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

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

Prérequis: Module 1 (ISIS)

Topologie :

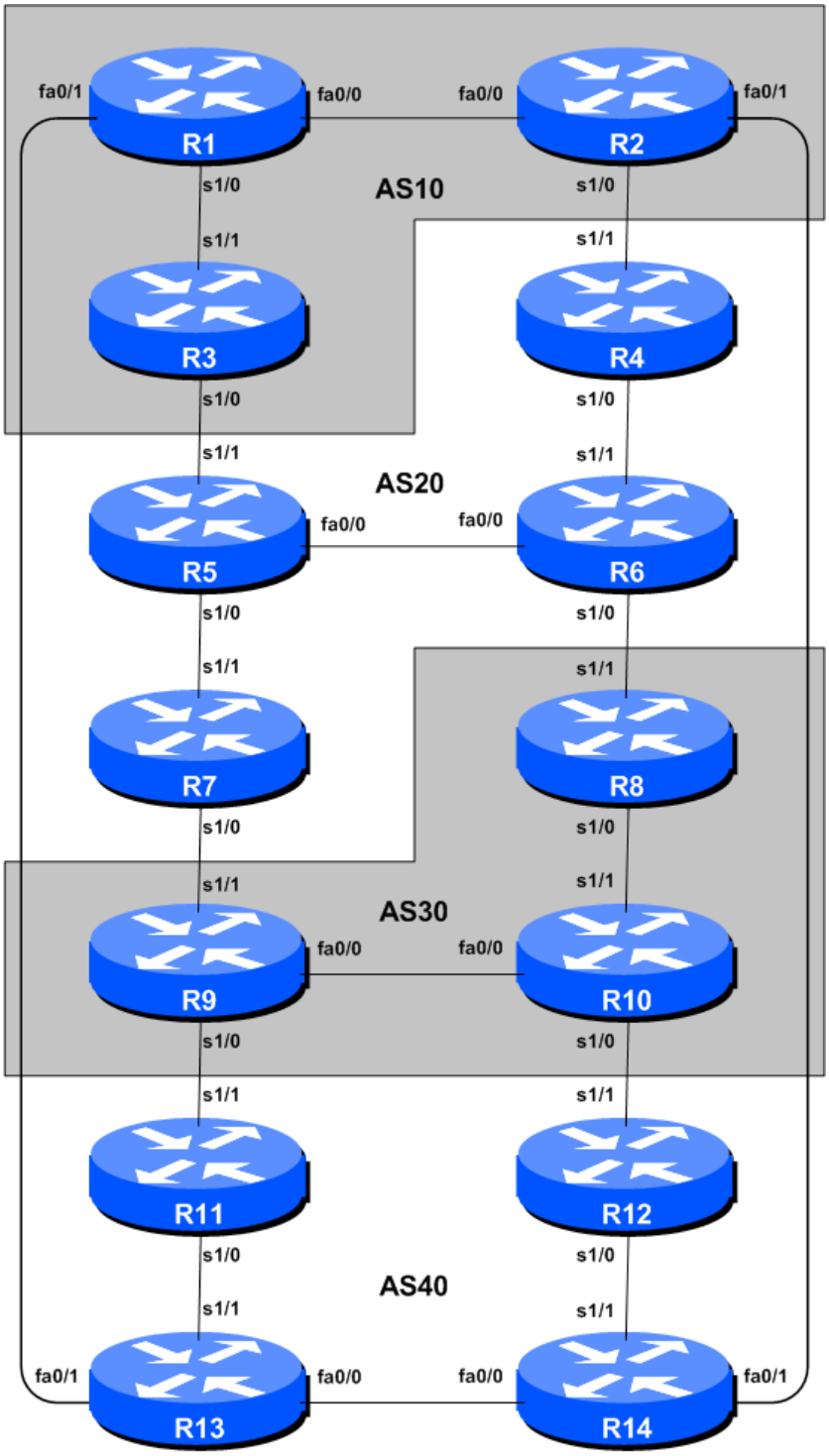

Figure 1 – BGP AS Numbers

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 illustrée à 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.

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.

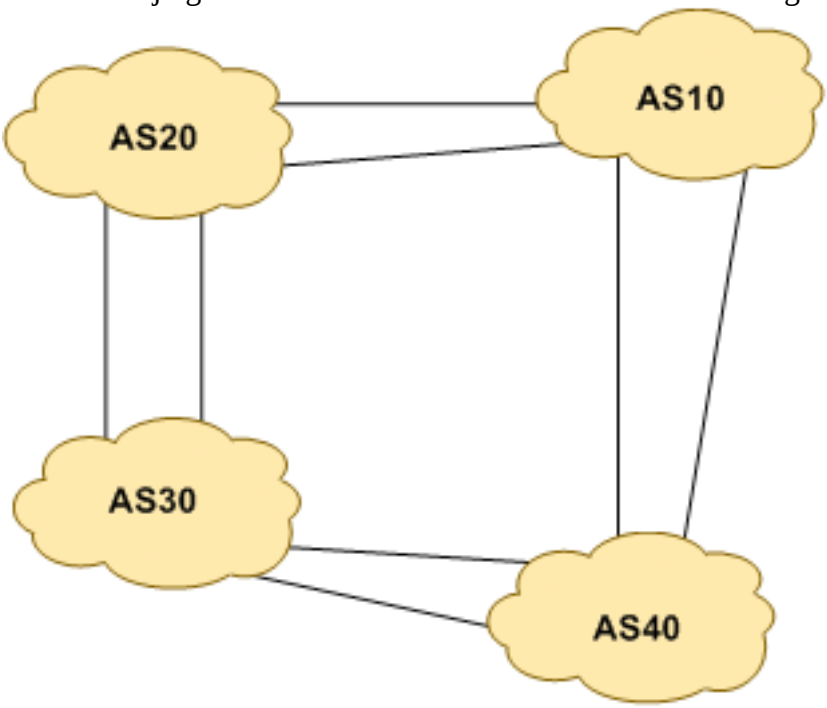

Figure 2 – AS relationship

2. **Supprimez l'adressage IP.** 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 IP 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 IP.

(L'alternative est de simplement supprimer toute la configuration du routeur avec la commande `write erase` et ensuite de faire un *reload* du routeur. Apres le reload, recommencer toute la configuration des points 1 à 9 du Module 1.)

3. **Re-configurez BGP et ISIS.** Sur cahque routeur, supprimez les process BGP et ISIS du Module 1 à l'aide des 2 commandes suivantes:

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

```
Router1 (config)# no router isis workshop
```

Ceci enlève la configuration BGP et ISIS afin de redémarrer proprement pour le module courant.

4. **Adressage IP.** Comme pour l'étape 10 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 / 20 (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	**10.10.0.0/20**	**AS30**	**10.30.0.0/20**
AS20	**10.20.0.0/20**	**AS40**	**10.40.0.0/20**

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. Figure 3 ci-dessous nous rappelle comment ceci peut être fait :

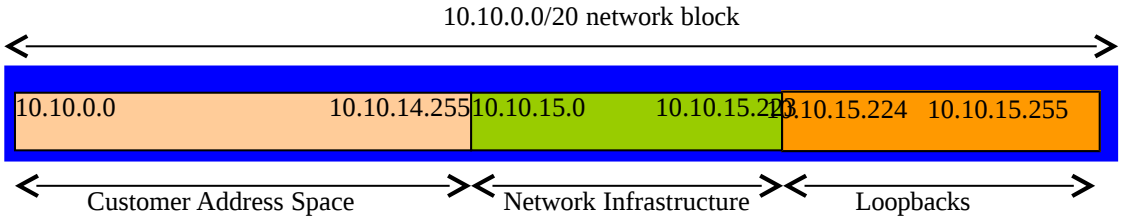

Figure 3 – Dividing allocated block of /20 into Customer, Infrastructure and Loopbacks

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.

5. **Adresses pour les interfaces loopback des routeurs.** Nous avons réservé un /27 pour les loopbacks même si leur AS ont seulement 3 ou 4 routeurs – ceci laisse suffisament d'espace poru des expansions futures. Les adresses attribuées aux loopbacks pour ce module sont les suivantes:

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 ISIS sur les routeurs de chaque AS.** Dans chaque AS, configurez ISIS. Cela signifie que chaque équipe *router ISIS* avec comme ISIS ID *asY* sur son routeur, où *Y* est le numéro d'AS. Les liens **internes** a l'AS vers chaque routeur de l'AS doivent être configurés avec *ip router ISIS asY*. L'adresse NET est *49.0001.x.x.x.00*, où *x.x.x* est construit a partir de l'adresse loopback (voir Module 1 pour plus de détails).

ISIS est configuré **uniquement** sure 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 *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).

Par exemple, Router 1, qui a deux interfaces dans AS 10, est configuré comme suit :

```
Router1 (config)# router isis as10
Router1 (config-router)# net 49.0001.0100.1001.5224.00
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)# set-overload-bit on-startup wait-for-bgp
!
Router1 (config)# interface fastethernet 0/0
Router1 (config-if)# ip router isis as10
Router1 (config-if)# isis metric 2 level-2
Router1 (config-if)# isis circuit-type level-2-only
!
Router1 (config)# interface serial 1/0
Router1 (config-if)# ip router isis as10
Router1 (config-if)# isis metric 20 level-2
Router1 (config-if)# isis circuit-type level-2-only
```

Note:

- 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*).

7. **Interfaces passives en ISIS.** Marquez maintenant les interfaces sur lesquelles vous ne voulez pas ISIS comme interfaces *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. Dans ce laboratoire, nous marquons les interfaces loopback comme passive. 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 (comme fait au point 6). Voici un exemple pour Router1:

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

Quelques règles concernant les interfaces:

1. "`ip router isis`" sur une interface signifie qu'une adjacence CLNS est requise et que le sous-réseau IP de cette interface est injecté dans ISIS.
2. "`passive interface`" dans la configuration ISIS d'une interface signifie que l'on ne veut pas d'une adjacence CLNS mais que le sous-réseau IP de l'interface est injecté dans ISIS.
3. Pas de configuration ISIS pour une interface signifie qu'il n'y a pas d'adjacence CLNS requise et que le sous-réseau IP de l'interface ne sera pas annoncé par ISIS.

Note: Par défaut, ISIS établi des adjacences et annonce les prefixes des interfaces activées à l'aide de la commande "`ip 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).

8. **ISIS sur des liens Ethernet Point-a-Point.** Une des caractéristiques mentionnées lors de la présentation ISIS est l'option de pouvoir modifier le comportement ISIS pour les liens point-à-

point sur un media broadcast, tel qu'Ethernet, lorsqu'il n'y a que deux appareils sur le media. Si l'on déclare la situation comme étant point à point, ISIS n'essaye pas de déterminer quel est le routeur désigné. Ceci conduit a une simplification lors des calculs SPF (Shortest Path First) et une amélioration des besoins en terme de mémoire sur le routeur.

Les équipes qui ont configure ISIS sur leur interfaces Ethernet **internes** vont maintenant convertir ISIS vers le mode point-à-point mode, 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. Notez qu'il n'est pas nécessaire de configurer le point-à-point mode pour les interfaces Ethernet sur lesquelles ISIS ne tourne pas.

9. **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"*.

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

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

11. **Activation de l'authentification pour les voisins ISIS – Partie 1.** ISIS supporte l'authentification des voisins; ceci est considéré comme étant de plus en plus important pour un réseau d'ISP. Alors que les attaques visant leur infrastructure augmentent, les ISPs ont recours à tous les outils disponibles pour sécuriser leurs réseaux. (Malgré le fait qu'il est plus difficile d'attaque ISIS qui tourne au dessus de la couche 2 (link layer) au lieu de d'au dessus d'IP comme OSPF, certains operateurs d'ISPs sont prudents et implémentent « neighbour authentication ».)

    Chaque équipe active maintenant *neighbour authentication* pour ISIS. La première étape est d'établir une keychain – nous utilisons la clé "cisco" pour ce laboratoire:

```
Router1(config)# key chain lab-key
Router1(config-keychain)# key 1
Router1(config-keychain-key)# key-string cisco
```

12. **Activation de l'authentification pour les voisins ISIS – Partie 2.** Maintenant que la *keychain* est définie, nous activons le support d'authentification sur toutes les interfaces du routeurs. La première étape est d'activer MD5 pour level-2 IS's:

```
Router1(config)# interface fastethernet 0/0
Router1(config-if)# isis authentication mode md5 level-2
```

    Ensuite nous associons la key-chain définie précédemment à l'authentification que nous venons de configurer :

```
Router1(config)# interface fastethernet 0/0
Router1(config-if)# isis authentication key-chain lab-key level-2
```

    Notez maintenant que les adjacences ISIS ne s'établissent pas à moins que le routeur voisin n'ai également entré la même configuration et la même clé. Remarquez également comme les adjacences

sont réinitialisées lorsque la configuration est saisie – Nous avons introduit de la sécurité, ce qui redémarre les adjacences.

13. **Vérification finale.** Utilisez les différentes commandes "*show isis*" pour voir le statut actuel d'ISIS dans le réseau. Vérifiez le routage et la table de routage. Assurez vous que toutes les adjacences sont de nouveau établies. Si une adjacence n'a pas su se rétablir et vous observez le message suivant plusieurs fois dans le log :

    ```
    *Mar  1 00:05:17.825: %CLNS-4-AUTH_FAIL: ISIS: LAN IIH authentication failed
    ```

    vous pouvez raisonnablement supposer que soit vous sont votre voisin avez oublié de configurer l'authentification sur votre interface avec le voisin.

    Note: A partir de maintenant, lorsqu'une session ISIS est configurée, toutes les équipes DOIVENT utiliser un mot de passe sur ces sessions ISIS.

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

14. **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.

    ```
    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 next-hop-self
    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 next-hop-self
    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
    ```

15. **Configuration de Next-hop-self.** Au point précédent nous avons introduit la commande next-hop-self. Comme vu lors de la présentation BGP, la configuration de next-hop-self fait que le routeur parlant en iBGP utilise comme next-hop l'adresse source de la session iBGP (dans ce cas la loopback) plutôt que l'adresse du next-hop externe (comme mentionné dans la spécification BGP). Ceci est une bonne pratique appliquée par les ISPs. Cela signifie qu'un ISP n'a pas besoin d'annoncer les IPs des next-hop (NH) externes dans son IGP.

16. **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.

17. **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 :

```
Router2 (config)# router bgp 10
Router2 (config-router)# neighbor 10.10.15.226 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. Un mot de passe manquant d’un côté d’une session BGP donne l’erreur suivante sur 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 mot de passe incohérent résulte en le message suivant :

```
%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’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.*

18. **Configuration des peerings eBGP.** Réferez-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).

```
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 `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 ip bgp 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 ip 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.)

19. **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:

```
Router2 (config)# router bgp 10
Router2 (config-router)# neighbor 10.10.15.10 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.*

20. **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 /26 pour plus 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 installe une route statique pointant vers l'interface **NULL0** pour le /26 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:

```
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
```

21. **Vérification de la table 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 de chaque AS, ainsi que les quatorze / 26s 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 ip route sum", "show ip bgp sum", "show ip bgp", "show ip route", et "show ip bgp neigh x.x.x.x route | advertise". Il doit y avoir 4 préfixes agrégés (un pour chaque ISP) et 14 prefixes clients, des /26's, dans la table BGP.*

22. **Importance d'agréger.** Chaque a reçu un bloc /20 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.

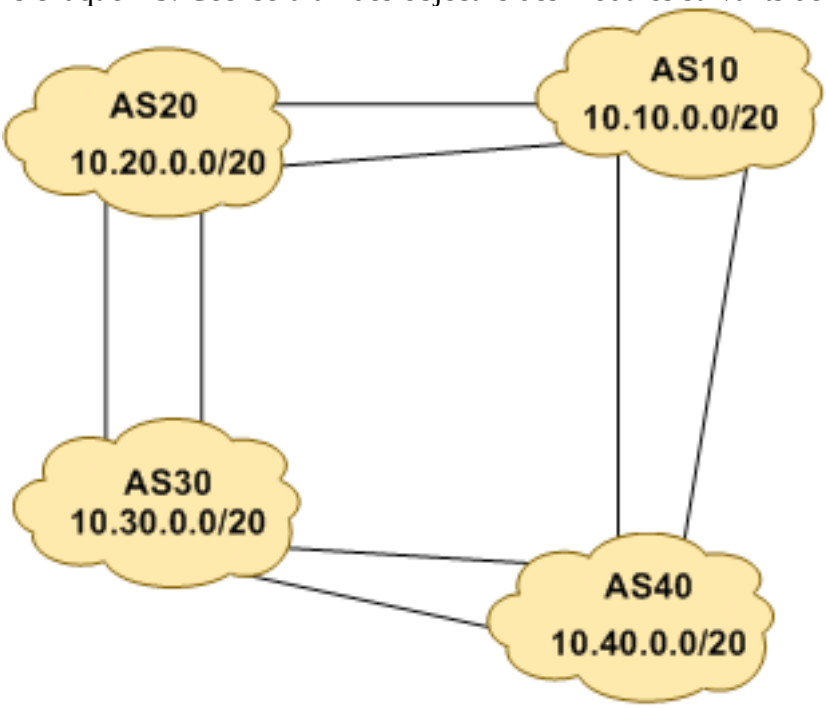

Figure 4 – Agrégats pour chaque ASN

23. **Quantité d'updates BGP (Optionnel).** Utilisez la commande *debug ip bgp update* pour voir l'activité en termes de messages BGP apres un « clear » de session BGP session. Pour arrêter le debug, faites *undebug ip bgp update.*

Avertissement: Ce n’est pas une bonne idée de lancer cette commande de debug sur un routeur recevant la table complète de l’Internet. En la testant dans notre reseau de laboratoire vous verrez certainement pourquoi c’est le cas.

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?