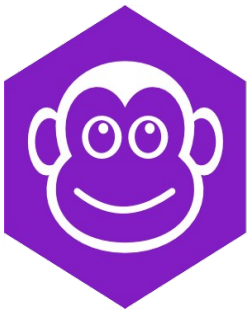

MOOC

Objectif IPv6 !

vers l'internet nouvelle génération

Travaux Pratiques

Séquence 2

Configurez votre premier réseau IPv6

Licence Creative Nommons CC BY-SA 4.0 International

Attribution - Partage dans les Mêmes Conditions 4.0 International (CC BY-SA 4.0)

Avertissement Ce résumé n'indique que certaines des dispositions clé de la licence. Ce n'est pas une licence, il n'a pas de valeur juridique. Vous devez lire attentivement tous les termes et conditions de la licence avant d'utiliser le matériel licencié.

Creative Commons n'est pas un cabinet d'avocat et n'est pas un service de conseil juridique. Distribuer, afficher et faire un lien vers le résumé ou la licence ne constitue pas une relation client-avocat ou tout autre type de relation entre vous et Creative Commons.

Clause C'est un résumé (et non pas un substitut) de la licence.

http://creativecommons.org/licenses/by-sa/4.0/legalcode

Vous êtes autorisé à :

- **Partager** — copier, distribuer et communiquer le matériel par tous moyens et sous tous formats
- **Adapter** — remixer, transformer et créer à partir du matériel
- pour toute utilisation, y compris commerciale.

L'Offrant ne peut retirer les autorisations concédées par la licence tant que vous appliquez les termes de cette licence.

Selon les conditions suivantes :

Attribution — You must give **appropriate credit**, provide a link to the license, and **indicate if changes were made**. You may do so in any reasonable manner, but not in any way that suggests the licensor endorses you or your use.

Partage dans les Mêmes Conditions — Dans le cas où vous effectuez un remix, que vous transformez, ou créez à partir du matériel composant l'Oeuvre originale, vous devez diffuser l'Oeuvre modifiée dans les même conditions, c'est à dire avec **la même licence** avec laquelle l'Oeuvre originale a été diffusée.

No additional restrictions — Vous n'êtes pas autorisé à appliquer des conditions légales ou des **mesures techniques** qui restreindraient légalement autrui à utiliser l'Oeuvre dans les conditions décrites par la licence.

Notes: Vous n'êtes pas dans l'obligation de respecter la licence pour les éléments ou matériel appartenant au domaine public ou dans le cas où l'utilisation que vous souhaitez faire est couverte par une **exception.**

Aucune garantie n'est donnée. Il se peut que la licence ne vous donne pas toutes les permissions nécessaires pour votre utilisation. Par exemple, certains droits comme l**es droits moraux, le droit des données personnelles et le droit à l'image** sont susceptibles de limiter votre utilisation.

Les informations détaillées sont disponibles aux URL suivantes :

- http://creativecommons.org/licenses/by-sa/4.0/deed.fr
- http://fr.wikipedia.org/wiki/Creative_Commons

Les auteurs

Bruno Stévant

Bruno STEVANT est enseignant chercheur à l'IMT Atlantique. Il intervient dans l'enseignement et sur les projets de recherche autour d'IPv6 depuis plus de 10 ans. Il est secrétaire et responsable des activités de formation de l'association G6, association pour la promotion et le déploiement d'IPv6 en France.

Jacques Landru

Enseignant chercheur au département Informatique et Réseaux à l'IMT Lille Douai, Jacques est responsable de l'UV de spécialisation ARES (Architecture des RESeaux) à la fois dans le mode traditionnel présentiel que dans sa forme à distance dans le cadre du cursus diplômant TutTelNet.

Jean-Pierre Rioual

Ingénieur Conseil Réseaux – EURÊKOM. Fort de 30 années d'expérience dans le domaine des réseaux, il intervient auprès des entreprises pour des missions d'expertise sur leurs réseaux de transmission de données (intégration, mesures, optimisation, administration), conçoit et anime des actions de formation "réseaux".

Pascal Anelli

Pascal ANELLI est enseignant-chercheur à l'Université de la Réunion. Il enseigne les réseaux depuis plus 20 ans. Il est membre du G6 depuis sa création. A ce titre, il est un des contributeurs du livre IPv6. En 1996, il a participé au développement d'une version de la pile IPv6 pour Linux.

Joël Grouffaud

Joël GROUFFAUD est professeur agrégé de mathématiques. Il est chef du département Réseaux et Télécommunications de l'IUT de la Réunion, une composante de l'université de La Réunion. Au sein du département, il enseigne les réseaux et IPv6. Il anime l'académie Cisco (formations CCNA) de La Réunion.

Pierre Ugo TOURNOUX

Pierre Ugo TOURNOUX est enseignant chercheur à l'Université de la Réunion. Il est responsable des enseignements d'administration réseau, de routage et des réseaux sans fil dans lesquels il intègre IPv6 depuis de nombreuses années.

Remerciements à :

- Vincent Lerouvillois, pour son travail de relecture attentive ;
- Bruno Di Gennaro (Association G6) ;
- Bruno Joachim (Association G6) pour sa contribution à l'activité « Contrôler la configuration réseau par DHCPv6 » ;
- Richard Lorion (Université de la Réunion) pour sa contribution à l'activité « Etablir la connectivité IPv6 tunnels pour IPv6 ».

Tables des activités

Les auteurs.....5

Activité 26 : Etudiez le fonctionnement du protocole d'IPv6.....9
Etape 0: Démarrage de la plateforme.....9
Identification des liens physiques.....10
Activation des équipements.....11
Arrêt/Pause de GNS3.....11
Etape 1: Capture et analyse d'un flux IPv6.....12
Etape 2: Routage et acheminement d'un paquet.....14
Analyse de la route pour atteindre le serveur web.....15
Etape 3: Fonction de fragmentation.....18
Arrêt/Pause du simulateur.....19
Conclusion.....19

Activité 26 : Etudiez le fonctionnement du protocole d'IPv6

Après avoir vu comment un réseau en IPv6 s'utilise dans la première activité pratique, dans cette seconde activité pratique, nous allons voir comment il fonctionne. Vous pourrez ainsi constater que les principes de son fonctionnement sont très similaire à ceux d'IPv4. Nos objectifs sont ici :

- mettre en oeuvre une capture de paquets IPv6,
- analyser le format des paquets IPv6,
- découvrir le routage des paquets dans un réseau IPv6,
- observer la fragmentation d'un paquet IPv6

Les différentes étapes dans cette activité vont vous permettre d'observer les communications locales au lien et des communications impliquant plusieurs liens. Le réseau de la plateforme est similaire à celui de l'activité précédente comme le montre la figure 1. Il comporte 5 noeuds et repose uniquement sur IPv6. Un serveur web et un serveur DNS sont installés et configurés sur l'hôte appelé SRV-3.

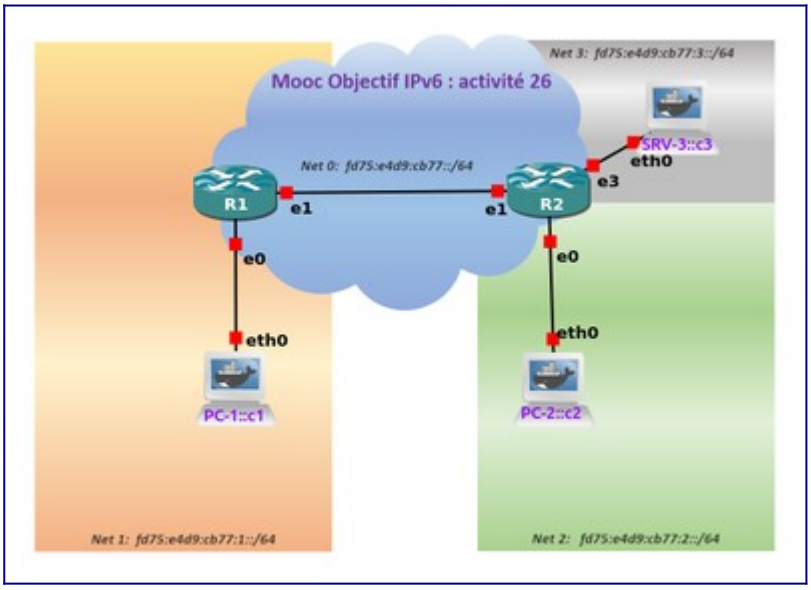

Figure 1: Topologie du réseau étudié.

Le support vous donne l'ensemble des opérations à réaliser pour aller jusqu'au bout de l'activité. Vous trouverez un résumé de ces commandes dans le Manuel Apprenant disponible dans l'onglet documentation du cours Objectif IPv6 du site de FUN.

Etape 0: Démarrage de la plateforme

Démarrer la machine virtuelle **"MOOCIPv6_S5"**. Une fois que la machine virtuelle a démarré, vous voyez, sur le bureau, des dossiers prêts pour les travaux pratiques des séquences 1 à 4.

Pour l'adapter à la taille de votre écran : clic-droit sur le bureau - Modifier l'arrière plan du bureau - choisir la flèche en haut à gauche. Dans la section Matériel, choisir écran puis choisir affichage inconnu. Enfin, appliquer la taille la mieux adaptée à votre écran, puis conserver les modifications si cela convient.

Double cliquer sur le lien intitulé "moocipv6.gns3" (icône symbolisé par un caméléon), présent dans la partie haute du bureau de votre machine virtuelle.

Vous devez restaurer le Snapshot *(Activité-26)* depuis ***Edit > Manage snapshots*** ce qui rechargera les configurations initiales des équipements.

Attendre que la fenêtre `moocipv6-GNS3` apparaisse à l'écran comme présentée par la figure 2. Double cliquer sur la barre de titre de cette fenêtre pour qu'elle occupe la totalité de votre écran. Si besoin, vous pouvez ensuite recentrer l'image de la topologie dans la fenêtre centrale avec les boutons ascenseurs horizontal et vertical.

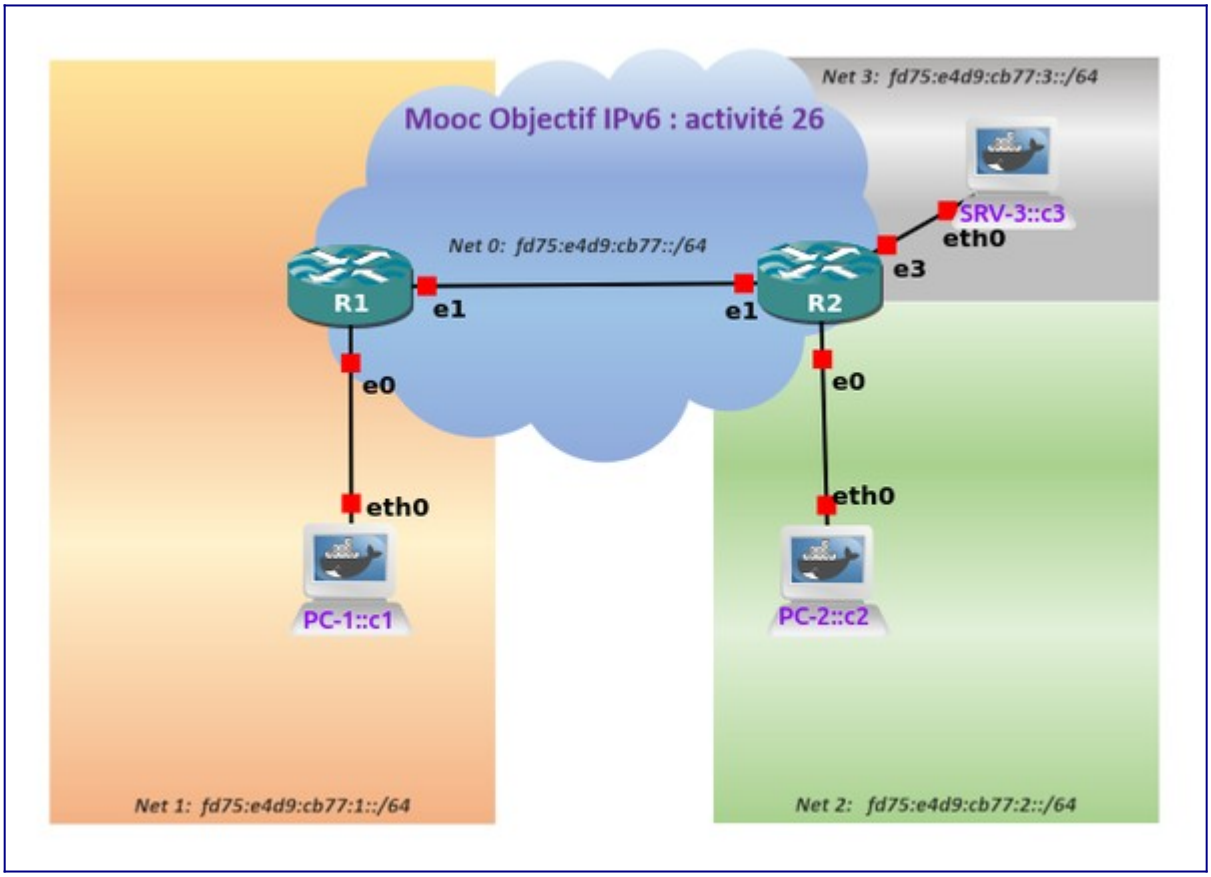

Figure 2: Ecran de GNS3

Identification des liens physiques

Il est possible d'afficher les numéros des interfaces des équipements représentés sur la maquette, appuyer sur le bouton carré **"a b c"** situé juste en dessous du menu déroulant *Device*.

Une fois que vous aurez bien identifié les numéros d'interfaces des liaisons, nous pouvons constater ceci : Ce réseau est constitué de 4 liens.

- lien PC-1 - R1 : les interfaces eth0 de PC-1 et R1 sont reliées à travers le réseau Net1 ;
- lien R1 - R2 : les interfaces eth1 de R1 et R2 sont reliées à travers le réseau Net0 ;
- lien PC-2 - R2 : les interfaces eth0 de PC-2 et R2 sont reliées à travers le réseau Net2.
- lien SRV-3 - R2 : les interfaces eth0 de SRV-3 et eth3 de R2 sont reliées à travers le

réseau Net3.

Activation des équipements

Si tout est correct, vous pouvez activer les équipements du réseau dans GNS3, à l'aide du bouton triangulaire vert démarrer *"Start/Resume all devices"*.

Dans la fenêtre centrale les témoins verts des liens indiquent que les équipements démarrent, et sur la droite la fenêtre *"Topology Summary"* montre aussi les témoins verts des équipements réseaux.

Lorsque tous les noeuds sont actifs, il faut cliquer sur le bouton *"Console connect to all devices"* symbolisé par >_ situé à gauche du bouton triangulaire vert, juste en dessous du menu déroulant *"Annotate"*. Ainsi vous aller faire apparaitre les consoles de contrôle pour les routeurs et pour les hôtes comme le montre la figure 3.

Les consoles de contrôle dites CLI (*Command Line Interface*) affichent le démarrage des différents équipements réseaux. Notons que le démarrage des PC est plus rapide que celui des routeurs (le temps de démarrage dépendant des capacités de votre machine: compter quelques minutes). Comptez entre trois et dix minutes, parfois plus. Une fois que tous les noeuds ont leur console avec l'invite pour se connecter comme le montre la figure 4, votre plateforme de réseau est dorénavant opérationnelle.

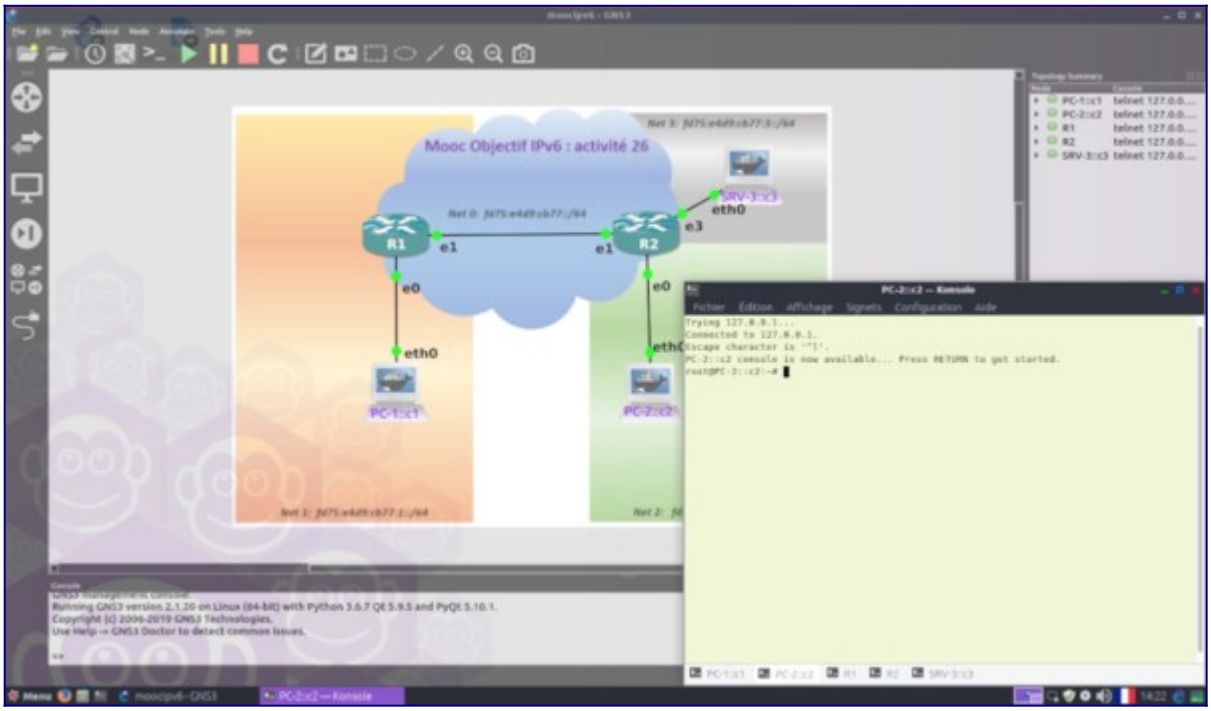

Figure 3: Ecran GNS3 avec les interfaces CLI.

Arrêt/Pause de GNS3

Au besoin vous pouvez aussi figer l'exécution des équipements avec le bouton Pause *"Suspend All devices"*, voire arrêter les équipements avec le bouton Stop *"Stop All devices"*.

L'état des équipements est sauvegardé en quittant. Pour quitter proprement GNS3, faire

CTRL+Q ou faire, avec le menu déroulant *File* et l'action *Quit*.

Etape 1: Capture et analyse d'un flux IPv6

Nous allons capturer le trafic d'une connexion SSH vers R1 depuis PC-1, ensuite nous pourrons analyser les échanges.

Pour étudier ce qui circule sur le support, nous allons mettre en oeuvre une capture de réseau. La plateforme dispose de l'analyseur de protocoles Wireshark. Pour effectuer une capture, il est possible de l'utiliser sur les points de connexions symbolisés par un point vert sur la topologie.

En survolant avec votre pointeur un de ces points, faire un clic-droit et choisir "Start Capture". Il est également possible de lancer une capture,en pointant dans la fenêtre en haut à droite "Topology Summary", puis appuyez sur le + d'un élément réseau.

Choisissez une interface : elle passe en rouge sur la fenêtre centrale. Ensuite, avec un clic-droit, vous pouvez lancer une capture sur ce lien en choisissant "Start capture".

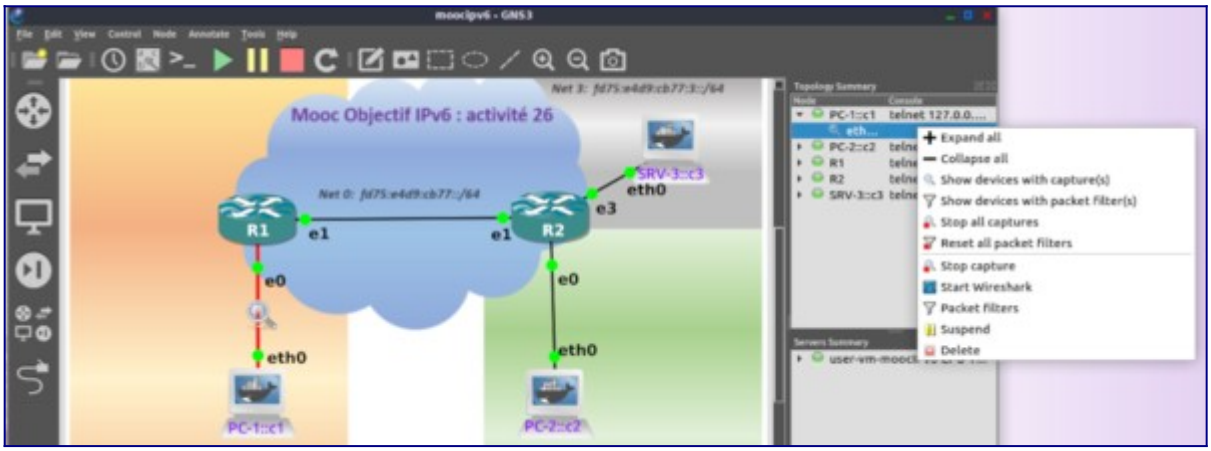

Figure 4: Préparation d'une capture avec Wireshark.

L'arrêt des captures est possible, toujours depuis cette fenêtre "Topology Summary", en choisissant **"Stop all captures"**.

Vous pouvez réaliser ainsi une capture des paquets circulant sur un lien lors d'une communication entre un client et un serveur. Le déroulement des actions est le suivant:

- Activer Wireshark sur le lien PC-1 eth0<->eth0 R1, puis clic-droit et choisissez **"Start capture"**.

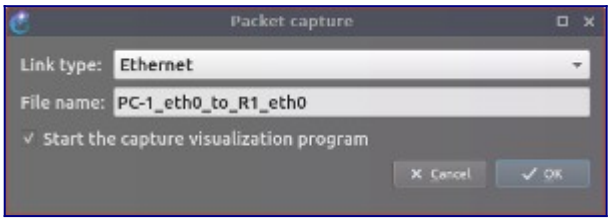

Figure 5: Lancement d'une capture.

Vous pouvez laisser la capture en route le temps que l'on initialise une connexion.

Choisissez l'onglet PC-1, puis tapez les commandes suivantes:

```
root@PC-1:~# ifconfig eth0
root@PC-1:~# ssh vyos@fd75:e4d9:cb77:1::1
Welcome to VyOS
vyos@fd75:e4d9:cb77:1::1's password:vyos
The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.
Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Sat Jun 1 14:24:36 2019 from
fd75:e4d9:cb77:1:583d:54ff:fec1:1e7b
vyos@r1:~$ sh ver
vyos@r1:~$ exit
logout Connection to fd75:e4d9:cb77:1::1 closed.
root@PC-1:~#
```

A ce stade, vous pouvez arrêter la capture, soit depuis cette fenêtre "Topology Summary", en choisissant "Stop all captures". soit en surlignant le lien sur la topologie, clic-droit et "Stop capture". En prenant en main, Wireshark, nous retrouvons la séquence des paquets correspondant à notre connexion, retrouvez en un parmi ceux qui comportent un message TCP à destination du port 22.

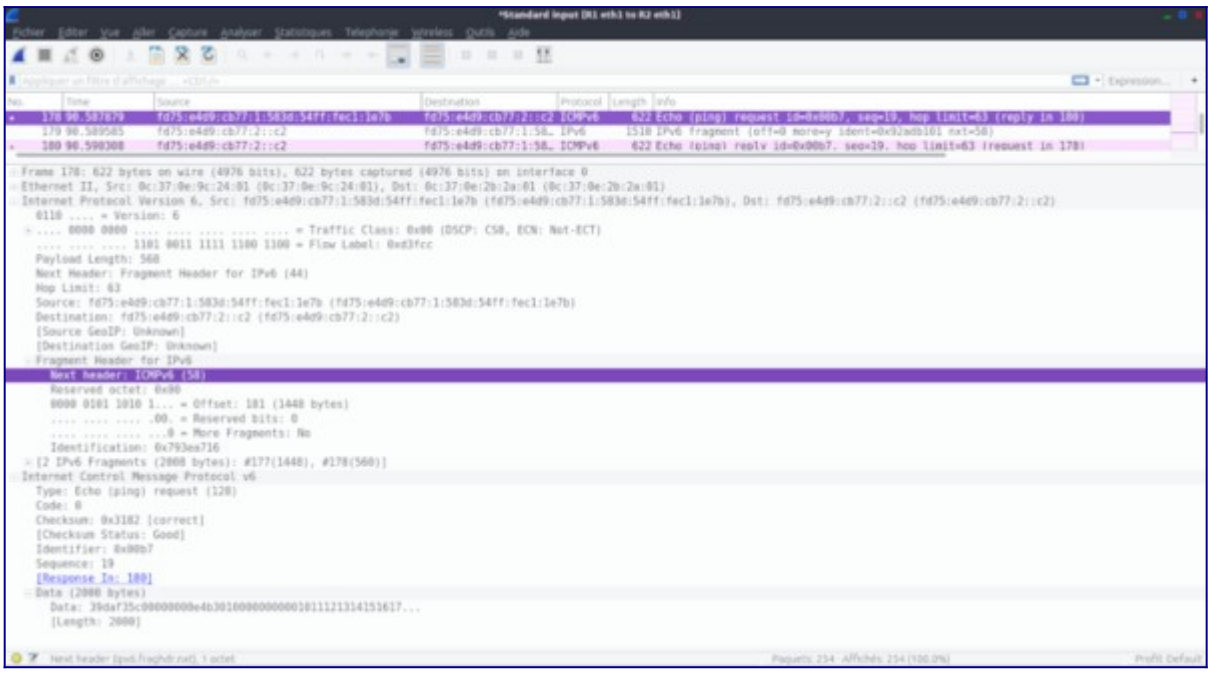

Figure 6: Analyse d'une capture.

Vous pouvez explorer les différents champs de l'en-tête du paquet IPv6 pour répondre aux questions suivantes:

- Quelle est la valeur du champ *Hop Limit* ?
- Quel est le type de l'adresse source utilisée ?
- Quelle est la valeur du champ Next Header ?
- Quelle est la longueur des données utiles du paquet ?

Enfin pour terminer cette analyse de cette capture du paquet IPv6, vous pouvez également

explorer les différents champs de la trame Ethernet encapsulant le paquet IPv6. Vous devriez voir la valeur du champ EtherType à 0x86dd indiquant que la trame Ethernet contient un paquet IPv6.

Etape 2: Routage et acheminement d'un paquet

Les échanges sont possibles entre noeuds en passant par des routeurs si ces derniers sont capables de déterminer la route pour joindre la destination. A cet effet, les routeurs possèdent une table de routage qui contient les informations nécessaires pour acheminer un paquet vers sa destination.

Observation d'une table de routage

La consultation de la table de routage de R1 s'effectue par la commande

```
vyos@r1:~$ show ipv6 route
```

ou bien

```
vyos@r2:~$ vtysh
r2# sh ipv6 route
r2# exit
vyos@r2:~$
```

La table de routage de PC-2 est obtenue soit par la commande

```
root@PC-2::c2:~# ip -6 route show
```

ou la commande

```
root@PC-2::c2 netstat -6 -nr
```

Nota : *pour améliorer la lisibilité de la table de routage de PC2, vous serez peut être amené à agrandir la fenêtre de la console avant de lancer la commande précédente, de manière à afficher une entrée de la table de routage par ligne.*

Vous remarquerez qu'il y a deux routes pour une remise directe. Il s'agit des routes dont la destination partage le même préfixe que la source sur 64 bits. Enfin une troisième route passe par eth0, il s'agit de la route par défaut notée `::/0` ou `default`. Cette route indique une remise indirecte.

Si nous voulons faire apparaitre la route prise pour aller de PC-2 à R1, nous disposons de la commande `traceroute6`:

```
root@PC-2:~$ traceroute6 -n  fd75:e4d9:cb77::1
```

Naturellement vous reconnaissez l'adresse IPv6 de R2 puis celle de R1. Cet affichage indique la route prise pour joindre R1 mais également que R1 est accessible par l'adresse alloué à eth1.

Analyse de la route pour atteindre le serveur web

L'hôte sur le PC-1 comporte l'utilitaire web cURL (*client URL Request Library*). Ce dernier permet de consulter les pages hébergées sur le serveur web SRV-3. Sur le terminal de PC-1, entrer la commande de téléchargement :

```
root@PC-1::c1:~# curl  -6 http://[fd75:e4d9:cb77:3::c3]
```

Oups, vous devez voir rien arriver. Vous pouvez interrompre l'attente avec la combinaison de touches (CTRL+C).

```
. CTRL+C
```

Nous avons ici un problème de connectivité entre PC-1 et SRV-3. Voyons voir d'où viens le problème.

Commençons par vérifier que la source et la destination ont bien une adresse IPv6, sur PC-1 et SRV-3 faire l'affichage des adresses alloués sur l'interface eth0: sur PC-1

```
root@PC-1::c1:~# ip -6 addr show eth0
```

sur SRV-3

```
root@SRV-3::c3:~# ip -6 addr show eth0
```

Si au niveau des adresses tout est normal. Regardons, si PC-1 et PC-2 ont bien tous les deux une route par défaut:

```
root@PC-1::c1:~# route -A inet6 -n

root@SRV-3::c3:~# route -A inet6 -n
```

Un affichage comportant la ligne ci-dessous indique qu'il y a une route par défaut. L'adresse du *Next Hop* doit être l'adresse IPv6 du routeur local.

```
::/0               fd75:e4d9:cb77:1::1    UG  1024   1   0 eth0
```

Voyons maintenant au niveau de la route, commençons par afficher la route pour atteindre SRV-3 depuis PC-1:

```
root@PC-1::c1:~# traceroute6 -n fd75:e4d9:cb77:3::c3
traceroute to fd75:e4d9:cb77:3::c3 (fd75:e4d9:cb77:3::c3), 30 hops max, 80
byte packets
 1  fd75:e4d9:cb77:1::1 (fd75:e4d9:cb77:1::1)  1.119 ms  3.771 ms  3.865 ms
 2  * * *
 3  * * *
 4  * * *
 .
 .
 .
30  * * *
root@PC-1::c1:~#
```

Le résultat montre que la route s'arrête après le routeur R1. Recommençons le test mais depuis SRV-3 cette fois-ci pour atteindre PC-1

```
root@SRV-3::c3:~# traceroute6 -n fd75:e4d9:cb77:1:c1
traceroute to fd75:e4d9:cb77:1::c1 (fd75:e4d9:cb77:1::c1), 30 hops max, 80
byte packets
1   fd75:e4d9:cb77:3::3 (fd75:e4d9:cb77:3::3)   4.657 ms !N   6.011 ms !N
6.400 ms !N
root@SRV-3::c3:~#
```

Cette fois-ci, le résultat montre que la route s'arrête après R2. Il y a donc une erreur entre les routeurs R1 et R2.

Regardons ce qui circule sur le lien d'infrastructure. Pour cela démarrons une capture de réseau sur un point de connexion symbolisé par un point vert sur la topologie. Nous retiendrons l'interface eth1 du routeur R2 ou R1.

Après avoir surligné le lien d'interconnexion entre R1 et R2, faire un clic droit et lancer la capture wireshark avec *Start capture*

Depuis le terminal de PC-1, lancer un traceroute vers SRV-3.

```
root@PC-1::c1:~# traceroute6 -n fd75:e4d9:cb77:3::c3
traceroute to fd75:e4d9:cb77:3::c3 (fd75:e4d9:cb77:3::c3), 30 hops max, 80
byte packets
 1  fd75:e4d9:cb77:1::1 (fd75:e4d9:cb77:1::1)  1.119 ms  3.771 ms  3.865 ms
 2  * * *
 3  * * *
 4  * * *
 .
 .
 .
CTRL+C
root@PC-1::c1:~#
```

Prenez soin d'arrêter la capture avant d'aller explorer le résultat de l'analyse, pour cela en revenant sur la présentation Topologie, surligner la loupe qui est présente sur le lient d'interconnexion, puis clic-droit et chosissez **Stop capture**.

Vous pouvez maintenant analyser les messages échangés sur le lien R1-R2. Première remarque, le message de requête émis par la commande traceroute sur PC-1 arrive bien jusqu'à R2. Seconde remarque, on ne voit pas sur la capture une réponse émise suite à la reqùête. En somme, le routeur R2 reçoit un paquet IPv6 mais n'émet pas de paquet à destination de PC-1. Regardons alors le contenu de la table de routage de R2:

```
vyos@r2:~$ show ipv6 route
Codes: K - kernel route, C - connected, S - static, R - RIPng,
       O - OSPFv3, I - IS-IS, B - BGP, N - NHRP, T - Table,
       v - VNC, V - VNC-Direct, A - Babel, D - SHARP, F - PBR,
       f - OpenFabric,
       > - selected route, * - FIB route

C>* fd75:e4d9:cb77::/64 is directly connected, eth1, 02:48:50
C>* fd75:e4d9:cb77:2::/64 is directly connected, eth0, 02:48:51
C>* fd75:e4d9:cb77:3::/64 is directly connected, eth3, 02:48:49
```

```
C * fe80::/64 is directly connected, eth3, 02:48:49
C * fe80::/64 is directly connected, eth1, 02:48:50
C * fe80::/64 is directly connected, eth0, 02:48:51
C>* fe80::/64 is directly connected, eth2, 02:48:53
vyos@r2:~$
```

Le préfixe de l'adresse de PC-1 est fd75:e4d9:cb77:1::/64. On constate qu'il manque la route pour joindre le réseau Net 1 de préfixe fd75:e4d9:cb77:1::/64. La configuration de R2 est incomplète, il manque une route et c'est donc la raison du dysfonctionnement constaté. Corrigeons ce défaut en ajoutant la route manquante dans R2:

```
vyos@r2:~$ vtysh

Hello, this is FRRouting (version 7.0).
Copyright 1996-2005 Kunihiro Ishiguro, et al.

r2# conf t
r2(config)# ipv6 route fd75:e4d9:cb77:1::/64 fd75:e4d9:cb77::1 eth1
r2(config)# end
r2# copy run start
Note: this version of vtysh never writes vtysh.conf
Building Configuration...
Warning: /etc/frr/frr.conf.sav unlink failed
Integrated configuration saved to /etc/frr/frr.conf
[OK]
r2# show ipv6 route
Codes: K - kernel route, C - connected, S - static, R - RIPng,
       O - OSPFv3, I - IS-IS, B - BGP, N - NHRP, T - Table,
       v - VNC, V - VNC-Direct, A - Babel, D - SHARP, F - PBR,
       f - OpenFabric,
       > - selected route, * - FIB route

C>* fd75:e4d9:cb77::/64 is directly connected, eth1, 03:03:51
S>* fd75:e4d9:cb77:1::/64 [1/0] via fd75:e4d9:cb77::1, eth1, 00:00:25
C>* fd75:e4d9:cb77:2::/64 is directly connected, eth0, 03:03:52
C>* fd75:e4d9:cb77:3::/64 is directly connected, eth3, 03:03:50
C * fe80::/64 is directly connected, eth3, 03:03:50
C * fe80::/64 is directly connected, eth1, 03:03:51
C * fe80::/64 is directly connected, eth0, 03:03:52
C>* fe80::/64 is directly connected, eth2, 03:03:54
r2#
```

Une route statique vers le réseau Net1 est maintenant visible dans la table de routage. Vérifions maintenant si le client sur PC-1 arrive à joindre le serveur web sur SRV-3 :

```
root@PC-1::c1:~# traceroute6 fd75:e4d9:cb77:3::c3
traceroute to fd75:e4d9:cb77:3::c3 (fd75:e4d9:cb77:3::c3), 30 hops max, 80
byte packets
 1  fd75:e4d9:cb77:1::1 (fd75:e4d9:cb77:1::1)  8.846 ms  16.619 ms  17.164
ms
 2  fd75:e4d9:cb77::2 (fd75:e4d9:cb77::2)  24.339 ms  25.307 ms  31.630 ms
  3   fd75:e4d9:cb77:3::c3 (fd75:e4d9:cb77:3::c3)   32.021 ms   32.742 ms
33.043 ms
root@PC-1::c1:~#
```

Maintenant que le routage fonctionne, testons le service web :

```
root@PC-1::c1:~# curl -6 http://[fd75:e4d9:cb77:3::c3]
```

```
.
.  code source html de la page d'accueil
.

root@PC-1::c1:~#
```

Cela marche, le code source de la page HTML d'index est téléchargé. Nous avons bien corrigé le défaut.

Etape 3: Fonction de fragmentation

Nous allons terminer cette activité pratique en illustrant la fonction de fragmentation d'IPv6. Le cours rappelle que la fragmentation est faite par la source quand un paquet IPv6 a une taille supérieure à la taille que peut contenir une trame autrement dit quand le paquet IPv6 a une taille supérieure à la MTU du lien en sortie.

Au moyen de la commande ping6 entre PC-1 et PC-2, nous allons demander à émettre un paquet d'une longueur de 2000 octets. Pour les besoins de l'exercice, nous demandons à réduire la MTU à 1280 octets à l'interface eth1 de R1. Passer en mode configuration, et effectuer les modifications:

```
vyos@r1:~$ configure
[edit]
vyos@r1# set interfaces ethernet eth1 mtu 1280
[edit]
vyos@r1# commit;save
Saving configuration to '/config/config.boot'...
Done
[edit]
vyos@r1#
```

Lancer une capture de paquets IPv6, en surlignant le lien d'interconnexion entre R1 et R2 puis clic-droit et choisir *Start capture*.

Testez la connectivité entre PC-1 et PC-2

Depuis le terminal de PC-1, essayez de joindre PC-2.

```
root@PC-1::c1:~# ping6 -c 3 -n -s 2000 -M want fd75:e4d9:cb77:2::c2
PING fd75:e4d9:cb77:2::c2(fd75:e4d9:cb77:2::c2) 2000 data bytes
2008 bytes from fd75:e4d9:cb77:2::c2: icmp_seq=1 ttl=62 time=9.49 ms
2008 bytes from fd75:e4d9:cb77:2::c2: icmp_seq=2 ttl=62 time=3.82 ms
2008 bytes from fd75:e4d9:cb77:2::c2: icmp_seq=3 ttl=62 time=29.6 ms

--- fd75:e4d9:cb77:2::c2 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2004ms
rtt min/avg/max/mdev = 3.829/14.330/29.671/11.091 ms
root@PC-1::c1:~#
```

Prenez soin d'arrêter la capture avant d'aller explorer le résultat de l'analyse , pour cela en revenant sur la présentation de la topologie, surlignez l'icône loupe qui est présent sur le lien d'interconnexion puis clic-droit et choisissez *Stop capture*.

Analyse de la fragmentation

Vous pouvez miantenant analyser les messages échangés sur le lien R1-R2.

Analysez les paquets capturés, et concentrez-vous sur le champ *Next Header* ainsi que sur le codage de l'extension Fragmentation.

Figure 7: Capture Fragmentation

Pouvez-vous expliquer pourquoi il faut 2 paquets IPv6 pour transporter le message de requête ICMPv6 ?

Quelle est la taille des données transportées dans chaque paquet ?

Quelle est la taille de l'entête IPv6 dans ce cas ?

Arrêt/Pause du simulateur

Au besoin vous pouvez aussi figer l'exécution des équipements avec le bouton Pause *"Suspend All devices"*, voire arrêter les équipements avec le bouton Stop *"Stop All devices"*.

L'état des équipements est sauvegardé en quittant. Pour quitter proprement GNS3, faire CTRL+Q ou faire, avec le menu déroulant *File* et l'action *Quit*.

Conclusion

Grâce à cette deuxième séquence du Mooc IPv6 vous avez découvert et appréhendé différents aspects du protocole:

- Après avoir passé en revue le format de l'en-tête des paquets IPv6,
- Vous avez compris l'importance des mécanismes d'encapsulation,
- Vous avez intégré les principes de routage,
- Vous avez appréhendé les extensions de l'en-tête IPv6
- Enfin après avoir mis en oeuvre une configuration simplifiée

Dorénavant vous êtes aptes à approfondir d'autres mécanismes importants pour faciliter l'intégration du protocole dans toutes les infrastructures où IPv6 sera utile d'être déployer. C'est bien ce que vous allez découvrir dans les prochaines séquences.