Concepts de routage et commutation

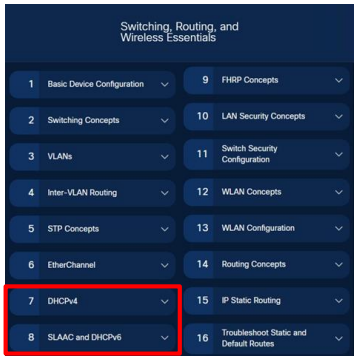
Chapitre 3

Cours de M. Petein Thomas

Email : thomas.petein@heh.be

Chapitre 3

UE - Télécommunications et réseaux – Routing & Switching



Chapitre 3

But du chapitre

Ce chapitre a pour but d'aborder le Dynamic Host Configuration Protocol.

Dans ce module, on parlera tout d'abord du protocole DHCPv4, qui est la version utilisée pour l'IPv4. On verra comment configurer un routeur Cisco IOS afin qu'il joue le rôle de serveur DHCPv4. Ensuite, vous apprendrez comment configurer un routeur Cisco IOS en tant que client.

Dans la deuxième partie de ce chapitre on abordera l'adressage IPv6 dans son ensemble. On étudiera en particulier certains types d'adresses spécifiques.

Finalement dans la troisième on abordera les protocoles d'adressage dynamique pour un réseau IPv6. On verra comment utiliser SLAAC pour permettre aux hôtes de créer leur propre adresse de monodiffusion globale IPv6. On verra également comment configurer un routeur Cisco IOS pour être un serveur DHCPv6, un client DHCPv6 ou un agent de relais DHCPv6.

Chapitre 3

Introduction au DHCP

Les administrateurs réseau attribuent des adresses IP statiques aux routeurs, aux serveurs, aux imprimantes et aux autres périphériques réseau dont les emplacements (physique et logique) sont peu susceptibles de changer.

Il s'agit généralement de périphériques qui fournissent des services aux utilisateurs et aux périphériques sur le réseau. Par conséquent, les adresses qui leur sont affectées doivent rester constantes.

Cependant, dans une entreprise, les ordinateurs et les utilisateurs changent souvent d'emplacements physique et logique. Il peut être difficile et fastidieux pour les administrateurs d'attribuer de nouvelles adresses IP chaque fois qu'un employé se déplace.

L'introduction d'un serveur DHCP (Dynamic Host Configuration Protocol) sur le réseau local simplifie l'affectation des adresses IP aux périphériques mobiles et de bureau.

L'utilisation d'un serveur DHCP centralisé permet aux entreprises de gérer toutes les attributions d'adresses IP dynamiques à partir d'un serveur unique.

Cette pratique permet d'optimiser la gestion des adresses IP et garantit la cohérence à l'échelle de l'entreprise, y compris dans les filiales.

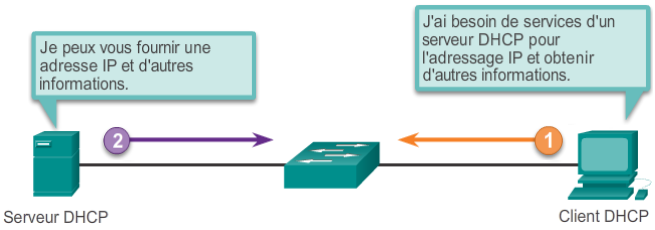
DHCPv4

Commençons par le fonctionnement d'un serveur DHCPv4.

Le protocole DHCPv4 attribue les adresses IPv4 et d'autres informations de configuration réseau de façon dynamique.

Un serveur DHCPv4 dédié est évolutif et relativement facile à gérer. Le serveur DHCPv4 attribue dynamiquement, ou loue, une adresse IPv4 à partir d'un pool d'adresses pour une période limitée choisie par le serveur, ou jusqu'à ce que le client n'ait plus besoin de l'adresse.

Cependant, dans le cas d'une petite filiale ou d'un bureau à domicile, un routeur Cisco peut être configuré pour fournir les services DHCPv4, évitant ainsi l'achat d'un serveur dédié.



Le DHCPv4 comprend trois mécanismes d'allocation d'adresses, offrant ainsi de la souplesse lors de l'attribution d'adresses IP :

- **Allocation manuelle** : l'administrateur attribue une adresse IPv4 préallouée au client et le DHCPv4 communique uniquement l'adresse IPv4 au périphérique.

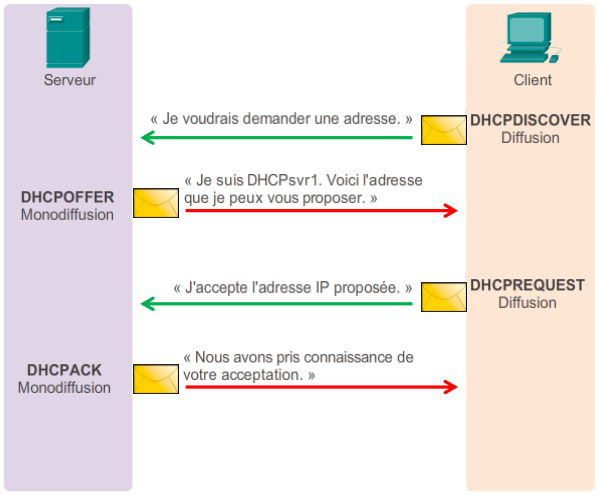
- **Allocation automatique** : DHCPv4 attribue de façon automatique et permanente une adresse IPv4 statique à un périphérique en sélectionnant cette adresse dans un pool d'adresses disponibles. Il n'y a pas de bail et l'adresse est attribuée de façon permanente au périphérique.

- **Allocation dynamique** : DHCPv4 attribue ou loue dynamiquement une adresse IPv4 d'un pool d'adresses pour une durée limitée définie par le serveur, ou jusqu'à ce que le client n'ait plus besoin de l'adresse. = le mécanisme DHCPv4 le plus répandu !

Lorsque vous utilisez l'allocation dynamique, les clients louent les informations au serveur pendant une période définie par l'administrateur. Les administrateurs configurent les serveurs DHCPv4 pour que les baux dépassent le délai d'attente à différents intervalles.

Le bail dure généralement entre 24 heures et une semaine voire plus. À l'expiration du bail, le client doit demander une autre adresse, même s'il obtient généralement la même.

Fonctionnement de l'allocation dynamique (4 étapes)



Chapitre 3

Etape 1 :

Lorsque le client démarre (ou qu'il souhaite se connecter à un réseau), il envoie un message DHCPDISCOVER.

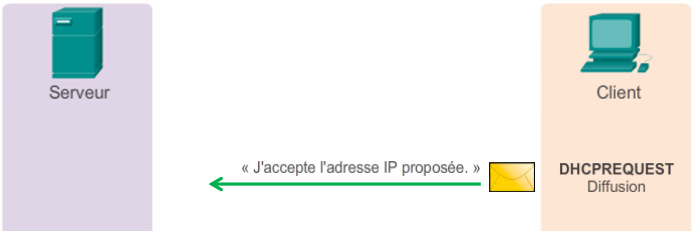
Ce message a pour but de détecter les serveurs DHCPv4 disponibles. Le périphérique client y indique sa propre adresse MAC et, vu qu'il ne possède par encore d'adresse IP, il utilisera les adresses de diffusion de couche 2 et de couche 3 pour communiquer avec le serveur.

Etape 2 :

Lorsque le serveur DHCPv4 reçoit un message DHCPDISCOVER, il réserve une adresse IPv4 disponible pour la louer au client.

Le serveur crée également une entrée ARP comprenant l'adresse MAC du client demandeur et l'adresse IPv4 louée du client.

Le serveur DHCPv4 envoie le message DHCPOFFER de liaison au client demandeur. Le message DHCPOFFER est envoyé en monodiffusion et utilise l'adresse MAC de couche 2 du serveur comme adresse source et l'adresse MAC de couche 2 du client comme destination.



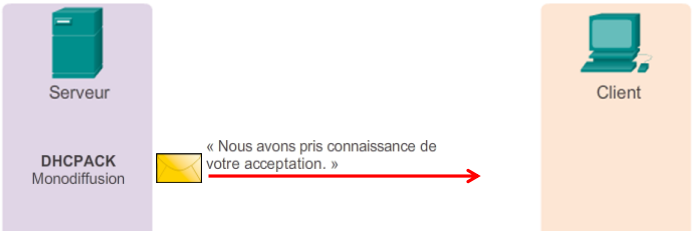
Etape 3 :

Lorsque le client reçoit le message DHCPOFFER du serveur, il renvoie un message DHCPREQUEST.

Ce message est utilisé à la fois pour émettre le bail et pour le renouveler.

Lorsqu'il est utilisé pour émettre le bail, le message DHCPREQUEST sert d'avis d'acceptation de la liaison au serveur sélectionné pour les paramètres qu'il a proposé et d'avis implicite de refus de tous les autres serveurs qui peuvent avoir fourni au client une offre de liaison.

Le message DHCPREQUEST est envoyé sous forme de diffusion afin d'informer ce serveur DHCPv4 et tous les autres que l'offre a été acceptée.



Etape 4 :

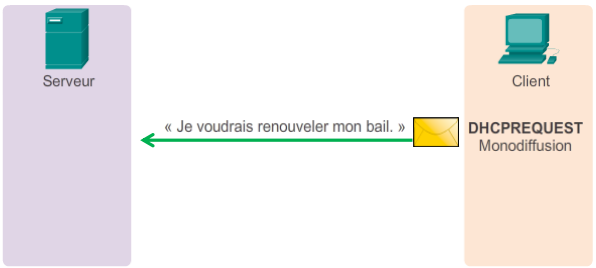
Lorsqu'il reçoit le message DHCPREQUEST, le serveur vérifie les informations de bail à l'aide d'une requête ping ICMP envoyée à cette adresse pour s'assurer qu'elle n'est pas encore utilisée.

Ensuite il crée une entrée ARP pour le bail du client, puis répond par un message de monodiffusion DHCPACK.

Lorsque le client reçoit le message DHCPACK, il consigne les informations de configuration et lance une recherche ARP sur l'adresse attribuée. Si la requête ARP n'obtient aucune réponse, le client comprend que l'adresse IPv4 est valide et se l'approprie.

Cas du renouvellement de bail :

Avant l'expiration du bail, le client commence un processus en deux étapes pour renouveler le bail avec le serveur DHCPv4.

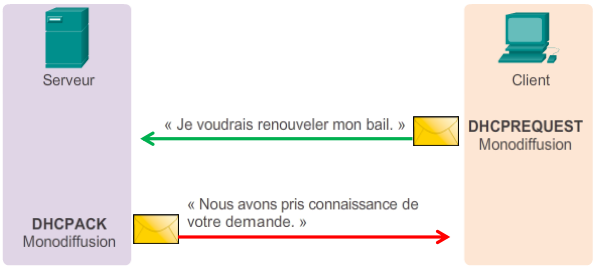


Avant l'expiration du bail, le client envoie un message DHCPREQUEST directement au serveur DHCPv4 qui a offert l'adresse IPv4 à l'origine.

S'il ne reçoit aucun message DHCPACK dans un certain délai, le client diffuse un autre message DHCPREQUEST afin qu'un des autres serveurs DHCPv4 puisse renouveler le bail.

Chapitre 3

Cas du renouvellement de bail :



À la réception du message DHCPREQUEST, le serveur vérifie les informations relatives au bail en renvoyant un DHCPACK.

Remarque : Ces messages (principalement le DHCPOFFER et le DHCPACK) peuvent être envoyés en unicast ou diffusés selon la norme IETF RFC 2131.

Chapitre 3

Au niveau du format de message utilisé par le DHCPv4. Les messages DHCPv4 sont encapsulés dans le protocole de transport UDP. Ceux envoyés par le client utilisent le port source UDP 68 et le port de destination 67

8	16	24	32
Code OP (1)	Type de matériel (1)	Longueur de l'adresse matérielle (1)	Sauts (1)
Identificateur de transaction			
Secondes - 2 octets		Indicateurs - 2 octets	
Adresse IP du client (CIADDR) - 4 octets			
Votre adresse IP (YIADDR) - 4 octets			
Adresse IP du serveur (SIADDR) - 4 octets			
Adresse IP de la passerelle (GIADDR) - 4 octets			
Adresse matérielle du client (CHADDR) - 16 octets			
Nom du serveur (SNAME) - 64 octets			
Nom du fichier de démarrage - 128 octets			
Options DHCP - variable			

Chapitre 3

- **Code OP (opération)** : indique le type de message général. Si la valeur est 1 = message de requête et si la valeur est 2 = message de réponse.
- **Type de matériel** : identifie le type de matériel utilisé sur le réseau (1 correspond à Ethernet et 20 à une ligne série).
- **Longueur de l'adresse matérielle** : indique la longueur de l'adresse.
- **Sauts** : contrôle le transfert des messages. Défini sur 0 par le client avant la transmission d'une requête.
- **Identificateur de transaction** : utilisé par le client pour mettre en correspondance la demande avec les réponses reçues des serveurs DHCPv4.
- **Secondes** : indique le nombre de secondes qui se sont écoulées depuis le début de la tentative d'acquisition ou de renouvellement d'un bail par un client. Utilisé par les serveurs DHCPv4 pour hiérarchiser les réponses lorsque plusieurs requêtes de client sont en attente.
- **Indicateurs** : utilisés par un client qui ne connaît pas son adresse IPv4 lorsqu'il envoie une requête. Un seul des 16 bits est utilisé, l'indicateur de diffusion. La valeur 1 dans ce champ indique au serveur DHCPv4 ou à l'agent de relais recevant la requête que la réponse doit être envoyée sous forme de diffusion.

HEH.be Sciences et technologies

Chapitre 3

- **Adresse IP du client** : champ utilisé par un client pendant le renouvellement de bail lorsque l'adresse du client est valide et utilisable, mais pas au cours du processus d'acquisition d'une adresse. Le client place sa propre adresse IPv4 dans ce champ si et seulement si il dispose d'une adresse IPv4 valide alors qu'il est relié ; sinon, il définit ce champ sur 0.
- **Votre adresse IP** : champ utilisé par le serveur pour attribuer une adresse IPv4 au client.
- **Adresse IP du serveur** : champ utilisé par le serveur pour indiquer l'adresse du serveur que le client doit utiliser pour l'étape suivante du processus d'amorçage. Il ne s'agit pas forcément du serveur envoyant cette réponse. Le serveur émetteur inclut toujours son adresse IPv4 dans un champ spécial appelé l'option Server Identifier DHCPv4.
- **Adresse IP de la passerelle** : achemine les messages DHCPv4 lorsque des agents de relais DHCPv4 sont impliqués. L'adresse de passerelle facilite les communications des requêtes DHCPv4 et les réponses entre le client et un serveur situés sur différents réseaux ou sous-réseaux.
- **Adresse matérielle du client** : spécifie la couche physique du client.

- **Nom du serveur** : champ utilisé par le serveur envoyant un message DHCPOFFER ou DHCPACK. Le serveur peut éventuellement saisir son nom dans ce champ. Il peut s'agir d'un simple surnom ou d'un nom de domaine DNS, tel que serveurdhcp.netacad.net.

- **Nom du fichier de démarrage** : champ facultatif utilisé par un client pour demander un type particulier de fichier de démarrage dans un message DHCPDISCOVER. Utilisé par un serveur dans un message DHCPOFFER pour spécifier un répertoire et un nom de fichier de démarrage.

- **Adresse IP de la passerelle** : achemine les messages DHCPv4 lorsque des agents de relais DHCPv4 sont impliqués. L'adresse de passerelle facilite les communications des requêtes DHCPv4 et les réponses entre le client et un serveur situés sur différents réseaux ou sous-réseaux.

- **Options DHCP** : comprend les options DHCP, notamment plusieurs paramètres requis pour le fonctionnement de base de DHCP. La longueur de ce champ est variable. Le client et le serveur peuvent utiliser ce champ.

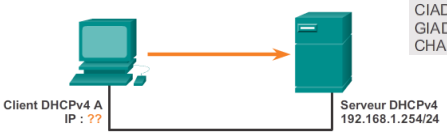
Code d'options	Signification
1	Subnet Mask
3	Router
6	Domain Name Server
54	DHCP Server Identifier
51	IP Address Lease Time
58	Renewal Time Value
59	Rebinding Time Value
255	End

Au niveau du fonctionnement proprement dit, si un client est configuré pour recevoir ses paramètres IPv4 de manière dynamique et souhaite se connecter au réseau, il demande des valeurs d'adressage au serveur DHCPv4.

Le client transmet un message DHCPDISCOVER sur son réseau local au démarrage ou lorsqu'il détecte une connexion réseau active.

Le client ne pouvant pas savoir à quel sous-réseau il appartient, le message DHCPDISCOVER est une diffusion IPv4 (l'adresse IPv4 de destination est 255.255.255.255). Le client n'ayant pas encore d'adresse IPv4 configurée, l'adresse IPv4 source utilisée est 0.0.0.0.

CIADDR : adresse IP du client
GIADDR : adresse IP de la passerelle
CHADDR : adresse matérielle du client



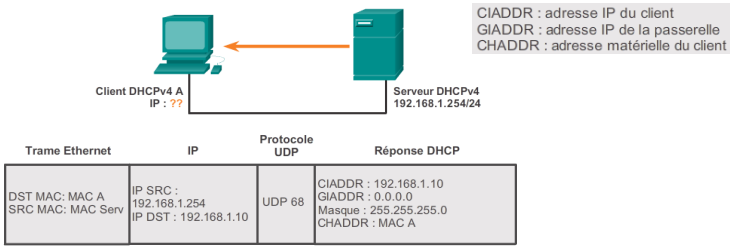
Trame Ethernet	IP	Protocole UDP	DHCPDISCOVER
DST MAC: FF:FF:FF:FF:FF:FF SRC MAC: MAC A	IP SRC : 0.0.0.0 IP DST : 255.255.255.255	UDP 67	CIADDR : 0.0.0.0 GIADDR : 0.0.0.0 Masque : 0.0.0.0 CHADDR : MAC A

Chapitre 3

Lorsque le serveur DHCPv4 reçoit le message DHCPDISCOVER, il répond par un message DHCPOFFER. Ce message contient des informations de configuration initiale pour le client, notamment l'adresse IPv4 proposée par le serveur, le masque de sous-réseau, la durée du bail et l'adresse IPv4 du serveur DHCPv4 à l'origine de la proposition.

Le message DHCPOFFER peut être configuré pour inclure d'autres informations, telles que la date de renouvellement du bail et l'adresse DNS.

Le serveur DHCP répond au message DHCPDISCOVER en attribuant des valeurs à l'adresse CIADDR et au masque de sous-réseau. La trame est créée à l'aide de l'adresse matérielle du client (CHADDR) et envoyée au client demandeur.



Chapitre 3

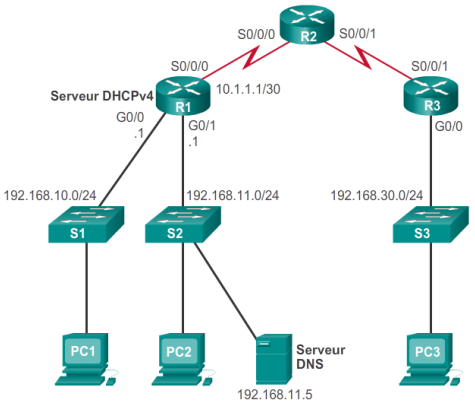
Configuration serveur Cisco IOS DHCPv4

Au niveau configuration, le logiciel Cisco IOS du routeur Cisco peut être configuré en tant que serveur DHCPv4. Le serveur DHCPv4 Cisco IOS attribue et gère les adresses IPv4 depuis les pools d'adresses spécifiés dans le routeur jusqu'aux clients DHCPv4.

Etape 1 : exclure certaines adresses

Le routeur agissant en tant que serveur DHCPv4 attribue toutes les adresses IPv4 dans un pool d'adresses DHCPv4 sauf s'il est configuré pour exclure certaines adresses.

En général, certaines adresses IPv4 d'un pool sont attribuées aux périphériques réseau nécessitant des adresses statiques, qui ne doivent pas être attribuées à d'autres périphériques.



Pour exclure certaines adresses, utilisez la commande **ip dhcp excluded-address** *low-address [high-address]*

```
R1(config)# ip dhcp excluded-address 192.168.10.1 192.168.10.9
R1(config)# ip dhcp excluded-address 192.168.10.254
```

Etape 2 : configuration le nom du pool d'adresses IPv4

Lorsque vous configurez un serveur DHCPv4, vous devez définir un pool d'adresses à attribuer. Cela se fait grâce à la commande **ip dhcp pool** *pool-name*, qui crée un pool portant le nom spécifié et place le routeur en mode de configuration DHCPv4.

```
R1(config)# ip dhcp pool LAN-POOL-1
R1(dhcp-config)#
```

Etape 3 : configuration du pool d'adresses DHCPv4

Attention , lorsqu'on configure le pool DHCPv4, certaines tâches sont absolument indispensables tandis que d'autres sont facultatives mais peuvent être définies.

Tâches requises	Commande
Définir le pool d'adresses	**network** *network-number* [*mask* | */prefix-length*]
Définir le routeur ou la passerelle par défaut	**default-router** *address*[*address2...address8*]

Le pool d'adresses et le routeur servant de passerelle par défaut doivent être configurés.

Pour définir la plage d'adresses, il suffit d'utiliser l'instruction **network** *network-number [network-mask | /prefix-length]*

La commande **default-router** servira à définir le routeur servant de passerelle par défaut. Généralement, la passerelle est l'interface de réseau local du routeur le plus proche des périphériques client. Vous pouvez spécifier jusqu'à huit adresses.

Tâches facultatives	Commande
Définir un serveur DNS	**dns-server** *address*[*address2...address8*]
Définir le nom de domaine	**domain-name** *domain*
Définir la durée du bail DHCP	**lease** {*days* [*hours*] [*minutes*] | *infinite*}
Définir le serveur WINS NetBIOS	**netbios-name-server** *address*[*address2...address8*]

Chapitre 3

Au niveau des commandes facultatives, l'adresse IPv4 du serveur DNS à la disposition d'un client DHCPv4 est configurée à l'aide de la commande **dns-server** *address*.

La commande **domain-name** *domain* sert à définir le nom de domaine.

La durée du bail DHCPv4 peut être modifiée à l'aide de la commande **lease**. La durée par défaut du bail s'élève à un jour.

La commande **netbios-name-server** est utilisée pour définir le serveur WINS NetBIOS.

Exemple :

```
R1(config)# ip dhcp excluded-address 192.168.10.1 192.168.10.9
R1(config)# ip dhcp excluded-address 192.168.10.254
R1(config)# ip dhcp pool LAN-POOL-1
R1(dhcp-config)# network 192.168.10.0 255.255.255.0
R1(dhcp-config)# default-router 192.168.10.1
R1(dhcp-config)# dns-server 192.168.11.5
R1(dhcp-config)# domain-name example.com
R1(dhcp-config)# end
```


Chapitre 3

Le service DHCPv4 est activé par défaut sur les versions du logiciel Cisco IOS qui le prennent en charge.

Pour désactiver le service, utilisez la commande **no service dhcp** du mode de configuration globale. Utilisez la commande **service dhcp** du mode de configuration globale pour réactiver le processus du serveur DHCPv4.

L'activation du service n'a aucun effet si les paramètres ne sont pas configurés.

```
R1(config)# no service dhcp
R1(config)# service dhcp
R1(config)#
```

Afin de vérifier les configurations DHCPv4 sur le routeur, vous pouvez utiliser la commande **show running-config | section dhcp** qui affichera uniquement les commandes DHCPv4 configurées (grâve au paramètre **| section**).

```
R1# show running-config | section dhcp
ip dhcp excluded-address 192.168.10.1 192.168.10.9
ip dhcp excluded-address 192.168.10.254
ip dhcp pool LAN-POOL-1
 network 192.168.1.0 255.255.255.0
 default-router 192.168.10.1
 dns-server 192.168.11.5
 domain-name example.com
```

Chapitre 3

Le bon fonctionnement du DHCPv4 peut être vérifié à l'aide de la commande **show ip dhcp binding**. Cette commande permet d'afficher la liste de toutes les liaisons entre adresse IPv4 et adresse MAC qui ont été fournies par le service DHCPv4.

```
R1# show ip dhcp binding
Bindings from all pools not associated with VRF:
IP address Client-ID/ Lease expiration Type State Interface
               Hardware address/
               User name
192.168.10.10 0100.5056.b3ed.d8 Sep 15 2019 8:42 AM Automatic ActiveGigabitEthernet0/0/0
```


HEH.be Sciences et technologies

Chapitre 3

Une autre commande, **show ip dhcp server statistics**, sert à vérifier que les messages sont reçus ou envoyés par le routeur. Cette commande permet d'afficher le nombre de messages DHCPv4 envoyés et reçus.

```
R1# show ip dhcp server statistics
Memory usage 19465
Address pools 1
Database agents 0
Automatic bindings 2
Manual bindings 0
Expired bindings 0
Malformed messages 0
Secure arp entries 0
Renew messages 0
Workspace timeouts 0
Static routes 0
Fixations relais 0
Relay bindings active 0
Relay bindings terminated 0
Relay bindings selecting 0
Message Received
BOOTREQUEST 0
DHCPDISCOVER 4
DHCPREQUEST 2
DHCPDECLINE 0
DHCPRELEASE 0
DHCPINFORM 0
```

Au niveau du client DHCPv4, vous pouvez vérifier à l'aide de la commande **ipconfig /all**

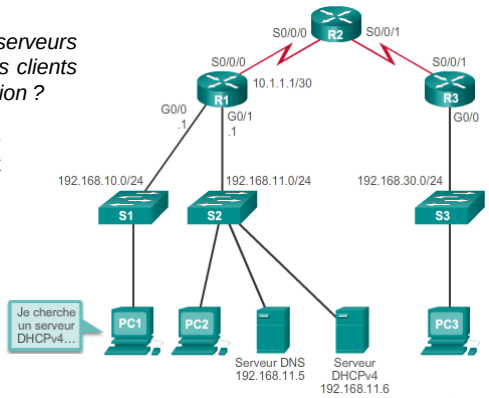
```
C:\Users\Student> ipconfig /all
Windows IP Configuration
   Host Name . . . . . . . . . . . . : ciscolab
   Suffixe DNS primaire. . . . . . . :
   Type de nœud. . . . . . . . . . . : Hybride
   Routage IP activé. . . . . . . . . : Non
   Proxy WINS activé. . . . . . . . . : Non
Ethernet adapter Ethernet0:
   Connection-specific DNS Suffix . : example.com
   Description . . . . . . . . . . . : Realtek PCIe GBE Family Controller
   Physical Address. . . . . . . . . : 00-05-9A-3C-7A-00
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   IPv4 Address. . . . . . . . . . . : 192.168.10.10
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained . . . . . . . . . . : Saturday, September 14, 2019 8:42:22AM
   Lease Expires . . . . . . . . . . : Sunday, September 15, 2019 8:42:22A
   Default Gateway . . . . . . . . . : 192.168.10.1
   DHCP Server . . . . . . . . . . . : 192.168.10.1
   DNS Servers . . . . . . . . . . . : 192.168.11.5
```


DHCPv4 relay

Dans le cas d'un réseau hiérarchique complexe, les serveurs d'entreprise se trouvent généralement dans une batterie de serveurs. Ces serveurs peuvent fournir au réseau des services DHCP, DNS, TFTP et FTP. Les clients du réseau ne sont généralement pas sur le même sous-réseau que ces serveurs.

Comment faire alors pour localiser les serveurs et de bénéficier des services puisque les clients utilisent souvent des messages de diffusion ?

Étant donné que le serveur DHCPv4 se trouve sur un autre réseau, PC1 ne peut pas recevoir d'adresse IP via DHCP.



Chapitre 3

Pour résoudre ce problème, configurer une adresse de diffusion Cisco IOS. Cette solution permet à un routeur de transférer les diffusions DHCPv4 au serveur DHCPv4. Lorsqu'un routeur transfère des requêtes de paramètre/attribution d'adresse, il agit comme agent de relais DHCPv4.

Pour que PC1 puisse contacter le serveur DHCPv4, l'interface sur R1 recevant la diffusion est configurée avec la commande du mode de configuration d'interface **ip helper-address** *@DHCP-address*. Ce que vous pouvez ensuite vérifier à l'aide de la commande **show ip interface**.

```
R1(config)# interface g0/0/0
R1(config-if)# ip helper-address 192.168.11.6
R1(config-if)# end
R1#
```

DHCPv4 n'est pas le seul service que le routeur peut relayer suite à une configuration spécifique. Par défaut, la commande **ip helper-address** transfère les huit services UDP suivants :

Port 37 : heure
Port 49 : TACACS
Port 53 : DNS
Port 67 : client BOOTP/DHCP
Port 68 : serveur BOOTP/DHCP
Port 69 : TFTP
Port 137 : service de noms NetBIOS
Port 138 : service de datagrammes NetBIOS

HEH be Sciences et technologies

Chapitre 3

Lorsqu'un routeur a été configuré en tant qu'agent de relais DHCPv4, il accepte les requêtes de diffusion liées au service DHCPv4, puis transmet ces demandes en monodiffusion à l'adresse IPv4 renseignée dans la commande ip helper-address.

L'administrateur réseau peut utiliser la commande **show ip interface** pour vérifier la configuration. Dans notre exemple, cela donnerait ceci :

```
R1# show ip interface g0/0/0
GigabitEthernet0/0/0 is up, line protocol is up
  Internet address is 192.168.10.1/24
  Broadcast address is 255.255.255.255
  Address determined by setup command
  MTU is 1500 bytes
  Helper address is 192.168.11.6
(output omitted)
```

Configuration en tant que client DHCPv4

Au niveau des routeurs haut débit pour les particuliers (ou petites entreprises), généralement ceux-ci peuvent être configurés pour acquérir automatiquement une adresse IPv4 à partir du FAI, via un modem câble ou DSL.

Dans l'exemple ci-dessus, le routeur SOHO (Small Office/Home Office) est connecté à un modem câble et il est considéré comme un client DHCPv4 et demande une adresse IPv4 au FAI.

Dans ce cas, au niveau de la configuration, la méthode suivie dépendra du FAI. Cependant, dans le cas de la configuration la plus simple, l'interface Ethernet est utilisée pour établir la connexion à un modem câble ou DSL.

Pour configurer une interface Ethernet en tant que client DHCP, utilisez la commande du mode de configuration d'interface **ip address dhcp**.

```
SOHO(config)# interface g0/1
SOHO(config-if)# ip address dhcp
SOHO(config-if)# no shutdown
SOHO(config-if)#
*Jan 31 17:31:11.507: %DHCP-6-ADDRESS_ASSIGN: Interface
GigabitEthernet0/1 assigned DHCP address 209.165.201.12, mask
255.255.255.224, hostname SOHO
SOHO(config-if)# end
SOHO# show ip interface g0/1
GigabitEthernet0/1 is up, line protocol is up
  Internet address is 209.165.201.12/27
  Broadcast address is 255.255.255.255
  Address determined by DHCP
<résultat omis>
```

Bien entendu, on peut avoir différents problèmes liés au DHCP.

En cas de problèmes, vous pouvez effectuer plusieurs choses afin de vérifier ou tester le DHCP.

Premièrement, utilisez la commande **show interfaces** *interface* pour vérifier que l'interface du routeur servant de passerelle par défaut pour le client est opérationnelle. L'interface doit être active sinon le port n'achemine pas le trafic et donc pas les requêtes DHCP.

Deuxièmement, vérifiez la connectivité du réseau en configurant des informations d'adresse statique IPv4 sur un poste de travail client.

Finalement, il est important de déterminer si DHCPv4 fonctionne correctement lorsque le client se trouve sur le même sous-réseau ou réseau local virtuel que le serveur DHCPv4. Si DHCPv4 fonctionne correctement dans ces situations, alors le problème peut provenir de l'agent de relais DHCP.

Chapitre 3

L'adressage IPv6

Une adresse IPv6 est longue de **128 bits** (16 octets) contre 32 bits pour IPv4.
La notation décimale pointée employée pour les adresses IPv4 (par exemple 192. 168.1.1) est abandonnée au profit d'une **écriture hexadécimale**, où les **8 groupes de 2 octets** (16 bits par groupe) sont séparés par un signe « **:** ».

Exemple de notation :

2A01:EF35:2421:4BE0:CDBC:C04E:A7AB:ECF3

Remarque : l'IPv6 étant sans classes nativement, les réseaux IPv6 sont notés en utilisant la notation CIDR.

Chapitre 3

L'adressage IPv6 étant long, il y a certaines règles à suivre qui permettent d'abréger la notation des adresses IPv6.

▪ La première règle est l'omission des zéros **en début de segment de 16 bits**.

01AB peut s'écrire **1AB**
0A00 peut s'écrire **A00**
00CD peut s'écrire **CD**

```
2001: DB8:   0:A300:ABCD:   0:   0:1234
2001:0DB8:0000:A300:ABCD:0000:0000:1234
```

Cette règle s'applique uniquement aux zéros de début de segment et NON aux zéros suivants.

▪ La deuxième règle permettant d'abréger la notation des adresses IPv6 est qu'une suite de deux fois deux-points (::) peut remplacer toute chaîne unique et contiguë d'un ou plusieurs segments de 16 bits comprenant uniquement des zéros.

Une suite de deux fois deux-points (::) **ne peut être utilisée qu'une seule fois par adresse** ! Cette notation s'appelle le format compressé.

Format compressé : `2001:DB8:0:1111::200`

Format recommandé : `2001:0DB8:0000:1111:0000:0000:0000:0200`

Chapitre 3

Souvenez-vous que le préfixe (ou la partie réseau) d'une adresse IPv4 peut être identifié par un masque de sous-réseau ou une longueur de préfixe en notation décimale à point (notation de barre oblique).

L'IPv6 utilise ***la longueur de préfixe*** pour représenter le préfixe de l'adresse. Elle est utilisée pour indiquer la partie réseau d'une adresse IPv6 à l'aide de la notation adresse IPv6 /longueur de préfixe.

La longueur de préfixe peut aller de 0 à 128.

La longueur de préfixe IPv6 standard pour les réseaux locaux et la plupart des autres types de réseau est /64.

Celle-ci signifie que le préfixe ou la partie réseau de l'adresse a une longueur de 64 bits, ce qui laisse 64 bits pour l'ID d'interface (partie hôte) de l'adresse.

Chapitre 3

Quant aux types d'adresses IPv6, il en existe trois différent :

▪ **Monodiffusion** – une adresse de monodiffusion IPv6 identifie une interface sur un périphérique IPv6 de façon unique.

▪ **Multidiffusion** – une adresse de multidiffusion IPv6 est utilisée pour envoyer un seul paquet IPv6 vers plusieurs destinations.

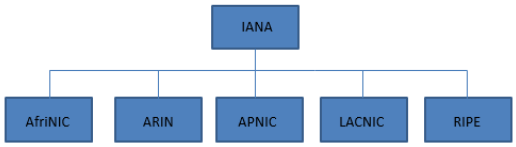
▪ **Anycast** – une adresse anycast IPv6 est une adresse de monodiffusion IPv6 qui peut être attribuée à plusieurs périphériques. Un paquet envoyé à une adresse anycast est acheminé vers le périphérique le plus proche ayant cette adresse.

Contrairement à l'IPv4, l'IPv6 n'a pas d'adresse de diffusion !

Cependant, il existe une adresse de multidiffusion à tous les nœuds IPv6 qui offre globalement les mêmes résultats.

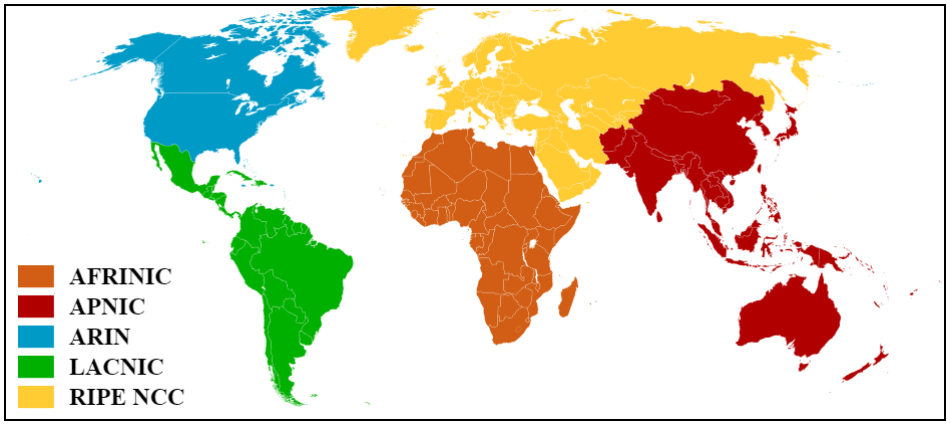
Chapitre 3

Comme vous le savez, les adresses IP sont distribuées par l'IANA (*Internet Assigned Numbers Authority*), via 5 Registres Internet Régionaux qui sont des organismes responsables de l'allocation de blocs d'adresses IP dans 5 régions du monde.



RIR	Responsible Regions
African Network Information Centre (AfriNIC)	Africa region
American Registry for Internet Numbers (ARIN)	The United States, Canada, several parts of the Caribbean region, and Antarctica regions.
Asia-Pacific Network Information Centre (APNIC)	Asia, Australia, New Zealand, and neighboring countries
Latin America and Caribbean Network Information Centre (LACNIC)	Latin America and parts of the Caribbean region
Réseaux IP Européens Network Coordination Centre (RIPE NCC)	Europe, Russia, the Middle East, and Central Asia

Chapitre 3



Chapitre 3

Pour le moment, seulement 1/8 des adresses IPv6 sont publiques et cela correspond aux adresses 2000:: /3.

Ok… mais cela représente quoi exactement ?

0010 0000 0000 0000 0000 0000 …. 0000 0000 (Binary)
2 0 0 0 : 0000:0000:0000:0000:0000:0000:0000 (Hexadecimal)

0011 1111 1111 1111 1111 1111 …. 1111 1111 (Binary)
3 F F F : FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF (Hexadecimal)

Ce qui veut dire que l'on dispose de la plage d'adresse de 2000:: à 3FFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF

Mais pour le moment, la plupart des adresses IPv6 commencent par 2001:: /16

L'IANA a distribué des blocs d'adresses aux 5 organismes régionaux et en général elle donne des blocs par tranche de préfixe /23.

Chapitre 3

Pour l'organisme **RIPE** (qui s'occupe de l'Europe notamment), celui-ci dispose par exemple du bloc *2001:0600::* */23*.

2 0 0 1 : 0 6 0 0 :0000:0000:0000:0000:0000:0000 /23
0010 0000 0000 0001 0000 0110 0000 0000 0000 0000 … …. … …0000 0000 /23
à
2 0 0 1 : 0 7 F F :FFFF:FFFF:FFFF:FFFF:FFFF:FFFF /23
0010 0000 0000 0001 0000 0111 1111 1111 1111 1111 … …. … … 1111 1111 /23

Que fait l'organisme RIPE ?

L'organisme RIPE va quant à lui adresser des blocs d'adresses (plus petits) aux différents ISP (*Internet Service Provider*)

Par exemple :
2001:0255::/32 à l'ISPa
2001:0266::/32 à l'ISPb
…
Et ces ISP vont eux-même assigner des blocs d'adresses aux différentes organismes qui en font la demande. Par exemple, pour l'ISPa :
2001:0255:8888::/48 à l'organisme A
2001:0255:9999::/48 à l'organisme B
…

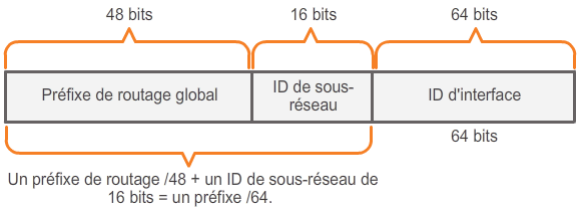
Chapitre 3

Une fois qu'une entreprise ou une organisation dispose de son bloc d'adresses IP, elle peut utiliser à sa guise le restant des bits, tout en gardant 16 bits pour faire ses sous réseaux.

Par exemple pour l'organisme A:
2001:0255:8888:0000::/64 to 2001:0255:8888:FFFF::/64

→ Une organisation peut donc posséder jusqu'à 65536 sous réseaux de 2^{64} hôtes chacun !

D'une manière générale, le format est comme ceci :



Chapitre 3

Une adresse de monodiffusion IPv6 identifie une interface sur un périphérique IPv6 de façon unique.

Un paquet envoyé à une adresse de monodiffusion est reçu par l'interface correspondant à cette adresse.

Il existe six types d'adresse de monodiffusion IPv6 :

▪ Une **adresse de monodiffusion globale** est *similaire à une adresse IPv4 publique*. Ces adresses sont uniques au monde et routables sur Internet. Les adresses de monodiffusion globale peuvent être configurées de manière statique ou attribuées de manière dynamique.

▪ Les **adresses link-local** sont *utilisées pour communiquer avec d'autres périphériques sur la même liaison locale*. Les adresses link-local sont confinées à une seule liaison. Leur caractère unique doit être confirmé uniquement sur cette liaison, car elles ne sont pas routable au-delà de la liaison. En d'autres termes, les routeurs ne transmettent aucun paquet avec une adresse source ou de destination link-local.

▪ Une **adresse de bouclage** est utilisée par un hôte *pour envoyer un paquet à lui-même*. Cette adresse ne peut pas être attribuée à une interface physique. Elle sert à tester la configuration TCP/IP de l'hôte local. L'adresse de bouclage IPv6 contient uniquement des 0, excepté le dernier bit. Elle est donc notée ::1/128, ou simplement ::1 au format compressé.

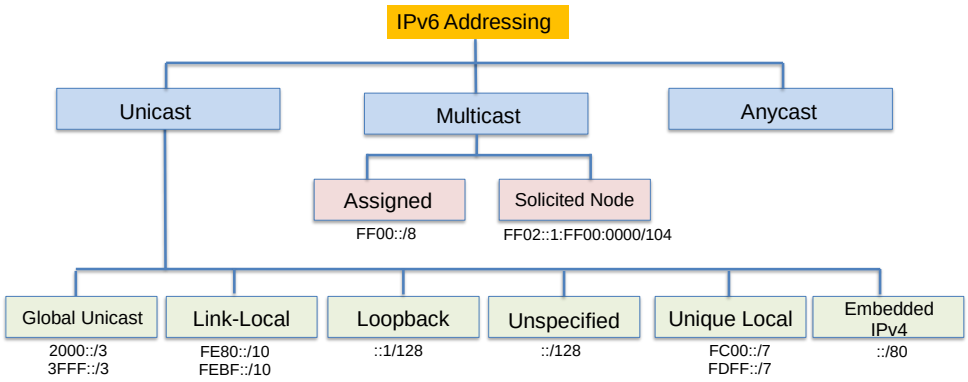
Chapitre 3

▪ Une **adresse non spécifiée** est une adresse contenant uniquement des 0 et notée ::/128 ou simplement :: au format compressé. Elle ne peut pas être attribuée à une interface et ne peut être utilisée que comme adresse source dans un paquet IPv6. Une adresse non spécifiée est utilisée comme adresse source lorsque le périphérique n'a pas encore d'adresse IPv6 permanente.

▪ Les **adresses IPv6 locales uniques** ont certains points communs avec les adresses privées pour l'IPv4, mais ces deux types d'adresse diffèrent également sur certains points. Des adresses locales uniques sont utilisées pour l'adressage local au sein d'un site ou entre un nombre limité de sites. Ces adresses ne doivent pas être routables sur le réseau IPv6 global. Les adresses locales uniques sont comprises entre FC00::/7 et FDFF::/7.

▪ Les **adresses IPv4 intégrées**, qui sont utilisées pour faciliter la transition de l'IPv4 vers l'IPv6.

Chapitre 3



Chapitre 3

Nous allons maintenant approfondir un peu le cas des **adresses *link-local IPv6*** qui permettent à un périphérique de communiquer avec d'autres périphériques IPv6 sur la même liaison et uniquement sur cette liaison (sous-réseau).

Les paquets associés à une adresse source ou de destination link-local ne peuvent pas être acheminés au-delà de leur liaison d'origine.

L'adresse de monodiffusion globale n'est pas obligatoire. Cependant, chaque interface réseau IPv6 doit avoir une adresse link-local.

Si une adresse link-local n'est pas configurée manuellement sur une interface, le périphérique crée automatiquement sa propre adresse sans communiquer avec un serveur DHCP.

Les hôtes IPv6 créent une adresse link-local IPv6 même si aucune adresse de monodiffusion globale IPv6 n'a été attribuée aux périphériques. Cela permet aux périphériques IPv6 de communiquer avec d'autres périphériques IPv6 sur le même sous-réseau. Cela inclut la communication avec la passerelle par défaut.

Les adresses link-local IPv6 se trouvent dans la plage **FE80:: /10**.

F E 8 0 :0000:0000:0000:0000:0000:0000:0000/10
1111 1110 1000 0000

to

F E B F :FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF/10
1111 1110 1011 1111

Chapitre 3

Avant même d'avoir une adresse unicast, chaque périphérique va générer une adresse link local (FE80:: /10) !

Comment ?

La génération de cette adresse se fait à l'aide d'une **méthode** appelée **EUI-64** et de l'adresse MAC du périphérique :

Admettons que l'adresse MAC (48 bits) du périphérique est **000D:BD22:22BB**

La méthode EUI-64 comporte 3 étapes :

Etape 1 : On va décomposer cette adresse en deux parties afin d'y insérer le groupe FFFE (16 bits) au milieu, afin de former les 64 bits nécessaires à la partie hôte.

Etape 2 : En plus de cela, dans le premier groupe de bits, on va inverser le 7ème bit.

Etape 3 : Finalement, on va combiner la partie réseau et la partie hôte de l'adresse pour former l'adresse complète link local.

Chapitre 3

Exemple de la création d'une adresse link-local avec la méthode EUI-64 :

Adresse MAC → 000D:BD22:22BB

Etape 1 → 000D:BDFF:FE22:22BB

0000 0000 0000 1101:BDFF:FE22:22BB

Etape 2 → 0000 0010 0000 1101:BDFF:FE22:22BB

020D:BDFF:FE22:22BB

= partie hôte

Etape 3 → FE80:0000:0000:0000:020D:BDFF:FE22:22BB /64

ou

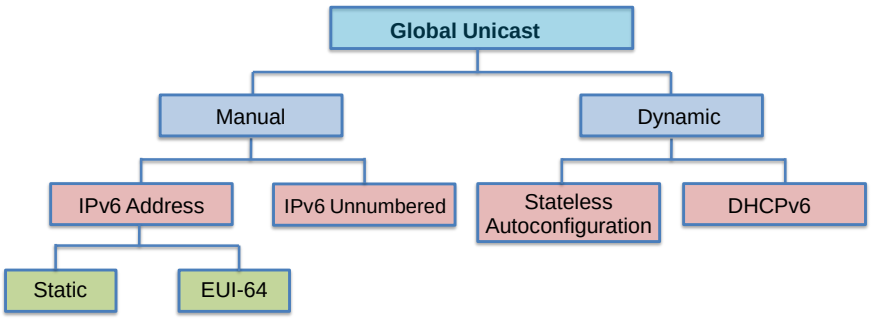
FE80::020D:BDFF:FE22:22BB /64

Chapitre 3

Maintenant si l'on revient aux adresses de **monodiffusion globale IPv6**, je vous rappelle que celles-ci sont uniques au monde et routables (Internet IPv6).

Ces adresses sont équivalentes aux adresses publiques IPv4.

Quels sont les différents moyens de configurer ces adresses ?



HEH be Sciences et technologies

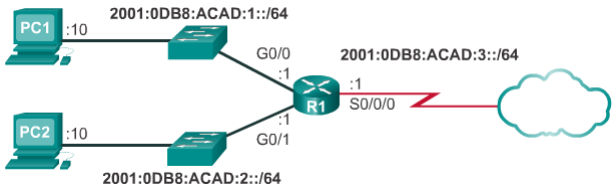
Chapitre 3

Configurations

Nous allons maintenant voir quelques configurations en IPv6.

1°) Configuration statique d'une adresse de monodiffusion globale :

Exemple :

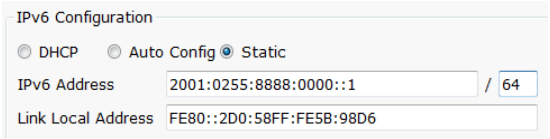


Router(config)#**interface** GigabitEthernet 0/0
Router(config-if)#**ipv6 address** 2001:DB8:ACAD:1::1/64
Router(config-if)#**no shutdown**

Il suffit bien entendu d'appliquer les mêmes commandes pour l'interface GigabitEthernet 0/1 et pour l'interface Serial 0/0/0.

Rappel : le routage IPv6 n'est pas activé par défaut. Pour sélectionner l'IPv6 sur un routeur, la commande de configuration globale **ipv6 unicast-routing** doit être utilisée.

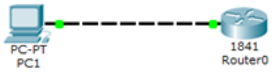
Sur un PC ou un périphérique disposant d'une interface graphique, il suffit de sélectionner l'option « static » et de mettre l'adresse souhaitée :



2°) Configuration automatique des adresses sans état (SLAAC) :

La configuration automatique des adresses sans état (SLAAC) est une méthode permettant à un périphérique d'obtenir son préfixe, la longueur de préfixe, et l'adresse de la passerelle par défaut depuis un *routeur IPv6*, sans l'intervention d'un serveur DHCPv6.

Lorsque la SLAAC est utilisée, les périphériques se basent sur les messages d'annonce de routeur ICMPv6 du routeur local pour obtenir les informations nécessaires.



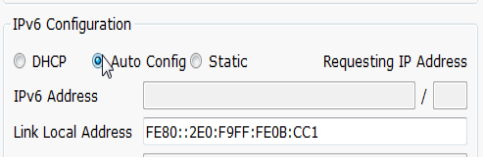
Les routeurs IPv6 envoient régulièrement des messages d'annonce de routeur ICMPv6 à tous les périphériques IPv6 du réseau.

Par défaut, les routeurs Cisco envoient des messages d'annonce de routeur toutes les 200 secondes à l'adresse du groupe de multidiffusion à tous les nœuds IPv6.

Un périphérique IPv6 du réseau n'a pas à attendre ces messages. Il peut envoyer un message de sollicitation de routeur au routeur, en utilisant l'adresse du groupe de multidiffusion à tous les routeurs IPv6.

Lorsqu'un routeur IPv6 reçoit un message de sollicitation, il répond immédiatement en envoyant un message d'annonce de routeur.

Au niveau de l'ordinateur, il suffit de choisir l'option « auto config » :



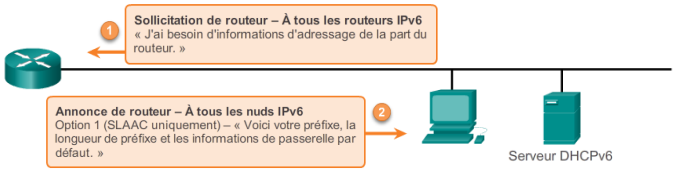
Même si une interface d'un routeur Cisco peut être configurée avec une adresse IPv6, cela ne fait pas du routeur un « routeur IPv6 » !!!

Un routeur IPv6 est un routeur qui :

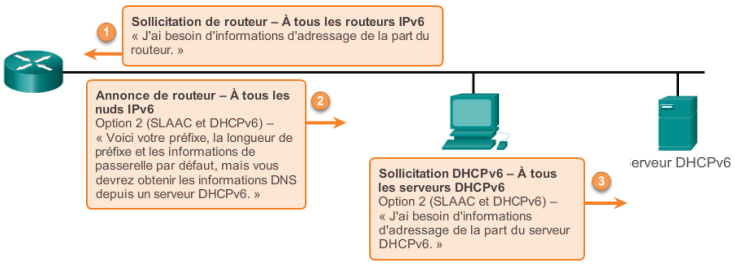
- transfère les paquets IPv6 entre les réseaux.
- peut être configuré avec des routes IPv6 statiques ou un protocole de routage IPv6 dynamique.
- envoie des messages d'annonce de routeur ICMPv6.

Le message d'annonce de routeur ICMPv6 contient le préfixe, la longueur du préfixe et peut contenir l'une des trois options suivantes :

➢ **Option 1 – SLAAC uniquement** : le 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.



Option 2 – SLAAC et DHCPv6 : le 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. Il existe d'autres informations à acquérir auprès d'un serveur DHCPv6 telles que l'adresse du serveur DNS.



Option 3 – DHCPv6 uniquement : le périphérique ne doit pas utiliser les informations contenues dans le message d'annonce de routeur en tant qu'informations d'adressage. Dans ce cas, le serveur DHCPv6 agit en tant que serveur DHCP avec état, tout comme le DHCP pour l'IPv4. Le périphérique utilise le serveur DHCPv6 pour obtenir toutes ses informations d'adressage.

Si le client n'utilise pas les informations contenues dans le message d'annonce de routeur et compte uniquement sur le DHCPv6, le serveur DHCPv6 fournit alors l'adresse de monodiffusion globale IPv6 complète, y compris le préfixe et l'ID d'interface.

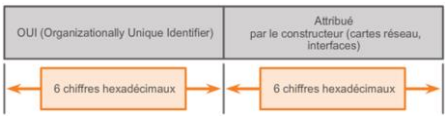
Cependant, si l'option 1 (SLAAC uniquement) ou l'option 2 (SLAAC avec DHCPv6) est utilisée, le client n'obtient pas la partie ID d'interface réelle de l'adresse grâce à ces processus.

Le périphérique client doit alors déterminer son propre ID d'interface de 64 bits, soit à l'aide de la méthode EUI-64.

Comme vu précédemment, le format EUI-64 (« Extended Unique Identifier »), créé par l'IEEE est un processus qui utilise l'adresse MAC Ethernet 48 bits d'un client et insère 16 autres bits au milieu de l'adresse MAC 48 bits pour créer un ID d'interface de 64 bits.

Je rappelle que les adresses MAC Ethernet sont généralement représentées au format hexadécimal et sont constituées de deux parties :

- **OUI (Organizationally Unique Identifier)** qui est un code de fournisseur de 24 bits (6 caractères hexadécimaux) attribué par l'IEEE.
- **ID de périphérique** qui est une valeur unique de 24 bits identifiant le périphérique.



L'avantage de la méthode EUI-64 est que l'adresse MAC Ethernet peut être utilisée pour déterminer l'ID d'interface. Elle permet également aux administrateurs réseau de suivre facilement une adresse IPv6 jusqu'à un périphérique final en utilisant une adresse MAC unique.

Toutefois, cela a entraîné des problèmes de confidentialité pour de nombreux utilisateurs. Ces derniers s'inquiètent du fait qu'il soit possible de remonter jusqu'à l'ordinateur physique en analysant les paquets. En raison de ces problèmes, un ID d'interface généré aléatoirement peut également être utilisé.

→ Selon le système d'exploitation, un périphérique peut utiliser un ID d'interface généré aléatoirement plutôt que l'adresse MAC et le processus EUI-64.

Il est simple de savoir si une adresse a été créée via la méthode EUI-64 : il suffit d'analyser la valeur FFFE située dans l'ID d'interface.

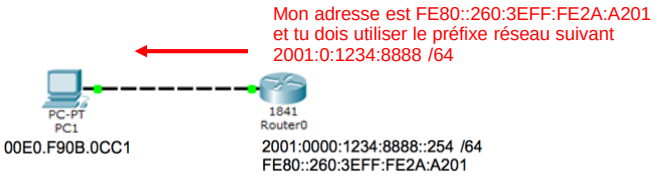
Une fois l'ID d'interface établi, via le processus EUI-64 ou par génération aléatoire, il peut être combiné avec un préfixe IPv6 pour créer une adresse de monodiffusion globale ou une adresse link-local :

- **Adresse de monodiffusion globale** : s'il utilise la SLAAC, le périphérique reçoit son préfixe par l'intermédiaire du message d'annonce de routeur ICMPv6 et l'associe à l'ID d'interface.
- **Adresse link-local** : un préfixe link-local utilise généralement FE80::/64 comme préfixe/longueur de préfixe, suivi de l'ID d'interface.

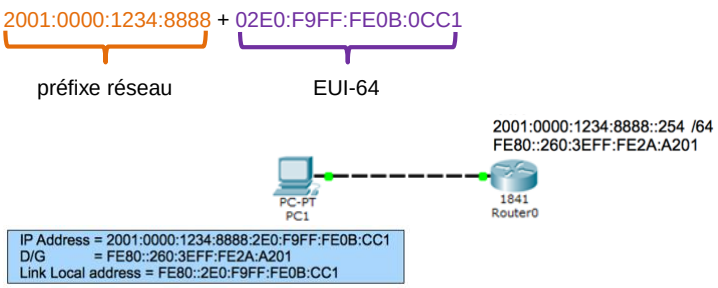
Explication en détail du premier cas, utilisation du SLAAC :

- Etape 1 : le PC qui est configuré en mode « auto configuration » et qui ne possède pas encore d'adresse IPv6 globale envoie un message de sollicitation de routeur.

- Etape 2 : le routeur répond alors avec un message d'annonce qui comprend le préfixe, la longueur du préfixe et la passerelle par défaut.



- Etape 3 : le PC va générer son adresse globale de monodiffusion à l'aide de la méthode EUI-64



Chapitre 3

Bien tendu, comme chaque fois que l'on configure quelque chose, il est impératif de vérifier ce que l'on a fait !

Tout comme pour l'IPv4, il existe pour l'IPv6 différentes commandes permettant la vérification :

```
R1#show ipv6 interface brief
GigabitEthernet0/0     [up/up]
    FE80::FE99:47FF:FE75:C3E0
    2001:DB8:ACAD:1::1
GigabitEthernet0/1     [up/up]
    FE80::FE99:47FF:FE75:C3E1
    2001:DB8:ACAD:2::1
Serial0/0/0            [up/up]
    FE80::FE99:47FF:FE75:C3E0
    2001:DB8:ACAD:3::1
Serial0/0/1            [administratively down/down]
    unassigned
```

```
R1#show ipv6 route
IPv6 Routing Table - default - 7 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user
Static

<output omitted>

C   2001:DB8:ACAD:1::/64 [0/0]
     via GigabitEthernet0/0, directly connected
L   2001:DB8:ACAD:1::1/128 [0/0]
     via GigabitEthernet0/0, receive
C   2001:DB8:ACAD:2::/64 [0/0]
     via GigabitEthernet0/1, directly connected
L   2001:DB8:ACAD:2::1/128 [0/0]
     via GigabitEthernet0/1, receive
C   2001:DB8:ACAD:3::/64 [0/0]
     via Serial0/0/0, directly connected
L   2001:DB8:ACAD:3::1/128 [0/0]
     via Serial0/0/0, receive
L   FF00::/8 [0/0]
     via Null0, receive
```

```
R1#ping 2001:db8:acad:1::10
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:DB8:ACAD:1::10,
timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5)
```


HEH.be Sciences et technologies

Chapitre 3

Vérification de la connectivité

Bien que le protocole IP ne soit pas un protocole fiable, la suite TCP/IP permet d'envoyer des messages si certaines erreurs se produisent.

Ces messages sont envoyés via les services du protocole ICMP et ont pour objectif de fournir des commentaires sur les problèmes liés au traitement de paquets IP dans certaines circonstances.

Il existe différents types de messages ICMP, mais les messages ICMP communs à ICMPv4 et à ICMPv6 sont notamment les suivants :

- **Host confirmation** (Confirmation de l'hôte) : Un message ICMP Echo (Écho ICMP) permet de déterminer si un hôte est fonctionnel. L'hôte local envoie un message ICMP Echo Request (Requête d'écho) à un autre hôte. Si l'hôte est disponible, l'hôte de destination répond en envoyant une réponse d'écho. C'est ce type de message qui est à la base de l'utilitaire ***ping***.
- **Destination or Service Unreachable** (destination ou service inaccessible) : Lorsqu'un hôte ou une passerelle reçoit un paquet impossible à acheminer, il ou elle peut utiliser un message ICMP de destination inaccessible pour avertir la source que la destination ou le service est inaccessible. Ce message comprend un code indiquant pourquoi le paquet n'a pas pu être acheminé.

Par exemple, pour l'ICMPv4, ces codes sont :

« **0** » dans le cas où le réseau est inaccessible.

« **1** » dans le cas où l'hôte est inaccessible.

« **2** » dans le cas où le protocole est inaccessible.

« **3** » dans le cas où le port est inaccessible.

Ces codes sont légèrement différents pour ICMPv6.

▪ **Time exceeded** (Délai dépassé) : Un message de dépassement de délai ICMPv4 est utilisé par un routeur pour indiquer qu'il ne peut pas transférer un paquet car le champ TTL de durée de vie du paquet a atteint 0. Si un routeur reçoit un paquet et décrémente le champ TTL de durée de vie du paquet IPv4 pour atteindre zéro, il abandonne le paquet et envoie un message de dépassement de délai à l'hôte source.

▪ **Route redirection** (Redirection de la route) : Un routeur peut envoyer un message de redirection ICMP Redirect pour notifier l'hôte sur un réseau, qu'une meilleure route est disponible jusqu'à une destination particulière. Ce message ne peut être utilisé que si l'hôte source appartient au même réseau physique que les deux passerelles.

Les messages d'informations et d'erreur du protocole ICMPv6 sont très similaires aux messages de contrôle et d'erreur mis en œuvre par le protocole ICMPv4.

Cependant, l'ICMPv6 offre de nouvelles fonctions et fonctionnalités avancées introuvables dans l'ICMPv4.

ICMPv6 inclut quatre nouveaux protocoles dans le cadre du protocole ***Neighbor Discovery Protocol*** (NDP) :

- Message de sollicitation de routeur
- Message d'annonce de routeur
- Message de sollicitation de voisin
- Message d'annonce de voisin

Au niveau des messages de sollicitation de routeur et d'annonce de routeur, ceux-ci sont envoyés entre les hôtes et les routeurs.

➢ **Messages de sollicitation de routeur :** lorsqu'un hôte est configuré pour obtenir ses informations d'adressage à l'aide de la configuration automatique des adresses sans état (SLAAC), celui-ci envoie un message de sollicitation au routeur. Le message de sollicitation de routeur est envoyé sous forme de message de multidiffusion à tous les routeurs IPv6.

➢ **Messages d'annonce de routeur** : ces messages sont envoyés par les routeurs pour fournir les informations d'adressage aux hôtes via la SLAAC. Un message d'annonce de routeur peut inclure les informations d'adressage pour l'hôte telles que le préfixe et la longueur de préfixe. Un routeur envoie un message d'annonce de routeur régulièrement (200sec) ou en réponse à un message de sollicitation.

Le protocole NDP ICMPv6 comprend deux types de message supplémentaires : la sollicitation de voisin et l'annonce de voisin qui sont utilisés pour :

- ***La résolution d'adresse***
- ***La détection d'adresses en double***

La ***résolution d'adresse*** est utilisée lorsqu'un périphérique du réseau local (LAN) connaît l'adresse de monodiffusion IPv6 d'une destination, mais pas son adresse MAC Ethernet.

Pour déterminer l'adresse MAC de destination, le périphérique envoie un message de sollicitation de voisin à l'adresse du nœud sollicité.

Le message inclut l'adresse IPv6 (de destination) connue. Le périphérique avec l'adresse IPv6 ciblée répond par un message d'annonce de voisin contenant son adresse MAC Ethernet.

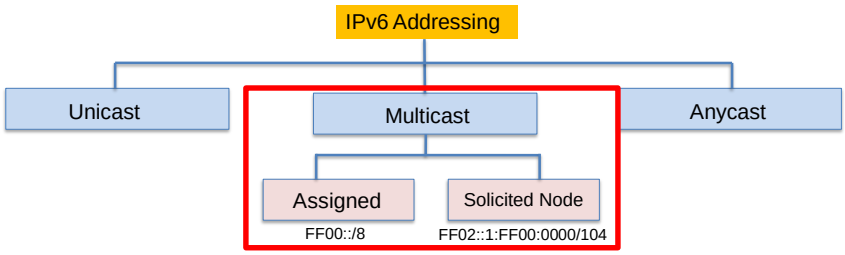
HEH.be Sciences et technologies

Chapitre 3

Lorsqu'une adresse de monodiffusion globale ou de monodiffusion link-local est attribuée à un périphérique, il est recommandé (mais pas obligatoire) d'utiliser ***la détection d'adresses en double*** sur l'adresse pour s'assurer qu'elle est unique.

Pour vérifier le caractère unique d'une adresse, le périphérique envoie un message de sollicitation de voisin avec sa propre adresse IPv6 comme adresse IPv6 ciblée.

Si cette adresse est attribuée à un autre périphérique du réseau, ce dernier répond en envoyant un message d'annonce de voisin.



Maintenant qu'on a fait le tour des adresses monodiffusion, on va regarder les adresses de multidiffusion IPv6, qui sont semblables aux adresses de multidiffusion IPv4, c-à-d est utilisée pour envoyer un paquet à un ou plusieurs destinataires (groupe de multidiffusion).

Il existe deux types d'adresses de multidiffusion IPv6 :

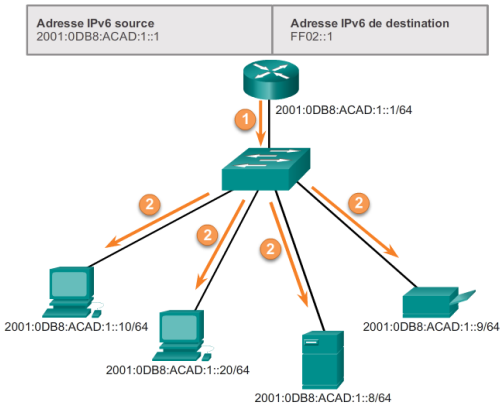
- **Les adresses de multidiffusion attribuées.**
- **Les adresses de multidiffusion de nœud sollicité.**

Les ***adresses de multidiffusion attribuées*** (préfixe FF00::/8) sont des adresses de multidiffusion réservées à des groupes ou périphériques prédéfinis. Une adresse de multidiffusion attribuée est une adresse unique utilisée pour joindre un groupe de périphériques exécutant un service ou un protocole commun.

Par exemple DHCPv6 utilise des adresses de multidiffusion attribuées.

Les deux groupes suivants de multidiffusion IPv6 attribuée sont les plus courants :

- **Groupe de multidiffusion à tous les nœuds FF02::1** : il s'agit d'un groupe de multidiffusion que tous les périphériques IPv6 peuvent joindre. Un paquet envoyé à ce groupe est reçu et traité par toutes les interfaces IPv6 situées sur la liaison ou le réseau. Cette opération a le même effet qu'une adresse de diffusion IPv4.



- **Groupe de multidiffusion à tous les routeurs FF02::2** : il s'agit d'un groupe de multidiffusion que tous les routeurs IPv6 peuvent joindre. Un routeur devient un membre de ce groupe lorsqu'il est activé en tant que routeur IPv6 (**ipv6 unicast-routing**). Un paquet envoyé à ce groupe est reçu et traité par tous les routeurs IPv6 situés sur la liaison ou le réseau.

Principales adresses de multidiffusion IPv6 :

FF02::1	All IPv6 nodes	Link Local Scope
FF02::2	All IPv6 routers	
FF02::5	OSPF routers	
FF02::6	OSPF Designated Routers	
FF02::9	RIP routers	
FF02::A	EIGRP Routers	
FF02::1:2	DHCP Srvs/Relay agents	

Chapitre 3

Une ***adresse de multidiffusion de nœud sollicité*** est semblable à une adresse de multidiffusion à tous les nœuds. Tous les périphériques du réseau doivent traiter le trafic envoyé à l'adresse de multidiffusion à tous les nœuds.

Une adresse de multidiffusion de nœud sollicité est une adresse correspondant uniquement aux 24 derniers bits de l'adresse de monodiffusion globale IPv6 d'un périphérique.

Une adresse de multidiffusion de nœud sollicité IPv6 est créée automatiquement lorsque l'adresse de monodiffusion globale ou l'adresse link-local est attribuée. L'adresse de multidiffusion de nœud sollicité IPv6 est créée grâce à la combinaison d'un préfixe spécifique, FF02:0:0:0:0:1:FF00::/104, et des 24 derniers bits de son adresse de monodiffusion.

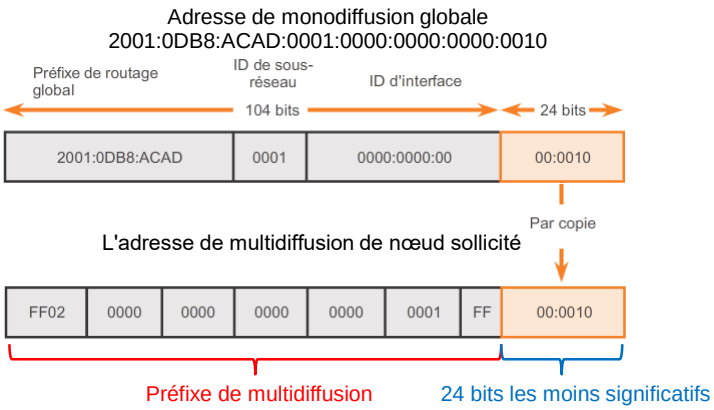
L'adresse de multidiffusion de nœud sollicité comprend deux parties :

- **Le préfixe de multidiffusion FF02:0:0:0:0:1:FF00::/104 :** les 104 premiers bits de l'adresse de multidiffusion de nœud sollicité.
- **Les 24 bits les moins significatifs :** il s'agit des 24 derniers bits de l'adresse de l'adresse de monodiffusion globale ou de l'adresse de monodiffusion link-local du périphérique.

HEH.be Sciences et technologies

Chapitre 3

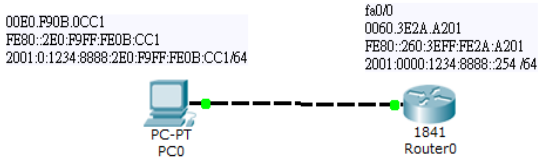
Exemple :



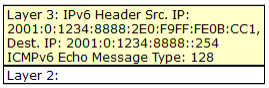
Chapitre 3

Concrètement, ce type d'adresses va servir pour déterminer l'adresse MAC d'un périphérique dont on connait l'adresse IPv6.

En effet, il n'existe pas de protocole ARP en IPv6 mais celui-ci est remplacé le protocole NDP (Neighbor Discovery Protocol ») qui utilise des messages de sollicitation de voisins (« neighbor solicitation ») et des annonces de voisins (« neighbor advertisement »).



Si on effectue un ping depuis le PC0 vers le Router0, le PC0 remplira le message ICMPv6 avec comme adresse pour la couche 3 ceci :



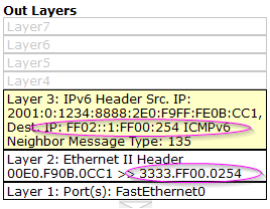
Mais il ne connait pas l'adresse MAC associée à l'adresse IPv6 du routeur…

HEH be Sciences et technologies

Chapitre 3

Du coup, afin d'avoir l'information manquante, le PC0 va d'abord envoyer un message de sollicitation avec comme adresse de destination, une adresse IPv6 de multidiffusion de nœud sollicité (FF02::1:FF00:254).

Au niveau de la couche 2 il utilisera son adresse MAC comme source et l'adresse MAC de destination sera l'équivalent de l'adresse IPv6.

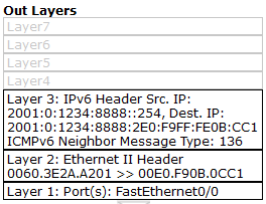


Si on effectue un ping depuis le PC0 vers le Router0, le PC0 remplira le message ICMPv6 avec comme adresse pour la couche 2 ceci :

33:33:FF + 24 bits de l'adresse IPv6 du nœud sollicité
→ 33:33:FF:00:02:54

Le routeur va donc recevoir le message ICMPv6 et il va voir que celui-ci lui est destiné.

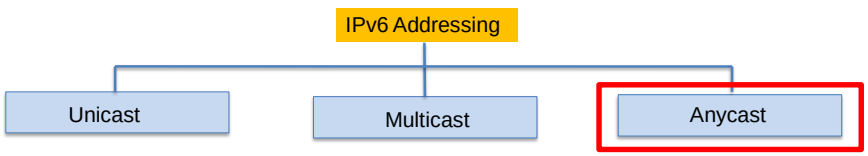
Il va donc répondre avec un message ICMPv6 d'annonce de voisin. Attention, cette fois-ci il s'agira d'un message unicast IPV6 à destination de PC0.



Bien entendu, vu que les adresses de multidiffusion de nœud sollicité sont rarement destinées à d'autres hôtes que celui-ci dont on veut connaître l'adresse MAC, cela est donc équivalent à un trafic de monodiffusion.

Ce qui rend le protocole NDP plus efficace que le protocole ARP utilisé en IPv4.

Finalement, nous allons discuter du nouveau type d'adresse présent dans l'IPv6, les adresses **anycast** :



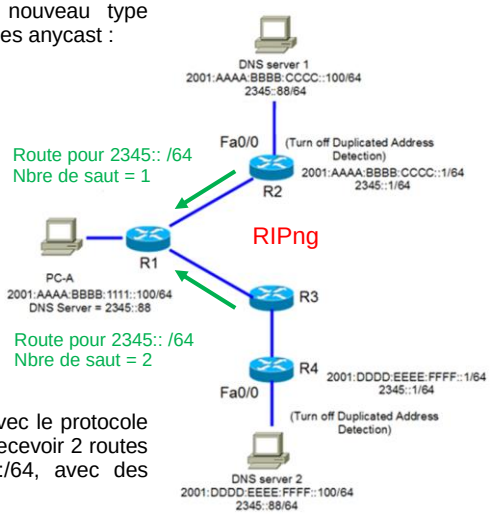
Ces adresses sont surtout utilisées pour faire de la redondance.

Chapitre 3

Finalement, nous allons discuter du nouveau type d'adresse présent dans l'IPv6, les adresses anycast :

Prenons l'exemple ici où l'on voit qu'il y a deux serveur DNS qui desservent la même zone.

Ces serveurs ont des adresses globales de monodiffusion différentes mais elles ont également une adresse globale de monodiffusion supplémentaire qui est identique (2345:: /64)



L'ensemble des routeurs est configuré avec le protocole dynamique RIPng ce qui fait que R1 va recevoir 2 routes possibles concernant le réseau 2345::/64, avec des nombres de sauts différents...

Chapitre 3

Le PC-A est bien entendu configuré pour utiliser le DNS avec l'adresse 2345::/64 et en temps normal, les requêtes DNS seront transmises à R1 qui décidera de les transmettre vers R2 puis vers le serveur DNS 1.

Bien entendu, dans le cas où R2 serait inaccessible par exemple, R1 remplacera la route pour atteindre 2345:: /64 par le chemin donnant vers R3 puis R4 afin de joindre le serveur DNS 2.

De cette manière la redondance DNS est assurée grâce à l'adresse IPV6 anycast 2345::88. Ce mécanisme fonctionne uniquement avec l'aide de routeur et de protocoles de routage. Attention, une adresse anycast utilise le même range IP que les adresses de monodiffusions globales.

→ Il est impossible de distinguer une adresse anycast d'une adresse globale unicast simplement en regardant la valeur de l'adresse IPv6 !

Coexistence IPv4 et IPv6

Bien que nous utilisons encore tous l'IPv4 au quotidien, le passage à l'IPv6 est déjà en cours. En effet, la transition de l'IPv4 vers l'IPv6 n'aura pas lieu en une fois et à une date fixe. Celle-ci prendra probablement plusieurs années. D'ailleurs l'IETF a créé divers protocoles et outils pour aider les administrateurs réseau à migrer leurs réseaux vers l'IPv6.

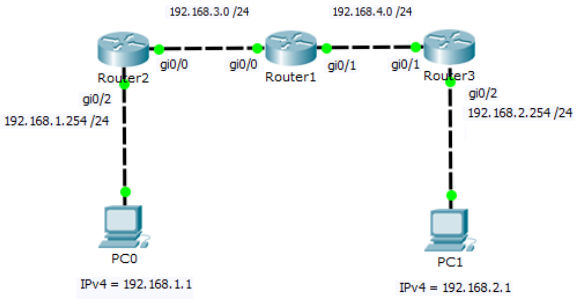
Les techniques de migration peuvent être classées en trois catégories :

- **Double pile** (« Dual stack ») : la double pile permet à l'IPv4 et à l'IPv6 de coexister sur le même réseau. Les périphériques double pile exécutent les piles de protocoles IPv4 et IPv6 simultanément.
- **Tunneling** : le tunneling est une méthode de transport des paquets IPv6 via un réseau IPv4. Les paquets IPv6 sont encapsulés dans des paquets IPv4, de la même manière que d'autres types de données.
- **Traduction** : les périphériques IPv6 peuvent utiliser la traduction d'adresses réseau 64 (NAT64) pour communiquer avec les périphériques IPv4 à l'aide d'une technique de traduction similaire à la NAT pour l'IPv4. Un paquet IPv6 est traduit en un paquet IPv4, et inversement.

1°) Dual stack

Les hôtes et les routeurs utilisent simultanément l'IPv4 et l'IPv6. Ils peuvent donc communiquer aussi bien avec l'un ou l'autre protocole.

Pour mettre en place le dual stack, nous allons voir dans un exemple les différentes étapes à suivre :



- Configurez les adresses IPv4 sur les hôtes et sur les routeurs.

Chapitre 3

- Implémenter un protocole de routage dynamique (par exemple RIPv2)

Routeur(config)#**router rip**

Routeur(config-router)#**version 2**

Routeur(config-router)#**no auto-summary**

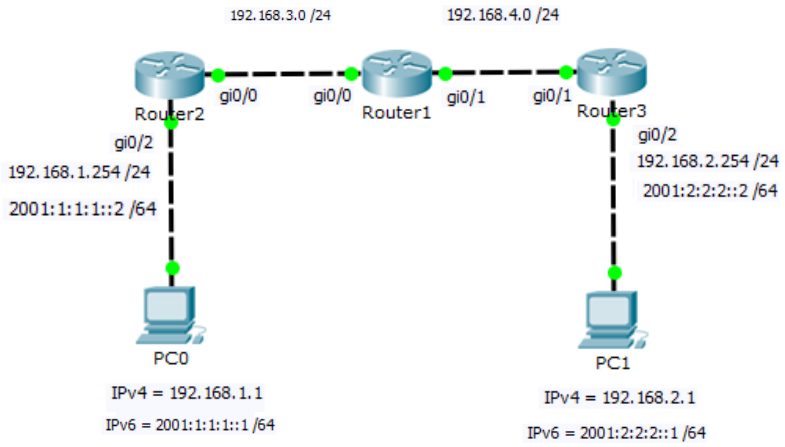
Routeur(config-router)#**network** *@réseaux*

Vérifiez à l'aide de **sh ip run** et **sh ip route** puis testez la connectivité à l'aide d'un ping entre les 2 PCs.

- Configurez la commande **ipv6 unicast-routing** sur l'ensemble des routeurs afin qu'ils prennent en charge le routage en IPv6.

Chapitre 3

Maintenant on va se charger de l'IPv6 :



Chapitre 3

- Configurez les adresses IPv6 global unicast sur les PCs en n'oubliant pas les adresses de passerelles IPv6.
- Configurez les adresses IPv6 global unicast sur toutes les interfaces des routeurs. Vous pouvez générer les adresses entre les routeurs à l'aide de la méthode EUI-64 ou les définir vous-même de manière statique.

Routeur(config-if)#**ipv6 address** *@addressIPv6/prefix* **EUI-64**

- Activer le routage RIPng

Routeur(config)#**ipv6 router rip** *nom*

- Activer le protocole RIPng sur chacune des interfaces qui intervient dans le réseau

Routeur(config-if)#**ipv6 rip** *nom* **enable**

Vérifiez à l'aide de **sh ipv6 route**, **sh run** et **sh ipv6 rip database** puis testez la connectivité à l'aide d'un ping en IPv6 entre les 2 PCs.

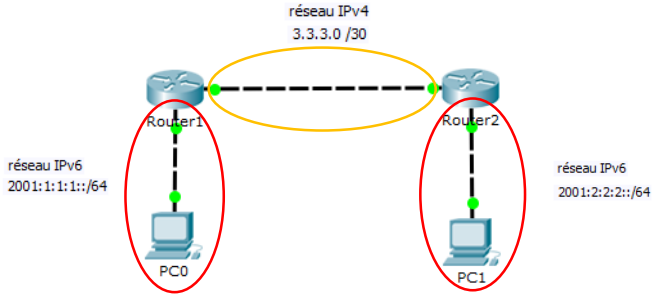
Comme vous voyez, l'utilisation de la double pile impose un accès complet à toute l'infrastructure réseau ainsi qu'une charge de travail assez importante mais par contre c'est assez fiable quand c'est bien configuré !

HEH be Sciences et technologies

Chapitre 3

2°) Tunneling

Le but ici est de pouvoir transporter des paquets IPv6 à travers un réseau qui fonctionne en IPv4.

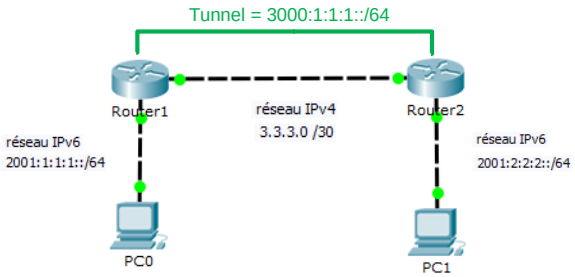


- Premièrement, il faut bien entendu configurer les réseaux d'extrémités avec les adresses IPv6 et les passerelles par défaut sur les PCs puis il faut configurer l'interface de sortie de chaque réseau avec l'adresse correspondante au réseau.

Chapitre 3

PS : n'oubliez pas d'appliquer la commande **ipv6 unicast-routing** sur les routeurs !

- Vérifiez la configuration et la connectivité entre chaque PC et son routeur de sortie fonctionne correctement. (show ipv6 route, show run, ping)
- Entre les deux routeurs, configurez des adresses IPv4 pour qu'ils puissent communiquer entre eux et vérifiez que cela fonctionne.
- Maintenant on va créer le tunnel qui va permettre d'encapsuler de l'IPv6 dans de l'IPv4.



Chapitre 3

Pour créer le tunnel on utilisera les commandes suivantes :

R1(config)#**interface tunnel** *numéro*

R1(config-if)#**ipv6 address** *@addresseIPv6/prefix*

R1(config-if)#**ipv6 enable**

R1(config-if)#**tunnel source** *@interface*

R1(config-if)#**tunnel destination** *@adresseIPv4*

R1(config-if)#**tunnel mode ipv6ip**

- Finalement il faut configurer un protocole de routage dynamique ou du routage statique entre les routeurs.

Par exemple ici, le plus simple est d'implémenter du routage statique :

R1(config)#**ipv6 route** *@réseauIPv6/préfix @tronçonsuivantIPv6*

3°) Traduction 6to4

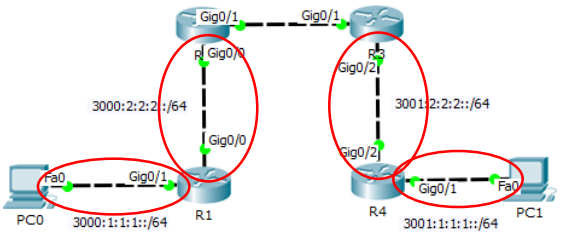
Le but ici est de traduire des adresses IPv6 en adresses IPv4 (et inversément) à l'aide du NAT64 (« Network Address Translation 64 »).

6to4 est une technique de tunneling où les hôtes 6to4 ne requièrent aucune configuration manuelle mais créent les adresses 6to4 par le biais d'une configuration automatique standard.

En fait le mécanisme 6to4 utilise le préfixe d'adresse global 2002:WWXX:YYZZ::/48 où WWXX:YYZZ représente la forme hexadécimale d'une adresse IPv4 publique (w.x.y.z) affectée à un site ou un hôte.

6to4 permet ainsi aux sites/hôtes compatibles IPv6 de communiquer au moyen du protocole IPv6 via une infrastructure IPv4 (comme Internet) et cela sans obtenir de préfixe d'adresse global IPv6 auprès d'un FAI.

Exemple :



- Premièrement, dans l'exemple ci-dessus, vous remarquez qu'on a 4 réseaux IPv6. La première chose à faire est donc de configurer des adresses IPv6 pour ceux-ci.

Il faut donc activer le routage IPv6 à l'aide de la commande **IPv6 unicast-routing** et ensuite configurer les adresses IP. Par exemple pour R1 :

R1(config)#**int** *gi0/1*

R1(config-if)#**ipv6 address** *3000:1:1:1::254/64*

R1(config-if)#**ipv6** *enable*

Chapitre 3

- Une fois que c'est fait pour chacune des interfaces des différents périphériques IPv6, vous pouvez vérifier que la connectivité entre deux périphériques fonctionne correctement (à l'aide d'un ping).
- Il faut maintenant implémenter un protocole de routage dynamique (tel que RIPng) sur les routeurs afin que les réseaux IPv6 puissent communiquer entre eux (c-à-d 3000:1:1:1/64 avec 3000:2:2:2/64 et 3001:1:1:1/64 avec 3001:2:2:2/64)

R1(config)#**ipv6 router rip** *RIPng*

R1(config)#**int** *gi0/1*

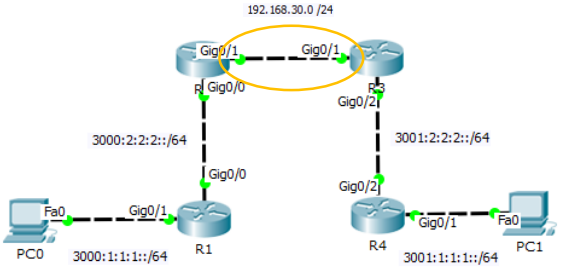
R1(config-if)#**ipv6 rip** *RIPng* **enable**

R1(config-if)#**int** *gi0/0*

R1(config-if)#**ipv6 rip** *RIPng* **enable**

- Il vous reste à vérifier que PC0 sait joindre R2 et que PC1 sait joindre R3.

Chapitre 3



- Entre R2 et R3 on va avoir un réseau IPv4, du style 192.168.30.0 /24
- Il va maintenant falloir traduire l'adresse IPv4 utilisée par R2 par exemple en hexadécimal :

192.168.30.1 → 11000000.10101000.00011110.00000001

→ 11000000.10101000.00011110.00000001

→ C0A8:1E01

- Grâce à ce calcul, on obtient l'adresse IPv6 à utiliser pour la création de notre tunnel 6to4 :

R2(config)#**int** tunnel0

R2(config-if)#**ipv6 address** *2002:C0A8:1E01::/48*

R2(config-if)#**tunnel source** *192.168.30.1 (ou gi0/1)*

R2(config-if)#**tunnel mode** *ipv6ip 6to4*

Bien entendu il faut faire la même chose sur R3.

- Finalement il ne nous reste plus qu'à mettre en place du routage statique pour assurer la connectivité via le tunnel 6to4.

R2(config)#**ipv6 route** *2002:C0A8:1E02::/48 Tunnel0*

R2(config)#**ipv6 route** *3001:1:1:1::/64 2002:C0A8:1E02::*

R2(config)#**ipv6 route** *3001:2:2:2::/64 2002:C0A8:1E02::*

A faire également sur R3 pour pouvoir joindre R2 ainsi que les réseaux 3000:1:1:1::/64 et 3000:2:2:2::/64.

DHCPv6

Comme pour IPv4, les adresses de monodiffusion globale IPv6 peuvent être configurées manuellement ou de façon dynamique. Concernant l'attribution dynamique des adresses de monodiffusion globale IPv6, deux méthodes sont possibles :

- Configuration automatique des adresses sans état (SLAAC)
- Protocole DHCP pour IPv6 (DHCPv6 avec état)

Au niveau de l'utilisation de la méthode SLAAC, un périphérique peut obtenir une adresse de monodiffusion globale IPv6 sans les services d'un serveur DHCPv6.

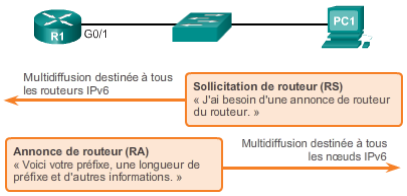
Le SLAAC utilise des messages d'annonce et de sollicitation de routeur ICMPv6 pour fournir les informations d'adressage et d'autres informations de configuration autres qui seraient normalement fournies par un serveur DHCP :

Message de sollicitation de routeur (RS) : lorsqu'un client est configuré pour obtenir ses informations d'adressage automatiquement via le processus SLAAC, celui-ci envoie un message RS au routeur.

Message d'annonce de routeur (RA) : les messages RA sont envoyés par les routeurs pour fournir des informations d'adressage aux clients configurés pour obtenir leurs adresses IPv6 automatiquement. Le message RA inclut le préfixe et la longueur de préfixe du segment local. Les clients utilisent ces informations pour créer leur propre adresse de monodiffusion globale IPv6.

Le processus SLAAC est dit « sans état », c-à-d qu'il ne fait appel à aucun serveur pour maintenir à jour les informations d'adresse réseau. *Contrairement au DHCP, aucun serveur SLAAC ne sait quelles adresses IPv6 sont utilisées et lesquelles sont disponibles.*

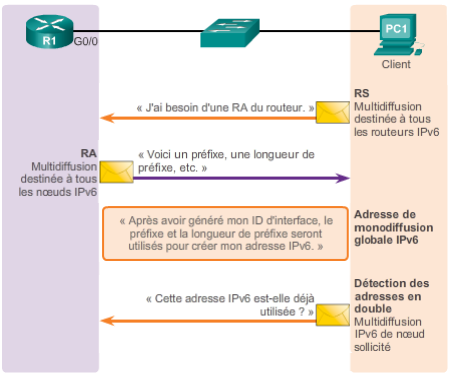
Représentation de la méthode SLAAC :



Chapitre 3

Fonctionnement du SLAAC :

Avant toute chose, pour qu'il puisse envoyer des messages RA, le routeur doit être activé en tant que routeur IPv6. → Router(config)# **ipv6 unicast-routing**



A l'étape 3, PC1 peut créer son propre IID unique de deux façons :

- **EUI-64** : à l'aide du processus EUI-64, PC1 crée un IID à partir de son adresse MAC de 48 bits.
- **Génération aléatoire** : l'IID de 64 bits peut être un nombre aléatoire généré par le système d'exploitation du client.

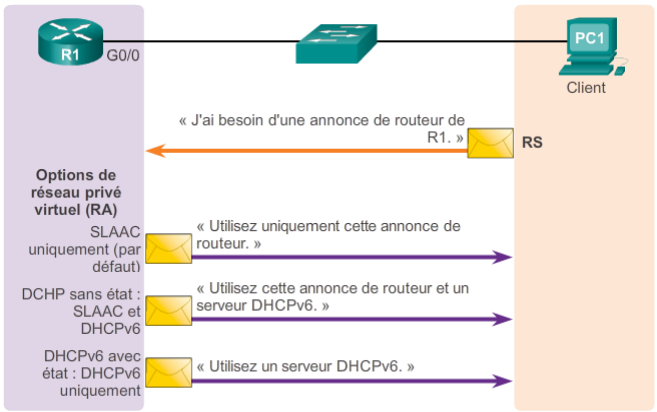
A l'étape 4, étant donné que SLAAC est un processus sans état, avant que PC1 puisse utiliser cette adresse IPv6 nouvellement créée, il doit vérifier qu'elle est unique.

Ce processus fait partie de la détection de voisin ICMPv6 et est appelé « détection d'adresses en double » (ou DAD pour Duplicate Address Detection).

Ce sont les paramètres indiqués dans le message RA qui déterminent si un client est configuré pour obtenir automatiquement ses informations d'adressage IPv6 via SLAAC, DHCPv6 ou une combinaison des deux.

Les messages RA ICMPv6 contiennent **deux indicateurs (« M » et « O »)** qui signalent l'option à utiliser par le client.

Différentes combinaisons des indicateurs **M** et **O** permettent aux messages RA d'indiquer une des trois options d'adressage pour le périphérique IPv6 :



Quelle que soit l'option utilisée, on recommande que tous les périphériques IPv6 effectuent une *détection des adresses en double* (**DAD**) sur toutes les adresses de monodiffusion, y compris les adresses configurées via SLAAC ou DHCPv6.

1) Option SLAAC

SLAAC est l'option par défaut sur les routeurs Cisco. Les indicateurs **M** et **O** sont tous deux définis sur **0** dans l'annonce de routeur

Cette option indique au client d'utiliser exclusivement les informations fournies dans le message RA. Il s'agit du préfixe, de la longueur du préfixe, du serveur DNS, du paramètre MTU et des informations sur la passerelle par défaut.

L'adresse de monodiffusion globale IPv6 est créée en combinant le préfixe indiqué dans l'annonce de routeur et un ID d'interface obtenu via le processus EUI-64 ou généré de manière aléatoire.

Les messages RA sont configurés sur une interface d'un routeur. Pour réactiver l'option SLAAC sur une interface qui a été définie sur une autre option, les indicateurs M et O doivent être réinitialisés à 0 :

Router(config-if)# **no ipv6 nd managed-config-flag** → Paramètre M = 0

Router(config-if)# **no ipv6 nd other-config-flag** → Paramètre O = 0

Chapitre 3

2) Option DHCPv6 sans état (annonce de routeur et DHCPv6)

Cette option ordonne le client à utiliser les informations dans le message RA pour l'adressage, mais les paramètres de configuration supplémentaires sont fournis par un serveur DHCPv6.

Dans ce cas, le client crée son adresse de monodiffusion globale IPv6 à l'aide du préfixe et de la longueur de préfixe indiqués dans le message RA (M = 0 et O = 1), et de l'IID généré via le processus EUI-64 ou aléatoirement.

Ensuite, le client communique alors avec un serveur DHCPv6 sans état pour obtenir des informations complémentaires non fournies dans le message RA (comme par exemple une liste d'adresses IPv6 de serveurs DNS).

Ce processus est appelé DHCPv6 sans état, car le serveur ne conserve aucune information sur l'état des clients (c'est-à-dire une liste des adresses IPv6 disponibles et attribuées). Le serveur DHCPv6 sans état fournit uniquement des paramètres de configuration pour les clients !

Pour modifier le message RA envoyé sur l'interface d'un routeur pour indiquer DHCPv6 sans état, utilisez la commande suivante :

Router(config-if)# **ipv6 nd other-config-flag** → Paramètre O = 1

3) Option DHCPv6 avec état

Dans ce dernier cas, qui est fort similaire au fonctionnement du DHCPv4, le message RA enjoint le client de ne pas utiliser les informations qu'il contient.

Toutes les informations d'adressage et de configuration doivent être obtenues auprès d'un serveur DHCPv6 avec état (car le serveur DHCPv6 maintient à jour les informations relatives à l'état des adresses IPv6).

Pour activer cette option, l'indicateur M doit avoir la valeur 1 et l'indicateur O n'a pas d'effet.

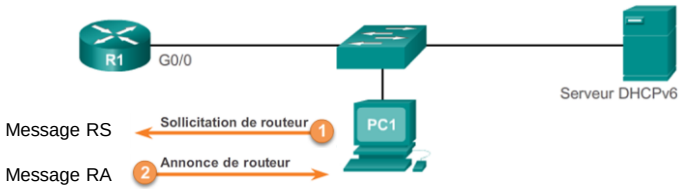
Pour passer celui-ci à 1, il faut utiliser la commande :

Router(config-if)# **ipv6 nd managed-config-flag** → Paramètre M = 1

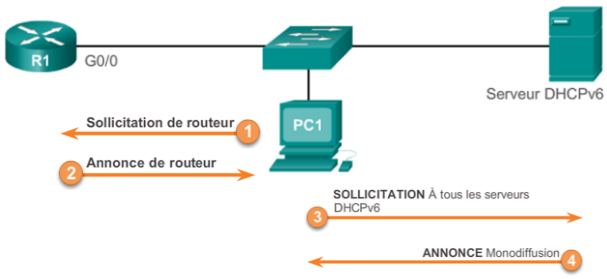
<u>Fonctionnement du DHCPv6 :</u>

Lorsqu'on utilise un DHCPv6 (avec ou sans état), le fonctionnement commence toujours par la réception d'un message RA ICMPv6 du routeur (en réponse à un message de sollicitation bien entendu).

Celui-ci, grâce aux valeurs des paramètres M et O, indiquera si le client utilise un DHCPv6 avec ou sans état.

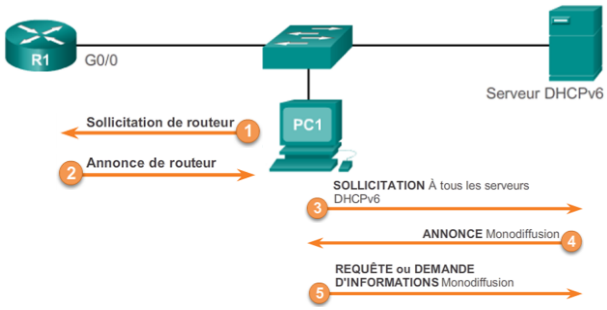


Le client envoie des messages DHCPv6 au serveur via le port de destination UDP 547 tandis que les messages DHCPv6 envoyés par le serveur au client utilisent le port de destination UDP 546.



Une fois que le client sait qu'il doit demander des informations à un serveur DHCPv6, il envoie un message SOLLICITATION DHCPv6 à l'adresse de multidiffusion IPv6 réservée pour tous les serveurs DHCPv6 (FF02::1:2).

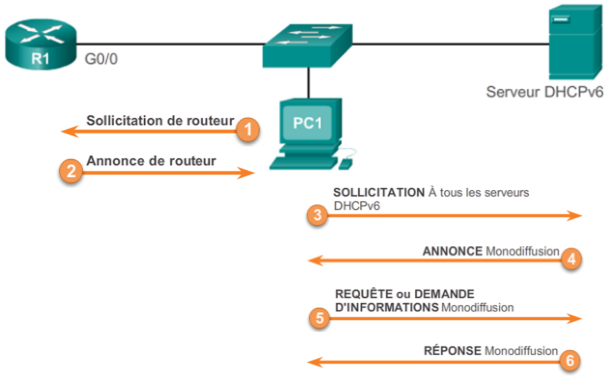
Un ou plusieurs serveurs DHCPv6 répondent par un message ANNONCE DHCPv6 afin d'informer le client qu'ils sont disponibles pour le service DHCPv6.



Le client répond au serveur par un message DHCPv6 REQUÊTE ou DEMANDE D'INFORMATIONS, selon qu'il utilise DHCPv6 avec ou sans état.

- **Client DHCPv6 sans état** : le client envoie un message DEMANDE D'INFORMATIONS DHCPv6 au serveur DHCPv6 demandant uniquement les paramètres de configuration, tels que l'adresse du serveur DNS.
- **Client DHCPv6 avec état** : le client envoie un message REQUÊTE DHCPv6 au serveur pour obtenir du serveur une adresse IPv6 et tous les autres paramètres de configuration.

Finalement, Le serveur envoie un message RÉPONSE DHCPv6 au client contenant les informations demandées dans le message REQUÊTE ou DEMANDE D'INFORMATIONS



Chapitre 3

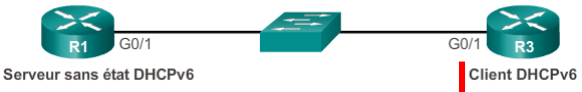
Maintenant que nous avons les différentes options qui s'offrent à nous en tant que paramètres afin d'obtenir les informations IPv6, voyons un peu comment configurer le matériel afin d'utiliser ces options.

Configuration du DHCPv6 sans état

Il va falloir passer par 4 étapes :

- Activation du routage IPv6 à l'aide de la commande **ipv6 unicast-routing**
- Configuration d'un pool DHCPv6 à l'aide de la commande **ipv6 dhcp pool** *pool-name.* Cela crée un pool et sélectionne le routeur en mode de configuration DHCPv6.
- Configuration des paramètres du pool comme l'adresse du serveur DNS à l'aide de la commande **dns-server** *@dns_address* et le nom de domaine à l'aide de la commande **domain-name** *@name.*
- Configuration de l'interface DHCPv6 à l'aide de la commande de mode de configuration d'interface **ipv6 dhcp server** *pool-name* qui relie le pool DHCPv6 à l'interface. L'indicateur O doit être modifié pour passer de 0 à 1 à l'aide de la commande d'interface **ipv6 nd other-config-flag**.

Exemple :




```
R1(config)# ipv6 unicast-routing
R1(config)# ipv6 dhcp pool IPV6-STATELESS
R1(config-dhcpv6)# dns-server 2001:db8:cafe:aaaa::5
R1(config-dhcpv6)# domain-name example.com
R1(config-dhcpv6)# exit
R1(config)# interface g0/1
R1(config-if)# ipv6 address 2001:db8:cafe:1::1/64
R1(config-if)# ipv6 dhcp server IPV6-STATELESS
R1(config-if)# ipv6 nd other-config-flag
```

```
R3(config)# interface g0/1
R3(config-if)# ipv6 enable
R3(config-if)# ipv6 address autoconfig
```

Le routeur client (R3) a besoin d'une adresse link-local IPv6 sur l'interface pour envoyer et recevoir des messages IPv6 tels que les messages RS et DHCPv6.

L'adresse link-local d'un routeur est créée automatiquement lorsqu'IPv6 est activé sur l'interface. Cela peut se produire lorsqu'une adresse de monodiffusion globale est configurée sur l'interface ou lorsque vous exécutez la commande **ipv6 enable**.

La commande **ipv6 address autoconfig** active la configuration automatique de l'adressage IPv6 à l'aide de SLAAC. Un message RA est ensuite utilisé pour indiquer au routeur client d'utiliser DHCPv6 sans état.

Au niveau de la vérification de la configuration du serveur DHCPv6 sans état, la commande **show ipv6 dhcp pool** vérifie le nom du pool DHCPv6 et ses paramètres. Le nombre de clients actifs est 0, car le serveur ne conserve aucune information sur les états.

```
R1# show ipv6 dhcp pool
DHCPv6 pool: IPV6-STATELESS
  DNS server: 2001:DB8:CAFE:AAAA::5
  Domain name: example.com
  Active clients: 0
```

La commande **show running-config** permet également de vérifier toutes les commandes qui ont été configurées précédemment.

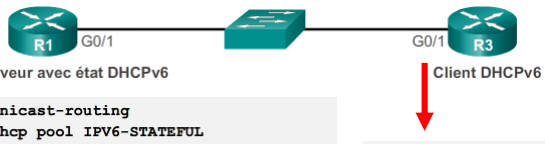
Au niveau de la vérification de la configuration du client DHCPv6, la commande **show ipv6 interface** indique « Stateless address autoconfig enabled », ce qui signifie que la configuration automatique des adresses sans état est activée sur le routeur et qu'il dispose d'une adresse de monodiffusion globale IPv6.

Configuration du DHCPv6 avec état

La configuration d'un serveur DHCPv6 avec état est très similaire à celle d'un serveur sans état (4 étapes également). La principale différence réside dans le fait que les serveurs avec état disposent également des informations d'adressage IPv6 :

- Activation du routage IPv6 à l'aide de la commande **ipv6 unicast-routing**
- Configuration d'un pool DHCPv6 à l'aide de la commande **ipv6 dhcp pool** *pool-name.*
- Configuration de tous les paramètres du pool ! En plus de l'adresse du serveur DNS à l'aide de la commande **dns-server** *@dns_address* et du nom de domaine à l'aide de la commande **domain-name** *@name, l*a commande **address** *prefix/length* sert à indiquer le pool d'adresses à attribuer par le serveur. L'option **lifetime** indique la durée de validité et la durée préférée des baux, en secondes.
- Configuration de l'interface DHCPv6 à l'aide de la commande de mode de configuration d'interface **ipv6 dhcp server** *pool-name* qui relie le pool DHCPv6 à l'interface. L'indicateur M doit être modifié pour passer de 0 à 1 à l'aide de la commande d'interface **ipv6 nd managed-config-flag**.

Exemple :




```
R1(config)# ipv6 unicast-routing
R1(config)# ipv6 dhcp pool IPV6-STATEFUL
R1(config-dhcp)# address prefix 2001:DB8:CAFE:1::/64
                  lifetime infinite
R1(config-dhcp)# dns-server 2001:db8:cafe:aaaa::5
R1(config-dhcp)# domain-name example.com
R1(config-dhcp)# exit
R1(config)# interface g0/1
R1(config-if)# ipv6 address 2001:db8:cafe:1::1/64
R1(config-if)# ipv6 dhcp server IPV6-STATEFUL
R1(config-if)# ipv6 nd managed-config-flag
```

```
R3(config)# interface g0/1
R3(config-if)# ipv6 enable
R3(config-if)# ipv6 address dhcp
```

Le routeur R3 est configuré en tant que client grâce à la commande **ipv6 address dhcp**.

Au niveau de la vérification de la configuration du serveur DHCPv6 avec état, la commande **show ipv6 dhcp pool** vérifie le nom du pool DHCPv6 et ses paramètres. Le nombre de clients actifs est maintenant à 1, puisqu'on a R3 qui reçoit son adresse de monodiffusion globale IPv6 de ce serveur.

```
R1# show ipv6 dhcp pool
DHCPv6 pool: IPV6-STATEFUL
  Address allocation prefix: 2001:DB8:CAFE:1::/64 valid
4294967295 preferred 4294967295 (1 in use, 0 conflicts)
  DNS server: 2001:DB8:CAFE:AAAA::5
  Domain name: example.com
  Active clients: 1
```

La commande **show ipv6 dhcp binding** affiche la liaison automatique entre l'adresse link-local du client et l'adresse attribuée par le serveur.

```
R1# show ipv6 dhcp binding
Client: FE80::32F7:DFF:FE25:2DE1
  DUID: 0003000130F70D252DE0
  Username : unassigned
  IA NA: IA ID 0x00040001, T1 43200, T2 69120
    Address: 2001:DB8:CAFE:1:5844:47B2:2603:C171
            preferred lifetime INFINITY, , valid lifetime INFINITY,
```

Dans notre exemple, il s'agit de l'interface G0/1 de R3, qui est liée à l'adresse de monodiffusion globale IPv6, 2001:DB8:CAFE:1:5844:47B2:2603:C171, attribuée par le serveur DHCPv6 (R1).

HEH.be Sciences et technologies

Chapitre 3

Au niveau de la vérification de la configuration du client DHCPv6 avec état, la commande **show ipv6 interface** permet de vérifier sur le client DHCPv6 (R3) l'adresse de monodiffusion globale IPv6 qui a été attribuée par le serveur DHCPv6.

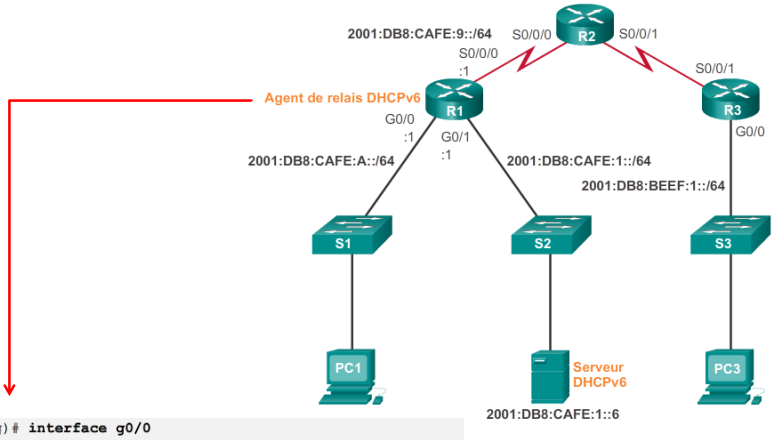
Comme nous l'avons vu pour le DHCPv4, si le serveur DHCP se trouve sur un réseau différent de celui du client, alors un routeur peut être configuré en tant qu'agent de relais DHCP. Cette configuration est également possible avec un DHCPv6.

La configuration d'un agent de relais DHCPv6 s'effectue à l'aide de la commande **ipv6 dhcp relay destination**. Cette commande est configurée sur l'interface reliée au client DHCPv6 en utilisant l'adresse du serveur DHCPv6 comme destination.

La commande **show ipv6 dhcp interface** permet de vérifier que l'interface choisie est bien en mode relais et qu'elle est configurée avec l'adresse du serveur DHCPv6.

Chapitre 3

Exemple :




```
R1(config)# interface g0/0
R1(config-if)# ipv6 dhcp relay destination 2001:db8:cafe:1::6
R1(config-if)# end
R1# show ipv6 dhcp interface g0/0
GigabitEthernet0/0 is in relay mode
  Relay destinations:
    2001:DB8:CAFE:1::6
```