Module 6 - Plus d'iBGP, et configuration de base eBGP

Objectif: Simuler quatre différents backbones ISP interconnectés en utilisant une combinaison d'OSPF, BGP interne et externe.

Prérequis: Module 1

Topologie :

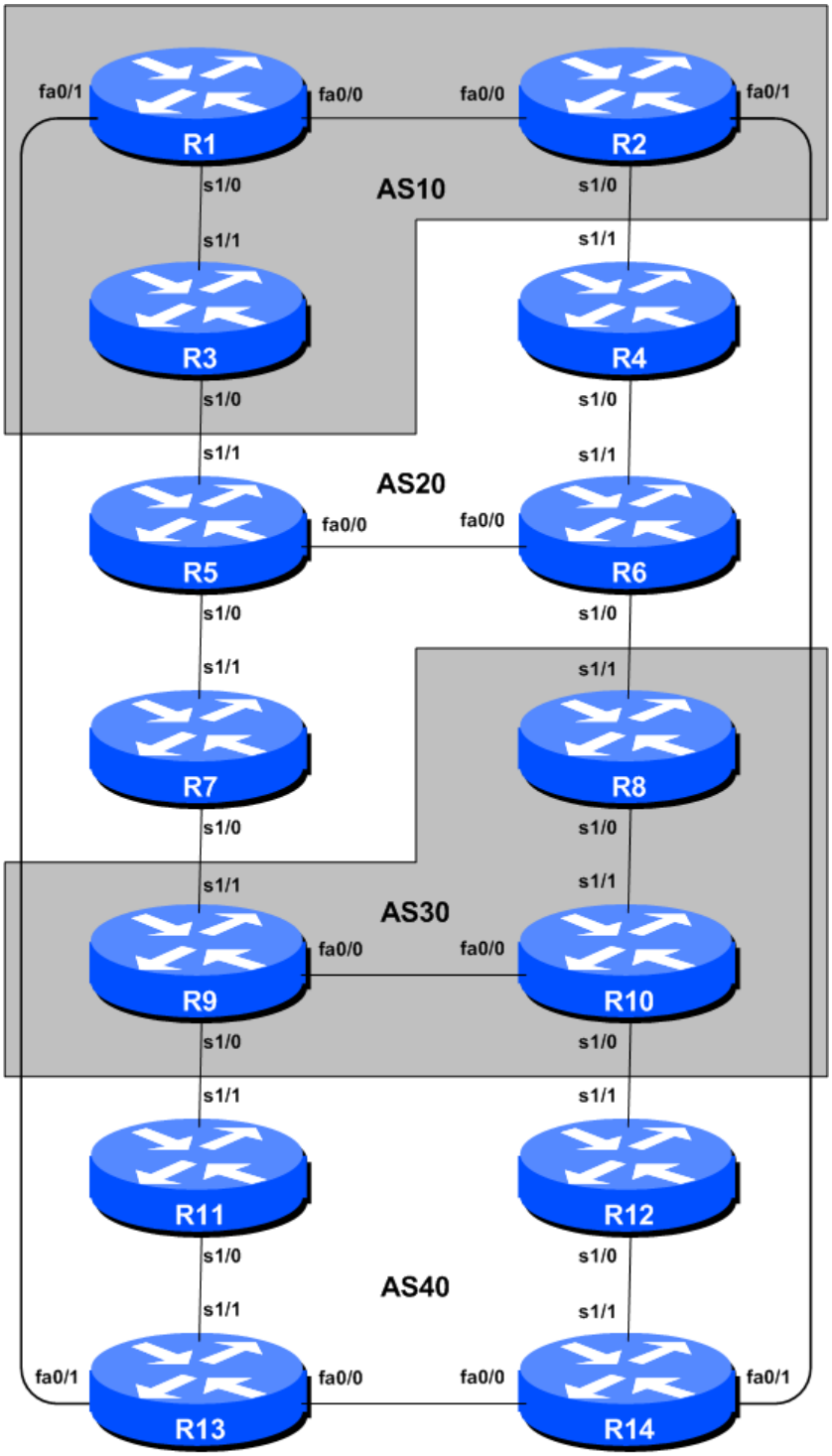

Figure 1 – Numéros AS BGP

Notes de laboratoires

Le but de ce module est d'initier l'étudiant à BGP externe (eBGP). Il s'agit de la relation entre les différents systèmes autonomes dans "Internet". La salle de classe est divisée en quatre réseaux distincts, et les équipes appartenant à chaque réseau travaillent ensemble comme un ISP typique. Chaque AS a deux liens vers les AS voisins, et ce caractéristique est utilisé tout au long d'une partie importante de cet atelier.

La connectivité indiquée dans les diagrammes représente les liens entre les AS. Il est supposé que tous les routeurs au sein d'un AS sont physiquement connectés les uns aux autres selon la Figure 1.

Exercices de laboratoire

1. Connectez les routeurs comme indiqué dans Figure 1. Tous les routeurs au sein d'un AS doivent être physiquement connectés et joignables. La relation entre les AS est tel que représenté dans la Figure 2 et donne une vue qui correspond à ce qui se passe en réalité.

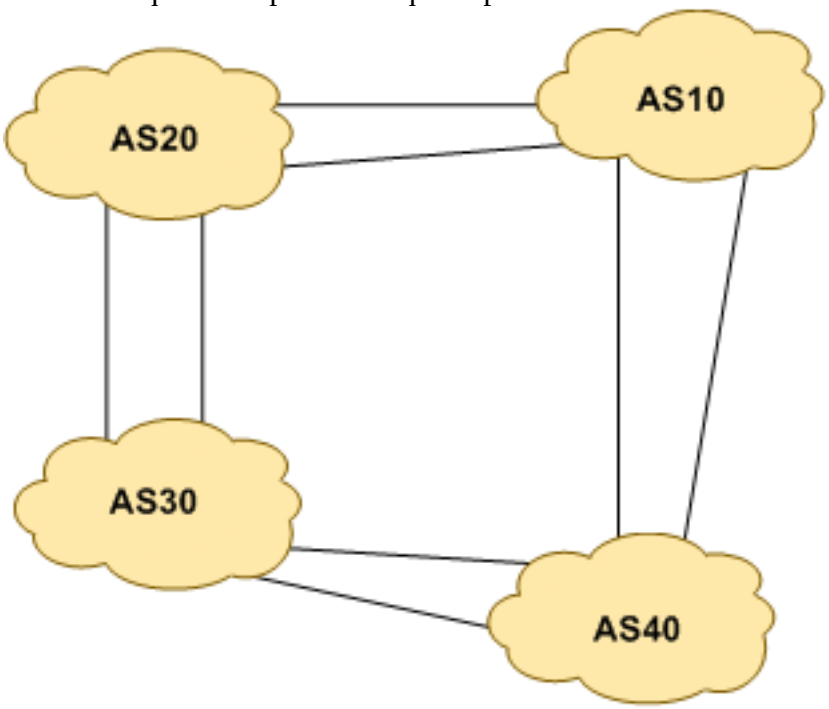

Figure 2 – Relations AS

2. **Reconfigurez BGP et OSPF.**Sur chaque routeur, retirez les processus BGP et OSPF des modules précédents en utilisant les deux commandes suivantes:

```
Router1(config)# no router bgp 10
Router1(config)# no router ospf 41
```

   Ceci effacera la configuration OSPF et BGP prêt pour le module en cours.

3. **Retirez l'adressage IP.** Avant même de penser à configurer les protocoles de routage pour les faire correspondre à la disposition AS précédente, il faut clarifier l'adressage des modules précédents. Dans cette étape, nous enlevons les adresses IP de toutes les interfaces physiques, et

interface de loopback. Cela ramène effectivement le laboratoire à la configuration qu'il avait avant l'étape 10 du module 1. Ne pas oublier d'enlever **tout** l'adressage IP.

4. **Adressage IP.** Comme nous l'avons fait à l'étape 10 du module 1, nous avons besoin de venir avec un plan d'adressage raisonnable et évolutif pour chaque AS dans ce réseau. Chaque AS obtient son propre bloc d'adresse, encore un / 20 (allocation minimale typique d'un ISP démarreur). Ce bloc adresse doit être affecté à des liens et des loopback sur les routeurs qui composent chaque ASN. Les allocations sont les suivantes:

AS10	**10.10.0.0/20**	**AS30**	**10.30.0.0/20**
AS20	**10.20.0.0/20**	**AS40**	**10.40.0.0/20**

Encore une fois, nous devons diviser chaque bloc d'adresse afin que nous ayons l'espace d'adresse du client, l'espace d'adresse d'infrastructure réseau, et un peu d'espace pour les loopback. Figure 3 ci-dessous rappelle comment cela pourrait se faire:

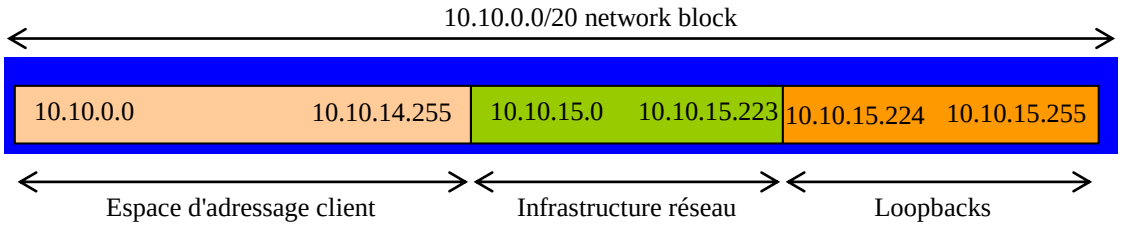

Figure 3 – Diviser le bloc alloué de / 20 en client, Infrastructure et Loopbacks

S'il vous plaît se référer au hand out sur le plan d'adressage qui doit être utilisé pour ce module et la suite - il est intitulé "Addressing Plan – Modules 6 to 9". Comme pour le module 1, configurez les adresses sur chaque interface qui sera utilisée pour ce module, et vérifier la connectivité IP de base avec vos voisins à proximité immédiate.

5. **Adressage de l'interface loopback de routeur.** Nous avons réservé un / 27 pour les loopback, même si chaque AS contient 3 ou 4 routeurs - ceci laisse une place plus que suffisante pour de futures expansions. Les affectations d'adresses loopback qui seront utilisées pour ce module sont:

Router1	**10.10.15.224**	**Router8**	**10.30.15.224**
Router2	**10.10.15.225**	**Router9**	**10.30.15.225**
Router3	**10.10.15.226**	**Router10**	**10.30.15.226**
Router4	**10.20.15.224**	**Router11**	**10.40.15.224**
Router5	**10.20.15.225**	**Router12**	**10.40.15.225**
Router6	**10.20.15.226**	**Router13**	**10.40.15.226**
Router7	**10.20.15.227**	**Router14**	**10.40.15.227**

6. **Configurez OSPF sur les routeurs au sein de chaque AS.** Dans chaque AS configurer le routage OSPF. Cela signifie la mise en place du processus OSPF et la configuration de chaque interface avec le processus OSPF, sans oublier de veiller à ce que l'interface de loopback soit marquée comme passive. Tous les routeurs d'un AS seront dans le même OSPF *zone 0* et utilisent le même ID de processus OSPF. Par exemple, le routeur 1, avec deux interfaces connectées à d'autres routeurs dans leur AS, aurait :

```
Router1 (config)# router ospf 10
Router1 (config-router)# passive-interface default
```

```
Router1 (config-router)# no passive-interface fastethernet 0/0
Router1 (config-router)# no passive-interface serial 1/0
Router1 (config-router)# log-adjacency-changes
!
Router1 (config)# interface fastethernet 0/0
Router1 (config-interface)# ip ospf 10 area 0
!
Router1 (config-interface)# interface fastethernet 0/1
Router1 (config-interface)# ip ospf 10 area 0
!
Router1 (config-interface)# interface serial 1/0
Router1 (config-interface)# ip ospf 10 area 0
!
Router1 (config-interface)# interface loopback 0
Router1 (config-interface)# ip ospf 10 area 0
!
```

Notes:

- *Passive-interface* par défaut fait en sorte qu'OSPF ne tente pas de mettre en place des contiguïtés sur aucune des interfaces en dehors de celles qui sont spécifiées par les commandes *no passive-interface*.
- Le nombre qui suit "*router ospf*" est un ID de processus et est utilisé uniquement dans le routeur (donc il peut être n'importe quel nombre). Mais pour ce laboratoire nous recommandons à ce que l'ID de processus OSPF soit identique avec le nombre AS (qui est la convention utilisée par un certain nombre d'ISP).

7. **OSPF sur les liaisons Ethernet point-à-point.** Une caractéristique mentionnée dans le protocole OSPF pour les présentations ISP est la possibilité de modifier le comportement d'OSPF sur les médias audiovisuels point-à-point, comme Ethernet, quand il y a seulement deux appareils sur ce support. Si nous déclarons une telle situation comme point à point, alors OSPF ne va pas essayer de déterminer un routeur désigné ou de sauvegarde ; de plus, il y aura une amélioration / simplification des calculs SPF et des besoins en mémoire sur le routeur.

   Les équipes routeur qui ont OSPF configuré via une interface Ethernet devraient à présent passer à OSPF mode point à point, par exemple:

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

   Le résultat sera que l'entrée DR ou BDR dans la colonne status de *"show ip ospf neighbor"* va disparaître, pour être remplacée par FULL. Le lien est maintenant traité comme une connexion série point-à-point.

8. **Ping Test.** Vérifiez les routes via OSPF. Assurez-vous que vous pouvez voir tous les réseaux au sein de votre AS. Ping toutes les interfaces de loopback au sein de votre AS. Utilisez les commandes "*show ip ospf neighbor"* et *"show ip route"*. Si vous ne pouvez pas voir les autres routeurs dans votre AS, vous ne serez pas en mesure d'utiliser BGP dans les prochaines étapes.

9. **Enregistrez la configuration.** N'oubliez pas de sauvegarder la configuration dans la NVRAM!

Checkpoint N ° 1 : *appeler l'assistant de laboratoire pour vérifier la connectivité.*

10. **Authentification intra zone - Partie 1.** OSPF prend en charge l'authentification de voisins. Ceci est très important à l'intérieur des réseaux ISP pour empêcher l'introduction de matériel mal configuré ou non voulu.

    Chaque équipe routeur va activer l'authentification. Cette première étape permettra à la région de supporter l'authentification à l'aide de la commande *area N authentication message-digest*. Dès que cela est fait, toutes les adjacences seront appelées à utiliser l'authentification de voisin.

    Un exemple de configuration pour Router6 pourrait être:

    ```
    Router6(config)#router ospf 20
    Router6(config-router)# area 0 authentication message-digest
    ```

    Notez que cela n'affecte pas les adjacences réelles sur les routeurs - ça annonce seulement au routeur que la zone mentionnée utilisera l'authentification, si elle est configurée.

11. **Authentification intra zone - Partie 2**. Maintenant que l'aide à l'authentification dans chaque zone a été configurée, la deuxième étape est en fait de mettre en place le mot de passe d'authentification à utiliser et l'interface sur laquelle il doit être utilisé. Le mot de passe qui doit être utilisé pour toutes les zones dans cet exemple est *cisco*. Le cryptage MD5 devrait être utilisé plutôt que le simple cryptage standard - pour ce faire, utilisez la commande sous-interface *message-digest-key* .

    Un exemple de configuration pour Router6 pourrait être:

    ```
    Router6(config)# interface fastethernet 0/0
    Router6(config-if)# ip ospf message-digest-key 1 md5 cisco
    !
    Router6(config-if)# interface serial 1/1
    Router6(config-if)#  ip ospf message-digest-key 1 md5 cisco
    ```

    Remarquez maintenant que les contiguïtés OSPF n'apparaissent pas à moins que le routeur voisin a également adopté la même la configuration et clé. Remarquez aussi comment les adjacences OSPF ont été réinitialisées quand la configuration a été conclue- la sécurité est mise en place, donc les adjacences sont remises à zéro.

    Note: Le *message-digest-key* permet jusqu'à 255 clés à être définies par interface. Il n'est généralement pas recommandé de définir plus d'une par interface, car le routeur va essayer de communiquer avec ses voisins en les utilisant toutes. Si une clé doit être mise à niveau, la pratique courante consiste alors à définir une seconde clé, ce qui permet un passage gracieux sans compromettre le fonctionnement du réseau. Une fois que tous les routeurs sur le réseau utilisent la nouvelle clé, l'ancienne doit être supprimée.

12. **Contrôle final.** Utilisez les différentes commandes "*show ip ospf*" pour voir l'état d'OSPF du réseau laboratoire maintenant. Vérifiez le routage et la table de routage. S'il vous manque des adjacences, travaillez avec les routeurs voisins dans votre AS pour comprendre pourquoi, et ce qui aurait mal tourné avec l'authentification voisin.

    Remarque: Chaque fois qu'une session de OSPF est configurée à partir de maintenant dans l'atelier, toutes les équipes routeur doivent utiliser des mots de passe sur ces séances OSPF.

Checkpoint N ° 2 : *appeler l'assistant de laboratoire pour vérifier la connectivité.*

13. **Configurez iBGP peering entre des routeurs au sein d'un AS.** Utilisez l'adresse de loopback pour les peerings iBGP. Vous pouvez également configurer la commande de *réseau* pour ajouter le bloc d'adresses attribué à chaque AS pour la publicité dans BGP. Chaque équipe routeur devrait annoncer ce bloc d'adresses depuis ses routeurs.

```
Router1 (config)# router bgp 10
Router1 (config-router)# distance bgp 200 200 200
Router1 (config-router)# no synchronization
Router1 (config-router)# network 10.10.0.0 mask 255.255.240.0
Router1 (config-router)# neighbor 10.10.15.225 remote-as 10
Router1 (config-router)# neighbor 10.10.15.225 update-source loopback 0
Router1 (config-router)# neighbor 10.10.15.225 description iBGP Link to R2
Router1 (config-router)# neighbor 10.10.15.226 remote-as 10
Router1 (config-router)# neighbor 10.10.15.226 update-source loopback 0
Router1 (config-router)# neighbor 10.10.15.226 description iBGP Link to R3
Router1 (config-router)# no auto-summary
Router1 (config-router)# exit
Router1 (config)# ip route 10.10.0.0 255.255.240.0 Null0
```

14. **Tester la connectivité interne BGP.** Utilisez les commandes BGP Show pour assurer que vous recevez les routes de tout le monde de l'intérieur de votre AS.

15. **Configurez des mots de passe sur les sessions iBGP.** Des mots de passe doivent maintenant être configurés sur les sessions iBGP. Revoir la présentation pour comprendre pourquoi cela est nécessaire. Tous les membres d'équipe dans votre AS doivent s'accorder sur ce que le mot de passe doit être pour la session iBGP, et ensuite l'appliquer à tous les peerings iBGP sur votre routeur. Par exemple, sur le peering du Router2 avec le Router3, avec "cisco" utilisé comme mot de passe:

```
Router2 (config)# router bgp 10
Router2 (config-router)# neighbor 10.10.15.226 password cisco
```

IOS réinitialise actuellement la session iBGP entre vous et votre routeur voisin à chaque fois qu'un mot de passe MD5 est ajouté. Donc, lorsque des mots de passe sont ajoutés aux sessions BGP sur des réseaux opérationnels en direct, ce travail devrait être fait au cours d'une période de maintenance lorsque les clients savent qu'il peut y avoir des perturbations de service. Dans le laboratoire de l'atelier, cela n'a pas tant d'importance. (Des versions futures d'IOS éviteront d'avoir cette interruption de service assez grave.)

Observez les journaux du routeur - avec les changements de voisins des sessions BGP étant enregistrés, toute anomalie dans le mot de passe doit être facile à repérer. Un mot de passe manquant d'un côté de la session BGP se traduira par l'émission d'erreurs chez le routeur voisin :

```
%TCP-6-BADAUTH: No MD5 digest from 3.3.3.3:179 to 2.2.2.2:11272
%TCP-6-BADAUTH: No MD5 digest from 3.3.3.3:179 to 2.2.2.2:11272
%TCP-6-BADAUTH: No MD5 digest from 3.3.3.3:179 to 2.2.2.2:11272
```

Alors qu'un décalage (mismatch) dans les mots de passe configurés entraînera ces messages:

```
%TCP-6-BADAUTH: Invalid MD5 digest from 3.3.3.3:11024 to 2.2.2.2:179
%TCP-6-BADAUTH: Invalid MD5 digest from 3.3.3.3:11024 to 2.2.2.2:179
%TCP-6-BADAUTH: Invalid MD5 digest from 3.3.3.3:11024 to 2.2.2.2:179
```

Checkpoint #3: *Appelez l'assistant de laboratoire et montrer le mot de passe comme réglé sur la session iBGP. Une fois confirmé par l'assistant de laboratoire, passez à l'étape suivante.*

16. **Configurez eBGP peering.** Utilisez Figure 1 afin de déterminer les liens entre les AS. L'adressage pour des liens eBGP entre 2 AS va utiliser les adresses des interfaces point-à-point, ***PAS*** les adresses de loopback (revoir la présentation BGP si vous ne comprenez pas pourquoi).

    ```
    Router1 (config)# router bgp 10
    Router1 (config-router)# neighbor 10.10.15.14 remote-as 40
    Router1 (config-router)# neighbor 10.10.15.14 description eBGP to Router13
    ```

    Utilisez les commandes BGP Show pour vous assurer d'envoyer et de recevoir les annonces BGP de vos voisins eBGP.

    Q. Pourquoi les interfaces de loopback ne peuvent être utilisées pour les peerings eBGP?

    A. L'adresse IP de l'interface loopback d'un routeur n'est pas connue des pairs BGP externes, donc les pairs externes n'auront aucun moyen de savoir comment communiquer entre eux pour établir le peering.

    Q. Quelle commande BGP Show vous permet de voir l'état de la connexion BGP à votre pair?

    A. Essayez *show ip bgp neighbor x.x.x.x* – ceci donnera des informations détaillées sur l'état de votre pair. Il y a des sous-commandes de celui-ci, donnant plus d'informations sur le peering.

    Q. Quelle commande BGP Show vous permet de voir exactement quels réseaux vous annoncez et recevez de vos pairs eBGP?

    A. Essayez *show ip bgp neighbor x.x.x.x received-route* – Cela montrera quelles routes vous recevez de votre pair. De même, remplacer *received-route* par *advertised-routes* donnera la liste des réseaux qui sont annoncés à votre pair. (Notez qu'en terme de pratique opérationnelle générale des ISP, il y a des mises en garde ici - si vous appliquez des route-maps et certaines politiques BGP, ceux-ci ne seront pas traités par la commande *advertised-routes*. Utilisez la sous-commande *advertised-routes* avec prudence.)

17. **Configurez des mots de passe sur les sessions eBGP.** Les mots de passe doivent maintenant être configurés sur les sessions eBGP entre votre AS et ceux qui vous avoisinent. Accordez vous avec votre AS voisin sur le mot de passe qui doit être utilisé sur la session eBGP, puis l'appliquer au peering eBGP. Par exemple, sur le peering du Router2 avec le Router4, avec "cisco" utilisé comme mot de passe:

    ```
    Router2 (config)# router bgp 10
    Router2 (config-router)# neighbor 10.10.15.10 password cisco
    ```

Comme précédemment pour la session iBGP, regarder les journaux pour des incohérences de mot de passe, ou pour des mots de passe manquants. Comme pour les sessions iBGP auparavant, vous verrez que le routeur réinitialisera la session eBGP dès que le mot de passe est appliqué.

Remarque:À chaque fois qu'une session BGP (iBGP ou eBGP) est configurée à partir de maintenant dans l'atelier, toutes les équipes routeur doivent utiliser des mots de passe sur ces sessions BGP.

Checkpoint #4: *Appelez l'assistant de laboratoire et montrer le mot de passe comme réglé sur la session eBGP. Une fois confirmé par l'assistant de laboratoire, passez à l'étape suivante.*

18. **Ajout d'une route "client" dans BGP.** Comme nous l'avons fait dans le module 1, nous allons maintenant ajouter une route "client" dans BGP sur chaque routeur. Nous n'avons pas de «clients» en tant que tels connectés à nos routeurs dans le laboratoire, donc nous allons simuler la connectivité en utilisant simplement une interface Null0. L'espace adresse "client" que chaque équipe routeur va introduire dans iBGP figure dans la liste ci-dessous - encore une fois, chacun d'entre nous utilisera un /26, par souci de simplicité.

R1	**10.10.0.0/26**	**R8**	**10.30.0.0/26**
R2	**10.10.0.64/26**	**R9**	**10.30.0.64/26**
R3	**10.10.0.128/26**	**R10**	**10.30.0.128/26**
R4	**10.20.0.0/26**	**R11**	**10.40.0.0/26**
R5	**10.20.0.64/26**	**R12**	**10.40.0.64/26**
R6	**10.20.0.128/26**	**R13**	**10.40.0.128/26**
R7	**10.20.0.192/26**	**R14**	**10.40.0.192/26**

Chaque équipe doit maintenant mettre en place une route statique pointant vers l'interface **Null0** pour le / 26 dont elle est à l'origine. Une fois que la statique est mise en place, l'équipe doit ensuite ajouter une entrée dans la table BGP. Voici un exemple pour Router8:

```
Router8 (config)# ip route 10.30.0.0 255.255.255.192 Null0
Router8 (config)# router bgp 30
Router8 (config-router)# network 10.30.0.0 mask 255.255.255.192
```

19. **Vérifiez le tableau BGP.** Y a t-il des routes vues par ***show ip bgp***? Si non, pourquoi pas? Une fois que toutes les équipes de la classe ont terminé leur configuration, chaque équipe doit voir l'agrégat ainsi que les quatorze / 26s introduit dans l'étape précédente. Si ce n'est pas le cas, travaillez avec vos voisins pour résoudre le problème.

Checkpoint N ° 5 : *appeler l'assistant de laboratoire pour vérifier la connectivité. Utilisez les commandes telles que "show ip route sum", "show ip bgp sum", "show ip bgp", "show ip route", and "show ip bgp neigh x.x.x.x route | advertise". Devrait y avoir 4 préfixes agrégés (un pour chaque ISP) et les 14 clients /26 dans la table BGP.*

20. **L'importance de l'agrégation.** Chaque AS a été attribué un bloc adresse /20. Il est prévu par tous les opérateurs Internet que tout espace d'adresse qu'un ISP utilise est agrégé autant que possible avant d'être annoncé au reste de l'Internet. Subdiviser l'espace d'adressage à l'intérieur d'un AS est parfaitement acceptable et évidemment très fréquent (comme nous l'avons fait ici) - mais la plupart

des opérateurs estiment que les fuites de cet espace d'adressage subdivisé à l'Internet en général comme un comportement antisocial et antipathique.

Q. Comment pouvez-vous agréger automatiquement via BGP de petits blocs d'adresses de votre réseau en un bloc d'adresse plus grand en dehors de votre réseau? ***Astuce:*** *Revoir la documentation BGP.*

A. La commande "aggregate-address" est souvent utilisée pour atteindre cet objectif.

Nous ne faisons aucun filtrage ou limitation des annonces des blocs adresse "client" que nous avons introduis dans chaque ASN. Ce sera l'un des objectifs des modules suivants de l'atelier.

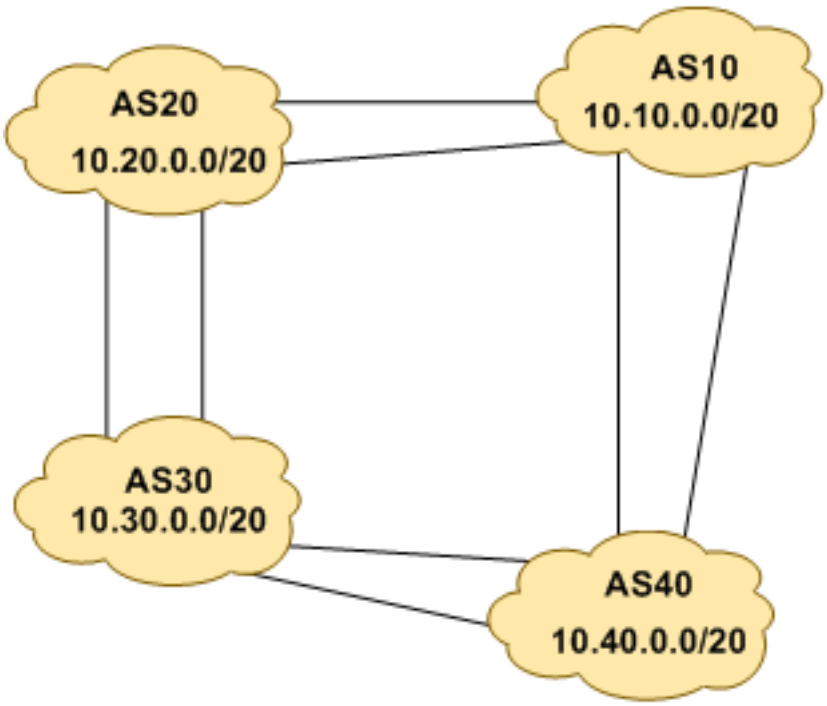

Figure 4 – Agrégats pour chaque ASN

21. **Activité de mise à jour BGP (en option).** Utilisez *debug ip bgp update* pour voir les activités de mise à jour BGP après avoir nettoyé une session BGP. Pour arrêter le fonctionnement de débogage, faites *undebug ip bgp update.*

    Attention: ce n'est pas une bonne idée d'exécuter cette commande de débogage sur un routeur qui reçoit la table de routage Internet complète; utiliser cette commande dans un réseau de laboratoire comme celui-ci pourrait vous montrer pourquoi!

Questions de révision

1. Combien de *types d'origine* existent dans BGP?

2. Énumérer les types d'origine. **Indication:** Revoir les présentations BGP.

3. Comment sont-ils utilisés?

4. Pourquoi les mots de passe sont nécessaires à la fois sur les sessions iBGP et eBGP? De quoi protègent-ils?

5. Pourquoi l’agrégation est importante pour l'Internet?