

IPv6 sous UNIX/LINUX

Noms et prénoms des étudiants : Omar BITEYE , Abdel-malik FOFANA

Le but de ce TP est une initiation à IPv6. Vous êtes fortement encouragés à relire votre cours, ainsi que le document complémentaire IPV6 en anglais sur le Drive, et à faire une recherche sur le Web, en particulier pour le compte rendu.

1 Trouvez l'adresse IPv6 de vos machines

1.1 Tester si Ipv6 est déjà présent sur votre machine virtuelle (cmd ifconfig -a) et renseigner les informations suivantes associées à l'interface eth0 :

```
wlp0s20f3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 10.10.44.155 netmask 255.255.192.0 broadcast 10.10.63.255
    inet6 fe80::aaf:93ff:70a3:d75e prefixlen 64 scopeid 0x20<link>
    ether 98:5f:41:66:05:8a txqueuelen 1000 (Ethernet)
    RX packets 1032853 bytes 1161849013 (1.1 GB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 305851 bytes 94588860 (94.5 MB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

Adresse IPv4 : 10.10.44.155

Adresse MAC : 98:5f:41:66:05:8a

1.2 Combien d'adresses IPv6 différentes trouvez vous sur l'interface eth0 ?

Réponse : il y a une seule adresse ipv6 : fe80::aaf:93ff:70a3:d75e

1.3 S'il y a plusieurs adresses IPv6, on s'intéressera à celle commençant par "fe80". Indiquez l'adresse complète ci-dessous :

Réponse : fe80::aaf:93ff:70a3:d75e

1.4 Quelle est la taille de cette adresse ?

Réponse : La taille d'une adresse IPv6 est toujours de 128 bits ou 16 octets, quel que soit le format dans lequel elle est affichée.

1.5 Cette adresse « fe80 :.... » a-t-elle un format particulier ? si oui lequel ?

Réponse : L'adresse fe80::aaf:93ff:70a3 est une adresse IPv6 link-local avec le préfixe fe80::/10, utilisée pour les communications au sein du réseau local. Le format est le même que pour toutes les adresses IPv6 link-local, avec un préfixe fe80 et un identifiant d'interface unique

1.6 A quoi correspond cette adresse par rapport à IPv4 ? Aidez vous du support de cours, du RFC 2373 et de l'Internet

Réponse :

L'adresse IPv6 fe80::aaf:93ff:70a3:d75e est une adresse link-local utilisée uniquement pour les communications sur le réseau local. Elle correspond, en IPv6, aux adresses IPv4 link-local dans la plage 169.254.0.0/16. Ces adresses ne sont pas routables et sont générées automatiquement par chaque interface réseau.

En IPv6, les adresses link-local commencent par fe80::/64 (défini dans le RFC 2373, remplacé par le RFC 4291). Elles ont une taille de 128 bits (contre 32 bits en IPv4). Leur suffixe peut être dérivé de l'adresse MAC via le format EUI-64, ou assigné dynamiquement.

1.7 Pourquoi si je tape ping6 fe80:.... , la commande me donne une erreur ? Comment faire marcher le ping ?

```
(maliki@maliki-club) - [~]  
$ ping6 fe80::aaf:93ff:70a3:d75e  
PING fe80::aaf:93ff:70a3:d75e(fe80::aaf:93ff:70a3:d75e) 56 data bytes  
^C  
--- fe80::aaf:93ff:70a3:d75e ping statistics ---  
12 packets transmitted, 0 received, 100% packet loss, time 11286ms  
  
(maliki@maliki-club) - [~]  
$ ping6 fe80::aaf:93ff:70a3:d75e%wlp0s20f3  
PING fe80::aaf:93ff:70a3:d75e%wlp0s20f3(fe80::aaf:93ff:70a3:d75e%wlp0s20f3) 56 data bytes  
64 bytes from fe80::aaf:93ff:70a3:d75e%wlp0s20f3: icmp_seq=1 ttl=64 time=0.050 ms  
64 bytes from fe80::aaf:93ff:70a3:d75e%wlp0s20f3: icmp_seq=2 ttl=64 time=0.064 ms  
64 bytes from fe80::aaf:93ff:70a3:d75e%wlp0s20f3: icmp_seq=3 ttl=64 time=0.082 ms  
^C  
--- fe80::aaf:93ff:70a3:d75e%wlp0s20f3 ping statistics ---  
3 packets transmitted, 3 received, 0% packet loss, time 2072ms  
rtt min/avg/max/mdev = 0.050/0.065/0.082/0.013 ms
```

Réponse : Lorsque vous tapez ping6 fe80:.... sans spécifier l'interface, le système ne sait pas sur quel réseau local (lien) envoyer le paquet, ce qui cause l'erreur.

Pour faire fonctionner le ping, vous devez spécifier l'interface réseau avec la commande :

ping6 fe80::aaf:93ff:70a3:d75e%wlp0s20f3

Cela indique à ping6 d'utiliser l'interface wlp0s20f3 pour communiquer avec l'adresse link-local.

1.8 Est ce qu'un client IPv4 peut ouvrir une connexion sur un serveur IPv6, ou inversement ?

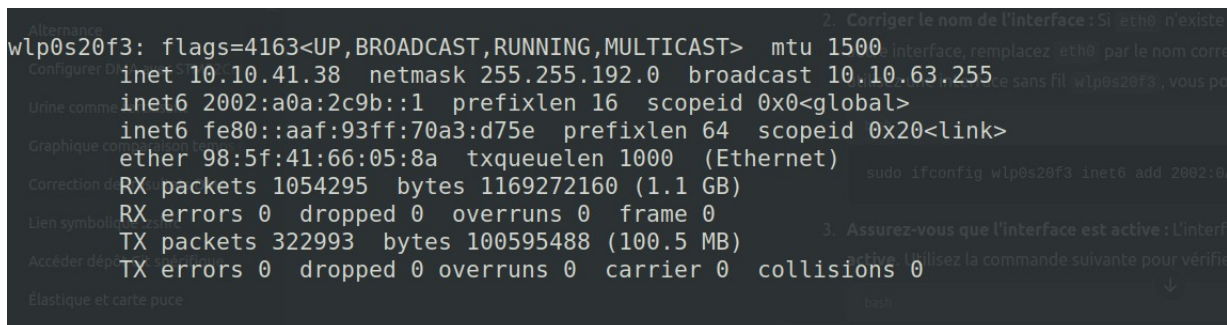
Réponse : Non, un client IPv4 ne peut pas directement ouvrir une connexion sur un serveur IPv6, et inversement. IPv4 et IPv6 sont des protocoles différents, et ils ne sont pas directement compatibles entre eux. Des solutions comme Dual Stack, Tunneling, ou NAT64 peuvent faciliter la communication entre les deux protocoles dans certains cas, mais elles nécessitent une configuration réseau spéciale.

2 Ajouter une adresse IPv6 statique.

Convertissez votre adresse IPv4 en hexadecimal. (vous devez donc avoir 8 chiffres hexadécimaux, que l'on va dire AABBCDD). L'adresse 10.10.44.155 en hexadécimal est 0A0A2C9B.

A partir de cette conversion, on va essayer d'associer notre interface à l'adresse ipv6 2002:AAB:CCDD::/48. (2002:... permet d'effectuer un tunnel 6to4).

On utilise la commande `ifconfig eth0 inet6 add 2002:::1/16`



```
wlp0s20f3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 10.10.41.38 netmask 255.255.192.0 broadcast 10.10.63.255
    inet6 2002:a0a:2c9b::1 prefixlen 16 scopeid 0x0<global>
    inet6 fe80::aaf:93ff:70a3:d75e prefixlen 64 scopeid 0x20<link>
    ether 98:5f:41:66:05:8a txqueuelen 1000 (Ethernet)
    RX packets 1054295 bytes 1169272160 (1.1 GB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 322993 bytes 100595488 (100.5 MB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

Une fois cette commande effectuée on regarde si elle est bien prise en compte avec `ifconfig eth0`

2.1 Pourquoi avons nous deux adresses ipv6 distinctes lorsqu'on tape ifconfig sur l'interface eth0 ?

Réponse :

il y a 2 ipv6 distinctes sur l'interface wlp0s20f3 :

Une adresse globale pour la communication sur Internet via un tunnel 6to4 (2002::/48).

Une adresse link-local pour la communication interne au réseau local (fe80::/10).

Cela permet de gérer la communication dans différentes zones : Internet avec l'adresse globale et le réseau local avec l'adresse link-local.

2.2 Une interface peut elle avoir plus que deux adresses ipv6 ?

Réponse : Une interface réseau peut avoir **plus de deux adresses IPv6**, selon la configuration du réseau, l'utilisation de tunnels, l'attribution d'adresses locales ou globales, et les mécanismes de confidentialité.

2.3 Que représente le "/16" ?

Réponse : C'est le préfixe **/16** signifie que 16 bits sont utilisés pour identifier le réseau dans l'adresse IPv6, et les 112 bits restants sont utilisés pour attribuer des adresses uniques aux appareils sur ce réseau.

2.4 Quelle est la commande qui permet d'afficher le contenu de la table de routage IPv4 ?

Réponse : La commande est `ip route show`

```
(maliki@maliki-club) - [~]  
$ ip route show  
default via 10.10.8.2 dev wlp0s20f3 proto dhcp metric 600  
10.10.0.0/18 dev wlp0s20f3 proto kernel scope link src 10.10.45.87 metric 600  
172.16.39.0/24 dev vmnet8 proto kernel scope link src 172.16.39.1  
192.168.187.0/24 dev vmnet1 proto kernel scope link src 192.168.187.1
```

2.5 Quelle est la commande qui permet d'afficher le contenu de la table de routage IPv6 ?

Réponse : `ip -6 route show`

```
$ ip -6 route show  
::1 dev lo proto kernel metric 256 pref medium  
2002::1/16 dev wlp0s20f3 proto kernel metric 256 pref medium  
fe80::/64 dev vmnet1 proto kernel metric 256 pref medium  
fe80::/64 dev vmnet8 proto kernel metric 256 pref medium  
fe80::/64 dev wlp0s20f3 proto kernel metric 1024 pref medium
```

2.6 Cette table de routage IPv6 contient elle des informations équivalente à celle d'une table de routage IPv4 ?

Réponse : La table de routage IPv6 contient des informations similaires à celles de la table de routage IPv4, bien que les adresses et certaines conventions de notation soient différentes. Les deux types de tables servent à acheminer le trafic réseau en fonction des préfixes de réseau, des interfaces et des passerelles.

2.7 En utilisant wireshark (analyseur de réseau) et la commande ping, indiquez ci-dessous la valeur des différents champs de l'en-tête IPv6 et Ethernet lors de l'envoi d'un paquet ping.

Ça marche pas pour toute la classe du coup on a fait un fait sur notre 4g (donc ip modifié)

```

Ethernet II, Src: 98:5f:41:66:05:8a (98:5f:41:66:05:8a), Dst: IntelCor_20:06:43 (28:c6:3f:20:06:43)
Internet Protocol Version 6, Src: fe80::dc82:a683:fc0c:9ab6, Dst: fe80::7976:9fab:5324:1d97
  0110 .... = Version: 6
  .... 0000 0000 .... = Traffic Class: 0x00 (DSCP: CS0, ECN: Not-ECT)
  .... 1101 1000 0010 1100 0111 = Flow Label: 0xd82c7
  Payload Length: 64
  Next Header: ICMPv6 (58)
  Hop Limit: 64
  Source Address: fe80::dc82:a683:fc0c:9ab6
  Destination Address: fe80::7976:9fab:5324:1d97

```

En-tête IPv6 :

Traffic class : 0x01
Flow Label : 0x12345
Payload Length : 0x0040
Next Header : 0x3A
Hop Limit : 128

En-tête Ethernet :

Protocole : 0x86DD

```

Ethernet II, Src: 98:5f:41:66:05:8a (98:5f:41:66:05:8a), Dst: IntelCor_20:06:43 (28:c6:3f:20:06:43)
  Destination: IntelCor_20:06:43 (28:c6:3f:20:06:43)
  Source: 98:5f:41:66:05:8a (98:5f:41:66:05:8a)
  Type: IPv6 (0x86dd)

```

3 Analyse d'un paquet IPV6.

Décrire dans un tableau, la fonction de chaque champ de l'en-tête d'un paquet IPV6.

Version : Indique la version du protocole (IPv6 = 6).

Traffic Class : Utilisé pour la gestion de la qualité de service (QoS), permettant de prioriser certains types de trafic.

Flow Label : Identifie un flux de données pour permettre un traitement spécifique, comme la gestion de la qualité de service.

Payload Length : Indique la longueur du contenu du paquet (données), excluant l'en-tête IPv6.

Next Header : Spécifie le protocole du segment suivant après l'en-tête IPv6 (par exemple, ICMPv6, TCP, UDP, etc.).

Hop Limit : Indique le nombre maximal de sauts (hops) que le paquet peut faire avant d'être abandonné.

Source Address : L'adresse IPv6 de l'expéditeur.

Destination Address : L'adresse IPv6 du destinataire.

Quelle est la fonction du champ TRAFFIC CLASS ? Comment est-il utilisé par les opérateurs réseaux (Orange, FREE, etc ...) ?

Fonction : Il permet de définir des priorités de transmission et de traitement des paquets en fonction de leur type, comme la gestion de la bande passante ou le contrôle de la latence.

Utilisation par les opérateurs : Les opérateurs utilisent ce champ pour prioriser certains types de trafic (par exemple, la voix sur IP ou les flux vidéo en temps réel) afin de garantir une qualité de service (QoS) optimale.

Quel est le rôle du champ NEXT HEADER ? Quel serait sa valeur numérique dans le cas du transport d'un segment TCP dans ce paquet IPV6 ? d'un paquet IPv4 ? d'un paquet IPSEC ?

Le champ Next Header indique quel protocole suit l'en-tête IPv6 (ex. : TCP, UDP, etc.).

- Valeur pour TCP : 6 (0x06)
- Valeur pour un paquet IPv4 : 4 (0x04)
- Valeur pour IPsec (ESP) : 50, ou 51 pour AH (Authentication Header). 0x32

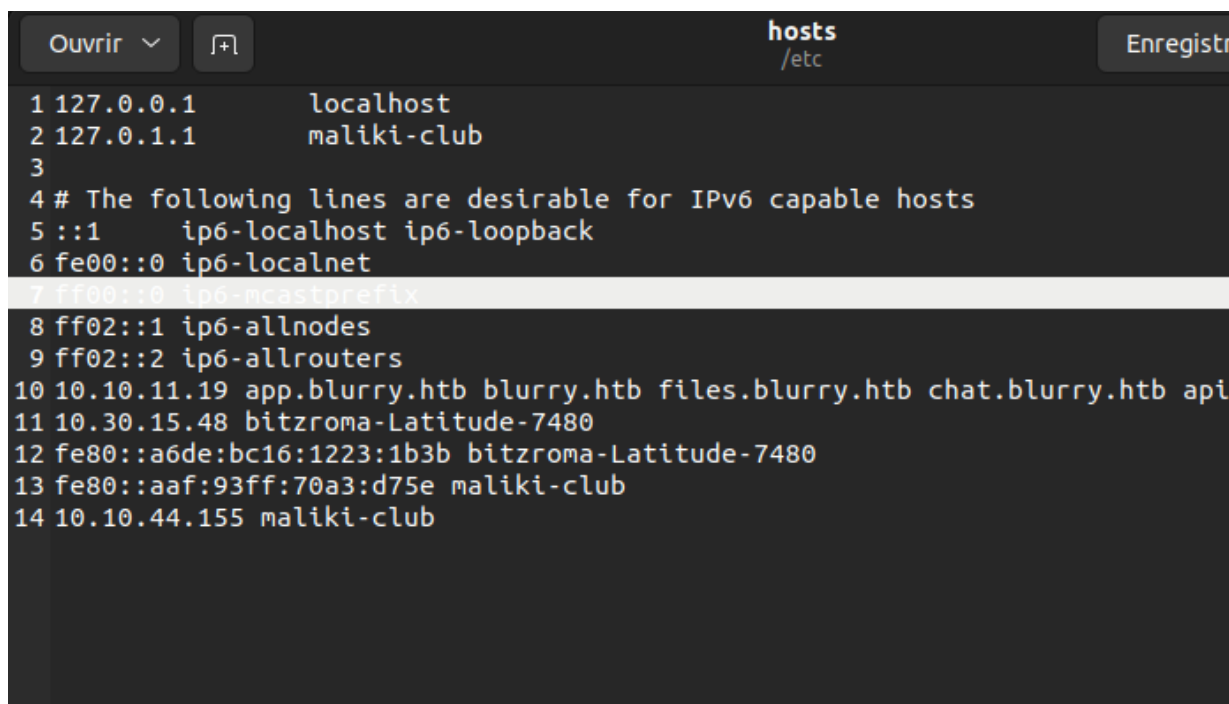
4 Commandes systèmes et réseaux IPV6.

La plupart des commandes acceptent en arguments des adresses IPv4 ou IPv6. Si l'argument est un nom et si IPv6 est active sur la machine, une commande normale utilise d'abord les adresses IPv6 (les adresses IPv4 sont utilisées seulement s'il y a un problème de connectivité IPv6).

Certaines commandes ont des options pour changer ce choix (par exemple ssh -4 ou -6). Il existe aussi des commandes qui ne respectent pas ces règles, ou ne connaissent pas IPv6. La commande ping est une exception en FreeBSD/Linux, elle est seulement IPv4, pour IPv6 il faut utiliser ping6.

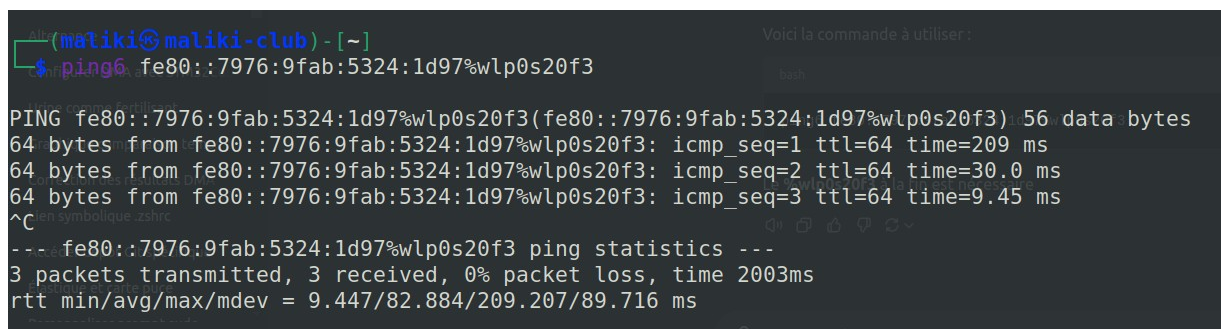
1. Mettez les adresses IPv4 et IPv6 de deux machines voisines dans le fichier `/etc/hosts` (le champ nom est libre, mais utilisez le même pour les adresses IPv4 et IPv6 : on a une seule machine avec plusieurs adresses).

On modifie `/etc/hosts`



```
1 127.0.0.1      localhost
2 127.0.1.1      maliki-club
3
4 # The following lines are desirable for IPv6 capable hosts
5 ::1           ip6-localhost ip6-loopback
6 fe00::0       ip6-localnet
7 ff00::0       ip6-mcastprefix
8 ff02::1       ip6-allnodes
9 ff02::2       ip6-allrouters
10 10.10.11.19    app.blurry.htb blurry.htb files.blurry.htb chat.blurry.htb api
11 10.30.15.48    bitzroma-Latitude-7480
12 fe80::a6de:bc16:1223:1b3b bitzroma-Latitude-7480
13 fe80::aaf:93ff:70a3:d75e maliki-club
14 10.10.44.155  maliki-club
```

2. Faites un ping6 entre vos deux machines. Capturez les paquets à ce moment. Quel protocole est utilisé pour effectuer la résolution d'adresse Ethernet (équivalent de ARP en IPv4) ? Expliquez son fonctionnement. Expliquez le contenu des paquets ICMPv6. On peut consulter la table Adresse IPv6/Ethernet à l'aide de la commande `ndp -a` (suppression d'une ligne par `ndp -d hostname`).



```
(maliki@maliki-club) - [~]
$ ping6 fe80::7976:9fab:5324:1d97%wlp0s20f3
Voici la commande à utiliser :
ping6
PING fe80::7976:9fab:5324:1d97%wlp0s20f3(fe80::7976:9fab:5324:1d97%wlp0s20f3) 56 data bytes
64 bytes from fe80::7976:9fab:5324:1d97%wlp0s20f3: icmp_seq=1 ttl=64 time=209 ms
64 bytes from fe80::7976:9fab:5324:1d97%wlp0s20f3: icmp_seq=2 ttl=64 time=30.0 ms
64 bytes from fe80::7976:9fab:5324:1d97%wlp0s20f3: icmp_seq=3 ttl=64 time=9.45 ms
^C
-- fe80::7976:9fab:5324:1d97%wlp0s20f3 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2003ms
rtt min/avg/max/mdev = 9.447/82.884/209.207/89.716 ms
```

En IPv6, le protocole utilisé pour résoudre les adresses Ethernet, l'équivalent de l'ARP (Address Resolution Protocol) en IPv4, est NDP (Neighbor Discovery Protocol).

Fonctionnement de NDP (Neighbor Discovery Protocol)

Lors de l'envoi du premier paquet, la machine source envoie un message Neighbor Solicitation (NS) à l'adresse de multidiffusion solicited-node associée à fe80::dc82:a683:fc0c:9ab6. Si la machine cible est sur le même réseau local, elle répond par un Neighbor Advertisement (NA) avec son adresse MAC, permettant ainsi l'envoi des paquets suivants directement à l'adresse MAC résolue.

Voici la preuve wireshark

```
101 10.201219159 fe80::7976:9fab:532... fe80::dc82:a683:fc0... ICMPv6 118 Echo (ping) reply id=8x0019, seq=6, hop limit=64 (request in 97)
102 10.467362115 2a02:8440:b155:c7a0... 2a02:8440:b155:c7a0... ICMPv6 86 Neighbor Solicitation for 2a02:8440:b155:c7a0:daa8:3f01:15de:6a10 from 3e:7d:0a:06:fd:64
103 10.467429276 2a02:8440:b155:c7a0... 2a02:8440:b155:c7a0... ICMPv6 78 Neighbor Advertisement 2a02:8440:b155:c7a0:daa8:3f01:15de:6a10 (sol)
104 11.122593806 fe80::dc82:a683:fc0... fe80::7976:9fab:532... ICMPv6 118 Echo (ping) request id=8x0019, seq=7, hop limit=64 (reply in 105)
```

pour la commande ndp j'ai remplacé par \$ ip -6 neigh show

```
(maliki@maliki-club) - [~]
$ ip -6 neigh show
fe80::3c7d:aff:fe06:fd64 dev wlp0s20f3 lladdr 3e:7d:0a:06:fd:64 router REACHABLE
fe80::7976:9fab:5324:1d97 dev wlp0s20f3 lladdr 28:c6:3f:20:06:43 STALE
2a02:8440:b155:c7a0:b8f2:b47:abc6:7aeb dev wlp0s20f3 lladdr 3e:7d:0a:06:fd:64 router STALE
```

Le Neighbor Discovery Protocol (NDP) en IPv6 remplace l'ARP en IPv4. Il permet de résoudre les adresses MAC associées aux adresses IPv6, de détecter les voisins injoignables et d'auto-configurer les adresses. Les messages ICMPv6 utilisés sont :

Neighbor Solicitation (NS) : Demande d'une adresse MAC à partir d'une adresse IPv6.

Neighbor Advertisement (NA) : Réponse à la demande NS avec l'adresse MAC.

Router Solicitation (RS) : Demande d'informations aux routeurs.

Router Advertisement (RA) : Réponse des routeurs avec des informations de configuration.

Dans la commande ip -6 neigh show, les états indiquent si les adresses sont accessibles ou potentiellement injoignables (STALE).

3. Utilisez netstat, wireshark pour vérifier les règles de choix d'adresse destination sur quelques commandes (ping, ssh, wget, udpmt, tcpmt). On peut utiliser comme destination : des machines IPv6 bien connues" (comme www.kame.net, livre.g6.asso.fr, www.google.com...,). Utilisez host ou dig pour connaître leurs adresses. La résolution DNS est elle effectuée en IPV4 ou en IPV6 ? Pourquoi ?

La résolution DNS retourne à la fois des adresses IPv4 et IPv6 car les systèmes sont conçus pour gérer simultanément les deux protocoles. Cette double résolution est nécessaire en raison de la période de transition entre IPv4, largement utilisé, et IPv6, qui est progressivement adopté pour sa capacité à offrir un espace d'adressage beaucoup plus vaste.

Comme on peut voir pour www.kame.net on a l'adresse ip 2001:2f0:0:8800:226:2dff:fe0b:4311 pour nous le dns c'est effectuer en ipv4

dns						
No.	Time	Source	Destination	Protocol	Length	Info
5	1.099767100	172.20.10.3	172.20.10.1	DNS	83	Standard query 0x7fc4 A www.kame.net OPT
6	1.099917781	172.20.10.3	172.20.10.1	DNS	83	Standard query 0xec6c AAAA www.kame.net OPT
7	1.100047300	172.20.10.3	172.20.10.1	DNS	160	Standard query response 0x8800 AAAA www.kame.net OPT

```
(maliki@maliki-club)-[~]
$ host www.kame.net
www.kame.net is an alias for mango.itojun.org.
mango.itojun.org has address 210.155.141.200
mango.itojun.org has IPv6 address 2001:2f0:0:8800::1:1
mango.itojun.org has IPv6 address 2001:2f0:0:8800:226:2dff:fe0b:4311
```

Pareil pour google en ipv4 c'est probablement parce que le serveur DNS a renvoyé l'enregistrement IPv4 (A record) par défaut, soit en raison de la configuration du serveur DNS, de la configuration du système local, ou de l'absence d'enregistrement AAAA pour IPv6 pour ce domaine.

dns						
No.	Time	Source	Destination	Protocol	Length	Info
39	1.650895078	172.20.10.3	172.20.10.1	DNS	86	Standard query 0xdafe AAAA docs.google.com OPT
40	1.651101562	172.20.10.3	172.20.10.1	DNS	86	Standard query 0x3257 A docs.google.com OPT
41	1.651322204	172.20.10.3	172.20.10.1	DNS	86	Standard query 0x0008 HTTPS docs.google.com OPT