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

Nous allons mettre en œuvre des sessions eBGP entre chaque routeur de la salle et le routeur « backbone » étant raccordé à l'Internet. Nous utilisons pour cela les raccordement par port série :

- table 1 : AS 1 vers Serial0/1 sur f2-rtr-b (AS 17) ;
- table 2 : AS 2 vers Serial0/2 sur f2-rtr-b (AS 17) ;

- table 3 : AS 3 vers Serial0/3 sur f2-rtr-a (AS 16) ;
- table 4 : AS 4 vers Serial0/4 sur f2-rtr-a (AS 16) ;

- f2-rtr-a & f2-rtr-b établissent également une session BGP entre Se1/15 et Se1/15.

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 avec le port série (chez vous, le 1er port série) et le routeur Backbone qui vous a été attribué :
   - table 1 : PC 196.200.221.193/30 – .194 Cisco .197 – .198 Cisco Backbone Se1/1 ;
   - table 2 : PC 196.200.221.201/30 – .202 Cisco .205 – .206 Cisco Backbone Se1/2 ;
   - table 3 : PC 196.200.221.209/30 – .210 Cisco .213 – .214 Cisco Backbone Se1/3 ;
   - table 4 : PC 196.200.221.217/30 – .218 Cisco .221 – .222 Cisco Backbone Se1/4.

   Depuis votre routeur vous devez être en mesure de faire un « ping » du routeur Backbone et c'est tout, car votre Cisco ne dispose d'aucune route statique ou dynamique.

4. Vous allez annoncer à votre voisin BGP le réseau Ethernet où est connecté votre PC, et uniquement ce réseau.

5. Configurez BGP sur votre routeur afin d'ouvrir une session avec le routeur « backbone ». Dans un premier temps vous n'annoncez pas encore de réseau dans la table BGP. Prenez contact avec l'administrateur du routeur « backbone » pour qu'il configure à son tour la session BGP avec votre routeur. Quelques commandes pour vous aider :

```
R# config t
Enter configuration commands, one per line.  End with CNTL/Z.
R(config)# ip bgp-community new-format
R(config)# router bgp 1                                    // Utiliser votre numéro d'AS
R(config-router)# network 192.168.3.0 mask 255.255.255.240   // Utilisez votre réseau IP

R(config-router)# no synchronisation                       // Ces deux commandes sont utiles dans
R(config-router)# no auto-summary                          // votre configuration de base
```

   Le protocole BGP est maintenant configuré sur votre routeur, mais vous n'échangez de routes avec personne.

6. 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).

Vous allez maintenant, à tour de rôle et lorsque l'instructeur vous le demandera annoncer dans le routeur BGP votre réseau local (l'interface Ethernet où est raccordé votre PC) :

```
R(config)# router bgp 1                                    // Utiliser votre numéro d'AS
R(config-router)# network 192.168.3.0 mask 255.255.255.240   // Utilisez votre réseau IP
```

Sur l'ensemble des tables consultez vos tables BGP : « sh ip bgp », que constatez-vous. Répétez si nécessaire l'opération plusieurs fois jusqu'à changement (cela va prendre 30 secondes à 1 mn). Regardez ensuite la table de routage « sh ip route ». Que voyez-vous maintenant ?

Arrivez-vous à joindre le réseau que vous venez d'apprendre ? Pourquoi ? Que faut-il faire pour que vous arriviez à joindre ce réseau ?

(Nous allons maintenant répéter cette opération avec une 2ème table, puis l'ensemble des tables feront la même manipulation).

7. Regardez le contenu de la table BGP du routeur « backbone ».

8. L'instructeur va maintenant à son tour vous annoncez des réseaux extérieurs pour simuler l'Internet (toutes ces routes seront cependant dans l'AS 16 ou l'AS 17). Constatez le remplissage de votre table BGP puis de votre table de routage système.

   Avez-vous maintenant accès à l'Internet de votre poste de travail ? Pourquoi cela fonctionne-t-il ?

9. Annoncez (par erreur, mais volontairement) un « /30 » extrait du réseau de votre voisin de droite ou de gauche. 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.

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

```
R(config)# ip prefix-list mes-routes seq 10 permit 192.168.3.0/24 le 32
R(config)# ip prefix-list mes-routes seq 20 deny   0.0.0.0/0 le 32

R(config)# ip prefix-list ses-routes seq 10 permit 192.168.18.0/24 le 32
R(config)# ip prefix-list ses-routes seq 20 deny   0.0.0.0/0 le 32
```

11.

12. Ajoutez des filtres pour ne pas envoyer ou recevoir n'importe quoi

```
R(config)# router bgp 1                                        // Utiliser votre numéro d'AS
R(config-router)# neighbor 192.168.8.2 prefix-list mes-routes out
R(config-router)# neighbor 192.168.8.2 prefix-list ses-routes in
^Z
R# clear ip bgp *                                              // Ou clear ip bgp soft-reconfig
```

Vous devez bien sûr utiliser les vrais numéros de réseau annoncés dans vos sessions BGP avec votre voisin. Vous pouvez vérifier le bon fonctionnement des filtres en annonçant des routes interdites et en constatant le bon filtrage. A chaque modification des filtres un « clear ip bgp » est indispensable.

13. Regardez ce que votre voisin vous envoie (le routeur « backbone ») et comparez avec votre propre table BGP

```
R# sh ip bgp neighbor x.x.x.x advertised-routes
R# sh ip bgp
```

14. Quelles routes avez-vous dans votre table BGP ?

```
R# sh ip bgp
R# sh ip bgp x.y.z.t/nn [longer-prefix]
```

15. Supprimez maintenant le filtre en entrée, mais conservez par sécurité le filtre en sortie. Nous allons maintenant pouvoir passer à l'exercice suivant. Supprimez également l'annonce erronée du /28.

Quelques autres commandes BGP utiles :

```
R# sh ip bgp
R# sh ip bgp neighbor
R# sh ip bgp neighbor x.x.x.x received-routes  // Nécessite « soft-reconfig inbound »
```

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 un 2ème ISP pour chacun d'entre vous. Ce second ISP est le routeur numéro 2 de la salle (f2-rtr-a ou f2-rtr-b selon votre installation).

Nous conservons la session BGP avec le routeur « backbone » telle qu'elle a été définie.

Le mode opératoire de l'exercice est le suivant :

1. Il vous faut des adresses IP afin de configurer le raccordement entre vos deux tables. Cet exercice sera fait en commun à partir des adresses IP qui restent disponibles. Faites la re-configuration réseau qui est nécessaire à cette connexion.

   Testez le bon fonctionnement de l'interconnexion entre les deux routeurs (avec ping).

2. Configurez maintenant la session BGP supplémentaire sur votre routeur. Observez ce qu'il se passe lorsque celle-ci « monte ». Quelles routes avez-vous dans votre table BGP ? Quels chemins ?

3. 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 ?

   Nous allons ensuite couper la liaison entre les routeurs « a » et « b » et isoler « b » de l'Internet. Que se passe-t-il pour vous joindre ? Pourquoi servez-vous de point de transit pour joindre certains et pas d'autres ?

   Configurez votre routage BGP afin que votre réseau ne puisse pas être utilisé pour faire du transit vers les autres prestataires de la salle Vous devez pour cela mettre en œuvre un filtrage des réseaux BGP que vous annoncez en utilisant des « as-path list ».

```
R(config)# ip as-path access-list 1 permit ^1$              // Votre numéro d'AS
R(config)# ip as-path access-list 1 permit .*               // Votre numéro d'AS

R(config)# router bgp 1                                     // Utiliser votre numéro d'AS
R(config-router)# neighbor 192.168.8.2 filter-list 1 out
R(config-router)# neighbor 192.168.8.2 filter-list 2 in
R# clear ip bgp *
R# sh ip bgp neighbor
```

   Nous refaisons la même « grosse » panne que précédemment : que se passe-t-il cette fois-ci ?

   Nous allons maintenant manipuler les « local-preferences » : pour l'instant votre routeur BGP prends le chemin le plus court pour joindre une destination. Nous allons affecter un poids à chaque ISP : votre 2ème ISP devient votre ISP préféré, votre 1er sert de secours.

```
R(config)# router bgp 1                                     // Utiliser votre numéro d'AS
R(config-router)# neighbor f2-rtr-b local-preference 200
R(config-router)# neighbor f2-rtr-a local-preference 100
```

N’oubliez pas de redémarrer les sessions BGP. Que constatez-vous dans la table BGP ? Le routage obtenu est-il symétrique ? Comment pourrait-on modifier le trafic retour (provenant de l’Internet et allant chez-vous) ?

Manipulation de « as-path prepend ». Nous allons maintenant remplacer nos filtres par des « route-map » qui vont faire plusieurs choses : choisir « local-preference » en entrée, filtrer les préfixes (en sortie) et filtrer les AS (dans les deux sens) et éventuellement mettre un as-path prepend en sortie.

Exemples (à adapter) :

```
route-map prepend permit 10
   set as-path prepend 1       // Votre numéro d’AS

route-map localpref permit 10
   match as-path 4
   set local-preference 200
route-map localpref permit 20
   match as-path 5
   set local-preference 300
route-map localpref permit 30
   set local-preference 100
```

Fin de l’exercice BGP n°2