Module 16 – Un point d'échange Internet

Objectif: examiner les méthodes pour se connecter à un point d'échange Internet.

Pré requis: Modules 12 et 13, et la présentation sur les points d'échange

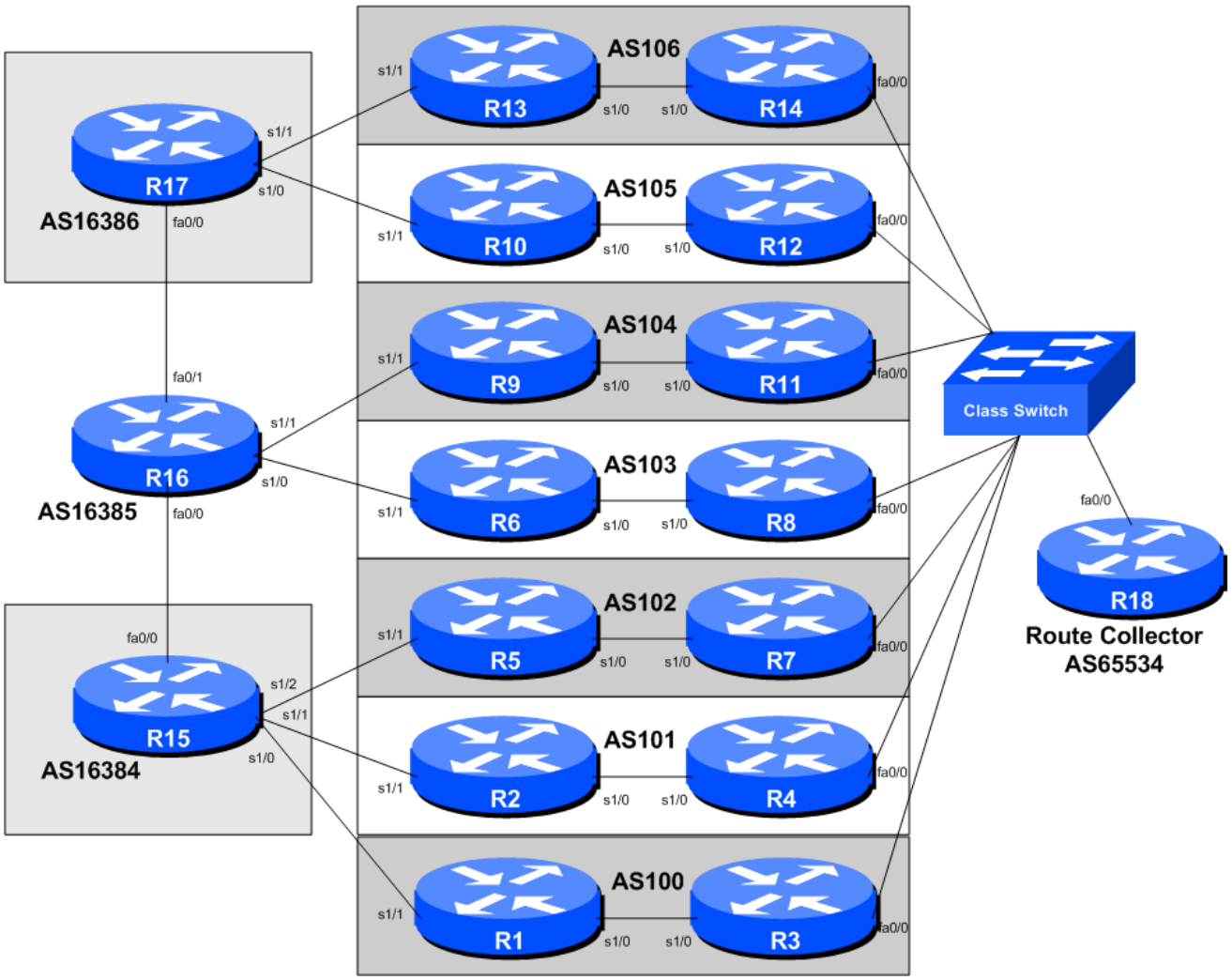

Figure 1 – Configuration IXP

Notes sur ce laboratoire

Le but de ce module est d'introduire le concept d'un point d'échange Internet, comment échanger au niveau des IXP, et de regarder certaines des pratiques de configuration recommandées.

Il a sept ASN participant à l'IXP, avec deux routeurs associés à chaque système autonome. Un routeur échange au niveau de l'IX, l'autre routeur est interne au système autonome (donc aura une session OSPF et iBGP avec le routeur faisant face à IX). On dispose également de trois routeurs fonctionnant comme trois fournisseurs de transit (ou Tier1). Cette version du module est se base sur le Module 10 et couvre les pratiques correctes de configuration OSPF et iBGP pour connecter le routeur face à l'IXP au reste du réseau de l'ISP.

Exercices de laboratoire

1. **Un IXP avancé.** Cet exemple d'IXP a sept ASN participant avec chaque ASN ayant deux routeurs. Un routeur échange à l'IXP; l'autre routeur est interne au réseau ISP et se connecte à un ISP en amont. Les deux routeurs de l'ISP utilisent OSPF et iBGP pour communiquer entre eux les informations de routage. Les 3 ISP de transit sont également interconnectés les uns aux autres, pour représenter le coeur de l'Internet. Ce que nous avons fait ici est de simuler un point d'échange Internet et les connexions de ses participants aux ISP en amont.

2. **Configuration de base.** Chaque équipe de routeur doit configurer son routeur pour s'adapter à la disposition du réseau illustrée dans la Figure 1. Vérifiez toutes les connexions. Notez que tous les liens vers le commutateur de l'IX sont par Ethernet. Les liens entre chaque routeur dans chaque AS sont des connexions série (pour représenter la connexion WAN de l' IX vers le réseau cœur de l'ISP). Les liens de chaque AS à leur transitaire se font par Ethernet (pour représenter la liaison WAN vers l'amont).

3. **Plan d'adressage.** Ces plages d'adresses doivent être utilisées tout au long de cette section du module. Vous pouvez utiliser votre propre plage au sein d'un AS si vous le désirez, du moment que vous consultiez les équipes dans d'autres AS pour s'assurer qu'il n'y a pas de chevauchement.

AS100	**10.1.0.0/20**	**AS105**	**10.6.80.0/20**
AS101	**10.2.16.0/20**	**AS106**	**10.7.96.0/20**
AS102	**10.3.32.0/20**	**AS16384**	**10.8.112.0/20**
AS103	**10.4.48.0/20**	**AS16385**	**10.9.128.0/20**
AS104	**10.5.64.0/20**	**AS16386**	**10.10.144.0/20**

4. **Configuration de base des routeurs.** Configurez les routeurs comme vous l'auriez fait dans les modules précédents. C'est à dire, sécurité de base, adressage IP, etc. L'adressage de la liaison point à point entre les deux routeurs dans chaque AS est laissé comme exercice pour les équipes de routeur. Mais rappelez-vous, une liaison point-à-point nécessite un bloc adresse / 30. Ne pas oublier aussi de configurer les interfaces de loopback.

5. **IXP LAN.** La plage d'adresses utilisée pour l'IXP LAN est 172.17.10.0/24 - le collecteur de routes (s'il est fourni dans ce module) a une adresse IP de 172.17.10.254. Chacun des AS est attribué une adresse de façon séquentielle pour utilisation sur le LAN du point d'échange. Ainsi, par exemple, AS100 a l'adresse 172.17.10.1; AS101 l'adresse 172.17.10.2; AS102 l'adresse 172.17.10.3. Et ainsi de suite.

6. **Configurez l'Ethernet de chaque routeur à l'IXP.** Les interfaces Ethernet connectées à l'IXP doivent être configurées de manière appropriée pour une connexion publique. Examiner les documents IOS Essentials et la présentation IXP. La configuration pour le routeur 3 pourrait être:

```
interface fastethernet 0/0
 description Exchange Point LAN
 ip address 172.17.10.1 255.255.255.0
 no ip directed-broadcast
 no ip proxy-arp
 no ip redirects
!
```

   Si vous n'êtes pas sûr de ce que ces lignes de configuration font, s'il vous plaît demandez à l'instructeur de laboratoire.

Checkpoint N ° 4: *Lorsque vous avez correctement configuré votre routeur, et les autres routeurs de l'IXP sont accessibles (vous pouvez pinger les autres routeurs), s'il vous plaît aviser l'instructeur.*

7. **Configuration OSPF (partie 1).** Évidemment, chaque équipe de l'IXP devrait configurer OSPF entre les deux routeurs dans son AS. Le routeur qui est interne au réseau de l'ASN devrait être simple à configurer. Il dispose d'une interface de loopback, d'une interface de connexion au routeur à l'IXP, et d'une interface de connexion vers l'amont. Donc OSPF doit avoir deux déclarations de réseau, et une interface active configurée. Notez que nous n'avons pas configuré l'interface pointant vers l'amont car nous allons utiliser *next-hop-self* pour nos sessions iBGP. Un exemple pour le routeur 10 pourrait être:

```
router ospf 105
 log-adjacency-changes
 passive-interface default
 no passive-interface serial 1/0
!
interface serial 1/0
 ip ospf 105 area 0
interface loopback 0
 ip ospf 105 area 0
!
```

8. **Configurer OSPF (partie 2).** La configuration d'OSPF sur le routeur se connectant à l'IXP a besoin de plus de soins. Il est très important que le réseau LAN de l'IXP **n'apparaisse jamais** dans la table de routage de l'ISP, que ce soit dans OSPF ou dans iBGP. Si c'est le cas, il y a la possibilité de fuite du réseau LAN de l'IX par le BGP à d'autres ASN, fournissant du transit à l'IXP. Ce ne serait pas une bonne chose, et de nombreux IXP ont des règles contre ce comportement.

   La configuration OSPF pour le routeur IXP ressemble, par exemple pour le routeur 8, à quelque chose comme ceci:

```
router ospf 103
 log-adjacency-changes
 passive-interface default
 no passive-interface serial 0/0
!
interface serial 1/0
 ip ospf 103 area 0
interface loopback 0
```

```
 ip ospf 103 area 0
!
```

NB. Il n'y a **PAS** de configuration pour l'interface Ethernet dans la configuration OSPF. N'en mettez **aucune**, on répète, **aucune**! Ce n'est **PAS** une erreur.

9. **Configurer iBGP entre les routeurs coté transitaire et le routeur du coté de l'IXP.** Tout routeur qui est connecté à d'autres ASN (les routeurs frontières de l'ISP) tels que ceux en amont de l'ISP ou les pairs de l'ISP a besoin d'avoir une configuration iBGP modifiée lorsqu'en échange (peering) avec le routeur tourné vers l'IXP. Si tous les préfixes appris de l'ISP en amont sont répercutés sur le routeur tourné vers l'IXP, alors il y a la possibilité que les pairs IXP (et les non pairs) peuvent indiquer des routes statiques pour ces destinations au niveau du routeur tourné vers l'IXP, gagnant ainsi du transit sortant à travers l'ASN local. Ceci n'est pas souhaitable, et est essentiellement un risque pour la sécurité. La configuration à l'étape précédente doit donc être modifiée pour les routeurs tournés vers l'IXP (le seul routeur dans cet exemple de module laboratoire) de sorte que les préfixes externes ne sont pas annoncés au routeur faisant face à l'IXP. En situation réelle, les ISP créent un groupe de pairs qui est utilisé uniquement durant les échanges (peering) avec les routeurs tournés vers l'IXP, par exemple:

```
router bgp 103
 no synchronization
 network 10.4.48.0 mask 255.255.240.0
 neighbor ibgp-ixp peer-group
 neighbor ibgp-ixp remote-as 103
 neighbor ibgp-ixp update-source loopback0
 neighbor ibgp-ixp next-hop-self
 neighbor ibgp-ixp password cisco
 neighbor ibgp-ixp description iBGP peering with IXP routers
 neighbor ibgp-ixp send-community
 neighbor ibgp-ixp filter-list 10 out
 neighbor router8-loopback peer-group ibgp-ixp
 no auto-summary
!
ip route 10.4.48.0 255.255.240.0 null0
!
ip as-path access-list 10 permit ^$
!
```

Notez l'ajout de l'as-path access-list 10 – essentiellement, cela permet aux préfixes d'origine locale seulement d'atteindre le routeur tourné vers IX. Par exemple, Router6 avec cette configuration n'enverra plus de préfixes appris à l'extérieur au Router8, garantissant ainsi la sécurité du réseau AS103.

10. **Configurer iBGP sur les routeurs du coté de l'IXP (Partie 1).** La configuration iBGP sur routeur tourné vers IXP a besoin de beaucoup plus de soins. Nous ne voulons **PAS** que le LAN IXP apparaisse dans notre iBGP. Et parce que le LAN IXP n'est pas dans OSPF, on ne peut utiliser ce filet pour des next-hops valides. Afin que BGP ait un next-hop valide, nous utilisons la configuration BGP `next-hop-self` comme nous l'avons fait pour nos autres sessions iBGP plus tôt. Par exemple, pour Routeur 7:

```
router bgp 102
 no synchronization
 neighbor ibgp-peers peer-group
 neighbor ibgp-peers remote-as 102
 neighbor ibgp-peers update-source loopback0
```

```
 neighbor ibgp-peers next-hop-self        ! set external next-hops to us
 neighbor ibgp-peers password cisco
 neighbor ibgp-peers descr iBGP peers
 neighbor ibgp-peers send-community
 neighbor router5-loopback peer-group ibgp-peers
 no auto-summary
!
```

Cette configuration est également valable pour d'autres pairs iBGP dans le réseau s'il y avait plus de deux routeurs dans l'ASN. Les ISP essayent de garder les différences de configuration au strict minimum, et ayant deux différents groupes de pairs définis pour iBGP est généralement suffisant!

11. **Configurer iBGP sur des routeurs tournés vers l'IXP (partie 2).** La deuxième différence importante requise pour l'iBGP au niveau du routeur de l'IXP est que le bloc d'adresse locale ne doit **PAS** avoir son origine ici. Si le routeur IX est déconnecté du backbone pour une raison quelconque, s'il est l'origine du bloc d'adresse de l'ISP, il finirait par créer un trou noir (blackholing) pour tout trafic depuis les participants IXP au réseau local. Ce n'est absolument pas souhaitable, donc la procédure correcte est de faire naître le bloc d'adresse ISP uniquement au centre du réseau, et non pas à la périphérie, de sorte que les règles normales de basculement (failover) BGP peuvent s'appliquer.

    Q. Quelles seraient les règles normales de basculement BGP dans ce cas?

    R. Si le routeur tourné vers l'IXP est déconnecté du réseau central, l'iBGP échoue, l'OSPF échoue. Ainsi, le routeur n'entend plus l'annonce du bloc d'adresse de l'ISP à partir du centre, donc il ne l'annonce plus aux pairs IXP, ses voisins eBGP. Lorsque cela se produit, les autres ASN vont utiliser les chemins de secours (alternatifs à l'IXP) pour atteindre l'ASN local. Ce sont les règles normales de basculement BGP.

12. **Configurer iBGP sur des routeurs tournés vers l'IXP (partie 3).** La deuxième exigence très importante à un point d'échange Internet, c'est que la route par défaut (ou les routes non émis par l'ASN local) ne doit pas être disponible au niveau de la LAN de peering. Si cette exigence n'est pas respectée, alors il est possible pour les participants du point d'échange d'utiliser le réseau local pour obtenir du transit vers le reste de l'Internet.

    Dans ce module, chaque ASN recevra une route par défaut à partir de son fournisseur en amont (un scénario courant dans l'Internet d'aujourd'hui). Cette route par défaut ne doit **PAS** être disponible au niveau du routeur du point d'échange de l'ISP. Il y a deux façons de faire cela. Soit bloquer l'annonce de la route par défaut par iBGP au niveau des routeurs frontières qui relient les projets en amont, ou établir une route statique par défaut vers l'interface Null au niveau du routeur IXP (voire les deux!). Par exemple:

    ```
    ip route 0.0.0.0 0.0.0.0 null0
    ```

    Ensuite, si l'un des participants IXP indique une route par défaut vers le réseau local, le trafic sera simplement jeté dans l'interface Null de leur routeur IXP. Seul le trafic à destinations spécifiques disponibles dans la table de routage sur le routeur IXP sera transmis au reste du réseau. Il s'agit d'une exigence très importante pour la **sécurité du réseau**.

13. **Configurer eBGP sur des routeurs tournés vers l'IXP.** Ensuite, eBGP doit être mis en place sur les routeurs IXP. Créer un groupe de pairs et appliquer ce groupe de pairs à chaque voisin eBGP. Un exemple de configuration pour Router8 pourrait être:

```
ip prefix-list myprefixes permit 10.4.48.0/20
ip prefix-list peer100 permit 10.1.0.0/20
..
ip prefix-list peer106 permit 10.7.96.0/20
!
router bgp 103
 no synchronization
 bgp log-neighbor-changes
 neighbor ixp-peers peer-group
 neighbor ixp-peers remove-private-AS
 neighbor ixp-peers prefix-list myprefixes out
 neighbor ixp-peers route-map set-local-pref in
 neighbor <router3> remote-as 100
 neighbor <router3> description Peering with AS100
 neighbor <router3> peer-group ixp-peers
 neighbor <router3> prefix-list peer100 in
..
 neighbor <router14> remote-as 106
 neighbor <router14> description Peering with AS106
 neighbor <router14> peer-group ixp-peers
 neighbor <router14> prefix-list peer106 in
 no auto-summary
!
route-map set-local-pref permit 10
 set local-preference 150
!
```

Les configurations pour les autres routeurs seront similaires à celui-ci. Toutes les équipes routeur auront fait suffisamment de configuration BGP tout au long de cet atelier pour pouvoir extrapoler à partir des exemples ci-dessus. En cas de doute, demandez de l'aide au démonstrateur de laboratoire.

Notez les listes de préfixes. Il y a une liste-préfixe entrante par pair. Certains fournisseurs de services ne filtrent que les AS – ce qui comporte des dangers inhérents, et n'empêche pas contre les fuites entrantes de préfixes incorrectement émis par l'AS pair. Mais seulement filtrer sur les préfixes n'est pas évolutif, surtout dans les grands IXP avec de grands fournisseurs de services participants car ils ajoutent fréquemment aux préfixes qu'ils annoncent. Le registre de routage Internet est généralement utilisé pour résoudre ce problème.

14. **Mettre en place des mots de passe sur les sessions eBGP à l'IXP.** Négocier avec chaque ASN un mot de passe que vous pouvez utiliser sur votre session BGP avec eux. Et puis acceptez de couper la session eBGP à l'utilisation de mots de passe de telle sorte que la session eBGP ne tombe pas en panne dû à l'inadéquation de mot de passe (comme dans le module 2). Un extrait de configuration du routeur 8 pourrait être:

```
router bgp 103
 ...
 neighbor <router11> password peer104
 ...
!
```

15. **Configurer eBGP entre les routeurs dans AS16384, AS16385 et AS16386.** Les instructeurs exploiteront les trois ASN transit/Tier1 ; ils vont maintenant configurer eBGP entre eux. Aucun filtrage n'est attendu ou requis entre les trois ASN, donc la configuration eBGP est assez simple, par exemple comme sur le routeur 15:

```
router bgp 16384
 no synchronization
 bgp log-neighbor-changes
 neighbor <router15b> remote-as 16385
 neighbor <router15b> password as16385-password
 neighbor <router15b> description Peering with AS16385
 no auto-summary
!
```

16. **Configurer eBGP avec les routeurs dans AS16384, AS16385 et AS16386.** Tous les membres des IXP doivent maintenant configurer les sessions eBGP avec les routeurs dans les trois ASN de transit. Ils doivent s'attendre à recevoir la route par défaut de leurs amonts, et seulement envoyer leur bloc d'adresse vers l'amont. Un exemple de configuration pour Routeur 2 pourrait être:

```
ip prefix-list myprefixes permit 10.2.16.0/20
!
router bgp 101
 no synchronization
 bgp log-neighbor-changes
 neighbor <router15> remote-as 16384
 neighbor <router15> description Peering with AS16384
 neighbor <router15> password as16384-password
 neighbor <router15> prefix-list default in
 neighbor <router15> prefix-list myprefixes out
 no auto-summary
!
```

17. **Test de connectivité.** Vérifiez la connectivité à travers le réseau IXP. Chaque équipe routeur devrait être en mesure de voir tous les autres routeurs de l'IXP. Lorsque vous êtes satisfait du fonctionnement correct de BGP, essayez d'exécuter traceroutes pour vérifier les chemins suivis.

    Q. Pourquoi les traceroutes d'un ASN à un autre ASN à travers l'IXP montrent le middle hop comme étant "star'ed out"?

```
Router9#trace 10.7.112.1

  1 10.5.64.6 4 msec 4 msec 4 msec
  2  *  *  *
  3 10.7.96.1 [AS 106] 4 msec *  4 msec
Router9#
```

Checkpoint # 5: *Une fois que la configuration BGP a été terminé, vérifiez la table de routage et veillez à ce vous avez accessibilité complète sur tout le réseau. S'il y a des problèmes, travaillez avec les autres équipes routeur pour les résoudre.*

18. **(Facultatif) Configuration de session eBGP avec routeur 18.** Les instructeurs de laboratoire auront configuré le routeur 18 à être un collecteur de route. Il s'agit d'un routeur qui recueille toutes les routes disponibles à l'IX. Il consiste essentiellement à être un dépôt d'informations indiquant le nombre de routes disponibles à l'IX - bien souvent, l'administration IXP utilise un tel routeur, connecté à une interface web Looking Glass, pour augmenter la valeur commerciale de l'IX. Plus il y de pairs qui sont attirés par les routes disponibles à l'IX, plus grande est la

proposition de valeur du IX pour le reste des membres. C'est dans l'intérêt de tous d'échanger avec le collecteur de routeur:

```
router bgp 103
...
 neighbor 172.17.10.254 remote-as 65534
 neighbor 172.17.10.254 description eBGP with the IX Route Collector
 neighbor 172.17.10.254 password ixp-collector
 neighbor 172.17.10.254 remove-private-AS
 neighbor 172.17.10.254 prefix-list deny-all in
 neighbor 172.17.10.254 prefix-list myprefixes out
...
!
ip prefix-list deny-all deny 0.0.0.0/0 le 32
...
```

Notez que le collecteur de route est en exécution dans un AS privé- il ne lui est pas vraiment nécessaire d'utiliser un AS publique car le collecteur n'a pas besoin d'être directement visible à l'extérieur de l'IXP.

Notez également le filtre de préfixe entrants bloquant tous préfixes sur la session eBGP avec le collecteur de route. Le collecteur n'annoncera aucun préfixe, de par sa conception. Cependant, les ISP ne devraient jamais faire confiance à un autre AS ou à son opérateur, donc le filtre de préfixe entrant est là pour la sécurité, juste au cas où des problèmes surviennent au niveau du collecteur de route.

19. **Test de connectivité.** Vérifiez la connectivité à travers le réseau IXP. Chaque équipe routeur devrait être en mesure de voir tous les autres routeurs de l'IXP. Lorsque vous êtes satisfait du fonctionnement correct de BGP, essayez d'exécuter traceroutes pour vérifier les chemins suivis.

20. **Terminé!** L'IXP est maintenant complet, et en fonctionnement. Les instructeurs de laboratoire se connecteront au collecteur de route et afficheront les préfixes visibles. Toutes les 6 annonces doivent être clairement vues dans le résultat de *sh ip bgp* sur le collecteur de route.

Checkpoint # 3: *Comparez votre table de routage BGP avec celle que vous voyez sur le collecteur de route. Si vous avez des préfixes manquants ou d'autres problèmes, demandez aux instructeurs de laboratoire.*

21. **Résumé.** Ce module a donné des exemples de configurations telles qu'elles sont utilisées par les fournisseurs de services Internet aux points d'échange Internet. Il s'est concentré sur l'utilisation de préfix-lists seulement - des configurations plus complexes sont possibles en utilisant des filtres as-path et les communautés BGP. Ces exemples sont laissés au lecteur à considérer. S'il reste du temps à la fin de l'atelier, demandez à l'instructeur de tester d'autres scénarios.