENDEZ-VOUS POINT :

- Il permet, tout d'abord, de savoir où se trouvent les sources de multidiffusion au sein du réseau. Via un mécanisme d'enregistrement, un routeur frontière, directement connecté à une source, enregistre les informations SSM, liées au flux reçu, sur le routeur RP (rendez-vous point).
- En parallèle, un routeur frontière directement connecté aux abonnés finaux rejoint l '«arbre partagé» (alias arborescence RP) entre lui-même et le RP le plus proche qui gère le groupe G.

Exemple

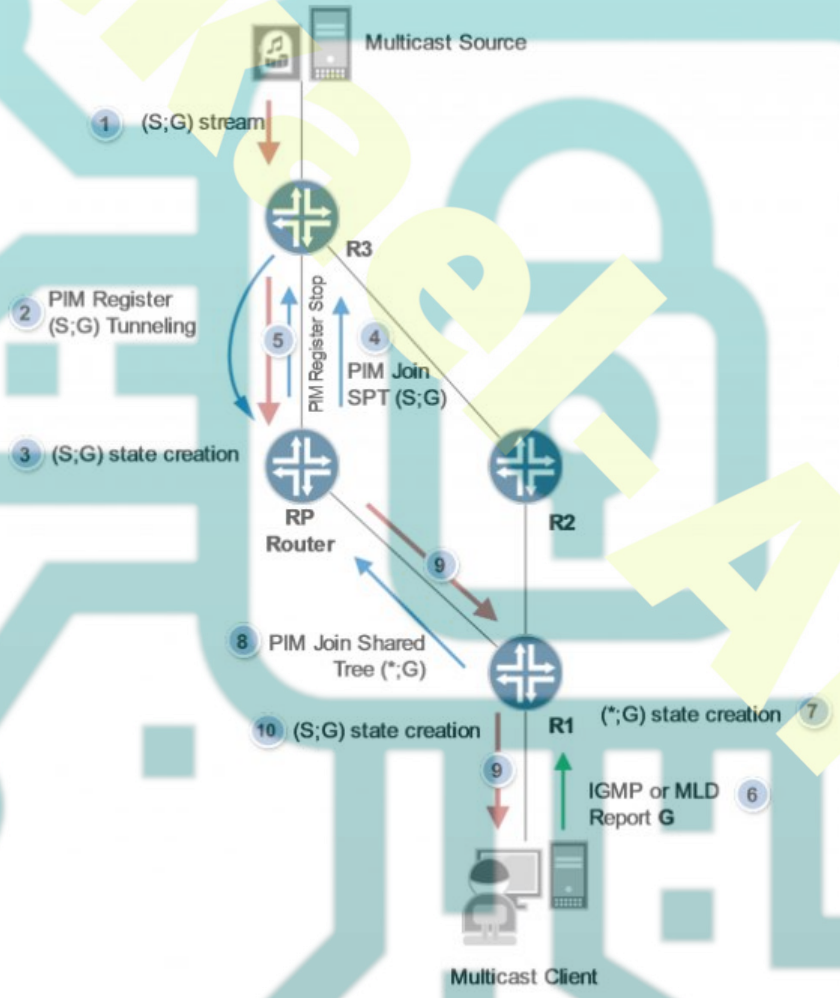


Schéma 1

1- Une source S commence à diffuser un flux de multidiffusion sur une adresse G. Le flux est noté (S; G)

2- Premier routeur directement connecté à la Source S, enregistre le flux en encapsulant le trafic multicast dans les messages de registre PIM

(datagrammes unicast). Ces messages atteignent le routeur RP

3- Le routeur RP crée des entrées (S; G) et (*; G).

4- Le routeur RP renvoie un message PIM Join (S; G) vers la source (il suit le chemin inverse)

5- Lorsque RP commence à recevoir nativement le flux (S; G) via le SPT (**S**hort **P**ath **T**ree), il arrête le processus d'enregistrement en envoyant un message d'arrêt de registre PIM vers le routeur frontière.

6- En parallèle un abonné multicast pour G apparaît et envoie un abonnement IGMPv2 ou MPLDv1 pour G.

7- Le routeur directement connecté crée l'état (*; G)

8- Ensuite, il envoie un PIM Join (*; G) vers le RP (il suit le chemin inverse)

9- RP envoie le flux de multidiffusion qui suit l'arborescence partagée jusqu'à l'abonné de multidiffusion.

10- En analysant le trafic multicast, le routeur du dernier saut crée maintenant l'état (S; G).

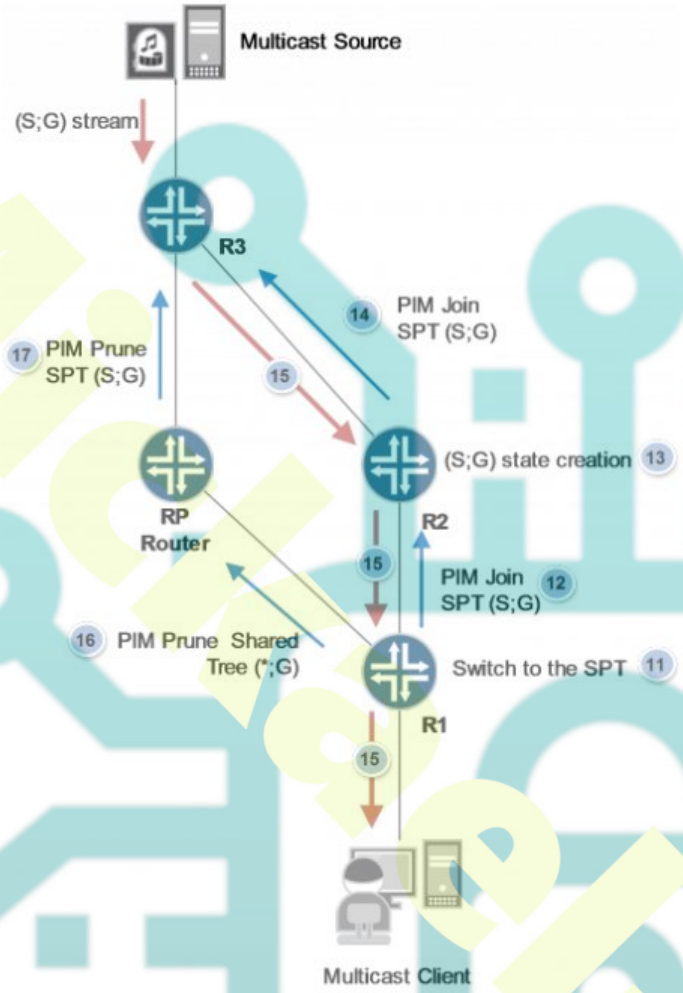


Schéma 2

11- Il passe au SPT.

12- Il envoie un message **PIM Join** vers la source (il suit le chemin inverse)

13- Entrée de création de routeur intermédiaire (S; G)

14- Et transmet le message **PIM Join (S; G)** vers la source.

15- Lorsque le routeur du premier bond reçoit le message de jointure (S; G), il commence à envoyer le trafic de multidiffusion vers l'abonné de multidiffusion

16- Lorsque le routeur du dernier saut commence à recevoir le flux (S; G) via le SPT, il déleste l'arbre partagé en envoyant un message PIM Prune pour (*; G) vers le RP

17- RP déleste ensuite le SPT s'il n'y a plus de routeurs sur l'arbre partagé en envoyant un message PIM Prune pour (S; G) vers la source.