ESIEE AMIENS
Majeure GRIT

Sujets TP
IPv6

Nicolas DAILLY

L'objectif de ce TP est de comprendre le mode de fonctionnement du protocole IPv6 et la manière de mettre en place une configuration basique.

Pour les besoins de ce TP, vous utiliserez une machine sous Windows et l'autre sous Linux (Ubuntu). Comme nous l'avons vu en cours, les machines en IPv6 s'auto-configurent. Il y aura donc peu de manipulations à faire sur les postes client.

Pour vous aider, décrochez la dernière page de ce sujet, qui contient le plan du réseau et le tableau d'adresses à compléter.

I. Analyse de la configuration des postes clients

1. Analyse de votre connexion

Débranchez vos machines du réseau GRIT expérimental (réseau rouge ou bleu) et ne laissez branchée que la carte principale (réseau Jaune ou réseau Vert).

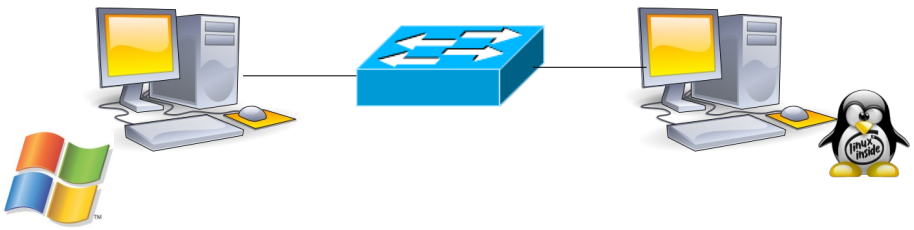
Q1. Sur un site externe, vérifiez l'état de votre connexion IPv4/IPv6 (plein de sites proposes des test IPv6 : tapez « IPv6 test » dans un moteur de recherche).

Ex : http://test-ipv6.com – http://ipv6-test.com - http://web6.remlab.net/pr/check

Q2. Vous en profiterez pour relever l'adresse IPv4 avec laquelle vous êtes vus de l'extérieur (passerelle GRIT).

2. Création d'un réseau local

Vous considérerez un PC sous Windows et un PC sous Linux (à installer en machine virtuelle). Afin de créer un réseau IPv6 autonome, vos PC seront totalement débranchés du Labo GRIT.
Pour cette première partie, reliez les cartes réseaux que vous utilisez à un switch.



3. Sous Linux (à adapter en fonction de votre distribution)

Pour voir la configuration des cartes actives, utilisez la commande « ip address ». Pour voir toutes les cartes, actives ou inactives, utilisez la commande « ifconfig -a ». Pour plus d'infos sur la commande ifconfig, tapez « man ifconfig ».

Q3. Relevez l'adresse MAC de cette carte et calculez l'adresse de lien locale que vous devriez obtenir.

La seconde carte réseau peut être inactive tant qu'elle n'a pas été configurée. En IPv6, il n'y a pas besoin de la configurer, il faut juste l'activer. Pour ce faire, tapez « ifconfig <NOM_INTERFACE> up ».

Q4. L'adresse de lien locale que vous obtenez est-elle générée à partir de l'adresse MAC ?

Q5. Si non, quel aurait été l'adresse de lien locale ?

4. Sous Windows

Avec les commandes « ipconfig » et « ipconfig /all », observez la configuration de la carte réseau (que vous aurez préalablement activé).

Pour les besoin du TP, veillez à ce que la carte réseau utilisée n'ai aucune adresse IPv4 (qu'elle soit fixe ou apprise par DHCP).

Q6. L'adresse de lien locale est-elle générée à partir de l'adresse MAC ?

Q7. Si non, quel aurait été l'adresse de lien locale ?

5. Test de connectivité

Testez la connectivité IPv6 de votre réseau.

Q8. A partir du PC sous Linux, pinguez le PC sous Windows, et inversement. Vous utiliserez pour cela la commande « ping6 » (ou simplement ping suivant les versions du système d'exploitation).

Remarque : Ne passez pas à l'étape suivante tant que la connectivité n'est pas assurée.

Q9. Pinguez l'interface de Loopback

Q10. Pinguez le groupe de toutes les machines (combien y a t'il de réponses par ping ?). Si pas de résponse, explorer pourquoi ?

Q11. Pinguez le groupe des routeurs. Quel est la réponse ? Pourquoi ?

6. Découverte de l'environnement réseau

Q12. Sous linux, tapez les commandes « netstat -rn » et « netstat -rnA inet6 ». Quelles informations vous donnent ces commandes ? La famille de commandes « ip -6 » peut également être très utile.

Q13. Sous Windows, lancez le script « netsh ». Allez ensuite dans « interface ipv6 ». Puis « show route ».

Remarque : Le script « netsh » est un script qui peut se révéler bien utile pour mettre en place des techniques réseau avancées sous Windows. (Cf. « netsh » dans la documentation Microsoft en ligne).

Remarque 2 : Comme dans l'IOS CISCO, pour voir la liste des commandes disponibles, il suffit de taper « ? ». Pour remonter d'un niveau dans l'arborescence des commandes, il suffit de taper « .. ».

Q14. Avec la commande show, regardez également les équipements voisins et les adresses multicast auquel le PC est abonné

7. Analyse du trafic avec Wireshark

Installez puis lancez « Wireshark ». C'est un analyseur réseau bien connu et assez puissant. Allez le menu, « capture/interfaces », puis cliquez sur start juste à côté du nom de l'interface dont vous souhaitez analyser le trafic.

Lancez un ping et regardez ce qui se passe.

Q15. Quels sont les messages (protocole et nom du message) échangés lors d'un ping vers le voisin ?

Q16. Quel type de message est envoyé lors d'un ping vers un équipement qui n'existe pas (par exemple si vous vous trompez dans l'adresse du destinataire) ? Quel protocole aurait été utilisé en IPv4 ?

II. Mise en place d'un routeur dans le réseau

Prenez un routeur et effacez sa configuration.

Q17. Regardez la configuration de vos interfaces (« show ip interface » et « show ipv6 interface »

On notera que la plupart des commandes « ip » fonctionnent en utilisant « ipv6 ».

Q18. Tapez « show ipv6 ? » pour voir toutes les commandes disponibles.

Q19. Allez sur l'interface de votre routeur et activez ipv6 (tapez « ipv6 ? » pour lister les commandes disponibles).

Q20. Regardez la configuration de l'interface, relevez son adresse IP, et vérifiez que vous pouvez pinguer les deux PCs et inversement (utilisez « ping » ou « ping ipv6 »).

Q21. Regardez, dans la configuration de l'interface, a quels groupes appartient le routeur.

Votre routeur devant être maitre sur le réseau, c'est à lui d'annoncer l'adresse globale du réseau. Nous allons donc affecter une adresse à l'interface de votre routeur (adresse fixe, entrée manuellement).

Pour les besoins du TP, nous allons utiliser le réseau suivant (fournie par le FAI) :

2001:470:C9F2:: /48

L'adresse de votre réseau sera la suivante (avec N votre numéro de plot en hexadecimal).

2001:470:C9F2:N:: /64

Pour que votre routeur agisse en tant que tel sur le réseau, il faut le déclarer.

Q22. Tapez « ipv6 unicast-routing ».

Q23. Entrez sur votre routeur la première adresse de votre réseau (commande « ipv6 address »).

Q24. Vérifiez la configuration ipv6 de votre routeur.

Q25. Regardez si votre PC a appris son adresse IP globale. Si ce n'est pas le cas, il faut activer les router advertisement. Allez sur l'interface et tapez : « ipv6 nd prefix <votre_adresse_reseau/votre_masque> »

III. Analyse de l'autoconfiguration

Vous devez analyser le fonctionnement de l'autoconfiguration avec Wireshark.

Q26. Analysez le trafic avec Wireshark. Activez Wireshark et lancer une nouvelle trace. Désactivez la carte réseau, puis réactivez là (ou débranchez et rebranchez le câble). Regardez les échanges sur votre réseau au moment de sa réactivation, le temps que votre PC apprenne sa configuration. Quels sont les messages échangés, sur quelles adresses MAC et adresse IP sont-ils envoyés ?

Q27. Avec la commande « ip -6 neigh show », regardez la liste des voisins.

Q28. Pinguez le PC d'à côté et analysez les échanges. Sur quelles adresses MAC et adresse IP sont envoyés les messages de Network Discovery (ND) et de Network Advertisement (NA) ?

Observez en même temps comment évolue la liste des voisins.

Remarque : A l'issue de cette partie, vous devez comprendre comment le PC génère son adresse de lien locale et son adresse globale. Vous devez également comprendre à quoi sert l'adresse de « groupe multicast sollicité ».

IV. Création d'un réseau « pur v6 »

Nous allons tout d'abord considérer un réseau d'interconnexion exclusivement IPv6. L'adresse du réseau d'interconnexion sera la suivante :

2001:470:C9F2:8000:: /64

L'adresse de votre routeur sera :

2001:470:C9F2:8000::X

avec X est votre numéro de plot en hexadecimal

La salle est normalement pré-cablée. Le port d'accès au switch central correspond au port rouge ou au port bleu.

Une configuration avec un groupe X=15 (0xF) a été mis en place pour que vous puissiez faire des tests.

Q29. Reliez la seconde interface de votre routeur au swith central, puis configurez l'interface.

Q30. Arrivez vous à pinguer les autres routeurs du réseau ? Arrivez vous à pinguer les autres PC (ex. l'adresse IP interne du routeur d'un réseau voisin) ? Pourquoi ?

Q31. En utilisant la commande « ipv6 router », donnez les protocoles de routage

disponibles.

Q32. Activez RIP – vous nommerez le processus de routage comme bon vous semble. Utilisez la commande de configuration « redistribute connected» pour distribuer les routes. Vous devez ensuite aller activer la diffusion des informations de routage sur chacune des interfaces participant à la diffusion des informations. Pour cela, tapez « ipv6 rip <nom_processus> enable ».

Q33. Testez la connectivité sur l'ensemble du réseau

Q34. Analysez la table de routage. Y a t'il désormais une connectivité vers l'ensemble de l'Internet v6 ?

Q35. Ajoutez une route par défaut vers le routeur du groupe « F ».

Q36. Testez votre connectivité vers l'Internet V6 (pinguez par exemple l'adresse IPv6 du DNS de Google : 2001:4860:4860::8888).

Q37. Que manque t'il à votre configuration pour pouvoir « surfer » facilement sur l'Internet V6 ?

Pour annoncer l'adresse d'un serveur DNS aux clients, on utilise le protocole DHCPv6 (en mode stateless).

Etape 1. Créer un pool DHCPv6 en tapant les commandes suivantes

(config)#ipv6 dhcp pool <nom_pool>

(config-dhcp)#dns-server <@ipv6_serveur_DNS>

(config-dhcp)#domain-name <nom_domaine>

Etape 2. Activer le pool DHCPv6 sur l'interface souhaitée et indiquez aux équipements - via le protocole Network Discovery – qu'ils doivent compléter leur configuration via une requête DHCP

(config-if)#ipv6 dhcp server <nom_pool>

(config-if)#ipv6 nd other-config-flag

Vous utiliserez comme serveur DNS :

- Celui d'Hurricane Electric : 2001:470:20::2
- Ceux de Google : 2001:4860:4860::8888 et 2001:4860:4860::8844 (Cf. **http://fr.wikipedia.org/wiki/Google_Public_DNS**)

Q38. Configurez DHCPv6 pour l'annonce des serveur DNS à vos PCs.

Rq : Sous Windows 10, il sera peut être nécessaire de forcer le PC à aller chercher la configuration DHCP. Pour cela, tapez « ipconfig /renew6 <nom_carte_reseau> ».

Q39. A ce stade, vous êtes capable de surfer sur l'Internet V6. Testez l'état de votre connexion (Cf. Question 1)

Q40. Trouver 5 sites accessibles en IPv6.

V. Création d'un réseau v6 à travers une dorsale v4

Vous allez maintenant considérer que votre réseau est relié à une dorsale V4.

L'adresse réseau de la dorsale est 192.168.0.0 /27

Vous utiliserez l'adresse IPv4 192.168.0.X avec X votre numéro de plot.

Q41. Réinitialiser l'interface de votre routeur reliée à la dorsale. Vous pouvez utiliser la commande « default interface <nom_interface> ».

Q42. Désactivez la route IPv6 par défaut vers le groupe F.

Q43. Reconfigurez l'interface de la dorsale en IPv4 et vérifiez la connectivité.

A ce stade, vous ne pouvez plus accéder à l'Internet V6. Vous allez monter un tunnel avec le groupe F, capable de vous fournir l'interconnexion avec l'internet V6.

Il va falloir transporter le trafic IPv6 à travers le réseau IPv4 : on met en place un tunnel 6over4. Un tunnel est une connexion point à point à travers le réseau. Chaque extrémité du tunnel doit donc avoir une adresse IPv6 valide.

Voici la configuration du tunnel fournie par le tunnel broker (groupe 15) :

```
IPv6 Tunnel Endpoints
```

- `Serveur IPv4 : 192.168.0.15`
- `Serveur IPv6 : 2001:470:C9F2:80XF::2/64`
- `Client IPv4 : 192.168.0.X`
- `Client IPv6 : 2001:470:C9F2:80XF::1/64`

Pour monter un tunnel, il faut utiliser les commandes suivantes :

```
Router(config)#interface tunnel <n° de tunnel>
```

```
Router(config-if)#tunnel source <interface_source>
Router(config-if)#tunnel destination <adresse IPv4 destination>
Router(config-if)#ipv6 address <adresse IPv6 d'interface tunnel>
Router(config-if)#tunnel mode ipv6ip
```

Q44. Montez votre tunnel vers le groupe 15 (prendre 15 comme numéro de tunnel)

Q45. Réactivez la connectivité avec les autres réseaux et l'Internet

Q46. Arrivez-vous à accéder au réseau de vos voisins ? Si oui, par où passe le trafic ?

Q47. Comment faire pour que le trafic aille directement chez chacun des voisins ?

Pour éviter que le trafic entre les groupes ne passe par le routeur F, activez des tunnels direct vers les autres groupes.

Pour les besoins du TP, nous affecteront aux extrémités du tunnel l'adresse IP suivante :

2001:470:CDA0:FFXY::Z/64

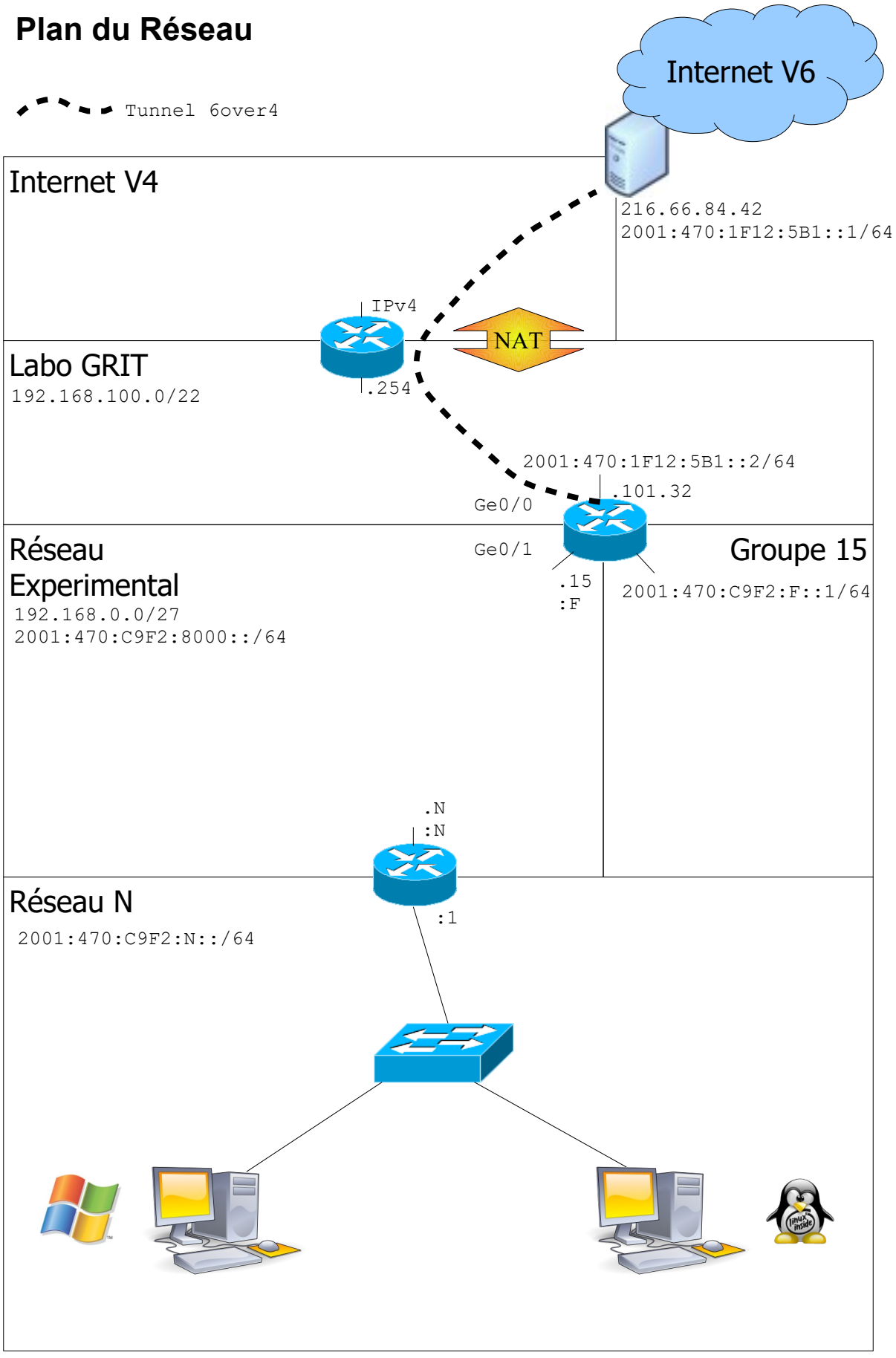
avec X et Y vos numéros de plots en hexadecimal tel que X<Y

Si votre numéro de plot est X alors Z=1 sinon Z=2

Q48. Montez les tunnels vers les autres groupes : (prendre pour numéro de tunnel, le numéro du groupe que vous reliez).

Q49. Observez l'évolution de la table de routage au fur et à mesure que vous activez vos tunnels

VI. Plan du Réseau



VII. Feuille à compléter

	Labo GRIT
Adresse IP publique	

	Configuration Linux
Adresse MAC	
Adresse de lien locale attendue (méthode l'EUI64)	
Adresse de lien locale obtenue	
Adresse globale	
Adresses de groupe Multicast utilisées	

	Configuration Windows
Adresse MAC	
Adresse de lien locale attendue (méthode l'EUI64)	
Adresse de lien locale obtenue	
Adresse globale	
Adresses de groupe Multicast utilisées	

	Configuration Routeur
Adresse MAC	
Adresse de lien locale attendue (méthode l'EUI64)	
Adresse de lien locale obtenue	
Adresse Globale	
Adresses de groupe Multicast utilisées	