Sommaire

Chapitre 2

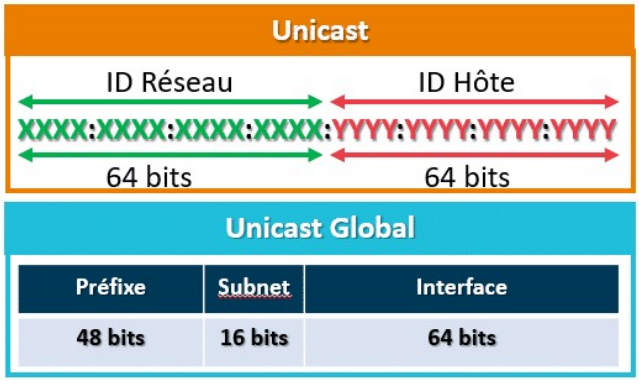
Configuration dynamique des adresses IPv6

Introduction

Chaque poste de travail et chaque interface des équipements réseaux active vont avoir deux types d'adresse ipv6:

Une adresse unicast global :

- Similaire aux adresses publiques en IPv4.
- Elles sont routables sur internet.
- De la forme : 2000::/3



Une adresse unique local : non routable

- Elles permettent à des équipements de communiquer entre eux, sans avoir besoin d'aller vers l'extérieur.
- L'avantage de ces adresses, c' est qu'elles se configurent automatiquement.
- De la forme : FE80::/10

Unique Local			
Préfixe	ID Globale	Subnet	Interface
8 bits	40 bits	16 bits	64 bits

I. Terminologie IPv6

- Un **lien** (*link*) est le support physique (ou la facilité telle un tunnel) de communication entre deux noeuds au niveau de la couche 2 liaisons de données/accès réseau (technologies LAN/WAN).
- Deux **noeuds** sur le même lien sont voisins (neighbors).
- Une **interface** est l'attachement d'un noeud au lien.
- Une **adresse** est un identifiant pour une interface (Unicast) ou pour un ensemble d'interfaces (Multicast). Une interface peut avoir plusieurs adresses IPv6 et être inscrite dans plusieurs groupes Multicast.
- Un **préfixe** désigne l'appartenance à un domaine IPv6.
- Le masque donne l'étendue du domaine IP : il se note après l'adresse et une barre oblique / ("slash"). Il indique le nombre de bits fixes dans une adresse

II. Méthodes de configuration des adresses ipv6

1. Présentation

Une adresse IPv6 attribuée à une interface est constituée d'un préfixe de 64 bits et d'un identifiant d'interface de 64 bits.

Un identifiant d'interface peut être créé de différentes manières :

- **Statique :** 2001:db8:14d6:1::1/64, 2001:db8:14d6:1::254/64, fe80::101, par exemple.
- **Autoconfiguration (SLAAC)** :

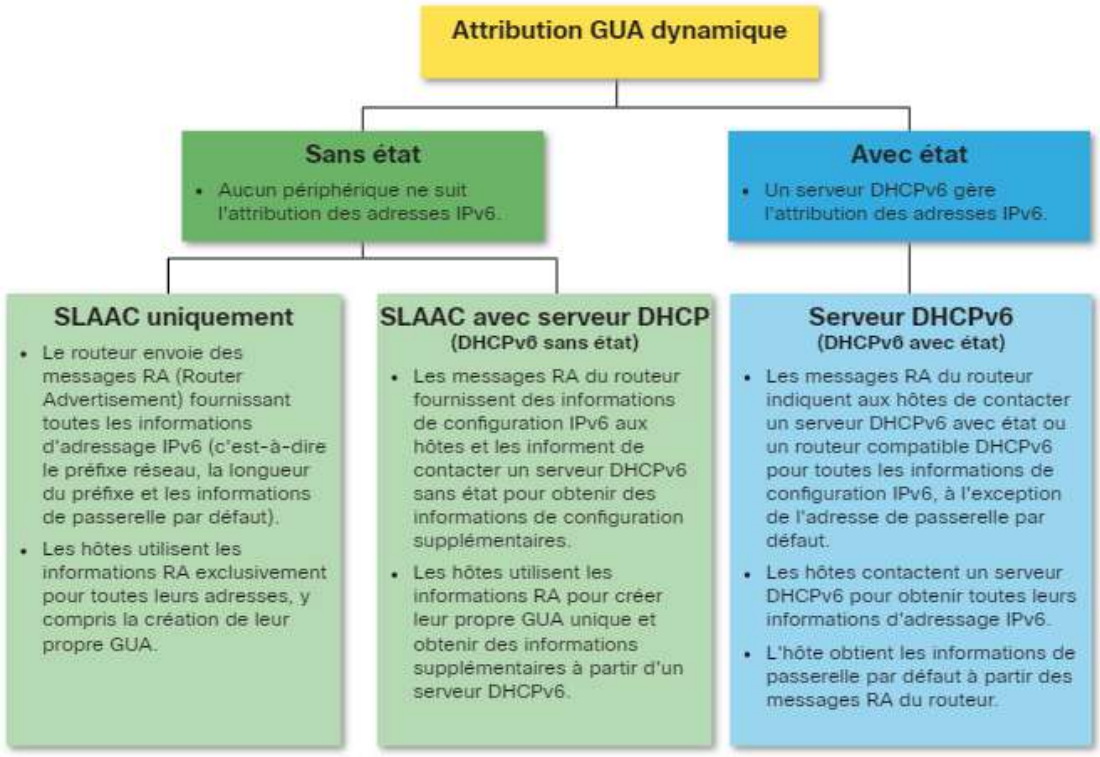
  en utilisant l'une de ces trois méthodes :

1. MAC EUI-64, par défaut (RFC 4291)
2. tirage pseudo-aléatoire, par défaut chez Microsoft, Ubuntu, Mac OSX (RFC 4941)
3. CGA, peu implémenté (RFC 3972)

- **Dynamique :** DHCPv6 (RFC 3315) stateful, si le client est installé et activé (par défaut sur Microsoft Windows et Mac OSX)

2. Choix de la méthode de configuration

Par défaut, un routeur compatible IPv6 annonce ses informations IPv6. Cela permet à un hôte de créer ou d'acquérir dynamiquement sa configuration IPv6.



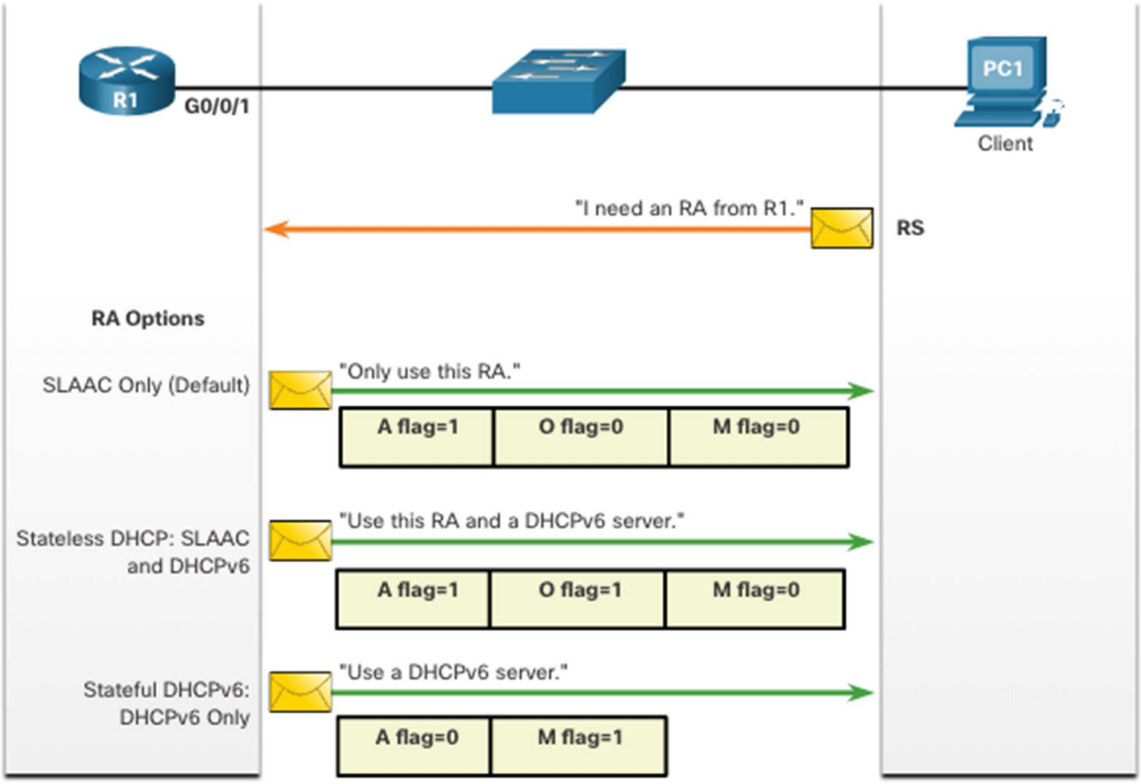
La décision de la façon dont un client obtiendra une GUA IPv6 dépend des paramètres du message RA.

Un message RA ICMPv6 comprend trois indicateurs permettant d'identifier les options dynamiques disponibles pour un hôte, comme suit:

- **Indicateur A** - Il s'agit de l'indicateur Address Autoconfiguration. Utilisez l'autoconfiguration des adresses sans état (SLAAC) pour créer un GUA IPv6.

- **Indicateur O** - Il s'agit de l'indicateur Autre configuration. D'autres informations sont disponibles à partir d'un serveur DHCPv6 sans état.
- **Indicateur M** - Il s'agit de l'indicateur de configuration des adresses gérées. Utilisez un serveur DHCPv6 avec état pour obtenir une GUA IPv6.

En utilisant différentes combinaisons des indicateurs A, O et M, les messages RA informent l'hôte des options dynamiques disponibles.



Remarque :

Bien que les systèmes d'exploitation hôtes suivent la suggestion de RA, la décision réelle revient finalement à l'hôte.

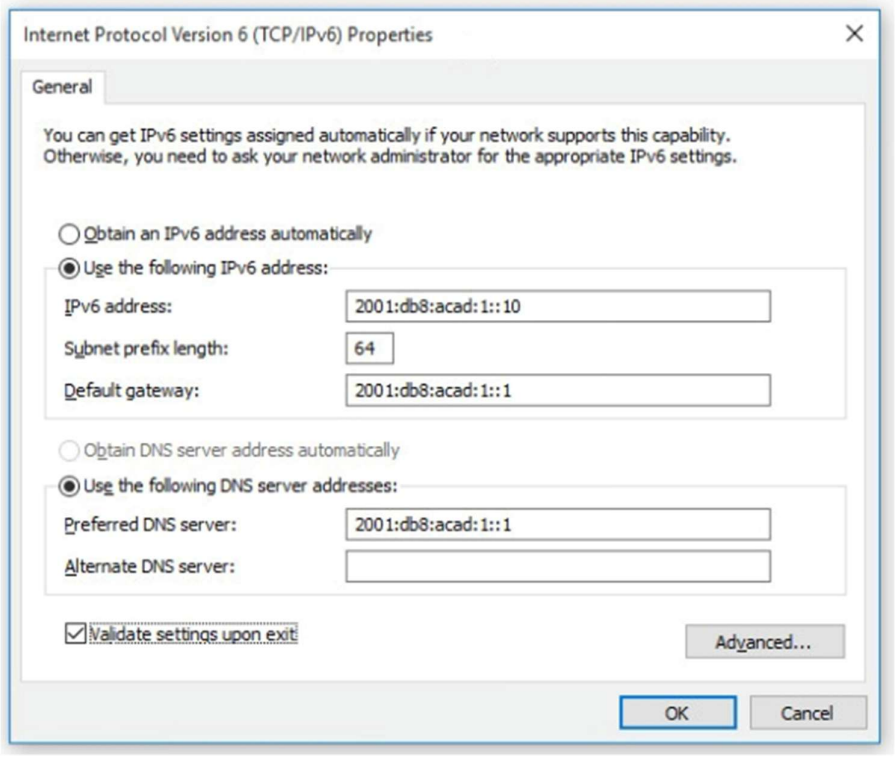
III. Configuration statique(manuelle)

1. Description

Configuration manuelle d'un hôte

Un hôte Windows peut être configuré manuellement avec une configuration d'adresse GUA [1]IPv6, comme illustré dans la figure ci-dessous :

[1] GUA (Golbal Unicat Address) : Adresses de monodiffusion globale



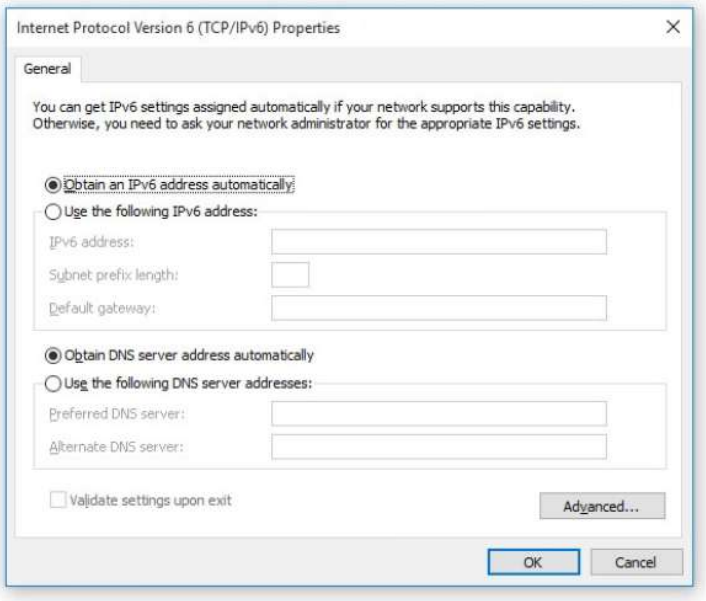
Configuration manuelle(statique) d'un routeur

Sur un routeur, une adresse de monodiffusion globale (GUA) IPv6 est configurée manuellement à l'aide de la commande de configuration ipv6 address ***ipv6-address/prefix-length*** interface.

2. Inconvénients

La saisie manuelle d'un GUA IPv6 peut prendre beaucoup de temps et est quelque peu exposée aux erreurs.

Par conséquent, la plupart des hôtes Windows sont activés pour acquérir dynamiquement une configuration GUA IPv6 :

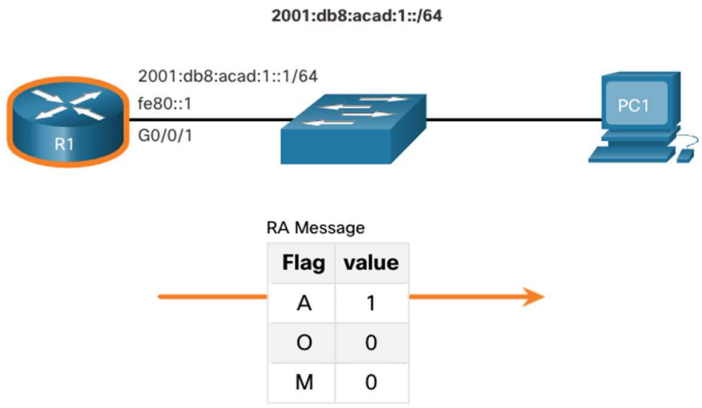


IV. Auto configuration d'adresse sans état (SLAAC)

Avec l'auto-Configuration des machines, les nœuds peuvent obtenir une adresse globale IPv6 de manière automatique via une auto-configuration sans état,

Cette méthode repose sur le protocole Neighbor Dicovery,

Périphérique doit utiliser le préfixe, la longueur du préfixe et l'adresse de la passerelle par défaut contenus dans le message d'annonce de routeur. Aucune information n'est acquise auprès d'un serveur DHCPv6.



En utilisant le SLAAC, un hôte acquiert généralement ses informations de sous-réseau IPv6 de 64 bits du routeur RA. Cependant, il doit générer le reste de l'identifiant d'interface (ID) de 64 bits en utilisant l'une des méthodes suivantes :

1. EUI-64

a. Description

MAC EUI-64 est une est des méthodes de configuration automatique des ID d'interface qui se fonde sur l'adresse MAC IEEE 802 (48 bits).

On passe d'une adresse codée sur 48 bits à 64 bits en insérant 16 **FF:FE** au milieu de l'adresse MAC entre les 24 premiers bits et les 24 derniers bits. De plus, la méthode exige que le 7ième bits de poids fort de l'adresse soit inversé passant de la valeur "Local" à "Universal" d'où ce terme "EUI64 Modified".

b. Inconvénients

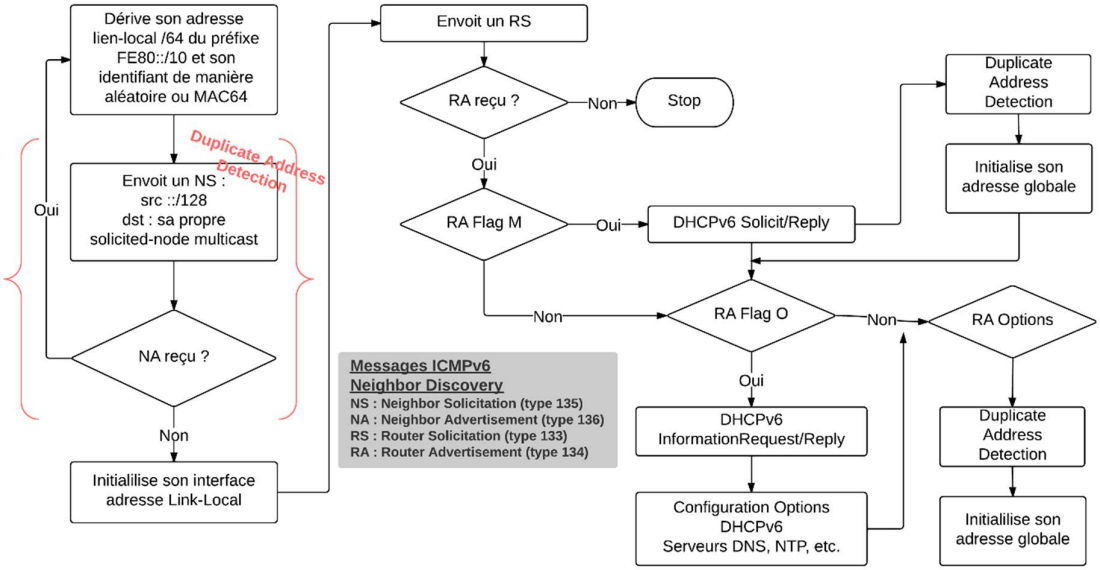
S'ils offrent l'avantage d'être uniques, les suffixes basés sur des informations immuables (adresses matérielles) peuvent poser des problèmes de confidentialité et de sécurité.

En effet, un tel suffixe étant toujours identique pour une interface donnée, il devient très facile de tracer une personne sur son lieu de travail ou à son domicile afin d'en retirer des informations cruciales : horaires de travail, présence ou non au domicile, itinérance d'un terminal entre le domicile et le lieu de travail, etc.

Adresse stable mais machine facilement identifiable, usage déconseillé par l'IETF depuis 2017

Illustration du mécanisme SLAAC

1. Toute interface activée en IPv6 génère une adresse "Link Local" avec le préfixe FE80::/10 suivi d'un identifiant d'interface.
2. Elle vérifie l'existence de l'adresse générée via un mécanisme appelé DAD (Duplicate Address Detection).
3. Sans réponse, elle peut utiliser cette adresse sur le lien local.
4. Elle sollicite un routeur en Multicast.
5. S'il est présent sur le réseau, le routeur IPv6 répond avec des paramètres de configuration RA et Options.
6. L'interface élabore son ou ses adresses selon ce qu'indique le routeur. Elle installe sa passerelle par défaut.
7. Régulièrement, l'interface va vérifier l'existence des noeuds voisins appris par processus ND (NUD).



Mécanisme Stateless Automatic Auto Configuration (SLAAC)

2. Méthode de Génération aléatoire

a. Description

Méthode autoconfiguration avec tirage pseudo aléatoire, l'adresse change dans le temps

autoconfiguration basée sur une clé secrète et sur le préfixe réseau, ne dévoile pas l'adresse MAC et est stable pour chaque préfixe réseau, c'est l'usage recommandé pour une adresse fixe

utilisation d'adresses générées cryptographiquement, qui lient l'adresse à la clé publique du client et qui peuvent être utilisées par SEND.

Il existe deux méthodes de génération différentes. La première La L'une comme l'autre crée un hash (MD5 prévu, mais d'autres algorithmes peuvent être considérés) du résultat qui sert par la suite de suffixe à l'adresse IPv6.

Méthode	Description	Avantages	Inconvénients
	se repose sur l'usage des suffixes précédemment générés afin de créer un nouveau suffixe, nécessitant du même fait une unité de stockage.	plus performante	nécessite une unité de stockage
	seconde méthode ne stocke aucune information, et crée à la volée des	autonomie intéressante puisqu'elle ne se repose pas sur une	besoin de générer à chaque fois des suffixes

	suffixes afin d'engager le même processus que précédemment.	unité de stockage potentiellement faillible (corruption des données, défectuosité, …) et recrée l'ensemble du mécanisme à chaque fois.	

a. Inconvénients

Renouveler régulièrement l'adresse d'une interface, évitant du même fait la potentielle exploitation des informations liées au mouvement d'une entité (homme ou machine), évitant dès lors de l'exposer trop fortement à des attaques ciblées.	Reposer sur des algorithmes de génération aléatoire performants

Remarque :

Toutefois, il n'est pas exempt de défaut, et certaines applications et services peuvent refuser de fonctionner correctement avec des adresses aléatoires, notamment s'ils tentent de faire correspondre un nom d'hôte avec un enregistrement DNS. Dès lors, l'usage d'adresses temporaires aléatoires se doit de rester une option du système, mais aussi des applications souhaitant l'utiliser.

3. Méthode cryptographique

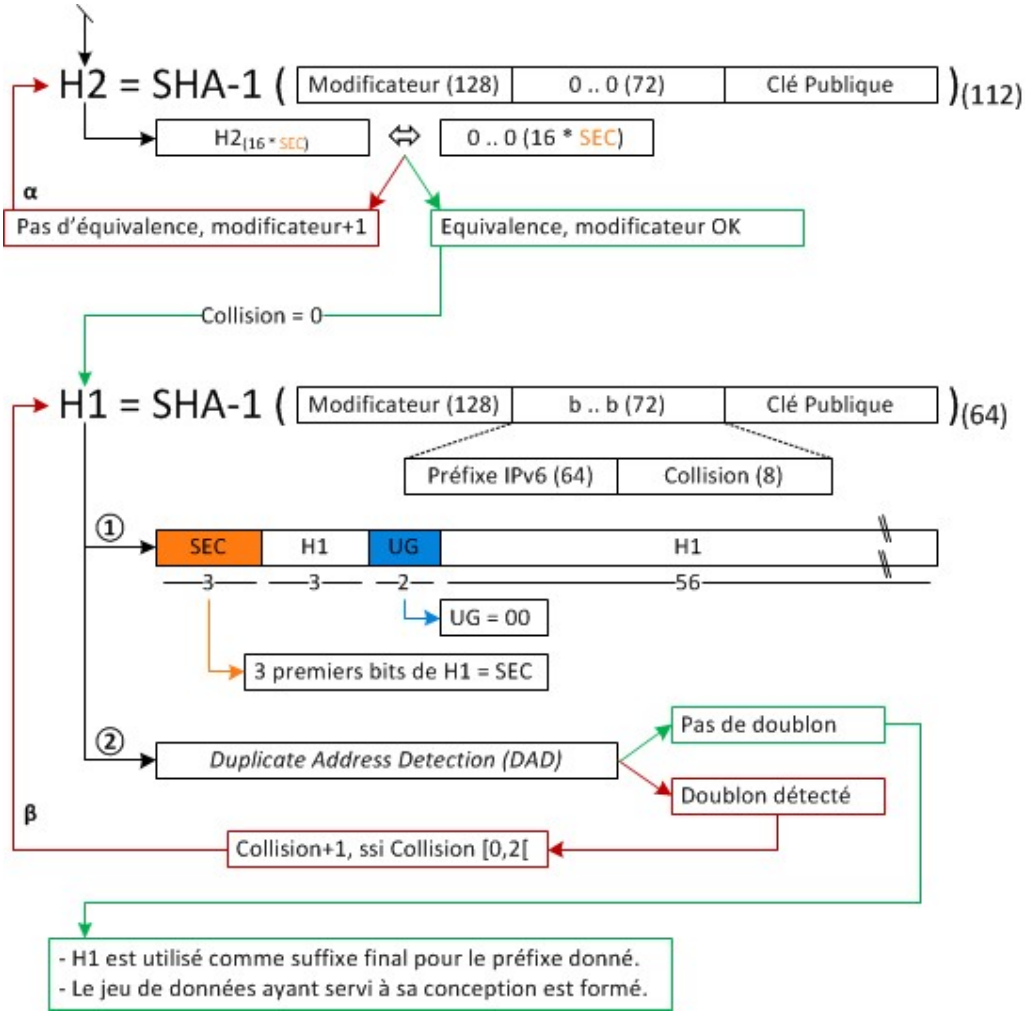
Définit une procédure permettant de créer, à partir de la clé publique de l'hôte, un identifiant d'interface à accoler à notre préfixe IPv6. Se reposant sur des notions cryptographiques, les mécanismes peuvent s'avérer rapidement complexes.

Si la clé publique représente le paramètre principal sur lequel se repose l'ensemble des mécanismes, il serait trop simplifier de définir le suffixe trouvé comme étant les 64 premiers bits du hash SHA-1 de celle-ci. En effet, de nombreux autres paramètres entrent en ligne de compte, permettant d'assurer l'authenticité, l'unicité et la confidentialité des informations utilisées pour créer le suffixe. L'approche cryptographique est majoritairement utilisée dans le cadre de SEND (*SEcure Neighbor Discovery*), et de ce fait nécessite des procédures robustes permettant de confirmer et valider une adresse en particulier. Ces paramètres sont les suivants :

- Un modificateur, soit une valeur de 128 bits (16 octets) aléatoires ou pseudo aléatoires.
- La clé publique en elle-même.

- Le préfixe IPv6.
- Un compteur de collision.
- Une série de 9 octets à 0 (soit 72 bits à 0 ou 18 digits hexadécimaux).

Deux étapes successives permettent de créer puis de valider le suffixe définit. Ces deux étapes sont décrites dans les figures suivantes. La première étape consiste à générer le suffixe à partir de la clé publique.



Il est intéressant de noter ici que la génération de H2 peut boucler pendant un certain temps (boucle α) avant qu'une correspondance soit trouvée. Cette correspondance sera d'autant plus compliquée à déterminer que le paramètre de sécurité SEC sera grand (dont la valeur est, pour rappel, comprise entre 0 et 7). Définir SEC = 0 permet de rentre l'ensemble du processus plus rapide, mais réduit d'autant la pertinence sécuritaire de cette approche. A l'heure actuelle, un paramètre SEC = 7 garantit un niveau de sécurisation infaillible (sur base des ressources accessibles actuellement).
La seconde étape, quant à elle, se déroule non pas au niveau de l'hôte détenteur de la clé publique, mais de sa destination. Celle-ci va opérer des vérifications à partir du premier jeu de

données reçu, correspondant aux paramètres utilisés pour générer le suffixe. Dans le cas où la moindre erreur surviendrait (incohérence ou résultat différent), le processus est immédiatement stoppé et la procédure complète doit être réinitialisée.

V. Détection des adresses dupliquées

Le processus permet à l'hôte de créer une adresse IPv6. Cependant, il n'y a aucune garantie que l'adresse est unique sur le réseau.

Le processus DAD (Duplicate Address Detection) est un mécanisme, est utilisé par un hôte, qui permet vérifier l'unicité d'une adresse auto-configurée sur un réseau (RFC 4862, section 5.4)

DAD est implémenté en **utilisant ICMPv6**. Pour effectuer le DAD, l'hôte envoie un message **ICMPv6 Neighbor Solicitation (NS)** avec une adresse multidiffusion spécialement construite, appelée adresse multicast de nœud sollicité. Cette adresse duplique les **24 derniers bits de l'adresse IPv6 de l'hôte.**

Si aucun autre appareil ne répond avec un **message NA,** alors l'adresse est pratiquement garantie d'être unique et peut être utilisée par l'hôte. *Si un NA est reçu par l'hôte, alors l'adresse n'est pas unique, et le système d'exploitation doit déterminer un nouvel ID d'interface à utiliser.*

IETF (Internet Engineering Task Force) recommande que la fonction DAD soit utilisée sur toutes les adresses de monodiffusion IPv6, qu'elle soit créée à l'aide de SLAAC uniquement, obtenue à l'aide de DHCPv6 avec état ou configurée manuellement.

DAD n'est pas obligatoire car un ID d'interface 64 bits fournit 18 possibilités de quintillion et la possibilité qu'il y ait une duplication est distante. Toutefois, la plupart des systèmes d'exploitation exécutent DAD sur toutes les adresses monodiffusion IPv6, quelle que soit la façon dont l'adresse est configurée.

Durée de vie des adresses IPv6

Les adresses IPv6 associées à une interface ont une durée de vie déterminée. La durée de vie est en général infinie, mais on peut configurer :

- Durée de vie préférée
- Durée de vie de validité.

Ces durées de vie sont configurées dans les routeurs qui fournissent les préfixes pour la configuration automatique (RA, Router Advertisement).

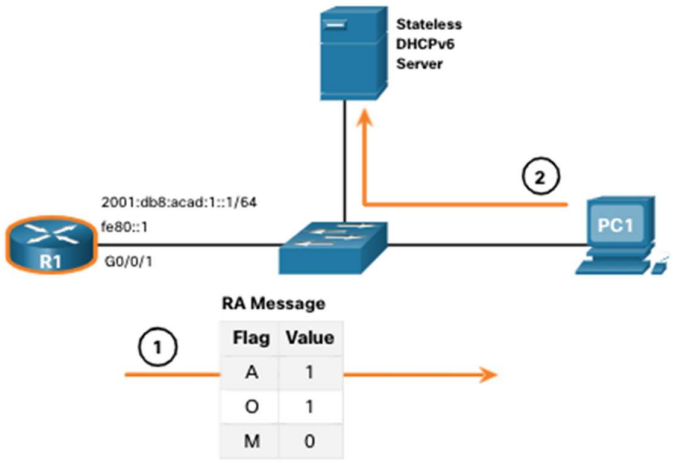
En combinaison avec un changement DNS correspondant, ces durées de vie permettent une transition progressive vers une nouvelle adresse IPv6 (appartenant à un nouveau fournisseur de service par exemple) sans interruption de service.

Quand la durée d'utilisation d'une adresse dépasse la durée préférée, elle n'est plus utilisée pour les nouvelles connexions. Quand sa période de validité est atteinte, elle est supprimée de la configuration de l'interface.

VI. DHCP « sans état »

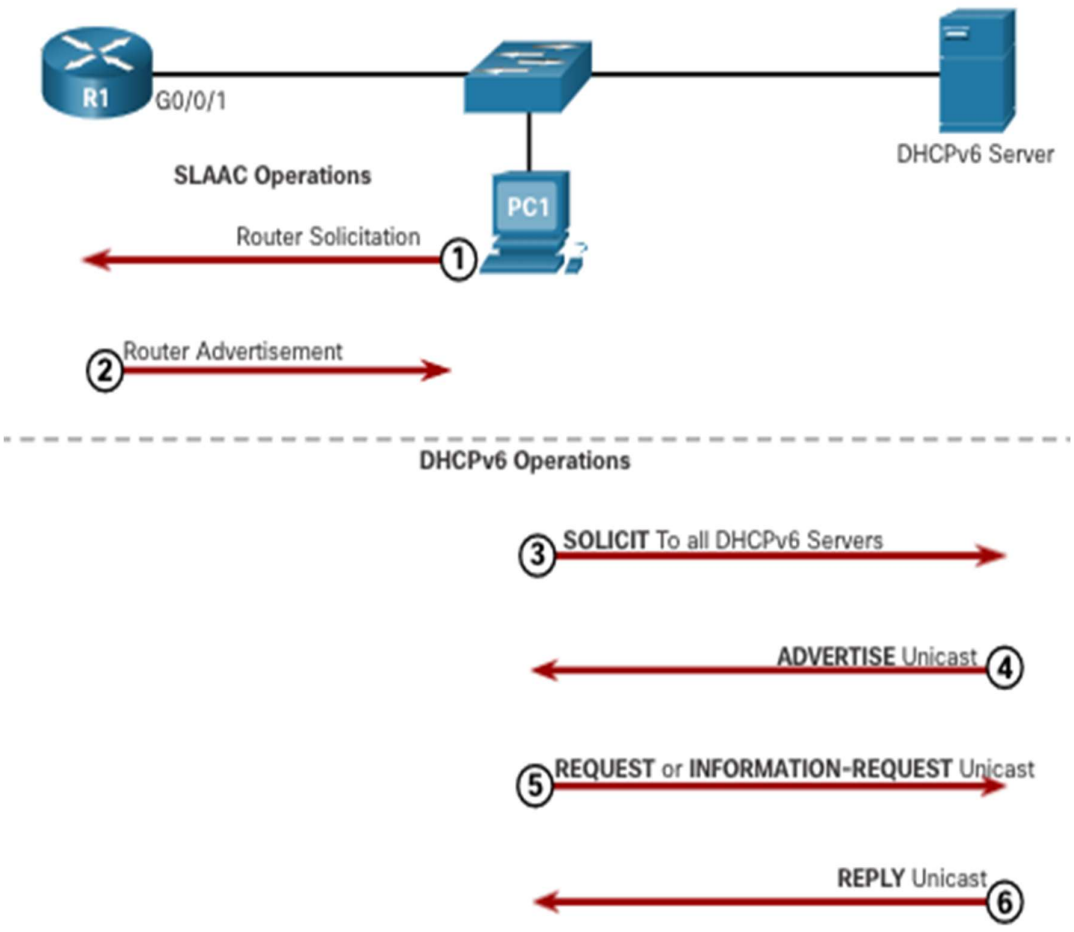
Si une RA indique la méthode DHCPv6 sans état, l'hôte utilise les informations contenues dans le message RA pour l'adressage et contacte un serveur DHCPv6 pour obtenir des informations supplémentaires.

Remarque: Le serveur DHCPv6 fournit uniquement des paramètres de configuration pour les clients et ne gère pas une liste de liaisons d'adresses IPv6



VII. DHCP « avec état »

Le périphérique ne doit pas utiliser les informations contenues dans le message d'annonce de routeur en tant qu'informations d'adressage. Au lieu de cela, le périphérique utilise le processus de découverte et d'interrogation d'un serveur DHCPv6 pour obtenir toutes ses informations d'adressage. Ces informations incluent une adresse de monodiffusion globale IPv6, la longueur du préfixe, une adresse de passerelle par défaut et les adresses des serveurs DNS. Dans ce cas, le serveur DHCPv6 agit en tant que serveur DHCP avec état, tout comme le DHCP pour l'IPv4. Le serveur DHCPv6 attribue et contrôle les adresses IPv6 afin de ne pas attribuer la même adresse IPv6 à plusieurs périphériques.


R1
G0/0/1
DHCPv6 Server
SLAAC Operations
PC1
Router Solicitation
1
2
Router Advertisement
DHCPv6 Operations
3
SOLICIT To all DHCPv6 Servers
ADVERTISE Unicast
4
5
REQUEST or INFORMATION-REQUEST Unicast
REPLY Unicast
6