

TP de réseaux

Étude du protocole IPv6

21 mars 2023

Le but de ce TP est une initiation à IPv6. Ce document contient une brève introduction, mais vous êtes fortement encouragés à relire votre cours ou à faire une recherche sur le Web, en particulier pour le compte rendu.

1 Introduction à IPv6

IP(v4) souffre d'un grave problème : l'espace d'adresses s'épuise rapidement. Dans les années 90, on avait estimé qu'il n'y aurait plus d'adresses globales à allouer mi 2012. Ce n'est pas encore le cas grâce à la mise en œuvre systématique des adresses sans classe et du NAT (Network Address Translation), mais le problème demeure. IPv6 est une évolution d'abord conçue pour résoudre ce problème. L'IETF en a profité pour "nettoyer" le protocole, mais de manière marginale.

Voici les principaux points d'innovation du protocole IPv6.

1.1 Adresses

Une adresse IPv6 est un mot de 128 bits (16 octets). Elle est notée par 8 mots de 16 bits en hexadécimal (format "network" : bit de poids fort en tête), séparés par des :

Exemples d'adresse IPv6 :

2001:660:5301:8000:0:0:0:1aed

2001:660:5301:8000:0:0:0:0

On utilise aussi une forme abrégée, remplaçant une suite de 0:0:0 par ::

2001:660:5301:8000::1aed

2001:660:5301:8000::

Pour les cas où le : a un sens (par exemple dans une URL) on met l'adresse entre [] ; par exemple : `http://[::1]/x`

1.2 Noms

Le DNS, ou */etc/hosts*, permet d'utiliser des noms et de trouver l'adresse IPv6 correspondante. Une machine (et chacune de ses interfaces) peut avoir plusieurs adresses, IPv4 ou IPv6.

Déclaration dans */etc/hosts* :

```
192.168.10.2          station
2001:660:5301:8000::1aed  station
```

Déclaration dans le DNS :

```
station  IN  A      192.168.10.2
station  IN  AAAA   2001:660:5301:8000::1aed
```

1.3 Réseaux, routage

Les adresses sont groupées en réseaux suivant la politique CIDR : un préfixe commun. Il n'y a pas de longueur prédéfinie, il faut **toujours** préciser la longueur du préfixe. La notation est *ad/lg_pref*.

Par exemple :

```
2001:660:5301:8000::/64    réseau Ethernet contenant la machine ci-dessus
::/0                        route par défaut
2001:660:5301:8000::1aed/128  route vers une machine "host"
```

Pour simplifier l'administration, il existe quelques règles de bon usage :

- On ne doit pas utiliser de préfixe plus long que 64 (sauf les routes "host").
- Un réseau de niveau 2 (câble Ethernet, réseau de ponts, ligne point à point) est toujours un /64. Ainsi le réseau de la machine ci-dessus est `2001:660:5301:8000::1aed/64` (ou, ce qui est la même chose `2001:660:5301:8000::/64`).
- Une allocation d'un FAI à un site est un /48. On a donc droit à 2^{16} réseaux locaux.
- Les adresses globales (unicast) sont dans `2000::/3` (**qui n'est pas `2::/3`!**)
- Il n'y a pas de plage pour NAT : les adresses "normales" sont globales et routables mondialement.

Comme en IPv4 il existe des adresses et plages spécifiques :

```
::1      Adresse localhost (équivalent à 127.0.0.1 en IPv4)
::       Adresse non spécifiée (équivalent à 0.0.0.0 en IPv4)
fe80::/10 Adresses link-local utilisées dans certains protocoles de service (auto-
         conf, routage)
ff00::/8 Multicast (équivalent à 224.0.0.0/4 en IPv4)
ff02::/16 Tous les multicast link-local (portée limitée au réseau local)
ff02::1  Remplace le broadcast d'IPv4 sur un réseau local
```

Une interface peut avoir plusieurs adresses IPv6 en même temps. En fait une interface a au moins 2 adresses, une adresse globale et une adresse *link-local* (`fe80::/10`) qui est allouée à la mise sous tension et sert aux protocoles d'initialisation. Plusieurs préfixes /64 peuvent être routés sur le même lien.

Le routage en IPv6 utilise le principe CIDR : on route selon le plus grand préfixe connu. Les protocoles de routage sont dérivés de ceux d'IPv4 : RIPng, OSPFv3, BGP4+, PIM, IS-IS, ...

Les routages IPv4 et IPv6 sont indépendants avec des configurations séparées ; il peut n'y avoir aucun routeur commun.

1.4 Format des paquets IPv6

Le transport IPv6 garde le principe d'IPv4 : les données sont acheminées dans des datagrammes, avec un en-tête contenant les adresses source et destination, la longueur des données et le type des données (ICMP, TCP, UDP, ...). L'en-tête a été simplifié en IPv6, et est calculé pour un alignement sur 32 bits (voir la figure 1).

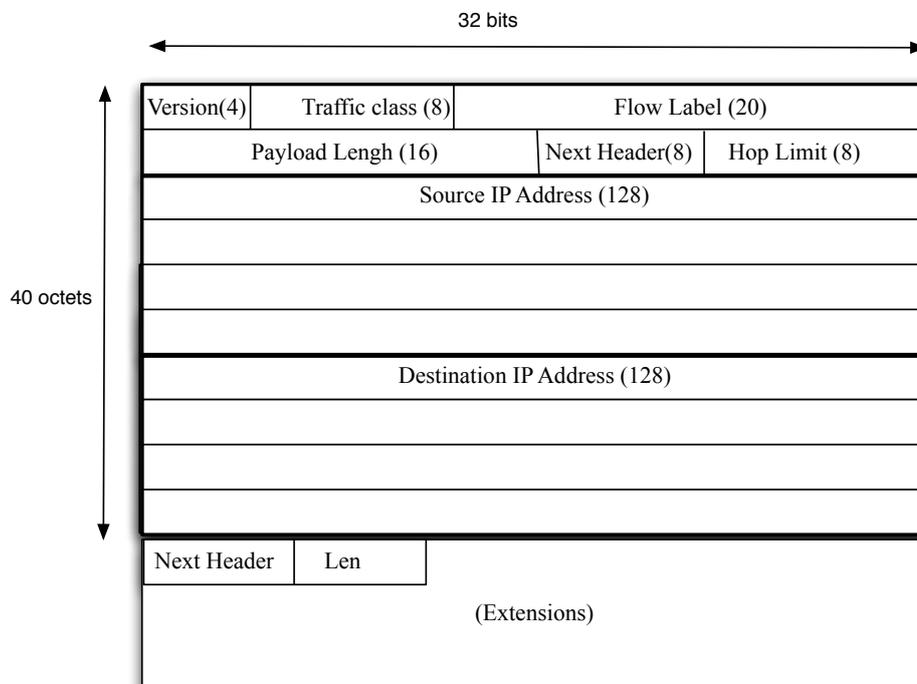


FIGURE 1 – Format de l'en-tête IPv6

- L'en-tête est de taille fixe : 40 octets.
- Version : 6.
- Classe/Identificateur flux : pour faire de la QoS.
- En-tête suivante : type de donnée transportée (TCP, ICMP...) ou de l'extension (fragmentation, IPSEC, ...).
- Nombre de sauts : remplace le TTL d'IPv4.
- Extensions : pour cas particuliers (routage par la source, IPSEC, fragmentation...).
- Données : entête (UDP, TCP...) + data

Par rapport à IPv4 :

- Le type du protocole niveau 2 change (pour Ethernet, 0x86DD au lieu de 0x0800).
- La taille maximum d'un paquet (MTU) sur un réseau Ethernet est 1280 octets. Si la fragmentation est nécessaire, elle doit être faite par l'émetteur (les routeurs intermédiaires ne fragmentent plus mais rejettent).
- Il n'y a plus de *checksum* : elle est dans l'entête du protocole niveau 4 transporté.
- Il n'y a plus de champ fragmentation ou option : on utilise une extension.
- TCP et UDP ne sont (presque) pas modifiés.
- ICMPv6 est similaire à ICMP(IPv4), mais a été "nettoyé".
- Le protocole ARP d'IPv4 est remplacé par le protocole *Neighbor discovery* basé sur ICMPv6.

1.5 Auto-configuration, *router discovery*

IPv6 permet la configuration automatique d'une machine hôte : "on branche et ça marche" (mécanisme d'*auto-configuration sans état*). Pour cela on utilise des messages ICMPv6 : les routeurs présents sur le câble local envoient des paquets *Router advertisement* qui contiennent les préfixes utilisables. Une machine auto-configurée écoute ces messages et construit ses adresses globales en concaténant chaque préfixe avec un suffixe de 64 bits fixe, dérivé de l'adresse Ethernet ou aléatoirement. Ces messages sont envoyés toutes les quelques minutes (par défaut environ 200 secondes pour Cisco, 10 minutes pour FreeBSD).

Pour accélérer le processus, la machine peut demander un *Router advertisement* en envoyant en multicast un message *Router solicitation*.

Les messages *Router advertisement* permettent aussi de trouver automatiquement une route par défaut ; en général en IPv6 seuls les routeurs ont des routes autres qu'une route par défaut.

Remarques

- Le *Router advertisement* peut aussi dire d'utiliser DHCPv6 plutôt que ce mécanisme.

1.6 Configuration des machines – cas de FreeBSD

Configurer manuellement IPv6 sur une machine n'est pas simple, car le noyau et divers processus doivent coopérer. C'est pourquoi en général on écrit des directives de configuration dans un fichier, et il faut alors "rebooter" la machine. Mais *ifconfig* et *route* sont toujours là, pour les spécialistes ; en FreeBSD :

```
ifconfig <IF> inet6 xx:xx::xx/64 [delete]
route (add|delete|show) -inet6 (xx:xx::xx/LL|default) xx:xx::x [-reject]
```

Dans le cas de FreeBSD, le fichier de configuration est */etc/rc.conf*, avec les valeurs par défaut dans */etc/defaults/rc.conf*. Voici les options qui peuvent être utiles. À adapter, ne pas copier sans réfléchir (et prendre seulement les lignes nécessaires). Faire attention aux noms des interfaces !

```

ifconfig_em0_ipv6="inet6 accept_rtadv"      # adresse calculée par RtAdv
ifconfig_em0_ipv6="inet6 2001:db8::100/64" # adresse manuelle
rtsold.enable="YES"                        # Envoi router solicitation (si host)
ipv6_defaultrouter="2001:db8::10"         # Set default router manually
ipv6_gateway_enable="NO"                  # YES to forward packets - machine is a gateway
route6d.enable="NO"                       # YES to enable the route6d routing daemon
rtadvd.enable="NO"                        # YES to send Rtadv - machine is a gateway
rtadvd.interfaces="xl0"                   # Interfaces rtadvd sends RA packets on

```

Après avoir modifié des paramètres dans `/etc/rc.conf`, il faut rebooter la machine.

Remarque

Si une machine ne peut plus rebooter à cause d'une erreur dans le fichier `/etc/rc.conf`, il faut sur le shell minimal que l'on obtient faire comme suit :

mount -rw -a (pour pouvoir modifier / et accéder à /var), **cd /etc**, **mv rc.conf rc.confNO**, **/var/b<TAB>/B<TAB>** (`/var/backups/BackToNormal` en utilisant la complétion), **reboot**.

Le clavier est en mode qwerty, mais l'affichage est correct : taper `,)zq!` : pour `m-wa/`.

2 Expérimentations

2.1 Configuration d'une machine hôte

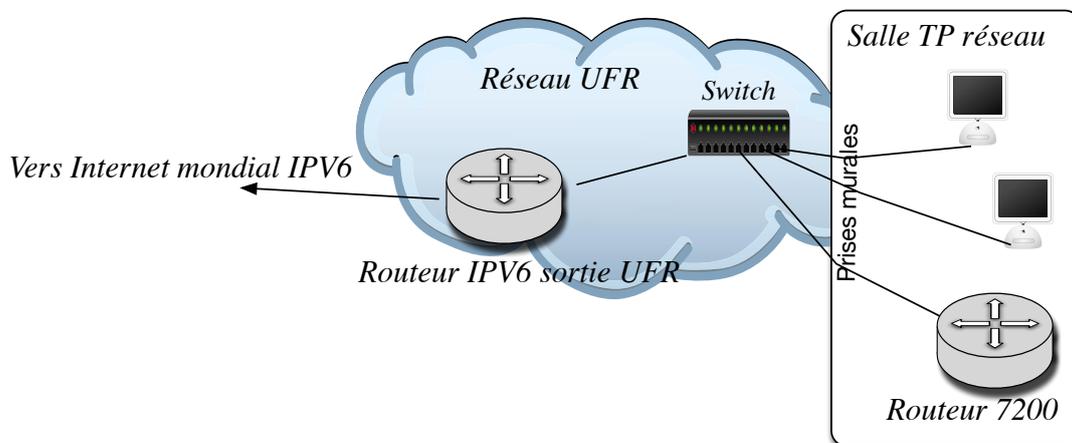


FIGURE 2 – Configuration du réseau

IPv6 n'est pas encore totalement déployé à l'université. Pour ce TP le réseau mural des salles a été relié à un routeur Cisco 7200 fournissant la connectivité IPv6 jusqu'à un routeur IPV6 permettant de sortir de l'UFR IM2AG (voir figure 2).

Cela permet de contrôler le routage et d'activer RIPng.

1. Allumez une machine, réinitialisez la à l'aide du script `/var/backups/BackToNormal`, puis reliez la (directement ou via un commutateur) à une prise murale via l'interface Ethernet standard (carte mère, appelé *em0* dans la suite).

2. IPv6 n'est pas configuré par défaut, il faut donc modifier le fichier `/etc/rc.conf` pour activer IPv6 sur l'interface voulue.
 - (a) Il faut accepter les *Router advertisement* sur l'interface en ajoutant :
`ifconfig_em0_ipv6="inet6 accept_rtadv"`
 - (b) Si vous voulez que la machine envoie des *Router solicitations*, il faut aussi ajouter `rtsold_enable="YES"` sinon on peut attendre plusieurs minutes avant de voir apparaître une adresse IPv6 globale.
3. Puis rebootez la machine, surveillez les messages de boot, et faire ***ifconfig***.
4. Constatez que la machine a bien des adresses IPv6, combien, de quel type? Expliquez à quoi sert chacune de ces adresses.
5. Quel est le préfixe diffusé par le routeur Cisco sur le réseau de la salle? En déduire le préfixe du site (/48).
6. Quelle est la partie "locale" (64 bits de poids faible)? Vérifiez que les adresses auto-configurées et *link-local* utilisent toujours la même valeur, et trouvez comment elle est calculée à partir de l'adresse Ethernet.
7. Analysez précisément les lignes de la table de routage par ***netstat -rn***. Commentez les lignes concernant IPV6.
A l'aide de la configuration du routeur 7200 (donnée en annexe), déduire les adresses IPV6 du routeur 7200 et du routeur de sortie de l'UFR (voir figure 2).
8. Lancez ***wireshark***.
 - Retrouvez dans la capture un paquet *ICMPv6-router advertisement*.
 - Retrouvez dans ce paquet l'annonce de l'adresse IPv6 du réseau et de l'adresse par défaut du routeur de sortie.
 - Quelle est l'adresse destination de ce paquet? Expliquez pourquoi cette adresse est utilisée.
 - L'adresse du routeur par défaut apparait elle dans le paquet? Si non comment est elle calculée?

2.2 Connectivité IP mondiale – Cohabitation IPv4/IPv6

La plupart des commandes acceptent en argument des adresses IPv4 ou IPv6. Si l'argument est un nom et si IPv6 est activé 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*** permet elle d'utiliser aussi IPv6?

1. Configurez une deuxième machine hôte comme précédemment, et mettez les adresses IPv4 et IPv6 des deux machines configurées 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).
2. Faites un ***ping6*** entre vos deux machines.
Attention pour pinger une adresse link local, il faut spécifier le nom de l'interface par exemple : `ping6 fe80 : :3b3 :799a :ba84 :b899%em0`
 - 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-Neighbor Solicitation*.
On peut consulter la table Adresse IPv6/Ethernet à l'aide de la commande ***ndp -a*** (suppression d'une ligne par ***ndp -d hostname***).
3. Utilisez ***wireshark*** pour vérifier les règles de choix d'adresse destination sur quelques commandes (***ping, ssh, wget, udpmt, tcpmt, navigateur web firefox ou opera***). On peut utiliser comme destination :
 - Les machines de la plate-forme,
 - Des machines IPv6 "bien connues" (limitées à ***ping*** ou ***www***) `www.kame.net`, `livre.g6.asso.fr`, `www.google.com...`,
 - Certains serveurs de noms des domaines racine ou `fr`.

Utilisez ***host*** ou ***dig*** pour connaître leurs adresses.

La résolution DNS est elle effectuée à travers le réseau IPV4 ou IPV6 ? Pourquoi ?

Rappel : sur vos machines, le compte utilisable par ssh est ***guest***, mot de passe : ***guest./***

Remarque : on peut "casser" la connectivité IPv6 en perturbant le routage des adresses globales, par exemple :

```
route add -inet6 2000::/3 ::1 -reject
(suppression par : route delete -inet6 2000::/3 ::1)
```

4. Capturez des paquets IPv4 et IPv6 et comparez les formats.

2.3 Configuration d'un sous-réseau test IPV6

On va configurer un sous-réseau séparé, comprenant un routeur et une machine hôte. Pour cela on prendra deux des stations déjà configurées dans la partie précédente.

1. Créez un réseau *test* comme sur la figure 3 en reliant via un commutateur (ou un câble croisé) la deuxième interface d'une machine A à l'autre machine B (interface de la carte mère *em0*). La machine A devenue ainsi routeur est toujours reliée au

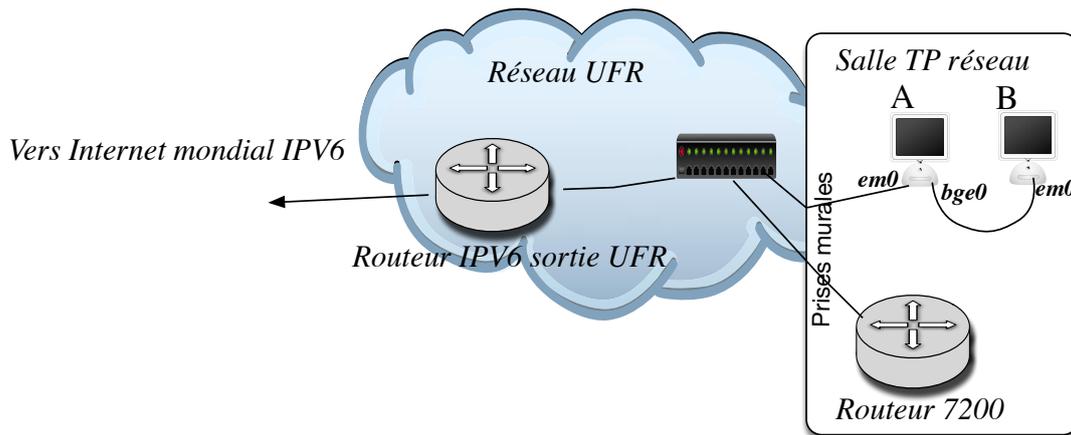


FIGURE 3 – ConfigIPv6

mur via l'interface de la carte mère *em0*.

- Configurez les machines : Pour la machine hôte B, il n'y rien à faire (on garde la configuration IPv6 faites précédemment).

Pour le routeur A, il a deux interfaces, l'un sur le réseau mural et l'autre sur le réseau local. L'auto-configuration n'est pas possible pour un routeur, il faut la définir "à la main" dans */etc/rc.conf* :

```

ip6_gateway_enable="YES" # forwarder les paquets, c'est un routeur
route6d_enable="NO"     # ne pas lancer de démon de routage Ripng
rtadvd_enable="YES"     # on envoie des Router advertisement
rtadvd_interfaces="bge0" # uniquement sur l'interface vers le réseau test

```

Il faut aussi définir le préfixe du réseau *test* et les adresses des 2 interfaces de A, manuellement car c'est un routeur.

Pour éviter des conflits d'adresse entre plate-formes, on intègre une valeur *xx* que l'on choisira aléatoirement entre 01 et 99. Par mesure de sécurité, vous pouvez demander aux autres étudiants leurs choix.

- Pour l'interface réseau mural/carte mère, dans le réseau `2001:660:5301:8800::/64`, on choisit comme suffixe *1xx* :

```
ifconfig_em0_ipv6="inet6 2001:660:5301:8800::1xx/64"
```

- Pour l'interface réseau test, on choisit le préfixe `2001:660:5301:88xx::/64`, et le suffixe *100* :

```
ifconfig_bge0_ipv6="inet6 2001:660:5301:88xx::100/64"
```

Notes :

- Attention, *xx* est limité à 2 chiffres hexadécimaux.
- Quand on configure à la main une adresse IPv6, on a le choix pour le suffixe : on peut prendre la valeur "standard" (à partir de l'adresse Ethernet), ou une

valeur facile à mémoriser.

- `0x100` a été choisi arbitrairement — 0 est impossible car réservé : anycast.

3. Rebootez le routeur A.

Vérifiez qu'il a toujours la connectivité IPv6 avec le routeur Cisco, d'adresse `2001:660:5301:8800::1000`).

- Le routeur A peut-il dialoguer en IPv6 avec le reste du monde ? Pourquoi (regardez sa table de routage ***netstat -rn***) ?
- Expliquez comment remédier au problème.
- Faites les modifications sur A (`route add -inet6 default ...`) ?

4. Lancez *wireshark* sur l'interface du routeur A vers le réseau test.

5. Rebootez la machine B et vérifiez qu'elle a bien une adresse IPv6 globale.

6. Comment est-elle calculée ?

7. Etudiez les échanges de paquet entre A et B. Ne cherchez pas à tout interpréter, mais commentez ce que vous pouvez.

2.4 Établir la connectivité IPv6

- Constatez que la machine B n'accède à rien en IPv4 (A ne route pas IPv4).
- Constatez que la machine B accède en IPv6 au routeur A(`2001:660:5301:88xx::100`), mais à rien d'autre, ni par adresse, ni par nom DNS.

2.5 Résolution du routage

Nous allons commencer par établir la connectivité de B à IPV6 (en oubliant pour l'instant la résolution de nom DNS).

1. Les paquets issus d'un *ping6 adresse_IPV6_extérieure* sur B sortent-ils du sous-réseau créé ?
2. Le problème est donc plus loin. Le routeur 7200 a-t-il connaissance de votre sous-réseau ? Comment peut-t-il savoir que la machine B est "derrière" le routeur A ?

Pour avoir la connectivité IPv6, il faut que le réseau `2001:660:5301:88xx::/64` soit connu du routeur 7200.

En effet si il n'a pas connaissance de votre réseau, il ne peut pas rediriger vers A les paquets à destination de B.

Pour cela on va démarrer le démon de routage *RIPng* (version IPv6 du protocole RIP) sur A.

A savoir, *RIPng* tourne déjà sur le routeur 7200 (voir sa configuration en annexe).

Pour lancer *RIPng*, il faut lancer le démon FreeBSD *route6d*.

On peut :

- soit lancez le démon par la commande **route6d** (ou par `service route6d onestart`) (à refaire quand on reboote A).
- soit mettre `route6d_enable="YES"` dans le `/etc/rc.conf` de A puis rebooter A.

1. Vérifiez que le routeur A envoie des paquets *RIPng* sur ses deux interfaces.
2. Étudiez les paquets *RIPng* capturés. Expliquez leur contenu.
3. Vérifiez que l'adresse IPv6 de votre réseau est bien annoncée dans les paquets *RIPng* envoyés par A vers l'extérieur.
4. Vérifiez que `ping6 adresse_IPV6_extérieure` fonctionne maintenant depuis la machine B vers l'extérieur.
5. Sur la routeur A, étudiez la table de routage (`netstat -rn -f inet6`).
La partie de la table issue de *RIPng* peut être obtenue en faisant `killall -INT route6d`, qui dump la table dans `/var/run/routed_dump`.

Vous devriez retrouver dans la table les adresses des sous-réseaux issues des annonces des autres plate-formes de la salle.

Étudiez la configuration du routeur 7200 donnée en annexe et répondez aux questions suivantes :

1. Quelle est l'adresse IPV6 du routeur de sortie de l'UFR (voir figure 2) vers lequel le routeur 7200 possède une route par défaut ?
2. Quel est le préfixe pour lequel le routeur de sortie de l'UFR redirige les paquets vers le routeur 7200 ?
3. Où voit on que le routeur 7200 fait tourner le protocole *RIPng* ?
4. A quoi sert la ligne : `ipv6 route 2001 :660 :5301 :8800 : :/56 Null0`.
Donnez un scénario problématique dans le cas où cette ligne n'existait pas. A savoir : Cette ligne permet de supprimer les paquets à destination du réseau spécifié dans le cas où une autre route n'a pas été trouvée dans la table de routage.
5. Le routeur 7200 est il connecté à Internet en IPV4 ? Quelle est son adresse IPV4 ? Quelle est la route par défaut IPV4 ?
6. Le routeur de sortie de l'UFR (apparaissant en route par défaut dans la configuration du 7200) envoie t il des paquets *Ripng* ?
7. A votre avis, votre sous-réseau est il connu à l'extérieur du bâtiment de l'UFR (après le routeur de sortie de l'UFR) ? Pourquoi ?

2.6 Résolution de nom DNS

La connectivité de B est établie mais la résolution de nom DNS ne fonctionne pas encore sur B. Le DNS sur B accède à un serveur IPv4 (voir */etc/resolv.conf*), et on n'a pas de connectivité IPv4.

Pour que B puisse utiliser le DNS, on va installer un serveur DNS sur le routeur A et l'interroger via IPv6.

- Sur le routeur A, éditez */etc/namedb/named.conf* (fichier de configuration du serveur DNS).
 - pour accepter les requêtes en IPv6, ajoutez (ou décommentez) dans les options la ligne :

```
listen-on-v6 { any; };
```

Elle permet au serveur DNS d'accepter les interrogations via IPV6.

- Commentez la ligne

```
listen-on { 127.0.0.1 };
```
- Lancez le démon serveur DNS par la commande *named -g*. Vérifiez qu'il n'y a pas de problème, par exemple avec les commandes :
 - `ps ax | grep named`
 - `tail /var/log/messages`
 - `host www.google.com ::1`

- Sur la machine B, éditez */etc/resolv.conf* pour utiliser comme serveur DNS le routeur A en IPv6. Remplacez les lignes `nameserver` par la ligne :

```
nameserver 2001:660:5301:88xx::100
```

- Vérifiez sur la machine B que le DNS marche de nouveau (adresses IPv6 et IPv4 mondiales).

3 Annexe – extrait de la configuration du routeur Cisco 7200

```
version 12.3
!
ipv6 unicast-routing
!
interface FastEthernet0/0
 ip address 152.77.84.123 255.255.255.128
 duplex full
 ! Adresse IPV6 attribuee a la salle de TP
 ipv6 address 2001:660:5301:8800::1000/64
 ! Adresse IPV6 permettant la communication avec le routeur de sortie de l UFR
 ipv6 address 2001:660:5305:32::C6/126
 ipv6 enable
 ipv6 nd prefix 2001:660:5301:8800::/64
 ipv6 rip UFRIMA enable
!
ip classless
ip route 0.0.0.0 0.0.0.0 152.77.84.1
!
! le routeur IPV6 de sortie de l UFR a une route:
! ipv6 route 2001:660:5301:8800::/56 2001:660:5305:32::C6
! Eviter une boucle de routage
ipv6 route 2001:660:5301:8800::/56 Null0
! route par defaut IPV6 vers routeur sortie UFR d adresse 2001:660:5305:32::C5/126
ipv6 route ::/0 2001:660:5305:32::C5
ipv6 router rip UFRIMA
 redistribute static
!
end
```

4 Notes pour l'encadrant

Relier le routeur Cisco 7200 au réseau mural par un câble droit sur *0/0* et à une machine par un câble bleu Cisco RJ/petit-femelle. Sur la machine appeler *minicom* puis faire *CTL-A W* pour “wrap on” (sortie par *CTL-A Q*).

Attention, la décompression du système prend plusieurs minutes. On peut tester la connectivité IPv6 par ***ping ipv6 imag.imag.fr***