IPv6 Module 6 – Plus d'iBGP et Configuration eBGP de Base

Objectif: Utilisant IPv6, simuler 4 backbones d'ISP interconnectés en utilisant une combinaison d'ISIS, internal BGP, et external BGP.

Prérequis:: Module 1 (ISIS)

Topologie :

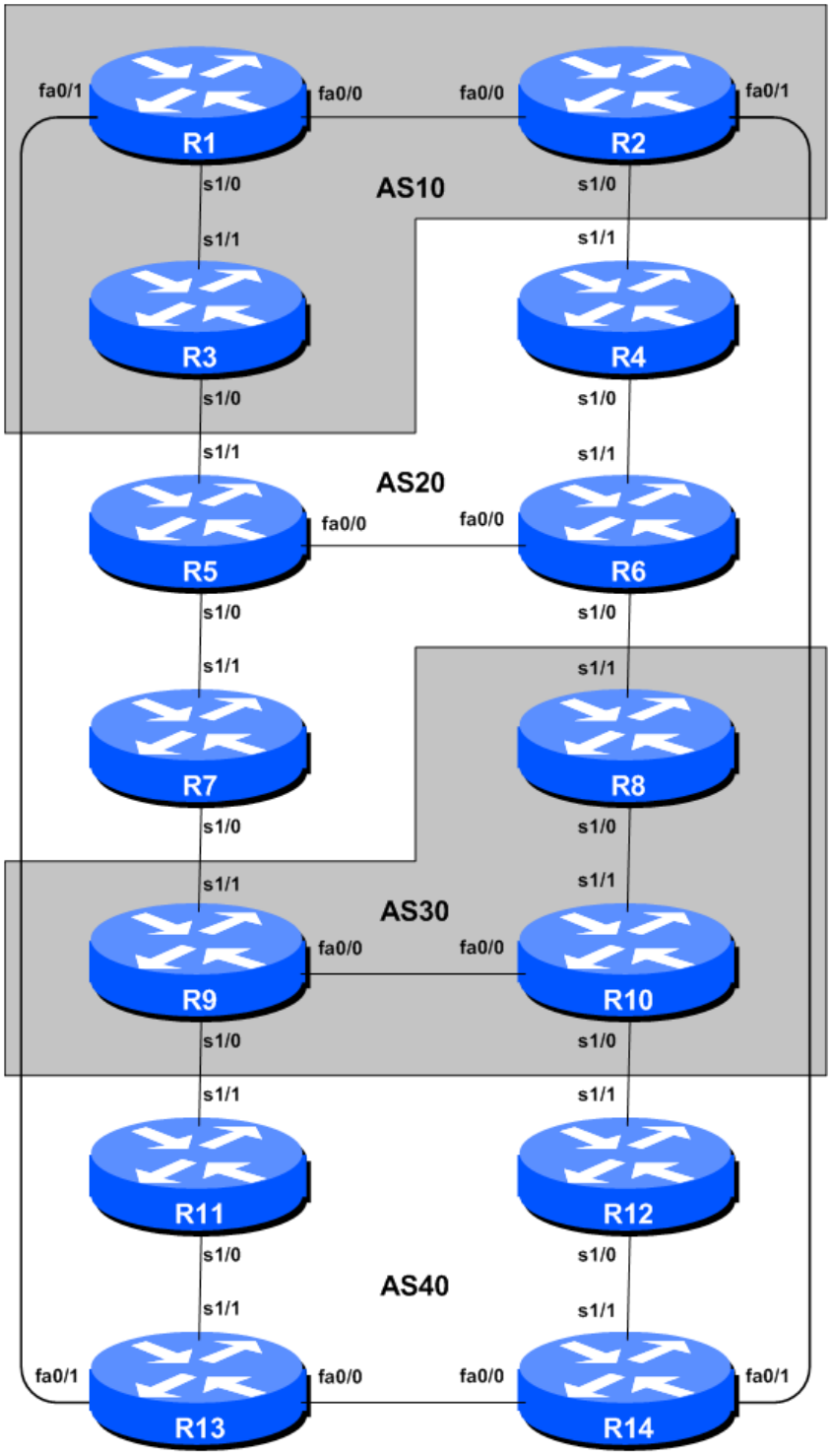

Figure 1 – BGP AS Numbers

Remarques

L'objectif de ce module est d'initier les étudiants à external (eBGP). eBGP est utilisé entre différents systèmes autonomes (AS) dans un "Internet". La classe est scindée en 4 réseaux distincts. Les équipes appartenant a une même réseau travaillent ensemble comme le font les opérateurs d'un même ISP. Chaque AS a deux liens avec ses ASs voisins. Ce concept est utilisé durant une partie significative des laboratoires de cet atelier.

The connectivité illustrées a la Figure 2 montre les liens entre ASs. Nous supposons que les routeurs d'un AS sont connectes physiquement comme illustre à la Figure 1.

Note: Ce module IPv6 est conçu pour être exécuté après la version IPv4 de ce module.

Configuration du laboratoire

1. Connectez les routeurs comme indiqué à la Figure 1. Tous les routeurs d'un AS doivent être physiquement connectes et joignables. Les relations entre AS sont fournies Figure 2.

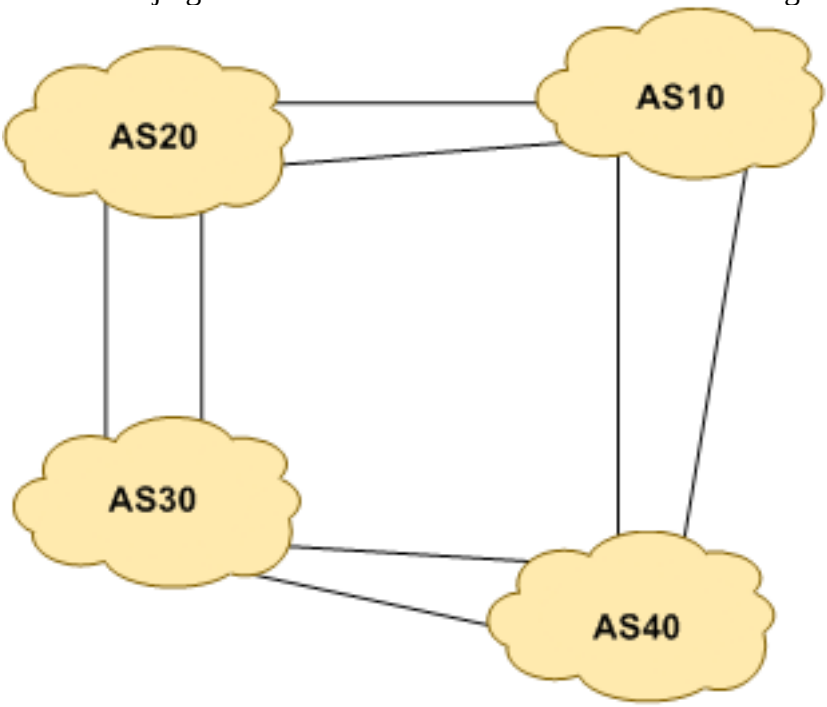

Figure 2 – AS relationship

1. **Supprimez l'adressage IPv6.** Avant de considérer la configuration des protocoles de routage selon les schémas 1 et 2, nous devons d'abord supprimer l'adressage des modules précédents. Lors de cette étape nous supprimons les adresses IPv6 de toutes les interfaces physiques et des loopback. Ceci ramène la configuration avant le point 10 du module 1. N'oubliez pas de supprimer toutes les adresses IPv6.

2. **Adressage IPv6.** Comme pour l'étape 5 du Module 1, nous avons besoin d'un plan d'adressage rationnel et *scalable* pour chaque AS du réseau. Chaque AS reçoit son propre bloc d'adresses, un /32 (l'allocation minimum typique pour un nouvel ISP). Ce bloc d'adresses est alloue aux liens et loopbacks des routeurs de chacun des AS. Les allocations sont comme suit:

AS10	**2001:db8::/32**	**AS20**	**2001:db9::/32**

AS30 2001:dba::/32 **AS40 2001:dbb::/32**

De nouveau, nous devons diviser chaque bloc d'adresses afin d'avoir de l'espace d'adressage pour les clients, l'infrastructure réseau et les loopbacks. ci-dessous nous rappelle comment ceci peut être fait:

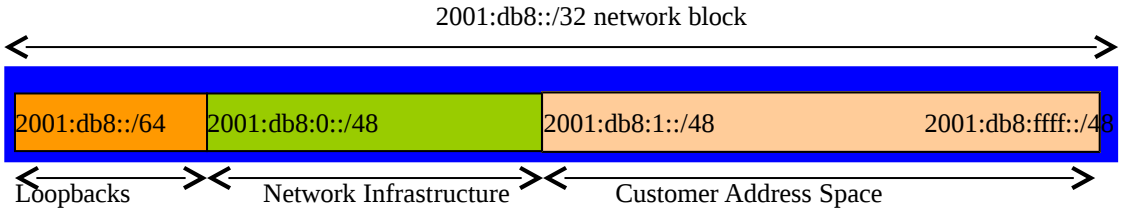

Figure 3 – Dividing allocated block of /32 into Customer, Infrastructure and Loopbacks

Veuillez vous référer au plan d'adressage fourni en annexe pour ce module. Le fichier est nommé "Addressing Plan – Modules 6 to 9". Comme fait pour le Module 1, configurez les adresses de chaque interface utilisée pour ce module, vérifiez la connectivité IP de base avec vos voisins immédiats.

2. **Adresses pour les interfaces loopback des routeurs.** Comme le plus petit sous-réseau possible pour IPv6 est un /64, nous allouons le premier /64 de notre /48 pour l'infrastructure, pour les loopbacks même si les ASs ont seulement 3 ou 4 routeurs. Les adresses attribuées aux loopbacks pour ce module sont les suivantes:

Router1	**2001:db8::1**	**Router8**	**2001:dba::1**
Router2	**2001:db8::2**	**Router9**	**2001:dba::2**
Router3	**2001:db8::3**	**Router10**	**2001:dba::3**
Router4	**2001:db9::1**	**Router11**	**2001:dbb::1**
Router5	**2001:db9::2**	**Router12**	**2001:dbb::2**
Router6	**2001:db9::3**	**Router13**	**2001:dbb::3**
Router7	**2001:db9::4**	**Router14**	**2001:dbb::4**

Configurez ISIS pour IPv6 sur les routeurs de chaque AS. Vérifiez que la configuration ISIS en place fonctionne normalement. Souvenez-vous qu'ISIS doit être configuré **uniquement** sur les interfaces internes. Pour des raisons de scalabilité (passage a l'échelle), il ne faut pas configurer d'adjacences vers des appareils hors de votre AS. Vérifiez qu'il n'y a pas de commande ipv6 *router isis* pour les interfaces externes. Une conséquence de cela est que les adresses des liens externes n'apparaissent pas dans l'IGP (voir section suivante pour une discussion sur le déploiement iBGP).

N'oubliez pas d'activer multi-topology ISIS lorsque vous configurez ISIS afin de supporter IPv6. Ceci vous permet de déployer ISIS pour IPv6 dans l'AS sans perte de connectivité IPv4. (Si vos routeurs ne supportent pas ISIS multi-topology, il vous faudra coordonner l'activation de la famille d'adresses IPv6 pour chaque interface avec l'équipe voisine qui opère le routeur pour cette l'interface). De plus, N'oubliez pas de configurer l'over-load bit comme nous l'avons fait au Module 1.

A titre d'exemple, l'équipe qui opère Router 1, avec deux interfaces dans AS 10, fait ceci :

```
Router1 (config)# router isis as10
Router1 (config-router)# net 49.0001.0100.0001.5224.00
Router1 (config-router)# is-type level-2-only
```

```
Router1 (config-router)# metric-style wide level-2
Router1 (config-router)# log-adjacency-changes
!
Router1 (config-router)# address-family ipv6
Router1 (config-router-af)# multi-topology
Router1 (config-router-af)# set-overload-bit on-startup wait-for-bgp
!
Router1 (config)# interface fastethernet 0/0
Router1 (config-if)# ipv6 router isis as10
Router1 (config-if)# isis ipv6 metric 2 level-2
!
Router1 (config)# interface serial 1/0
Router1 (config-if)# ipv6 router isis as10
Router1 (config-if)# isis ipv6 metric 20 level-2
```

Souvenez vous que les interfaces sur lesquelles vous ne voulez pas qu'ISIS tourne doivent être marquées comme *passives*. Pour ISIS, marquer une interface comme étant passive signifie qu'il n'y aura pas d'adjacence CLNS **et** que le sous-réseau IP utilisé pour l'interface sera injecté dans ISIS. Notez qu'il n'est pas possible de marquer une interface comme passive si ISIS n'est pas configuré sur au moins une des interfaces physiques de routeur.

```
Router1 (config)# router isis as10
Router1 (config-router)# passive-interface Loopback0
```

Notes:

- Par défaut, ISIS établi des adjacences et annonce les prefixes des interfaces activées à l'aide de la commande "`ipv6 router isis`". Ceci est différent du comportement OSPF. OSPF tente d'établir des adjacences pour les interfaces couvertes par la déclaration `network` (OSPF requière donc l'utilisation de `passive` et `no passive` pour contrôler son fonctionnement).
- Différents ISPs utilisent différentes méthodes pour les adresses NET. Il est cependant courant d'utiliser l'adresse IP de la loopback comme *system ID* au format hexadecimal ou decimal. Dans ce module tous les routeurs d'un AS sont de niveau-2 (level-2) et dans une seule aire (*49.0001*).

3. **ISIS sur des liens Ethernet Point-a-Point.** Verifiez qu'ISIS fonctionne en mode point-à-point sur les liens Ethernets point-à-point, par exemple:

```
Router1 (config)# interface fastethernet 0/0
Router1 (config-interface)# isis network point-to-point
```

Ce lien est maintenant traité comme une connexion série point-à-point.

4. **Test Ping.** Vérifiez les routes reçues via ISIS. Assurez vous que vous voyez tous les réseaux de votre AS et pas de réseaux d'autres ASs. Pingez toutes les loopback de votre AS. Utilisez les commandes "*show clns neighbor"* et "*show ip route"*.

5. **Sauvez la configuration.** N'oubliez pas de sauvez la configuration en NVRAM !

Checkpoint #1 : *appelez l'instructeur afin de vérifier la connectivité.*

6. **Activation de l'authentification pour les voisins ISIS.** Vérifiez que l'authentification avec le voisin fonctionne toujours pour l'adjacence ISIS. Ceci est indépendant du protocole IPv6 de telle sorte que les adjacences devraient rester actives.

Checkpoint #2 : *appelez l'instructeur afin de vérifier la connectivité.*

7. **Configuration des sessions iBGP entre routeurs d'un même AS.** Utilisez les adresses loopback pour les peerings iBGP. De plus, configurez la commande *network* pour ajouter les blocs d'adresses alloués à chaque routeur/équipe dans les annonces BGP.

```
router bgp 10
 no bgp default ipv4-unicast
 bgp log-neighbor-changes
 address-family ipv6
  no synchronization
  network 2001:db8::/32
  neighbor 2001:db8::2 remote-as 10
  neighbor 2001:db8::2 update-source loopback 0
  neighbor 2001:db8::2 next-hop-self
  neighbor 2001:db8::2 description iBGP Link to R2
  neighbor 2001:db8::3 remote-as 10
  neighbor 2001:db8::3 update-source loopback 0
  neighbor 2001:db8::3 next-hop-self
  neighbor 2001:db8::3 description iBGP Link to R3
!
ipv6 route 2001:db8::/32 Null0
```

8. **Testez la connectivité BGP interne.** Utilisez les commandes `show BGP` pour vous assurez que vous recevez les routes de tous les routeurs de votre AS.

9. **Configuration de mots de passe sur les sessions iBGP.** Il nous faut maintenant configurer des mots de passe sur les sessions iBGP. Révisez la présentation afin de comprendre pourquoi c'est nécessaire. Décidez entre toutes les équipes d'un même AS sur le mot de passe à utiliser pour les sessions iBGP. Ensuite appliquez le à tous les peerings iBGP de votre routeur. Par exemple, sur le peering de Router2 avec Router3, le mot de passe "cisco" est utilisé :

```
router bgp 10
 address-family ipv6
  neighbor 2001:db8::3 password cisco
```

Actuellement IOS réinitialise la session iBGP lorsqu'un mot de passe MD5 est ajouté. Dès lors, lorsqu'un mot de passe est ajouté sur une session BGP d'un réseau opérationnel, cette tâche doit être accomplie durant les fenêtres annoncées de maintenance, un moment où les clients s'attendent à des perturbations de service. Dans ce laboratoire, cela n'a pas tellement d'importance. (De futures versions d'IOS éviteront ce sérieux problème d'interruption de service.)

Consultez les logs du routeur – les changements de sessions BGP étant consignés, une incohérence dans le mot de passe devrait se repérer facilement.

Checkpoint #3: *Appelez l'instructeur et démontrez la configuration du mot de passe sur les session iBGP. Si l'instructeur vous en donne le feu vert, vous pouvez passer aux points suivants.*

10. **Configuration des peerings eBGP.** Référez-vous a la Figure 1 afin de déterminer les liens entre ASs. Les adresses utilisés pour les sessions eBGP entre 2 AS sont les adresses des interfaces

point-à-point **PAS** les adresses loopback (révisez la présentation BGP si vous ne comprenez pas pourquoi). Pour les peerings de Router1 avec Router13, la configuration ressemble à ceci:

```
router bgp 10
 address-family ipv6
  neighbor 2001:db8:0:4::1 remote-as 40
  neighbor 2001:db8:0:4::1 description eBGP to Router13
```

Utilisez les commandes `show BGP` pour vous assurer que vous envoyez et recevez les annonces BGP de vos voisins eBGP.

Q. Pourquoi ne pas utiliser les interfaces loopback pour les sessions eBGP ?

A. L'adresse IP loopback d'un routeur n'est pas connue des peers BGP externes. De ce fait les peers externes ne savent pas comment joindre la loopback afin d'établir la session de peering BGP.

Q. Quelle commande show BGP permet de voir l'état de la connexion avec un peer ?

A. Essayez *show bgp ipv6 unicast neighbor x.x.x.x* – Ceci fourni les détails concernant l'état d'un peer. Il existe des sous-commandes donnant plus d'information sur la session de peering.

Q. Quelle commande show BGP permet de voir les préfixes annoncés et reçus d'un peer eBGP ?

A. Essayez *show ipv6 bgp neighbor x.x.x.x route* – ceci montre les routes que vous recevez de votre voisin. De même, remplacez *route* par *advertised-routes* pour obtenir la liste des réseaux que vous annoncez à votre voisin. (Notez qu'en pratique, il y a une subtilité à prendre en compte ici – si vous appliquez des route-maps et/ou des politiques BGP, ces dernières ne sont pas prises en compte par la commande *advertised-routes*. Utilisez la commande *advertised-routes* avec précaution.)

11. Configuration de mots de passe pour les sessions eBGP. Configurez maintenant des mots de passe pour les sessions eBGP entre votre AS et les AS voisines. Mettez vous d'accord avec l'AS voisine sur le mot de passe à utiliser pour la session eBGP. Ensuite appliquez le mot de passe à la session eBGP. Par exemple, pour la session de Router2 avec Router4, "cisco" est utilisé comme mot de passe:

```
router bgp 10
 address-family ipv6
  neighbor 2001:db8:0:3::2 password cisco
```

Comme pour les sessions iBGP, consultez les logs à la recherche de mots de passe incohérents ou non configurés. De nouveau, vous observez que le routeur réinitialise la session eBGP dès qu'un mot de passe est configuré.

Note: A partie de maintenant, dès qu'une session BGP (iBGP ou eBGP) est configurée, tous les routeurs DOIVENT utiliser un mot de passe sur ces sessions.

Checkpoint #4: *Appelez l'instructeur et démontrez la configuration du mot de passe sur les session eBGP. Si l'instructeur vous en donne le feu vert, vous pouvez passer aux points suivants.*

12. **Ajout des routes "client" dans BGP.** Comme pour le Module 1, nous ajoutons maintenant les routes "clients" dans BGP sur chaque router. Nous n'avons pas de clients réels connectés à nos routeurs dans le laboratoire. Nous allons donc simuler la connectivité en utilisant l'interface Null0. Le bloc d'adressage "client" que chaque équipe annonce en iBGP est listé ci-dessous– nous utilisons encore un /48 pour plus de simplicité.

R1	**2001:db8:1::/48**	**R8**	**2001:dba:1::/48**
R2	**2001:db8:2::/48**	**R9**	**2001:dba:2::/48**
R3	**2001:db8:3::/48**	**R10**	**2001:dba:3::/48**
R4	**2001:db9:1::/48**	**R11**	**2001:dbb:1::/48**
R5	**2001:db9:2::/48**	**R12**	**2001:dbb:2::/48**
R6	**2001:db9:3::/48**	**R13**	**2001:dbb:3::/48**
R7	**2001:db9:4::/48**	**R14**	**2001:dbb:4::/48**

Chaque équipe installe une route statique pointant vers l'interface **NULL0** pour le /48 dont elle est a l'origine. Des que la route statique est installée, l'équipe ajoute une entrée dans sa table BGP pour ce préfixe. Voici ce que cela donne pour Router8:

```
ipv6 route 2001:dba:1::/48 Null0
!
router bgp 30
 address-family ipv6
  network 2001:dba:1::/48
!
```

13. **Vérification de la table BGP.** Y a t-il des routes vues par ***show bgp ipv6*** ? Si non, pourquoi pas? Une fois que toutes les équipes de la classe ont terminé leur configuration, chaque équipe doit voir l'agrégat de chaque AS, ainsi que les quatorze / 48s introduits à l'étape précédente. Si ce n'est pas le cas, travaillez avec vos voisins pour résoudre le problème.

Checkpoint #5: *Appelez l'instructeur afin de vérifier la connectivité. Utilisez entre autres les commandes "show ipv6 route sum","show bgp ipv6 unicast sum", "show bgp ipv6 unicast", "show ipv6 route", and "show bgp ipv6 unicast neigh x.x.x.x route | advertise". Il doit y avoir 4 préfixes agrégés (un pour chaque ISP) et 14 prefixes clients, des /48's, dans la table BGP.*

3. **Importance d'agréger.** Chaque a reçu un bloc /32 d'adresses. Les operateurs de l'Internet demandent à ce que les préfixes utilisés par un ISP soient agrégés le plus possible avant d'être annoncés au reste de l'Internet. Il est parfaitement acceptable de subdiviser une espace d'adresse a l'intérieur d'un AS et évidemment c'est très courant (comme nous l'avons fait ici) – mais la plupart des operateurs considèrent que répandre cet petits blocs d'adresses dans l'Internet comme une pratique asociale, irrespectueuse du bien-être général de l'Internet.

Q. Comment agréger automatiquement de petits blocs d'adresses utilises dans votre AS en un bloc plus large à annoncer à l'extérieur de votre réseau ? ***Indice:*** *Révisez la documentation BGP.*

A. La commande "aggregate-address" est fréquemment utilisée à cette fin.

Nous ne filtrons pas, nous ne limitons pas, les annonces des blocs d'adresses clients que nous introduisons dans chaque AS. Ceci sera un des objectifs des modules suivants de cet atelier.

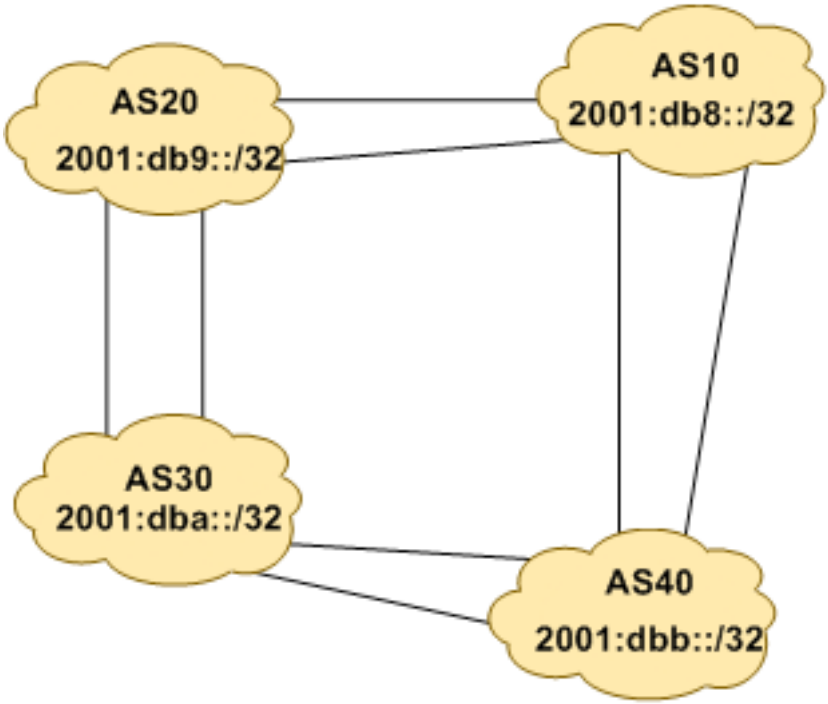

Figure 4 – Agrégats pour chaque ASN

Questions de révision

1. Combien de types d'origines de routes existe-t-il en BGP ?
2. Listez ces types. **Indice:** Voir présentations BGP.
3. Comment sont-ils utilisés ?
4. Pourquoi configurer des mots de passe sur les sessions iBGP et eBGP ? De quoi protègent ils ?
5. Pourquoi est que l'agrégation est importante pour/dans l'Internet?