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
- etc....

- Backbone AS 1

Le mode opératoire de l'exercice est le suivant :

1. Remettez votre routeur dans sa configuration de départ : supprimer les configurations de routage précédentes(OSPF et IBGP)

2. Désactiver votre connexion vers le backbone

```
int fast0/0
shutdown
```

3. Vous allez établir une session BGP(ebgp) avec votre voisin en utilisant les liens série.

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

```
R# config t
R(config)# router bgp 100                          // Utiliser votre numéro d'AS
 R(config-router)# no synchronisation
 R(config-router)# no auto-summary
 R(config-router)# no bgp default ipv4-unicast

 R(config-router)# address-family ipv4
 R(config-router-af)# neighbor  196.200.221.X remote-as 400 (adresse et AS de votre pair)
R(config-router-af)# neighbor  196.200.221.x description  Table4
 R(config-router-af)# neighbor 196.200.221.x  activate
 R(config-router-af)# network 196.200.221.y/29
 R(config-router-af)#  exit-address-family

 R(config-router)# address-family ipv6
 R(config-router)# neighbor 2001: 4348:221:2xx::y remote-as 400 (serial)
R(config-router)# neighbor  2001:4348:221:2xx::y description V6  Table4
 R(config-router-af)# neighbor 2001:4348:221:2xx::y  activate
 R(config-router-af)# network 2001:4348:221:z::/56 (bloc par table)
 R(config-router-af)#  exit-address-family
```

Verifier que votre session est UP

R#show bgp ipv4 unicast summary

R#show bgp ipv6 unicast 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.x next-hop-self

neighbor 2001: 4348:221:2xx::y 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(route refresh) 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 supporte cette possibilité.)

neighbor 196.200.221.x soft-reconfiguration inbound

neighbor 2001: 4348:221:2xx::y soft-reconfiguration inbound

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

R#sh bgp ipv4 unicast neighbor x.x.x.x advertised-routes

R#sh bgp ipv6 unicast neighbor X:X:X:X:X:X:X:X advertised-routes

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

R##sh bgp ipv4 unicast neighbors X.X.X.X received-routes

R##sh bgp ipv6 unicast neighbors Y:Y:Y:Y:Y:Y:Y:Y received-routes

Quelles routes recevez vous?

Autres commandes

R#sh bgp ipv4 unicast neighbor X.X.X.X routes

R#sh ipv6 bgp neighbor Y:Y:Y:Y:Y:Y::Y routes

Manipulez la table BGP et la table de routage de votre équipement. Que constatez-vous ?

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

7. Tests.

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

Etape 2

8. Annoncez (par erreur, mais volontairement) un « /30 » et « /64 » 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 vos peers ?

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

9. 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.y/29
R(config)# ip prefix-list mes-routes seq 20 deny   0.0.0.0/0 le 32


R(config)# ipv6 prefix-list mes-routes description Mes routes dehors
R(config)# ipv6 prefix-list mes-routes  seq 10 permit 2001:4348:221:z::/56
R(config)# ipv6 prefix-list mes-routes seq 20 deny   ::/0 le 128
```

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

10. 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.y/29 (le /29 du voisin)
R(config)# ip prefix-list peer-ASxxx seq 20 deny   0.0.0.0/0 le 32


R(config)# ipv6 prefix-list peer-ASxxx  desscription Routes de ASxxx
R(config)# ipv6 prefix-list peer-ASxxx seq 10 permit 2001:4348:221:z::/56 (le /56 du voisin)
R(config)# ipv6 prefix-list peer-ASxxx seq 20 deny   ::/0 le 128
```

11. Appliquez les filtres sur les sessions avec votre PAIR

```
R(config-router-af)#neighbor 196.200.221.x  prefix-list peer-ASxxx in

R(config-router-af)#neighbor 2001: 4348:221:2xx::y  prefix-list peer-ASxxx in
```

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

```
clear bgp all ASvoisin in      ! Applique la nouvelle politique en entree
```

13. Vérifier vos sessions BGP
vos sous préfixes(/30 et /64) announcés par votre voisin sont-ils encore dans la table BGP ?

Ils sont toujours pourtant réçus

show bgp all neighbor (X.X.X.X.X) ou (Y:Y:Y:Y:Y:Y:Y:Y) received-routes

14. Appliquer le prefix-list mes-routes defini plus haut en sortie pour filtrer ce que vous annouvez à votre voisin

Comment devez vous procéder ?

15. Qu'annouvez-vous à votre voisin que recevez-vous maintenant de votre voisin ?

show bgp all neighbor (X.X.X.X.X) ou (Y:Y:Y:Y:Y:Y:Y:Y) advertised-routes
show bgp all neighbor (X.X.X.X.X) ou (Y:Y:Y:Y:Y:Y:Y:Y) advertised-routes

16. Reprendre les prefix-list mais en refusant tous préfixes de vos pairs.

17. 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

Le mode opératoire de l'exercice est le suivant :

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

   R(config-router)# neighbor 196.200.221.126 remote-as 1 (adresse et AS du backbone)
   R(config-router)# neighbor 196.200.221.126 description Backbone

   R(config-router)# neighbor 2001:4348:221::126 remote-as 1 (adresse et AS du backbone)
   R(config-router)# neighbor 2001:4348:221:126 description Backbone

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. L'Administrateur du Backbone va vous annoncer son /24 et son /64

6. Vérifiez vos tables de routage

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

8. R(config-router-af)# neighbor 196.200.221.Y default-originate

9. R(config-router-af)# neighbor 2001:4348:221::Z default-originate

10. Vérifiez vous session BGP

11. Pouvez vous aller sur les réseaux annoncés par le backbone ?

12. 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

13. 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 à entrer dans votre réseau.

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

14. 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-af)#neighbor 196.200.221.x soft-reconfiguration in

R(config)#router bgp 100
R(config-router-af)#neighbor 2001:4348:221::z soft-reconfiguration in
```

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

```
R(config-router-af)#neighbor 196.200.221.x  filter-list 1 in
                        ! applique  as-path filter 1 en inbound

R(config-router-af)#neighbor 2001:4348:221::z  filter-list 1 in
                        ! applique  as-path filter 1 en inbound
```

16. 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 bgp all 400 in        ! router refresh sur la session avec AS400
```

17. Verifier votre table de routage. Avec cette configuration, votre peer pourra-t-il vous utiliser du transit ?

18. Donner à la priorité à la liaison vers le peer pour être sûr de toujours utiliser le lien local vers votre voison

```
Rconfig)#route-map IXP-IN permit 10
 set local-preference 120
```

19. Appliquer le route map en entrée avec un clear sur la session.

```
R(config-router-af)#neighbor 196.200.221.x  route-map IXP-IN in

R(config-router-af)#neighbor 2001:4348:221::z  route-map IXP-IN in
```