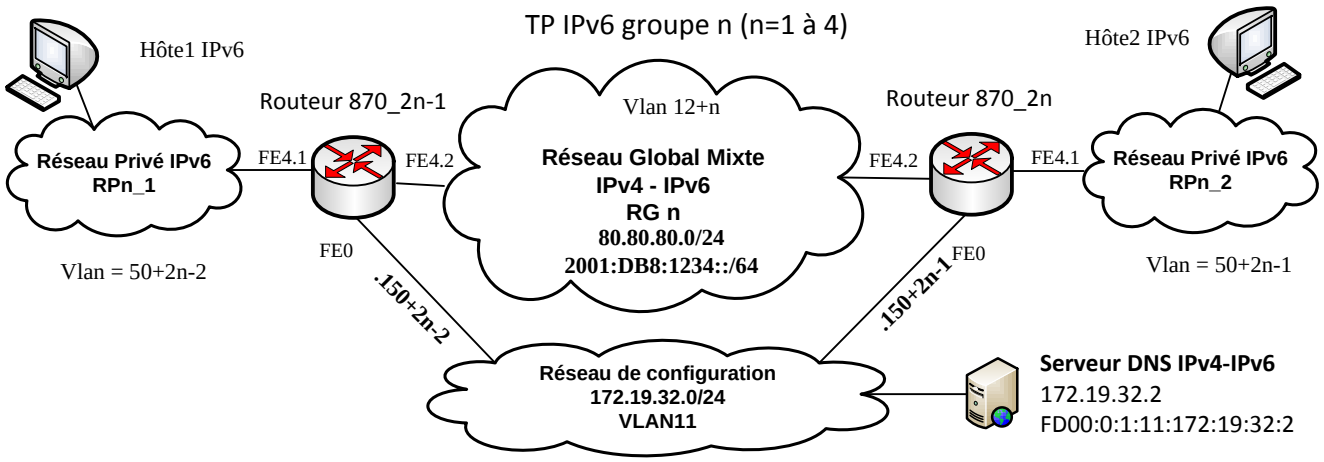
Travaux Pratiques IPV6

Partie 1 : Configuration de réseaux IPv6 automatiques « stateless » et « statefull »

Schéma du réseau initial à mettre en place :



Première étape de « mise en route ».

1) Configurer les interfaces du réseau de configuration et prendre la main sur ces routeurs via ces interfaces.
2) Configurer les interfaces globales IPv4, routeur **870_2n_1** adresse 80.80.80.1 et routeur **870_2n** adresse 80.80.80.2. Tester la liaison IPv4 entre les deux routeurs.
3) Configurer les interfaces globales IPv6 en mode « autoconfiguration ».
4) Vérifier les adresses obtenues (préfixe et identifiant d'interface IPv6 EUI64). Tester la liaison IPv6 entre les deux routeurs, vérifier la liste des voisins et l'état de la liaison. Quelques commandes de test à utiliser de préférence dans cet ordre :
   - ✓ **sh ipv6 interface xxx** pour visualiser l'adresse de lien attribuée
   - ✓ **show ipv6 neighbors** pour constater que le voisin n'est pas encore connu
   - ✓ **ping ipv6** pour déclencher la découverte des voisins
   - ✓ **show ipv6 neighbors** pour constater que le voisin est à présent connu

   et pour plus de détails et pour visualiser les annonces des routeurs
   - ✓ **debug ipv6 icmp**
   - ✓ **debug ipv6 nd**
   - ✓ **show ipv6 routers**

Configuration des adresses globales uniques.

5) Supprimer le mode d'autoconfiguration IPv6 et configurer les adresses globales uniques des routeurs 870_2**n-1** et 870_2**n** avec les adresses 2001 :DB8 :1234 ::**1**/64 et 2001 :DB8 :1234 ::**2**/64 respectivement.
6) Vérifier les adresses obtenues, ainsi que les groupes multicast de l'interface. Tester la liaison IPv6 entre les deux routeurs à l'aide d'un ping sur l'adresse globale puis de lien.

Configuration du réseau privé IPv6 RPn_2, configuration automatique sans état via ND et RA.

Le routeur fournira les informations d'adressage pour le réseau IPv6 privé auquel il est directement connecté via les messages « Neighbors Discovery » et « Router Advertissment ».

7) Configurer l'interface IPv6 privée du routeur 870_2**n** avec pour adresse un préfix FD00:2:2:**2::**/64 et un identificateur d'interface EUI64.
8) Configurer l'interface IPv6 du routeur 870_2**n** avec les annonces ND suivantes :
   - ✓ un préfix réseau FD00:2:2:**2 ::**/64,
   - ✓ une durée de vie de validité et préférée infinies,
   - ✓ un intervalle d'émission des annonces nd de 4s,
   - ✓ un intervalle d'émission des annonces ra de 15s,
   - ✓ une MTU d'interface de 1492 octets.
9) Vérifier la bonne distribution des adresses IPv6. On remarquera les adresses par défaut utilisées pour les serveurs DNS IPv6.
10) Vérifier si l'hôte est capable d'adresser l'interface de son routeur.
11) Modifier le préfixe annoncé et vérifier la renumérotation des hôtes puis reconfigurer le préfixe initial.
12) Eventuellement, capturer les trames RA sur un poste hôte en filtrant l'adresse multicast « adhoc » afin de vérifier les informations émises par le routeur (préfixe, MTU).
    Filtre Wireshark **ip6 host ff02 ::1** par exemple.

Commandes utiles :

- ✓ **ipv6 address xxxxx eui-64**
- ✓ **ipv6 nd prefix xxxx**
- ✓ **ipv6 nd ra xxxx**
- ✓ **ping -6**
- ✓ **tracert -6**
- ✓ **netsh interface ipv6 show nei**
- ✓ **netsh interface ipv6 show add**

Configuration du réseau privé IPv6 RPn_1, configuration automatique avec état par DHCPv6.

Le routeur fera fonction de serveur DHCP pour le réseau IPv6 privé auquel il est directement connecté.

13) Configurer l'interface IPv6 du routeur 870_2**n-1** avec l'adresse FD00:1 :1 :1 ::**1**/64.
14) Configurer la fonction serveur DHCPv6 du réseau RP**n_1** comme décrit ci-dessous :
    - ✓ Pool DHCPv6 nommé poolR**n**-DHCPv6 avec :
      - un préfix réseau IPv6 FD00:1 :1 :1**::**/64, et une durée de vie des adresses IPv6 du pool de 1800s et préférée de 1800s,
      - un serveur DNS IPv6 d'adresse précisée sur le schéma,
      - un nom de domaine domaineR**n.**
    - ✓ Affectation du pool à l'interface puis réglage des options d'avertissement du routeur :
      - activation du flag **M** « managed »,
      - intervalle d'émission des annonces ra de 15s,
      - intervalle d'émission des annonces de sollicitation des voisins de 10s.

Pour ceci il est conseillé de créer le pool (commande **ipv6 dhcp pool *poolName***) puis d'affecter celui-ci à l'interface et enfin d'ajouter les options, commandes :

- ✓ **ipv6 dhcp pool** …,
- ✓ **ipv6 nd managed-config-flag**,
- ✓ **ipv6 nd …**

15) Vérifier la bonne distribution des adresses IPv6 auprès des hôtes IPv6 et vérifier les paramètres de domaine et de serveur DNS.
16) Vérifier si l'hôte est capable d'adresser l'interface de son routeur et inversement (penser au pare-feu des postes…).
17) Ajouter les routes sur les deux routeurs afin que les deux hôtes soient capables de se « pinger ».

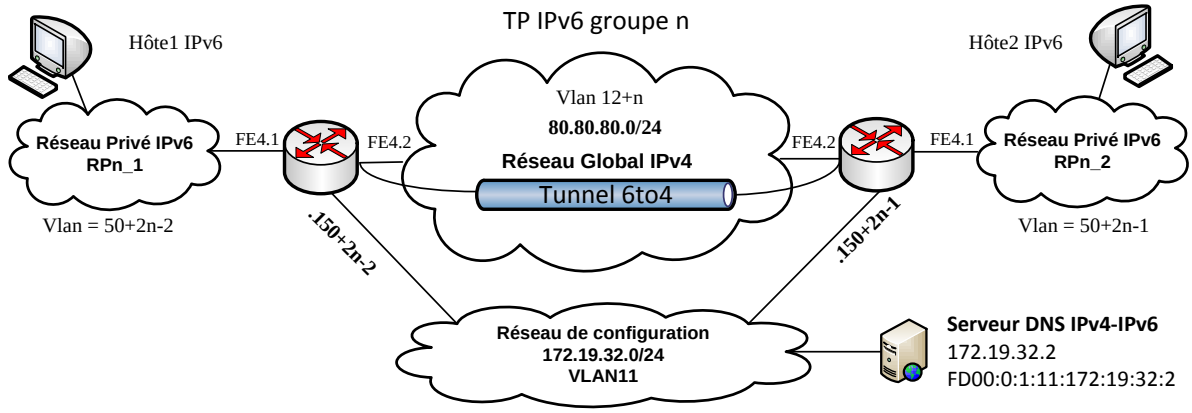
Commandes utiles :

- ✓ **ipv6 dhcp pool xxxxx**
- ✓ **ipv6 nd managed-config-flag**
- ✓ **ipv6 dhcp server xxxxx**
- ✓ **show ipv6 dhcp pool**
- ✓ **show ipv6 dhcp binding**
- ✓ **traceroute ipv6 xxxxxx**

18) Sauvegarder votre configuration dans la mémoire flash du routeur en la nommant **configIPV6-1.txt.**

Partie 2 : Configuration du tunnel 6to4 pour relier deux réseaux privés IPv6

Les routeurs relieront les réseaux privés IPv6 au travers d'un réseau IPv4 grâce à un tunnel 6to4.



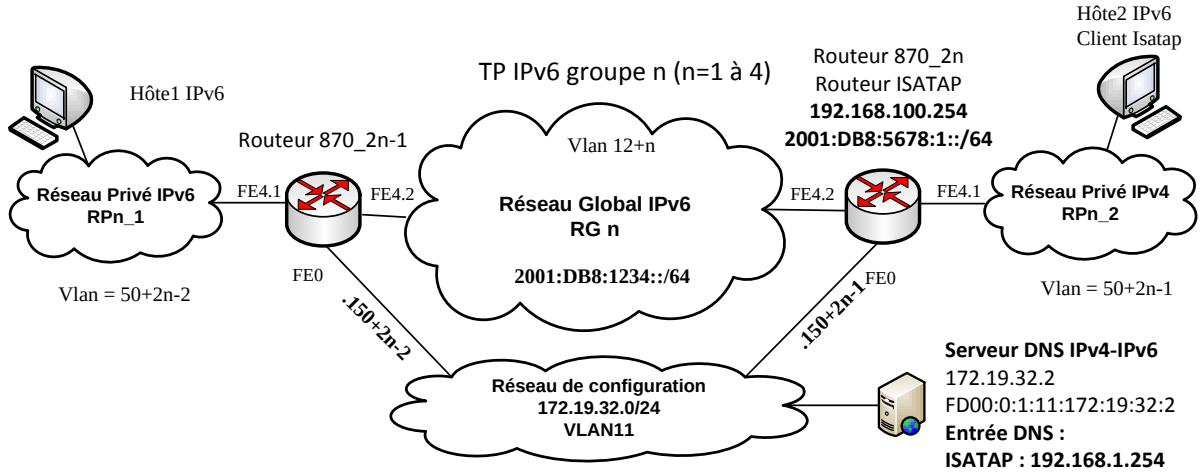
1) Supprimer la configuration IPv6 des interfaces du réseau global et les routes IPv6 vers les réseaux privés IPv6.
2) Calculer l'adresse 6to4 de chaque interface du réseau global.
3) Sur chaque routeur configurer une interface tunnel avec le paramétrage suivant :
   - ✓ Une description ****** tunnel 6to4 ******
   - ✓ une adresse IPv6 du tunnel de 2002:XXXX:XXXX::/128 pour le routeur **870_2n-1** et de 2002:XXXX:XXXX::/128 pour le routeur **870_2n**,
   - ✓ une source du tunnel connectée à l'interface du réseau global,
   - ✓ un mode de tunnel IPv6 vers IP 6to4,
2) Ajouter sur chaque routeur une route pour le préfix réseau 6to4 2002 ::/16 pointant vers le tunnel.
3) Ajouter sur chaque routeur la route vers le réseau privé à joindre afin qu'elle pointe sur l'interface d'extrémité du tunnel.
4) Vérifier que les deux hôtes sont capables de se « pinger » au travers du tunnel 6to4. Vous pouvez également tester le tunnel depuis le routeur en activant le débogage du tunnel à une extrémité et en réalisant un ping étendu depuis l'autre extrémité.

Commandes utiles :

- ✓ **debug tunnel**
- ✓ **show interface tunnel x accounting**
- ✓ **show interface tunnel x stat**

5) Sauvegarder votre configuration dans la mémoire flash du routeur en la nommant **configIPV6-2.txt.**

<u>Partie 3 :</u> Configuration du tunnel ISATAP pour communiquer en IPv6 depuis un réseau IPv4.



1) Repartir sur la configuration de la partie 1 puis supprimer les adresses IPv4 du réseau global pour obtenir un réseau global « IPv6 only ».
2) Supprimer également la configuration du réseau privé IPv6 du routeur 870_2n (ISATAP) celui-ci devenant pour cette partie un réseau « IPv4 only ».
3) Sur le routeur ISATAP, activer un serveur DHCP IPv4 pour le réseau privé de caractéristiques suivantes :
   - ✓ adresse réseau 192.168.100.0/24,
   - ✓ nœuds hybrides (DHCP puis Wins),
   - ✓ domaine RAMSES.II,
   - ✓ passerelle 192.168.100.254 (le routeur ISATAP),
   - ✓ serveur DNS 172.19.32.2,
   - ✓ plage d'exclusion des adresses .200 à .254.
4) Configurer l'interface FE4.1 du routeur ISATAP avec l'adresse IPv4 définie.
5) Sur le poste client activer la configuration IPv4 en client DHCP et vérifier que vous récupérez bien une adresse IP du pool DHCP et que vous joignez bien le routeur ISATAP.

Pour la configuration de l'interface ISATAP les postes clients interrogent le serveur DNS afin de résoudre le nom d'hôte réservé ISATAP. Celui-ci doit être associé à l'adresse du routeur ISATAP à utiliser pour monter le tunnel ISATAP leur permettant de joindre le monde IPv6 depuis leur réseau IPv4. A partir de cette réponse il monte l'interface ISATAP avec l'adresse ISATAP « ad hoc ».
Le serveur DNS double pile (serveurmedia.ramses.ii) a été préalablement configuré avec cette entrée :
ISATAP = 192.168.100.254

L'algorithme de configuration d'un équipement isolé qui utilise ISATAP est le suivant :
- ✓ dans un premier temps, l'équipement doit connaître l'adresse IPv4 du routeur gérant ISATAP, cette adresse est obtenue par résolution **DNS** ou configurée par une commande **netsh,**
- ✓ l'équipement envoie un message **IPv6 Router Sollicitation** au routeur en utilisant comme adresse de la source, son adresse lien-local (fe80::5efe:IPv4) et comme adresse de destination l'adresse de multicast des routeurs (FF02::02). Ce message est encapsulé dans un paquet IPv4 dont l'adresse destination est l'adresse IPv4 du routeur obtenue précédemment,
- ✓ le routeur répond au message **IPv6 Router Sollicitation** en renvoyant en point-à-point, toujours encapsulé dans un paquet IPv4, la liste des préfixes IPv6 utilisés pour joindre les équipements isolés (**Router Advertisement**),
- ✓ à partir du préfixe IPv6 l'équipement peut calculer son adresse IPv6 ISATAP prefixeIPv6:0:5efe:IPv4.

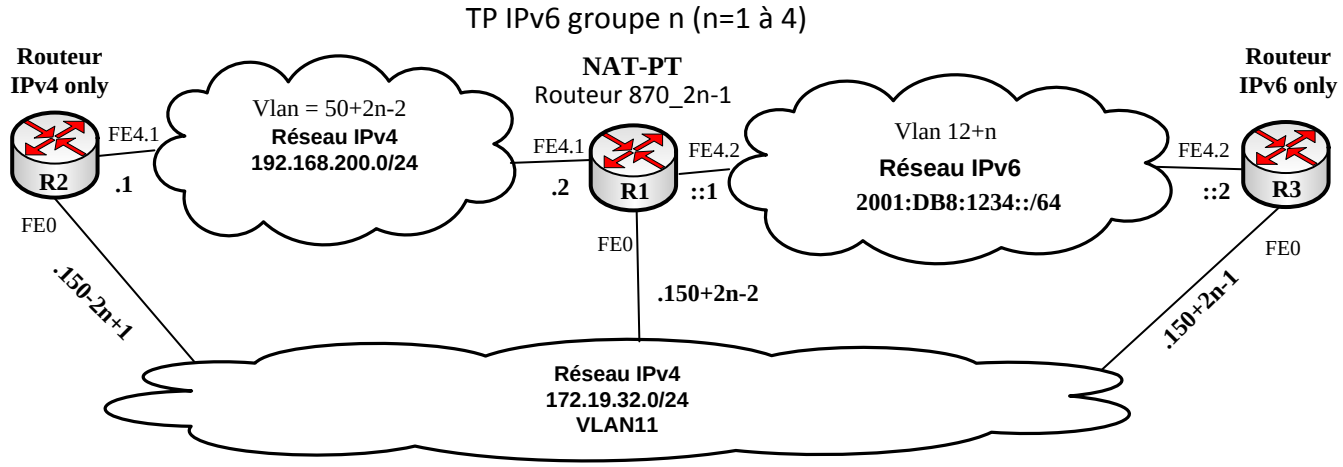
Les paquets IPv6 peuvent alors être encapsulés IPv4 (n° protocole 41) entre l'équipement et le routeur qui décapsulera pour retransmettre en IPv6 sur le réseau IPv6.

Pour joindre le serveur DNS depuis le réseau privé IPv4 et surtout pour obtenir sa réponse deux solutions sont envisageables :

- ✓ ajouter la route vers le réseau privé IPv4 sur le serveur DNS,
- ✓ installer la NAT pour les accès au réseau de configuration depuis le réseau privé IPv4 (solution choisie…).

6) Installer la NAT-PAT pour joindre le serveur DNS et tester l'accès à celui-ci et la résolution DNS depuis le poste client. Vérifier la bonne obtention de l'adresse ISATAP.
7) Configurer l'interface Tunnel de type ISATAP avec les paramètres suivants :
   - ✓ adresse **IPv6 2001:DB8:5678:1::/64** identificateur d'interface EUI64,
   - ✓ source du tunnel = adresse IPv4 du routeur ISATAP,
   - ✓ mode de tunnel = ISATAP,
   - ✓ activer les protocoles **nd** et **ra** pour le tunnel (**no ipv6 nd ra suppress**).
   - ✓
8) Ajouter une route sur le routeur870_2n-1 vers le routeur870_2n pour joindre les adresses préfixées ISATAP.
9) Tester le fonctionnement des accès IPv6 depuis le poste client ISATAP et capturer quelques paquets pour vérifier l'encapsulation des paquets IPv6.

<u>Partie 4 :</u> Configuration de la NAT-PT pour communiquer avec un réseau IPv4 depuis un réseau simple pile IPv6.



NAT-PT (Network Address Translation – Protocol Translation)

L'utilisation du protocole NAT-PT permet à des nœuds IPv6 uniquement de communiquer avec des nœuds IPv4 uniquement ou vice versa. Il s'agit une sorte de passerelle pour les réseaux IPv4/IPv6.
Cette méthode de transition est une solution à mettre en place lorsque l'on dispose d'un réseau totalement compatible IPv6 et que l'on ne veut plus « alourdir » son réseau par la gestion d'une double pile.

NAT-PT peut être utilisé de quatre manières différentes (proche de NAT pour IPv4) :

- ✓ NAT-PT statique,
- ✓ NAT-PT dynamique,
- ✓ NAT-PT avec surcharge PAT,
- ✓ NAT-PT avec mappage IPv4.

A ce jour le protocole NAT-PT a été remplacé par une version plus aboutie qu'il est conseillé d'utiliser, le protocole NAT64. Ce protocole n'est malheureusement disponible sur les matériels Cisco qu'à la condition de disposer d'un IOS de version >15 ce qui n'est pas le cas de nos matériels par manque de ressources mémoire. **Nous nous contenterons donc d'utiliser NAT-PT sur IOS 12.4 avec ses limitations qui ne seront pas corrigées c.f. doc Cisco… En voici deux importantes :**

- ✓ **impossibilité d'activer la gestion de cef « Cisco Express Forwarding » si on utilise NAT-PT,**
- ✓ **problèmes de routes incohérentes si des routes redondantes existent avec NAT-PT.**

NAT-PT Statique :

Cette partie va consister à mettre en place une « NAT-PT » sur le routeur R1 permettant aux routeurs R2 et R3 de communiquer.
Un ping vers une adresse IPv4 est impossible depuis R3, celui-ci ne comprenant que IPv6, de même un ping vers une adresse IPv6 est impossible depuis R2, celui-ci ne disposant que de la pile IPv4.

La configuration suivante met en place une relation NAT-PT statique entre le routeur R2 (adresse 192.168.200.1) et le routeur R3 (adresse 2001:DB8:1234::2).
Pour ceci sur le routeur R1 (groupe 1) :

- ✓ côté IPv6 l'adresse source 2001:DB8:1234:2 sera translatée vers l'adresse 192.168.1.222,
- ✓ côté IPv4 l'adresse source 192.168.200.1 sera translatée vers l'adresse 2010::222.

```
interface FastEthernet4.1
 encapsulation dot1Q 50
 ip address 192.168.200.2 255.255.255.0
 ipv6 enable
 ipv6 nat

interface FastEthernet4.2
 encapsulation dot1Q 13
 ipv6 address 2001:DB8:1234::1/64
 ipv6 enable
 ipv6 nat

 ipv6 nat v4v6 source 192.168.200.1 2010::222
ipv6 nat v6v4 source 2001:DB8:1234::2 192.168.1.222
ipv6 nat prefix 2010::/96
```

R3 : test du ping vers R2

```
routeur870_5#ping 2010::222

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2010::222, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/2/4 ms
```

R2 : activation du débogage ICMPv4 « debug ip icmp »

```
routeur870_6#
*Apr 10 12:47:32.504: ICMP: echo reply sent, src 192.168.200.1, dst 192.168.1.222
*Apr 10 12:47:32.508: ICMP: echo reply sent, src 192.168.200.1, dst 192.168.1.222
*Apr 10 12:47:32.512: ICMP: echo reply sent, src 192.168.200.1, dst 192.168.1.222
*Apr 10 12:47:32.516: ICMP: echo reply sent, src 192.168.200.1, dst 192.168.1.222
```

*Apr 10 12:47:32.532: ICMP: echo reply sent, src 192.168.200.1, dst 192.168.1.222

R1 : activation du débogage de NAT-PT « debug ipv6 nat detailled »

routeur870_4#
IPv6 NAT: IPv6->IPv4:
src (2001:DB8:1234::2 -> 192.168.1.222)
dst (:: -> 0.0.0.0)
ref_count = 1, usecount = 0, flags = 257,
rt_flags = 0, more_flags = 0

IPv6 NAT: IPv6->IPv4:
src (:: -> 0.0.0.0)
dst (2010::222 -> 192.168.200.1)
ref_count = 1, usecount = 0, flags = 513,
rt_flags = 0, more_flags = 0

IPv6 NAT: IPv6->IPv4: icmp src (2001:DB8:1234::2) -> (192.168.1.222), dst (2010::222) -> (192.168.200.1)
IPv6 NAT: Found prefix 2010::/96
IPv6 NAT: IPv4->IPv6:
src (192.168.200.1 -> 2010::222)
dst (192.168.1.222 -> 2001:DB8:1234::2)
ref_count = 1, usecount = 0, flags = 2,
rt_flags = 0, more_flags = 0

IPv6 NAT: IPv4->IPv6: src (192.168.200.1) -> (2010::222), dst (192.168.1.222) -> (2001:DB8:1234::2)

R2: test du ping vers R3

routeur870_6#ping 192.168.1.222

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.222, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/4/4 ms

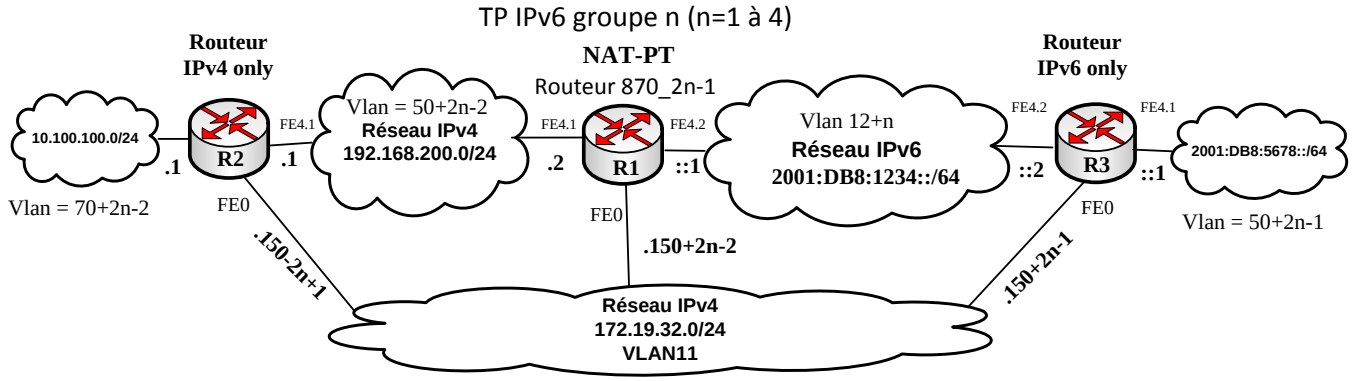
R3 : activation du débogage ICMPv6 « debug ipv6 icmp »

*Apr 18 14:46:41.622: ICMPv6: Received echo request, Src=2010::222, Dst=2001:DB8:1234::2
*Apr 18 14:46:41.622: ICMPv6: Sent echo reply, Src=2001:DB8:1234::2, Dst=2010::222

1) Mettre en place les réseaux selon le schéma proposé sur R1, R2, R3. Vérifier que R1 communique avec R2 et R3 mais que R2 et R3 ne peuvent pas communiquer.
2) Mettre en place NAT-PT sur R1 et vérifier la communication entre R2 et R3, contrôler les translations à l'aide des directives de débogage.

NAT-PT avec surcharge PAT et mappage IPv4 :

Cette partie va consister à mettre en place une « NAT-PT avec surcharge et mappage IPv4» sur le routeur R1 permettant aux réseaux IPv6 de R3 de communiquer avec les réseaux IPv4 de R2.



Le « mappage » IPv6 des adresses IPv4 va consister à utiliser le préfixe 2001::/96 pour former les adresses IPv4 afin de les rendre accessibles depuis R3.
Par exemple l'adresse IPv4 10.100.100.1 sera vue côté IPv6 comme 2001::10.100.100.1.

La configuration suivante sur R1 (groupe 1) met en place cette relation NAT-PT avec surcharge et mappage IPv4» :

```
interface FastEthernet4.1
 encapsulation dot1Q 50
 ip address 192.168.200.2 255.255.255.0
 ipv6 enable
 ipv6 nat

interface FastEthernet4.2
 encapsulation dot1Q 13
 ipv6 address 2001:DB8:1234::1/64
 ipv6 enable
 ipv6 nat

ipv6 nat v6v4 source list list-to-ipv4 interface FastEthernet4.1 overload
ipv6 nat prefix 2001::/96 v4-mapped what-to-ipv4

ipv6 access-list list-to-ipv4
 sequence 20 permit ipv6 2001:DB8::/32 any

ipv6 access-list what-to-ipv4
 permit ipv6 any 2001::/96
```

R3 : test du ping vers le réseau 10.100.100.0 de R2

routeur870_5#ping 2001::10.100.100.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001::A64:6401, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/4/4 ms

R1 : activation du débogage de NAT-PT « debug ipv6 nat detailled »

routeur870_4#
IPv6 NAT: address allocated :: -> 192.168.200.2
IPv6 NAT: IPv6->IPv4: icmp src (2001:DB8:1234::2) -> (192.168.200.2), dst (2001::A64:6401) -> (10.100.100.1)
IPv6 NAT: Found prefix 2010::/96
IPv6 NAT: IPv4->IPv6:
src (10.100.100.1 -> 2001::A64:6401)
dst (192.168.200.2 -> 2001:DB8:1234::2)
ref_count = 1, usecount = 0, flags = 2,
rt_flags = 0, more_flags = 16

IPv6 NAT: IPv4->IPv6: icmp src (10.100.100.1) -> (2001::A64:6401), dst (192.168.200.2) -> (2001:DB8:1234::2)
IPv6 NAT: IPv6->IPv4:
src (2001:DB8:1234::2 -> 192.168.200.2)
dst (2001::A64:6401 -> 10.100.100.1)
ref_count = 1, usecount = 0, flags = 2,
rt_flags = 0, more_flags = 16

R3 : test du ping depuis le réseau 2001 :DB8 :5678 ::/64 vers le réseau 10.100.100.0 de R2

routeur870_5#ping
Protocol [ip]: ipv6
Target IPv6 address: 2001::10.100.100.1
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands? [no]: y
Source address or interface: 2001:DB8:5678::1
UDP protocol? [no]:
Verbose? [no]:
Precedence [0]:
DSCP [0]:
Include hop by hop option? [no]:
Include destination option? [no]:
Sweep range of sizes? [no]:
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001::A64:6401, timeout is 2 seconds:
Packet sent with a source address of 2001:DB8:5678::1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/3/4 ms