Chapitre 33 : Ipv6 (Partie 3)

Dans cette vidéo nous allons continuer le cours sur l'IPV6.
Nous allons revoir une chose que nous avons lors du du précédent cours, nous verrons ensuite comment est composé l'entête IPV6, nous explorerons différents protocoles, les protocoles Neighbor Discovery Protocol (NDP) et SLAAC, nous finirons par apprendre comment configurer un routage statique en IPV6.

Nous allons revoir rapidement comment est composé l'IPV6, tout d'abord commençons par définir ce qu'est qu'une RFC.
Une RFC (Request for Comment) est une publication de l'ISOC (Internet Society) et de ses organisations associés comme l'IETF (Internet Enginneering Task Force), pour définir les normes officiels des protocoles, procédures et spécifications Internet etc.…
Donc si l'on veut en savoir sur le protocol OSPF par exemple il suffit de nous rendre sur l'RFC qui documente le protocole OSPF.
Le titre de l'RFC 5952 est 'A recommendation for IPV6 Address Text Representation' en Français 'Une recommendation pour les textes représentatifs des adresses IPV6'
Avant la publication de cette RFC, les représentation des adresses IPV6 était plus flexibles.
- On pouvait supprimer des 0 premiers
- On pouvait remplacer tous les 0 par des ::
- On pouvait utiliser les majuscules 0xA, B, C, D, E, F ou minuscules 0xa, b, c, d, e, f

La RFC 5952 a permis une standardisation de la représentation des adresses IPV6.
Sa publication a mis en place les changements suivants :
- Les 0 placés en début doivent obligatioment être supprimés
Exemple : 2001:0db8:0000:0001:0f2a:4fff:fea3:00b1→ 2001:db8:0:1:f2a:4fff:fea3:b1

- Les :: doivent obligatoirement être utilisés lorsque plusieurs groupes de quatres 0 sont placés de manière consécutives.
Exemple : 2001:0000:0000:0000:0f2a:0000:0000:00b1 → 2001::f2a:0:0:b1

(Lorsqu'il n'y a qu'un groupe de quatres 0 on n'utilise pas les ' ;;')
- Lorsqu'il y deux fois des groupes de quatres 0 séparés et que l'on peut utiliser deux fois les ' ::' on ne l'utilisera que pour celui le plus à gauche.
Exemple : 2001:0db8:0000:0f2a:0000:0000:0000:00b1 → 2001:db8::f2a:0:0:b1

- Les caractère hexadécimale 'a','b','c','d','e' et 'f' doivent obligatoirement être écris en minuscules et non pas en majuscules.

Il n'est pas grave si les caractères sont quelques fois écris en majuscules car aussi sur les routeurs il sont en majuscules alors que ça n'est pas réglementaire.

Voyons à présent de quoi se compose l'entête IPV6 :

Fixed header format

Offsets	Octet	0								1								2								3							
Octet	Bit	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
0	0	Version				Traffic Class								Flow Label																			
4	32	Payload Length																Next Header								Hop Limit							
8	64	Source Address																															
12	96																																
16	128																																
20	160																																
24	192	Destination Address																															
28	224																																
32	256																																
36	288																																

Voici en comparaison l'entête IPV4 que l'on a vu auparavant dans les précédent cours :

IPv4 header format

Offsets	Octet	0								1								2								3							
Octet	Bit	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
0	0	Version				IHL				DSCP						ECN		Total Length															
4	32	Identification																Flags			Fragment Offset											
8	64	Time To Live								Protocol								Header Checksum															
12	96	Source IP Address																															
16	128	Destination IP Address																															
20	160	Options (if IHL > 5)																															
24	192																																
28	224																																
32	256																																

L'entête IPV6 semble plus simple, les choses qui font que l'ipv6 est plus simple est le fais que ce soit un format d'entête fixe. L'entête IPV4 a un format variable de 12 à 60bits tandis que l'IPV6 a une entête fixe de 40bits c'est pour cela qu'il y a une partie pour la longueur du Payload et non pas pour la partie de l'entête comme dans IPV4.
Le processus de l'IPV6 est plus simple pour les routeurs donc les performance sont en conséquences améliorés.
Nous allons à présent détailler chaque partie utilisé :

- Version : d'une longueur de 4bits, il indique la version de l'IP utilisé. La valeur fixé est de 6 (0b0110) pour indiquer IP version 6

- Traffic class : d'une longueur de 8bits, il est utilisé pour la QoS (Quality of Service), pour indiquer la priorité du trafique. Par exemple le trafique IP d'un téléphone, un appel vidéo, etc. il aura une valeur de Traffic Class qui indique la priorité à travers les autres trafiques du réseau.

- Flow Label : d'une longueur de 20bits, il est utilisé pour identifier les flux spécifique de communication (la communication entre une source spécifique et sa destination)

- Longueur du Payload : Il indique la longueur du Payload (le segment de couche 4 encapsulé) en Octets. La longueur de de l'entête IPV6 n'est pas inclus car elle est toujours de 40 octets.

- Next Header : d'une longueur de 8 bits, il permet d'identifier le type de l'entête suivante (l'entête du segment encapsulé), par exemple TCP ou UDP.
Il a la même fonction que la partie « Protocol » de l'entête IPV4

- Hop Limit : d'une longueur de 8bits, la valeur de cette partie est soustraite par 1 à chaque fois qu'un routeur le repartage. S'il atteint 0 le paquet est perdue.
Il a la même fonction que la partie « TTL » de l'entête IPV4.

- Source/Destination : d'une longueur de 128 bits chacun (Source : 128, Destination : 128)
Ces parties contiennent l'adresse IPV6 pour la source du paquet ainsi que sa destination.

Un nœud IPV6 sollicité pour une adresse multicast est calculé à partir d'une adresse unicast.
L'adresse commence par un préfixe fixe par exemple : ff02:0000:0000:0000:0000:0001:ff
puis par l'ajout des 6 derniers chiffres hexadécimal de l'adresse Unicast

Prenons pour exemple l'adresse Unicast : 2001:0db8:0000:0001:0f2a:4fff:fea3:00b1

Pour générer un nœud IPV6 les derniers chiffres de l'adresse Unicast vont être utilisé ici ce sera : **a3:00b1**
l'adresse final utilisé sera : ff02::1:ffa3:b1

Pour une adresse Unicast : 2001:0db8:0000:0001:0489:4eda:073a:12b8
les 6 derniers chiffres de cette adresse sont **3a:12b8**
L'adresse final utilisé sera donc : ff02::1:ff3a:12b8

```
R1#sh ipv6 int g0/0
GigabitEthernet0/0 is up, line protocol is up
  IPv6 is enabled, link-local address is FE80::EF8:22FF:FE36:8500
  No Virtual link-local address(es):
  Global unicast address(es):
    2001:DB8::EF8:22FF:FE36:8500, subnet is 2001:DB8::/64 [EUI]
  Joined group address(es):
    FF02::1
    FF02::2
    FF02::1:FF36:8500
  MTU is 1500 bytes
  ICMP error messages limited to one every 100 milliseconds
  ICMP redirects are enabled
  ICMP unreachables are sent
  ND DAD is enabled, number of DAD attempts: 1
  ND reachable time is 30000 milliseconds (using 30000)
  ND advertised reachable time is 0 (unspecified)
  ND advertised retransmit interval is 0 (unspecified)
  ND router advertisements are sent every 200 seconds
  ND router advertisements live for 1800 seconds
  ND advertised default router preference is Medium
  Hosts use stateless autoconfig for addresses.
```

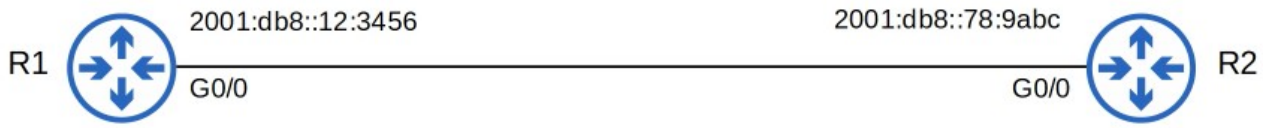
On peut voir que dans la partie encadré en rouge le routeur a joins les deux groupes multicast FF02::1 et FF02::2
il est à noter que le routeur a également joins l'adresse FF02::1:FF36:8500 ceci est le nœud sollicité pour l'adresse Multicast, on remarque que les 6 derniers chiffres sont les mêmes que ceux de l'adresse IPV6 utilisé.

Nous allons à présent expliquer comment fonctionne le protocole NDP (Neighbor Discovery Protocol) et son utilité pour IPV6.
Le protocole NDP (Neighbor Discovery Protocol) à des fonctions très variés, et l'unes de ces fonctions est de remplacer ARP, qui n'est plus utilisé dans IPV6.

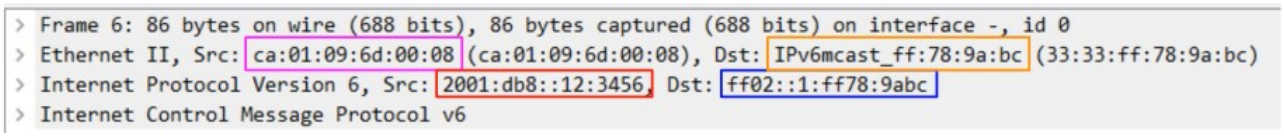
La fonction ARP de NDP utilise ICMPv6 et les nœud solicités de l'adresse multicast pour apprendre l'adresse MAC des autres hôtes du réseau. Pour rappel le protocole ARP utilise des requête de message en Broadcast. La méthode utilisé pour IPV6 est plus efficace car ce sont les hôtes

d’adresses spécifiques qui sont utilisés contrairement à des messages envoyés en Broadcast pour tous les hôtes.
Deux types de messages sont utilisés :
1) Neighbor Solicitation (NS) = ICMPv6 Type 135
2) Neighbor Advertisement (NA) = ICMPv6 Type 136

Voici le fonctionnement basique d’un message Neighbor Solicitation (NS) l’équivalent NDP d’une requête ARP
Nous utiliserons la topologie suivante :

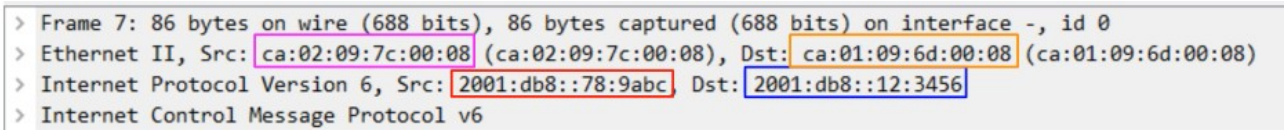


Disons que R1 veut faire un ping de l’adresse R2, pour cela il va d’abord envoyer une requête pour connaître l’adresse MAC
Pour comprendre comment cela est différent d’une requête ARP comparons les différentes adresses utilisés dans une capture Wireshark



On peut voir sur cette capture :
- En rouge : l’adresse IP source : R1 G0/0
- En bleu : l’adresse IP de destination avec l’adresse du nœud sollicité pour l’adresse Multicast
- En rose : L’adresse source MAC
- En jaune : l’adresse MAC Multicast basé sur l’adresse du nœud sollicité de R2

Voici à présent le fonctionnement basique d’un message Neighbor Advertisement (NA)
Pour répondre à la requête de R1 lui demandant son adresse MAC, R2 va répondre basiquement en lui envoyant son adresse MACvoyons donc les différentes adresses utilisés dans le message dans Wireshark :



- En rouge : l’adresse IP source (ici R2)
- En bleu : l’adresse IP de destination (ici R1)
- En rose : l’adresse MAC source
- En jaune : l’adresse MAC de destination

Voyons comment sont utilisés les Neighbor Table pour IPV6 dans notre exemple, il est possible de l'afficher avec la commande : `show ipv6 neighbor`

```
R1#show ipv6 neighbor
IPv6 Address                              Age Link-layer Addr State Interface
FE80::C802:9FF:FE7C:8                       0 ca02.097c.0008  REACH Gi0/0
2001:DB8::78:9ABC                           0 ca02.097c.0008  REACH Gi0/0
```

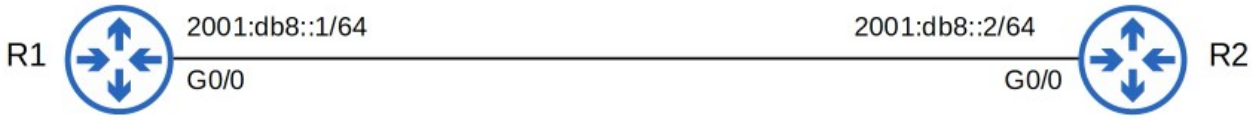
```
R2#show ipv6 neighbor
IPv6 Address                              Age Link-layer Addr State Interface
FE80::C801:9FF:FE6D:8                       0 ca01.096d.0008  REACH Gi0/0
2001:DB8::12:3456                           0 ca01.096d.0008  REACH Gi0/0
```

On peut voir d'abord la colonne des adresses IPV6 sur laquelle est contenu l'age qui indique depuis combien de temps en minutes les adresses IPv6 ont été identifiés, le Link-Layer Address montre les adresses MAC, la colonne Interface montre sur quelles interface cela à été appris.

Nous allons expliquer encore une chose à propos du protocole NDP
Une autre fonction de NDP permet aux hôtes de découvrir automatiquement les routeurs sur le réseau local.
Deux messages sont utilisés pour ce processus :
1) Router Solicitation (RS) = ICMPv6 Type 133
→ ils sont envoyés à des adresses Multicast FF02::2 (à tous les routeurs)
→ ce message demande à tous les routeurs du réseau local de s'identifier eux même
→ ce message est envoyé lorsqu'une interface est activé et que l'hôte est connecté au réseau

2) Router Advertisement (RA) = ICMPv6 Type 134
→ ces messages sont envoyés à des adresses multicast FF02::1 (à tous les nœud)
→ Le routeur annonce sa présence en plus d'autres informations à propos du réseau local
→ ces messages sont envoyés en réponse aux messages RS
→ ils sont aussi envoyés périodiquement, même si le routeur n'a pas reçu de RS

Nous allons utiliser la topologie suivante pour mieux comprendre :



R2 envoie automatiquement un message RS pour vérifier s'il y a un routeur sur le réseau local
R1 répond en s'identifiant et en envoyant un RA au routeur R2

Nous allons à présent expliquer comment fonctionne SLAAC.
SLAAC est l'acronyme de Stateless Address Auto-Configuration
C'est une autre manière pour configurer des adresses IPV6, en utilisant SLAAC, les hosts utilisent les messages RS/RA pour apprendre le préfixe IPV6 du réseau local (par exemple : 2001:db8::/64) ce qui permet de générer automatiquement une adresse IPV6.
Lorsque l'on utilise la commande : `ipv6 address` ***`prefix/prefix-length`*** `eui-64` il nous faut manuellement entrer le préfixe. En utilisant la commande :
`ipv6 address autoconfig` il ne devient plus nécessaire d'entrer le préfixe. L'appareil utilise NDP pour apprendre le préfixe utilisé dans le réseau local.
L'appareil utilisera EUI-64 pour générer l'interface ID, ou bien il sera automatiquement généré.

Voici un exemple de la commande utilisé sur un routeur Cisco :

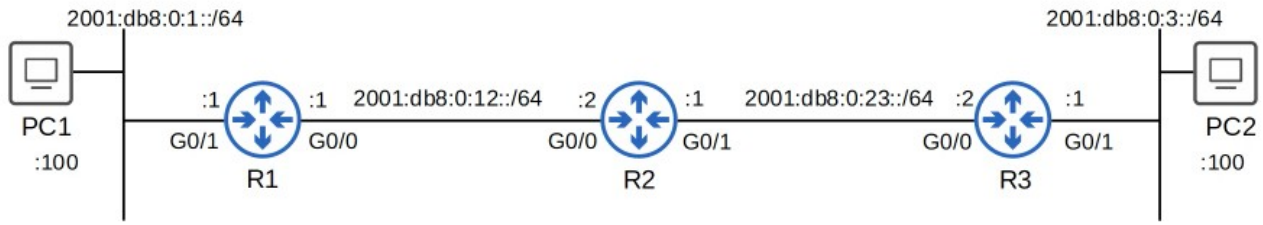
```
R2(config)#int g0/0
R2(config-if)#ipv6 address autoconfig
R2(config-if)#do show ipv6 interface brief
GigabitEthernet0/0     [up/up]
    FE80::EF8:22FF:FE56:A600
    2001:DB8::EF8:22FF:FE56:A600
GigabitEthernet0/1     [administratively down/down]
    unassigned
GigabitEthernet0/2     [administratively down/down]
    unassigned
GigabitEthernet0/3     [administratively down/down]
    unassigned
```

Une dernière chose que nous allons expliquer à propos de NDP est le DAD (Duplicate Address Detection) qui permet aux hôtes de vérifier si d'autres appareils sur le réseau local utilisent la même adresse IPV6.
A n'importe quelle moment ou une interface IPV6 est activé (avec la commande : `no shutdown`) ou qu'une adresse IPV6 est configurer sur une interface (en utilisant les méthodes : manuel, SLAAC, etc.) il fait fonctionner DAD.
DAD utilise deux messages utilisés plus tôt : NS et NA
L'hôte va envoyer un NS à sa propre adresse IPV6. S'il ne reçoit pas de réponse, il sais que l'adresse est unique sur le réseau. S'il reçoit une réponse, cela signifie qu'un autre hôte sur le réseau utilise également cette même adresse.
Sur un routeur Cisco on reçoit le message suivant si la même adresse est détecté :

```
*Oct 31 11:28:48.318: %IPV6_ND-4-DUPLICATE: Duplicate address 2001:DB8::1 on GigabitEthernet0/0
```

Voyons à présent comment configurer le routage statique d'une adresse IPV6.
Le routage IPV6 fonctionne de la même manière que le routage IPV4, même si les deux processus sont séparés sur le routeur et que les deux tables de routage sont aussi séparés.
Le routage IPV4 est activé par défaut, tandis que le routage IPV6 est désactivé par défaut et doit être activé avec la commande `ipv6 unicast-routing`
Si le routage IPV6 est désactivé, le routeur sera capable d'envoyer et de recevoir le trafique IPV5, mais ne pourra pas « router » le trafique IPV6 (ne partagera le trafique entre les réseau)

Pour démonter le fonctionnement d'IPV6 nous utiliserons la topologie suivante :



Voici la table de routage du routeur R1 :

```
R1#show ipv6 route
IPv6 Routing Table - default - 5 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
       B - BGP, HA - Home Agent, MR - Mobile Router, R - RIP
       H - NHRP, I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea
       IS - ISIS summary, D - EIGRP, EX - EIGRP external, NM - NEMO
       ND - ND Default, NDp - ND Prefix, DCE - Destination, NDr - Redirect
       RL - RPL, O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1
       OE2 - OSPF ext 2, ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
       la - LISP alt, lr - LISP site-registrations, ld - LISP dyn-eid
       lA - LISP away, a - Application
C   2001:DB8:0:1::/64 [0/0]
     via GigabitEthernet0/1, directly connected
L   2001:DB8:0:1::1/128 [0/0]
     via GigabitEthernet0/1, receive
C   2001:DB8:0:12::/64 [0/0]
     via GigabitEthernet0/0, directly connected
L   2001:DB8:0:12::1/128 [0/0]
     via GigabitEthernet0/0, receive
L   FF00::/8 [0/0]
     via Null0, receive
```

Comme pour l'adresse IPV4 un réseau de routage est automatiquement ajouté pour chaque réseau connecté. (La lettre C pour « connected » est utilisé dans le résultat de la commande)
Aussi un routage en localhost est automatiquement ajouté pour chaque adresse configuré sur le routeur. (La lettre L pour « local » est utilisé dans le résultat de la commande)
Une autre chose à préciser est que les adresses link-local ne sont pas ajoutés à la table de routage.

Voici la commande utilisé pour le routage statique d'une adresse IPV6 :
`ipv6 route` *`destination/prefix-length {next-hop | exit-interface [next-hop]}[ad]`*

La première partie est compréhensible, il faut indiquer l'adresse IP de destination ainsi que la longueur du préfixe dans la deuxième partie entre crochet il faut indiquer soit le next-hop ou bien l'interface de sortie, si l'on indique l'interface de sortie, le next-hop devient à ce moment là facultatif. Il y a ensuite le « ad » pour Administrative Distance qui est optionnel et qui permet d'entrer un routage floating static.

Dans un routage statique « directement attaché » il ne faut préciser que l'interface de sortie.
La commande sera donc la suivante :
`ipv6 route` *`destination/prefix-length exit-interface`*
Par exemple pour R1 on utilisera cette commande :
`R1(config)#ipv6 route 2001:db8:0:3 ::/64 g0/0`

Pour un routage statique récursif, seulement le next hop est précisé.
La commande sera donc la suivante :
`ipv6 route` `destination/prefix-Length next-hop`
Sur R1 on utilisera la commande suivante :
`R1(config)#ipv6 route 2001:db8:0:3 ::/64 2001:db8:0:12::2`

La dernière façon de faire le routage statique est la méthode de la « spécification totale » ou l'interface de sortie et le next-hop sont précisés. La commande sera la suivante :
`ipv6 route` `destination/prefix-Length exit-interface next-hop`
Sur R1 on utilisera la commande suivante :
`R1(config)#ipv6 route 2001:db8:0:3 ::/64 g0/0 2001:db8:0:12::2`

Une chose à préciser avec la première méthode (directement attaché), dans IPV6 on ne peut pas utiliser un routage statique directement attaché si l'interface est une interface Ethernet, il faut que l'interface doit d'un autre type comme par exemple une interface Serial.
La commande utilisé pour R1 ne sera donc pas fonctionnel.

Voyons à présent quelques exemples pour la configuration :
Un routage en réseau :

```
R1(config)#ipv6 route 2001:db8:0:3::/64 2001:db8:0:12::2
```

Le routage d'un hôte :

```
R2(config)#ipv6 route 2001:db8:0:1::100/128 2001:db8:0:12::1
R2(config)#ipv6 route 2001:db8:0:3::100/128 2001:db8:0:23::2
```

Le routage par défaut :

```
R3(config)#ipv6 route ::/0 2001:db8:0:23::1
```

Une chose à préciser avec la commande suivante :

```
R1(config)#ipv6 route 2001:db8:0:3::/64 FE80::EF8:22FF:FEE6:D300
% Interface has to be specified for a link-local nexthop
R1(config)#
R1(config)#ipv6 route 2001:db8:0:3::/64 g0/0 FE80::EF8:22FF:FEE6:D300
R1(config)#do show ipv6 route
IPv6 Routing Table - default - 6 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
       B - BGP, HA - Home Agent, MR - Mobile Router, R - RIP
       H - NHRP, I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea
       IS - ISIS summary, D - EIGRP, EX - EIGRP external, NM - NEMO
       ND - ND Default, NDp - ND Prefix, DCE - Destination, NDr - Redirect
       RL - RPL, O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1
       OE2 - OSPF ext 2, ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
       la - LISP alt, lr - LISP site-registrations, ld - LISP dyn-eid
       lA - LISP away, a - Application
C   2001:DB8:0:1::/64 [0/0]
     via GigabitEthernet0/1, directly connected
L   2001:DB8:0:1::1/128 [0/0]
     via GigabitEthernet0/1, receive
S   2001:DB8:0:3::/64 [1/0]
     via FE80::EF8:22FF:FEE6:D300, GigabitEthernet0/0
C   2001:DB8:0:12::/64 [0/0]
     via GigabitEthernet0/0, directly connected
L   2001:DB8:0:12::1/128 [0/0]
     via GigabitEthernet0/0, receive
L   FF00::/8 [0/0]
     via Null0, receive
```

On peut voir que la commande n'a pas fonctionné au départ car le routeur ne parvient pas à préciser à quelle interface le routeur est connecté et ne peut donc pas préciser le next hop.
C'est pour cela qu'il faut préciser en spécification totale pour cette commande.