Exercice BGP n°1 – mise en œuvre de sessions eBGP

Etape1

Nous allons mettre en œuvre des sessions eBGP entre chaque routeur de la salle et le routeur en face de vous.

- table 1 : AS 100
- table 2 : AS 200
- table 3 : AS 300
- table 4 : AS 400

- Backbone AS 1

Liaison série

196.200.221.128/26

Table1	196.200.221.128/30
Table2	196.200.221.132/30
Table3	196.200.221.136/30
Table4	196.200.221.140/30
Table5	196.200.221.144/30
Table6	196.200.221.148/30

Le mode opératoire de l'exercice est le suivant :

1. Remettez votre Cisco dans sa configuration de départ : « nvram erase » puis « reload ».

2. Configurez à nouveau la liaison Ethernet entre votre PC et votre Cisco, mettez les mots de passe pour vous y connecter.

3. Configurez la liaison Ethernet entre votre routeur et le backbone

4. Vérifier le câblage

5. Configurer la liaison série entre votre routeur et le routeur de la table en face de vous avec le port série (le 1er port série s 0/0) et le routeur de la table en face.

- Table 1: 196.200.221.129/30 – .130 pour Table 4
- Table 3: 196.200.221.137/30 – .138 pour Table 6

6. Vous allez établir une session BGP avec votre voisin.

7. Configurez BGP sur votre routeur afin d'ouvrir une session avec le routeur de votre voisin.

```
R# config t
Enter configuration commands, one per line.  End with CNTL/Z.
R(config)# ip bgp-community new-format
R(config)# router bgp 100                          // Utiliser votre numéro d'AS
R(config-router)# network 196.200.221.192 mask 255.255.255.248   // votre réseau IP
R(config-router)# no synchronisation
R(config-router)# no auto-summary
```

Le protocole BGP est maintenant configuré mais votre routeur ne parle à aucun routeur

8. Déclarer vos voisins.

R(config-router)# neighbor 196.200.221.xxx remote-as 400 (adresse et AS de votre pair)
R(config-router)# neighbor 196.200.221.xxxx description Table4 (description de votre pair)

XXX est l'adresse de l'interface série de votre voisin.

Vérifiez si votre session BGP est UP

R#show ip bgp summary

Options BGP

Cette commande demande au routeur de placer les passerelles pour toutes les routes supplémentaires à la table de routage à lui-même. Toujours mettre ceci lorsque vous faites du peering avec d'autres systèmes autonomes.

neighbor 196.200.221.xxx next-hop-self

Demander au routeur d'enregistrer les mises à jour reçues. Ceci nous permet de mettre à jour une session BGP sans devoir redémarrer la session. (Ceci utilise de la mémoire supplémentaire.

Dans l'IOS 12.0 ou plus, vous pouvez obtenir un effet semblable sans employer la mémoire supplémentaire, avec la possibilité BGP de rafraîchissement des routes.
Utiliser "show ip bgp neighbour x.x.x.x » pour vérifier si votre pair soutient ces possibilités.)

neighbor 196.200.221.xxx soft-reconfiguration inbound

9. Vérifier si vous envoyez des routes à votre voisin.

R#sh ip bgp neighbor x.x.x.x advertised-routes (nécessite soft-reconfiguration inbound)

10. Vérifier si vous recevez des routes de votre voisin.

R#show ip bgp

Quelles routes recevez vous?

Autres commandes

R#sh ip route
R#sh ip bgp
R#sh ip bgp neighbor
R#sh ip bgp neighbor x.x.x.x routes

Manipulez la table BGP et la table de routage de votre équipement. Que constatez-vous ? Utilisez les commandes « sh ip bgp », « sh ip route », « sh ip bgp sum ».

Toutes les tables doivent faire cette manipulation de façon simultanée (avant de passer à l'étape suivante de l'exercice).

11. Tests.

Faire un ping vers le PC de vos voisins.
Que constatez vous ?

Etape 2

12. Annoncez (par erreur, mais volontairement) un « /30 » extrait du réseau de votre voisin.
Comment ce réseau est-il routé depuis les autres tables ? Comment votre voisin reçoit-il ce réseau ?

Quelle sécurité pouvez-vous mettre en œuvre pour éviter d'apprendre vos propres réseaux en provenance de l'Internet ?

Mettez en œuvre le filtre adéquat, redémarrez les sessions BGP et constatez le progrès.

13. Définissez des filtres pour lister ce que vous envoyez et ce que vous allez accepter

```
R(config)# ip prefix-list mes-routes description Mes routes dehors
R(config)# ip prefix-list mes-routes  seq 10 permit 196.200.221.192/29
R(config)# ip prefix-list mes-routes seq 20 deny   0.0.0.0/0 le 32
```

Vérifier que vos mes-routes contient les routes que vous annoncez.

14. Définissez des filtres pour lister ce que vous voulez recevoir de vos pairs

```
R(config)# ip prefix-list peer-ASxxx  desscription Routes de ASxxx
R(config)# ip prefix-list peer-ASxxx seq 10 permit 196.200.221.216/29
R(config)# ip prefix-list peer-ASxxx seq 20 deny   0.0.0.0/0 le 32
```

15. Appliquez les filtres sur les sessions avec votre PAIR

```
R(config-router)#neighbor 196.200.221.xxx prefix-list mes-routes out
R(config-router)#neighbor 196.200.221.xxx prefix-list peer-ASxxx in
```

16. Pour implémenter la nouvelle politique redémarrer les sessions BGP.

```
clear ip bgp 100 in      ! Applique la nouvelle politique en outbound sur AS100
clear ip bgp 100 out    ! Applique la nouvelle politique en entrée sur  AS100
```

17. Vérifier vos sessions BGP

18. Reprendre les prefix-list mais en refusant de recevoir du trafic de vos pairs.

19. Comment devez vous procéder ?

Fin de l'exercice BGP n°1.

Exercice BGP n°2 – mise en œuvre d'un « multi-homing »

Pour terminer les exercices BGP nous allons mettre en œuvre une 2ème connexion avec le BACKBONE
Cette seconde session sera mise en place via les interfaces e0/0

Le mode opératoire de l'exercice est le suivant :

1. *vous mettez en place une session BGP avec le BACKBONE.*

   R(config-router)# neighbor 196.200.221.125 remote-as 1 (adresse et AS du backbone)
   R(config-router)# neighbor 196.200.221.125 description Backbone (description de votre pair)

2. *Prenez contact avec l'administrateur du routeur « backbone » pour qu'il configure à son tour la session BGP avec votre routeur.*

3. *Vérifiez vos tables de routages et vos informations BGP*

4. *Interpréter*

5. *Pouvez vous aller sur Internet ? pourquoi*

6. *L'Administrateur du Backbone va vous annoncer son /23*

7. *Vérifiez vos tables de routage*

8. *Pouvez vous allez sur Internet ?*

9. *L'administrateur du Backbone vous envois la route par default*

10. R(config-router)# neighbor 196.200.221.67 default-originate
    neighbor 196.200.221.68 default-originate
    neighbor 196.200.221.69 default-originate
    neighbor 196.200.221.70 default-originate

11. *Vérifiez vous session BGP*

12. *Pouvez vous aller sur Internet ?*

13. *Nous allons maintenant simuler différentes pannes. Vérifiez que votre connexion fonctionne toujours. Quels sont les changements dans les tables de routage ? Est-ce que la connexion fonctionne encore ?*

Exercice BGP n°3 FILTRAGE DES ANNONCES

Nous sommes maintenant dans le cas ou vous causez BGP avec votre fournisseur
Et que vous avez une relation de Peer avec un autre ISP dans votre pays.

Cependant vous n'avez pas de filtre ce qui vous amène a servir de transit Pour l'autre ISP

14. Cet exercice utilise les filtres AS Path sur les sessions. Ceci va assurer que seuls nos préfixes sont annonces A nos voisins.

Créer un filtre AS PATH qui ne permet que les préfixes originés par votre peer AS a entrer dans votre réseau.

```
Rconfig)#ip as-path access-list 1 permit ^asnum$
                        ! permit prefixes origins par asnum
```

15. Activer soft reconfiguration pour la session BGP. Ceci vous permet d'analyser les effets du filtre. N'utiliser cette commande que pour faire du debug.

```
R(config)#router bgp 100
R(config-router)#neighbor 196.200.221.xx soft-reconfiguration in
```

16. Appliquer le filtre sur la session avec votre peer,

```
R(config)# ip as-path access-list 1 permit ^asnum$          // asnum
R(config-router)#neighbor 196.200.220.xx filter-list 1 in
                        ! applique  as-path filter 1 en inbound
```

17. Maintenant que le filtre est actif redémarrer la session en utilisant l'option route refresh de BGP
Appliquer le filtre sur la session avec votre peer,

```
R#clear ip bgp 400 in        ! router refresh sur la session avec AS400
```