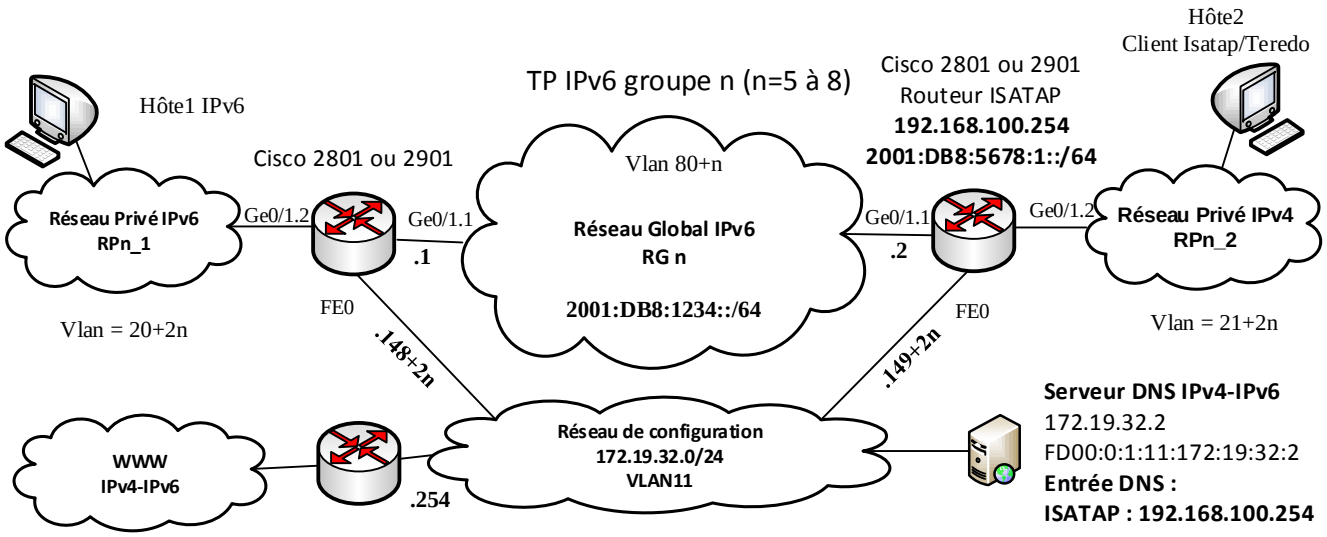
# Travaux Pratiques IPV6

***<u>Manip 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 :
   - ✓ nom du pool : dhcpIPv4,
   - ✓ adresse réseau 192.168.100.0/24,
   - ✓ durée de vie des adresses de 8 jours,
   - ✓ 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 du lien (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.

Exemple de NAT :

```
ip access-list standard AclNatDns
        permit 192.168.100.0 0.0.0.255
ip nat inside source list AclNatDns interface vlan11 overload
interface FastEthernet 4.1
        ip nat inside
interface vlan11
        ip nat outside
```

7) Configurer une interface Tunnel 0 de type ISATAP avec les paramètres suivants :
   - ✓ Une description « **** Tunnel ISATAP Network 192.168.100.0 **** »,
   - ✓ 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**) car les annonces de routeur sont désactivées par défaut sur les interfaces de type tunnel.

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 en « pingant » l'adresse FD00:1:1:1::1 par exemple et capturer quelques paquets pour vérifier l'encapsulation des paquets IPv6 dans IPv4 (protocole 41, filtre wireshark « ip proto 41 »).

Commandes utiles :

- ✓ ***netsh interface isatap show state***
- ✓ ***netsh interface isatap set state enabled/disabled***

## *Test d'un tunnel TEREDO depuis l'hôte pour accéder à l'internet IPv6 depuis un réseau IPv4 avec NAT.*

10) Sur le routeur ISATAP ajouter une route 0 pour joindre l'Internet.

11) Sur le poste situé dans le réseau **RPn_2** désactiver l'interface ISATAP.

12) Configurer l'interface TEREDO avec pour serveur TEREDO « **teredo.remlab.net** » puis configurer le type de tunnel en mode « **client** » pour un hôte non attaché à un domaine ou « **enterpriseclient** » pour un hôte faisant partie d'un domaine.

13) Capturer les paquets échangés avec le serveur TEREDO pour la négociation du tunnel en filtrant sur le protocole UDP port 3544, pour ceci réaliser un « ping » vers un hôte de l'internet IPv6 **ipv6.google.com**. Relever dans la réponse l'adresse et le port du relai TEREDO fournis dans le paquet IPv6 encapsulé IPv4. Vérifier que les échanges ICMPv6 sont bien encapsulés à destination du relai TEREDO précédent.

14) Vérifier l'état de l'interface tunnel TEREDO puis vérifier avec l'adresse IPv6 Teredo l'adresse et le port du serveur Teredo ainsi que votre IP publique.

Commandes utiles :

- ✓ ***netsh interface isatap set state disabled***
- ✓ ***netsh interface teredo show state***
- ✓ ***netsh interface teredo set state servername= ????***
- ✓ ***netsh interface teredo set state type= ????***