Atelier Technique AFIX: Session 4

Aspects techniques du Peering

Table des matières

Vue d'ensemble

Dans les sessions précédentes nous avons brièvement parcouru le routage dynamique et les protocoles qui sont habituellement utilisés pour accomplir la tâche. Dans cette section nous nous concentrons plus étroitement sur la façon d'installer le Peering dans la pratique.

Conditions pour le Peering

- Pour faire du Peering avec d'autres organismes vous devez avoir un espace d'adresses IP publiques (portables) et un numéro de Système Autonome AS ("AS number" ou "ASN"), tous les deux peuvent être obtenus à partir de votre Registre Internet Régional. Pour l'Afrique, ce serait AfriNIC (http://www.afrinic.net/).

  Il est important de comprendre ce qu'est l'espace adresse publique portable et pourquoi elle (et pas simplement tout espace adresse) est nécessaire pour le peering. Les petits FAIs et organismes reçoivent habituellement l'espace adresse de leur FAIs ascendant. Cet espace adresse ne peut être employé pour le peering avec d'autres FAIs aux points d'échange public (PEs) puisque leurs FAIs ascendant annoncent déjà cet espace d'adresse à leurs

pairs ; il est donc non portable. (il est techniquement possible de faire une exception à cette règle, si vous avez la coopération de votre FAI ascendant.)

Afin de faire du peering, vous devez obtenir un espace d'adresse directement de votre Registre Internet. L'espace d'adresse obtenu à partir d'un Registre Internet n'est pas employé n'importe comment par n'importe qui sur l'Internet ; il est de la responsabilité du destinataire d'annoncer cet espace d'adresse à ses Fournisseurs de Service Internet et à ses pairs ascendants.

Le nombre AS est employé pour identifier un ensemble de routeurs sous le même contrôle administratif et partageant la même politique de routage. Typiquement, tous les routeurs chez un même FAI font partie du même AS, et les routeurs chez des FAIs différents font partie des différents AS. Un réseau qui se relie par un seul fournisseur ascendant n'a pas besoin de son propre nombre AS, mais est traité en tant qu'élément du fournisseur ascendant AS ; ceci s'applique également aux petits FAIs qui se relient par seulement un fournisseur ascendant et n'ont aucun lien de peering avec un FAI voisin.

Tous les nombres AS de 64512 à 65536 sont privés et peuvent être employés par des organismes dans leurs propres réseaux privés, de la même manière que l'espace privé d'adresses IP (telles que 192.168.0.0/16, 10.0.0.0/8, et 172.16.0.0/12). En faisant du peering à un point d'échange Internet public, il est important d'employer un nombre AS unique et global (pas un nombre AS privé) pour les mêmes raisons qui exigent l'espace d'adresse unique et portable.

- Le BGP version 4 (Border Gateway Protocole) est la norme utilisée pour le peering entre Fournisseurs de Service Internet. Le BGP est un protocole de routage externe, utilisé entre les réseaux sous un contrôle administratif différent.

  Le terme "eBGP" ou "BGP externe" est souvent employé pour se rapporter à l'utilisation du BGP entre deux systèmes autonomes différents (tels qu'entre deux FAIs différents), tandis que le terme "iBGP" ou "BGP interne" est souvent employé pour se rapporter à l'utilisation du BGP à l'intérieur d'un même System Autonome (tel qu'entre deux routeurs à l'intérieur du même FAI).

- Une autre condition importante est de vérifier que votre routeur BGP a assez de mémoire pour recevoir toutes les routes (également connus sous le nom de préfixes dans le monde du peering) de tous vos pairs. Par exemple si vous allez recevoir la table de routage globale, votre routeur doit stocker plus de 165.000 routes (et leur information de chemin AS) qui exige une quantité considérable de mémoire. La mémoire 256MB est maintenant considérée comme une condition minimum absolue pour les routeurs qui reçoivent la table de routage globale entière tandis que une mémoire de 32MB devrait être suffisante pour recevoir toutes les routes du continent africain.

  Sommaire des conditions de peering

  - Routeur compatible BGP4 avec assez de mémoire (tel que Cisco, Juniper, ou Quagga)
  - Votre propre nombre Système Autonome (AS) unique
  - Votre espace d'adresses publiques portables

- Liste des préfixes qui seront annoncés aux pairs (votre espace d'adresse et celui de vos clients)

- Pour chaque pair, une liste de préfixes qu'ils vous annonceront (leur espace d'adresse et celui de leurs clients)

- Le nombre AS de chaque pair

- Les adresses IP qui seront employées pour la liaison BGP entre vous et chaque pair (ce serait typiquement les adresses utilisées au point d'échange)

Armés de ce qui précède vous êtes maintenant prêt à faire du peering.

Peering : Point par point

Supposons que vous êtes Fournisseur de Service Internet appelés « John Doe Communication » et vous voudrez faire du peering avec un Fournisseur de Service Internet appelé « Expert Network ». Parcourrons les étapes requises pour installer un lien de peering pour « John Doe Communications ».

Étape 1

Noter toute les informations énumérées ci-dessus pour chaque organisation :

A :	Nom de la société :	John Doe Communications
	Nombre AS :	AS100
	Espace d'adresses :	12.1.1.0/24, 196.25.0.0/16
	Routeur de bord :	Cisco 2621
	Adresse de pair BGP :	192.0.2.5
B :	Nom de la société :	Experts Networks
	Nombre AS :	AS200
	Espace d'adresses :	150.200.54.0/23
	Routeur de bord :	Quagga sous un PC Linux
	Adresse de pair de BGP :	192.0.2.8

Étape 2

Configurer une interface « loopback » sur le routeur. C'est nécessaire afin d'avoir le BGP parler par une interface qui sera toujours « up » même si certaines des interfaces physiques sur le routeur tombent. Vous devriez toujours employer des interfaces « loopback » pour l'iBGP, mais jamais pour l'eBGP.

```
interface loopback0
ip address 12.1.1.10 255.255.255.255
```

Définir les filtres pour n'annoncer et ne recevoir que uniquement les routes que nous voulons. C'est très important. Si cette étape est omise n'importe quel pair peut inonder votre table de routage avec des entrées fausses. Ca peut également faire craquer votre routeur si trop de préfixes sont acceptés par votre routeur.

```
! “ip prefix-list AS100” permet les routes pour tous les réseaux appartenant au AS100,
! y compris les routes plus spécifiques (avec des préfixes pas plus long que /24)

ip prefix-list AS100 seq 5 permit 12.1.1.0/24
ip prefix-list AS100 seq 10 permit 196.25.0.0/16 le 24

! “ip prefix-list AS200” permet les routes pour les réseaux appartenant au AS 200,
! y compris les routes plus spécifiques (avec des préfixes pas plus longs /24)

ip prefix-list AS200 seq 5 permit 150.200.54.0/23 le 24
```

Configurer les paramètres de base pour le routage BGP :

```
router bgp 100          ! "100" est notre propre nombre AS
```

Par défaut le BGP n'annonce pas une route jusqu'à ce que toutes les routeurs dans le AS aient appris la route par l'IGP. L’utilisation de la commande "no synchronization" permet d'arrêter ce comportement historique non désiré.

```
no synchronization
```

Par défaut le BGP suppose que le routage emploie les réseaux par classe (classe A, classe B, classe C), et tente de convertir quelques routes plus spécifiques en route par classe. C'est un comportement historique non désiré. Utilisez la commande "no auto-summary" pour l'arrêter.

```
no auto-summary
```

Noter tous les changements tels que des liens BGP qui tombent. Ces changements peuvent être surveillés en exportant les notes du routeur vers un serveur journal « syslog » (en utilisant d’autres commandes non données ici). La plupart des FAIs ont un serveur central d’enregistrement d’événement et ont des techniciens pour surveiller tous les événements.

```
bgp log-neighbour-changes
```

Assurez vous que vos propres réseaux sont importés dans le BGP. Ne pas employer la commande "redistribute", parce qu'elle le rend trop facile l’entrée des routes non désirées dans le BGP. Utilisez la commande "network" pour chaque préfixe que vous voulez avoir dans votre table BGP. Si le préfixe est un agrégat des sous réseaux, alors vous avez besoin également d'une route statique pour vous assurer que la route globale est toujours présente.

```
! s'assurer que la route globale agrégée 196.25.0.0/16 est toujours  présente

ip route 196.25.0.0  255.255.0.0 null0 254     !c'est une route statique « pullup »

! ajouter vos propres réseaux au BGP

router bgp100

network 12.1.1.0 mask 255.255.255.0

network 196.25.0.0 mask 255.255.0.0
```

Pour chaque pair BGP (également appelé un voisin), nous avons besoin des multiples commandes "neighbour". Chacune des ces commande indique l’adresse IP du voisin. La première des commandes indique le nombre AS du voisin. Nous allons installer maintenant

une session de peering avec le réseau « Expert Network » (AS 200, en utilisant l'adresse IP 1.2.3.4).

neighbour 1.2.3.4 remote-as 200

Ajouter une description. S'il y a beaucoup de voisins définis, il est utile de trouver le voisin approprié quand des changements de configuration doivent être faits en regardant ces descriptions.

neighbour 1.2.3.4 description Expert Networks

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.

neighbour 1.2.3.4 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.)

neighbour 1.2.3.4 soft-reconfiguration inbound

Annoncer et accepter seulement les routes permises par nos filtres afin d'empêcher l'inondation de notre table de routage.

neighbour 1.2.3.4 prefix-list AS100 out
neighbour 1.2.3.4 prefix-list AS200 in

Étape 3

Vérifier que tout fonctionne comme prévu. Les commandes suivantes peuvent être employées pour diagnostiquer des problèmes avec votre configuration BGP :

!montrer tous les itinéraires connus du noyau

show ip route

! montrer le sommaire des sessions de peering

show ip bgp summary

! montrer les détails du voisin

show ip bgp neighbour

! montrer les routes reçues des voisins

show ip bgp

! montrer les routes reçues du voisin 192.168.4.1 (avant votre filtre "in")

show ip bgp neighbour 192.168.4.1 received-routes

! montrer les routes annoncées au voisin 192.168.4.3 (après votre filtre "out")

show ip bgp neighbour 192.168.4.3 advertised-routes

! montrer toutes les routes connues du noyau

show ip route

Arrangements et options de peering

Il y a deux alternatives principales de peering à un point d'échange d'Internet (PE) :

1. Le PE peut mettre en application un peering multilatéral obligatoire à l'aide d'un serveur de route.
2. Les FAIs individuels peuvent signer des accords de peering bilatéraux, ayant pour résultat une maille totale (eBGP) si tous les participants choisissent de faire le peering avec tous les autres participants, ou une maille partielle si quelques participants choisissent de ne pas faire du peering les uns avec les autres.

Il est également possible d'avoir une combinaison des deux, créant un troisième, arrangement hybride :

3. Une combinaison du peering multilatéral à l'aide d'un serveur des routes (habituellement pour les nouveaux venus) et un peering bilatéral (utilisant la maille totale).

Chacune de ces options est revue plus en détail ci-dessous.

Option 1 : Peering multilatéral obligatoire

Sous cette option, tous les participants au PE sont pairs d'un serveur central des routes. Ceci force tous les participants au PE de faire du peering les uns avec les autres et réduit le nombre de sessions de peering qui doivent être maintenus par chaque pair.

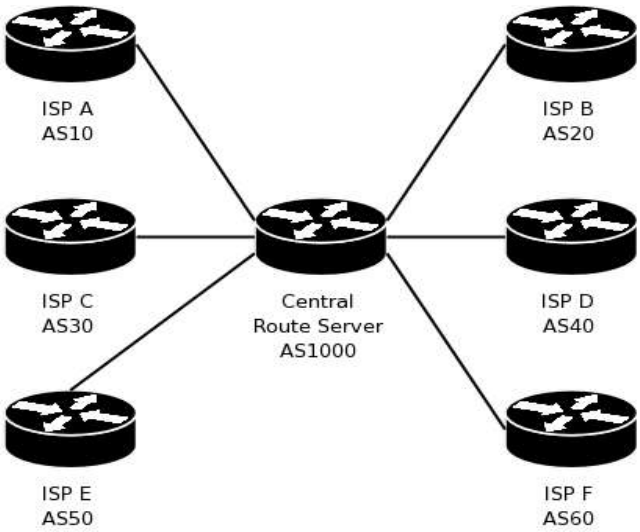
Serveur de routes contre réflecteur de routes : Obtenir la bonne terminologie

Un serveur de route central est parfois désigné inexactement sous le nom d'un réflecteur des routes. Puisque ceci peut causer beaucoup de confusion, ça vaut la peine d'expliquer la différence entre eux.

Un réflecteur de route est un concept dans le iBGP. D'habitude, les routes qu'un routeur apprend par iBGP ne sont pas redistribuées par l'intermédiaire de iBGP à d'autres routeurs dans le même AS. Ce comportement de iBGP a comme conséquence que le iBGP a habituellement besoin d'être configure en maille totale, dans laquelle chaque routeur parle iBGP à chaque autre routeur à l'intérieur du même AS. Dans certains cas (en dehors de la portée de cet atelier), un "réflecteur de route" peut être utilisé pour redistribuer des routes d'un routeur iBGP à un autre routeur iBGP, et ceci peut éliminer la nécessité de configurer une maille totale avec les voisins iBGP.

À un PE, où vous faites du peering avec d'autres systèmes autonomes, le protocole utilisé n'est pas iBGP mais eBGP. Sous ce protocole, les voisins distribuent automatiquement des routes à tous leurs voisins eBGP (dépendant seulement des filtres configurés par l'administrateur réseau) – ainsi un réflecteur de route n'est pas nécessaire, et le concept de réflecteur de route n'existe pas dans le eBGP.

Un serveur de route central, d'autre part, est un routeur à un PE, contrôlé par le PE lui-même, avec lequel tous les participants au PE sont des pairs – comme dans le diagramme ci-dessous :



L'arrangement de peering par serveur de route ci-dessus a plusieurs avantages et inconvénients.

Avantages :

- Tous les participants à l'échange sont automatiquement pairs avec tous les autres participants. C'est un avantage parce qu'il encourage l'échange local du trafic.
- La configuration la plus complexe est centralisée dans le serveur de route, où elle peut être contrôlée par une petite équipe des personnes habiles. Ceci permet aux FAIs avec un personnel moins habile de participer au point d'échange.
- Il est facile pour un nouveau participant de se connecter au point d'échange. Il doit seulement configurer une session eBGP avec le serveur central de route.

Inconvénients:

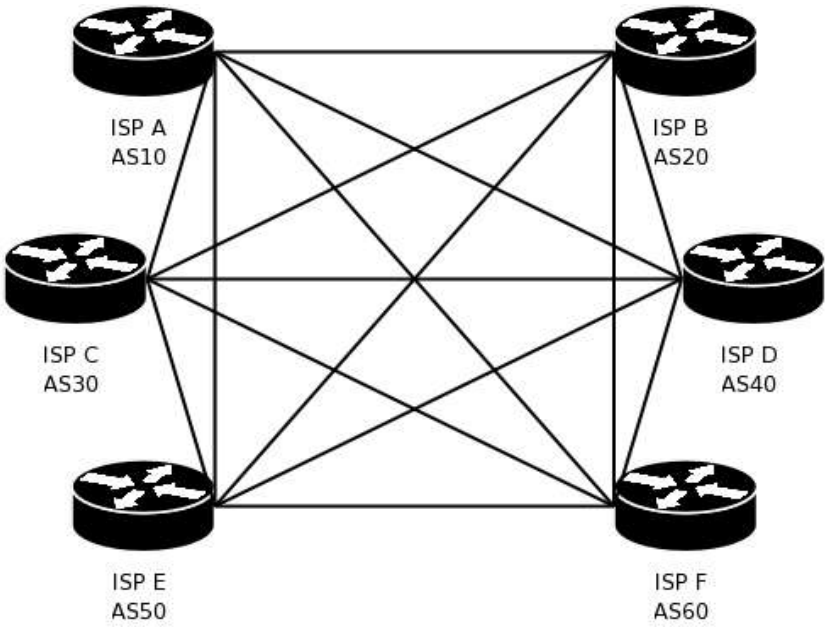
- Tous les participants à l'échange sont automatiquement pairs avec tous les autres participants. Ceci est un inconvénient parce qu'il empêcher aux participants de faire un choix individuel et décider avec qui être pairs.
- Le serveur de route central a une configuration complexe, ainsi le point d'échange doit nommer une ou plusieurs personnes habiles pour le gérer.
- Chaque participant au point d'échange doit annoncer exactement les mêmes routes à tous les autres participants. Ceci empêche la mise en place d'une politique de routage plus complexe.

Si le nombre de participants au PE est très grand, le serveur de route central ne peut pas gérer toutes les sessions de peering. Cette situation peut être évitée en créant une maille des serveurs centraux des routes et en laissant chaque participant faire du peering avec l'un des serveurs centraux de route. La meilleure option doit commencer par un serveur de route central simple comme expliqué ci-dessus et ajouter plus de serveurs au fur et à mesure que le nombre de participants augmente.

Option 2: Peering bilatéral

Un point d'échange qui permet un peering bilatéral permettra à tous les participants de négocier leurs propres arrangements de peering l'un avec l'autre, et n'essayera pas d'imposer le peering entre des participants qui ne veulent pas le faire l'un avec l'autre. Le modèle simple de

serveur de route mentionné plus haut ne supporte que des accords multilatéraux de peering (dans ce cas, chaque participant est d'accord d'être le pair de chaque autre participant),
Si chaque participant à un point d'échange choisit de faire du peering avec tous les autres participants, alors le résultat sera une maille des sessions de peering eBGP, comme représenté ci-dessous.



L'arrangement de peering bilatéral ci-dessus a plusieurs avantages et inconvénients.

Avantages:

- Chaque participant au point d'échange peut choisir si oui ou non il va être pair d'un autre participant. C'est un avantage parce qu'il ne force aucun participant à faire quelque chose qu'ils ne souhaitent pas faire.
- Il n'y a aucun routeur central qui doit être géré par l'opérateur de point d'échange. Toute la gestion des routeurs est exécutée par les FAIs qui actionnent leurs routeurs.
- Chaque participant au point d'échange peut choisir d'annoncer différentes routes à différents pairs (en plus du choix de faire du peering avec l'un ou l'autre participant). Ceci permet des politiques de routage plus complexes, comme convenu entre les participants eux-mêmes sans interférence de l'opérateur de point d'échange.

Inconvénients:

- Chaque participant au point d'échange peut choisir si oui ou non il va faire du peering avec l'un ou l'autre participant. C'est un inconvénient parce qu'il peut y avoir des participants qui choisissent de ne pas faire du peering du tout, ceci peut avoir comme conséquence le trafic local va continuer à passer par des liens internationaux chers.
- Chaque participant doit gérer une configuration complexe du routeur, qui devient de plus en plus complexe quand des pairs sont ajoutés.
- Il est quelque peu difficile pour un nouveau participant de se relie au point d'échange. Le nouveau participant doit être en pourparlers des accords de peering multiples avec les participants existants, et configure des sessions de peering multiples de BGP.

Option 3 : Modèle hybride

Il est possible d'avoir les deux modèles fonctionner simultanément à un PE, avec certains FAIs faisant du peering avec le serveur central des routes et les autres configurant manuellement leurs routeurs pour un peering bilatéral avec les pairs choisis.

Cette option n'est pas la plus souhaitable, mais en réalité elle peut se développer si, par exemple, les très grands FAIs et les très petits font partie du même PE. Le grand FAI pourrait pour des raisons d'affaires préférer traiter le petit FAI en tant que client de transit plutôt qu'un pair ; les accords bilatéraux lui donneront l'opportunité de contrôler ses rapports avec les autres FAIs individuellement.

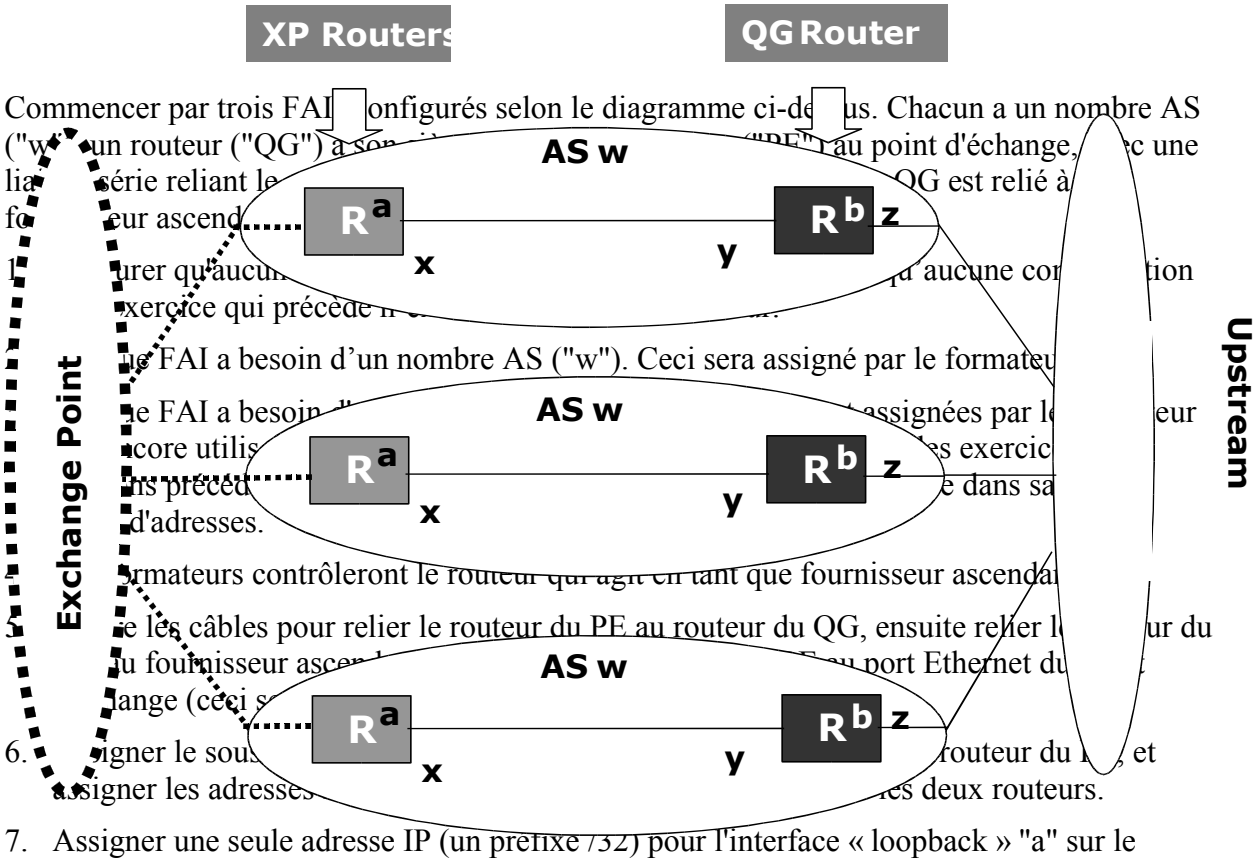
Une option simple doit commencer par un seul serveur de route central et un peering multilatéral, et alors laissé différentes demandes d'affaires déterminer ce qui va se produire après.

Exercices

Exercice 1

Dans cet exercice, nous simulerons la situation où il y a plusieurs FAIs, chaque FAI est relié à un fournisseur ascendant, et tous les FAIs sont en processus de se relier à un point d'échange. Nous configurerons le routage iBGP entre les routeurs existants ("QG") au siège social du FAI et le nouveau routeur ("PE") au point d'échange.

Dans l'exercice 1, nous configurerons iBGP entre les routeurs à l'intérieur de chaque FAI, mais nous ne configurerons pas eBGP entre un FAI et un FAI différent (ceci se fera dans l'exercice 2). Pour l'exercice 1, **le routeur du PE n'est pas encore relié au port Ethernet du point d'échange** (ceci se fera dans l'exercice 2).



Commencer par trois FAI[illegible] onfigurés selon le diagramme ci-de[illegible]us. Chacun a un nombre AS ("w"), un routeur ("QG") à so[illegible] "PE") au point d'échange, [illegible]c une lia[illegible] série reliant le[illegible] QG est relié à fo[illegible]eur ascend[illegible]

1. [illegible]urer qu'aucun[illegible] qu'aucune co[illegible]tion [illegible] exercice qui précède n[illegible]
2. [illegible]e FAI a besoin d'un nombre AS ("w"). Ceci sera assigné par le formateu[illegible]
3. [illegible]e FAI a besoin d[illegible] assignées par le[illegible]eur [illegible]core utilis[illegible]s exercic[illegible] [illegible]is précéd[illegible]e dans sa [illegible] d'adresses.
4. [illegible]rmateurs contrôleront le routeur qui agit en tant que fournisseur ascendan[illegible]
5. [illegible]e les câbles pour relier le routeur du PE au routeur du QG, ensuite relier l[illegible]ur du [illegible]u fournisseur asce[illegible] au port Ethernet du [illegible] [illegible]lange (ceci s[illegible]
6. [illegible]igner le sou[illegible] routeur du [illegible], et [illegible]assigner les adresses [illegible]es deux routeurs.
7. Assigner une seule adresse IP (un prefixe /32) pour l'interface « loopback » "a" sur le routeur du PE, et une adresse IP différente pour l'interface « loopback » "b" sur le routeur du QG.
8. Le fournisseur ascendant (formateur) vous indiquera quelle adresse IP utiliser pour le raccordement entre votre routeur de QG ("z") et le fournisseur ascendant.
9. Ajouter les lignes standard de configuration qui sont employées sur presque chaque routeur Cisco

```
hostname hq.example.net
ip subnet-zero
no ip source-route
no ip domain-lookup
```

```
ip classless
no cdp run
```

10. Configurer les adresses IP sur les interfaces "x", "y" et "z".

```
interface Serial0                  ! indiquer le nom de l'interface
 description liaison série du QG au PE
 encapsulation ppp
 ip address y.y.y.y 255.255.255.252   ! indiquer l'adresse IP et le masque
interface Ethenet0/0
 description ethernet vers le fournisseur ascendant
 ip address z.z.z.z m.m.m.m            ! indiquer l'adresse IP et le masque
 no ip redirects
 no ip proxy-arp
```

11. Configurer une route statique par défaut du routeur du QG vers le fournisseur ascendant.

```
ip route 0.0.0.0 0.0.0.0 u.u.u.u !"u.u.u.u" représente le fournisseur ascendant
```

12. Configurer les interfaces « loopback » à "**a** " et à "**b** "

```
interface loopback0
 ip address a.a.a.a 255.255.255.255 !          "a.a.a.a" est l'adresse IP
```

13. Configurer un protocole de routage intérieur (à l'aide de OSPF ou des routes statiques) de sorte que votre routeur de QG puisse pinger l'interface loopback "a" sur votre routeur du PE, et de sorte que votre routeur du PE puisse pinger l'interface de réalimentation "b" sur votre routeur du QG.

Employer les techniques apprises dans des exercices précédents

14. Configurer iBGP entre les interfaces loopback "a" et "b".

```
router bgp wwww       ! "wwww" représentent votre nombre AS
 no synchronization
 no auto-summary
 bgp log-neighbor-changes
 ! l'adresse IP a l'autre bout est l'interface loopback "b" de l'autre routeur.
 ! le nombre AS a l'autre bout est le même que le AS local ("w")
 neighbor b.b.b.b remote-as wwww
 neighbor b.b.b.b update-source loopback0
```

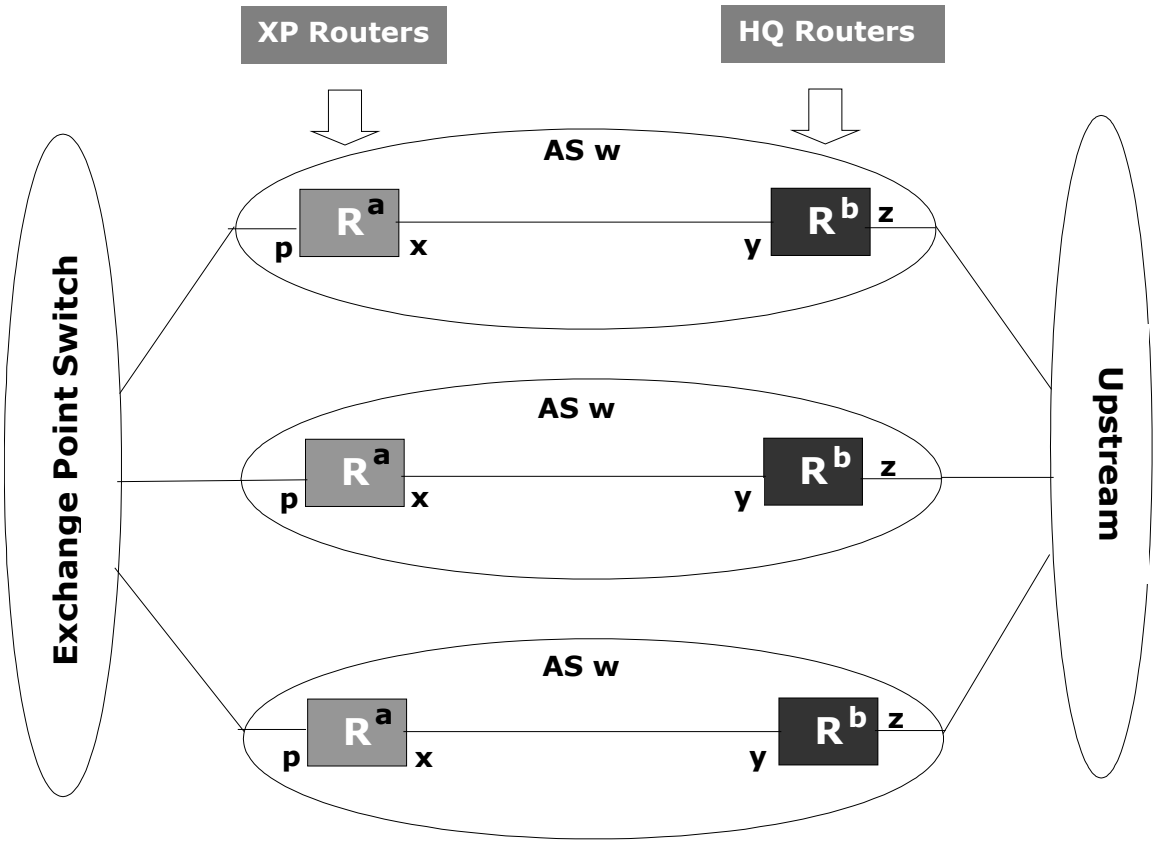
15. Ajouter les commandes BGP "network" et les routes statiques de « pullup » sur le routeur du QG. Ne pas le faire sur le routeur du PE.

```
! route statique "pullup" pour le reseau "n.n.n.n" netmask "m.m.m.m"
ip route n.n.n.n m.m.m.m null0 254
! ajoutter reseau "n.n.n.n" masque "m.m.m.m" au BGP
router bgp wwww
 network n.n.n.n mask m.m.m.m
```

16. Vérifier que le routeur du "PE" apprend toutes vos routes du routeur du "QG" par l'intermédiaire de iBGP. Utilisez « show ip bgp summary », « show ip bgp », « show ip bgp neighbor », « show ip route ».

Exercice 2

À la fin de l'exercice 1, nous avons plusieurs FAIs chacun ayant un routeur au point d'échange, mais le point d'échange ne fonctionne pas encore. Dans l'exercice 2, nous allons faire fonctionner le point d'échange en utilisant un modèle de peering bilatéral.



1. Commencer par tout installer comme s'était à la fin de l'exercice 1.
2. L'opérateur du point d'échange (formateur) assignera un bloc d'adresse IP pour l'usage au point d'échange lui-même, et fournira un commutateur Ethernet au point d'échange.
3. Demander à l'opérateur du point d'échange (formateur) sur quel port du commutateur vous pouvez vous connecter, et quelle adresse IP vous devriez employer (pour interface "p" sur votre routeur du PE). L'opérateur du point d'échange voudra connaître votre nombre AS ("w") et le nom de votre organisation.
4. Faire une feuille d'information contenant :
    - Votre nom d'organisation
    - Votre nombre AS ("w")
    - L'adresse IP que vous employez au point d'échange ("p")
    - Les plages d'adresses IP (préfixes) que vous annoncerez aux pairs au point d'échange. Celles ci incluent tous les réseaux de vos clients.
5. Obtenir les copies des feuilles d'information de tous vos pairs.

6. Connecter un câble Ethernet de votre routeur du PE à votre port assigné sur le commutateur du point d'échange, et configurer l'adresse IP sur l'interface "p" de votre routeur du PE.

7. Définir les filtres pour :

   - Permettre vos routes, refuser les autres.

     ip prefix-list my-routes seq 5 permit n.n.n.n/16 le 24

   - Permettre les routes du pair, refuser les autres. Il y aura plusieurs des tels filtres ; un pour chaque pair au point d'échange. Chaque filtre peut avoir plusieurs lignes ; un pour chaque préfixe que le pair peut vous annoncer.

     ip prefix-list peer-AS200 seq 5 permit n.n.n.n/20 le 24
     ip prefix-list peer-AS200 seq 10 permit x.x.x.x/24

   - Refuser le RFC1918, 127.0.0.0, et d'autres faux réseaux ; permettre les autres

     ip prefix-list no-bogons seq 5 deny 127.0.0.0/8 le 32
     ip prefix-list no-bogons seq 10 deny 0.0.0.0/8 le 32
     ip prefix-list no-bogons seq 15 deny 10.0.0.0/8 le 32
     ip prefix-list no-bogons seq 20 deny 172.16.0.0/12 le 32
     ip prefix-list no-bogons seq 25 deny 192.168.0.0/16 le 32
     ! ... ajouter plus des lignes ici pour tout autre faux réseau à votre connaissance
     ip prefix-list no-bogons seq 1000 permit 0.0.0.0/0 le 24

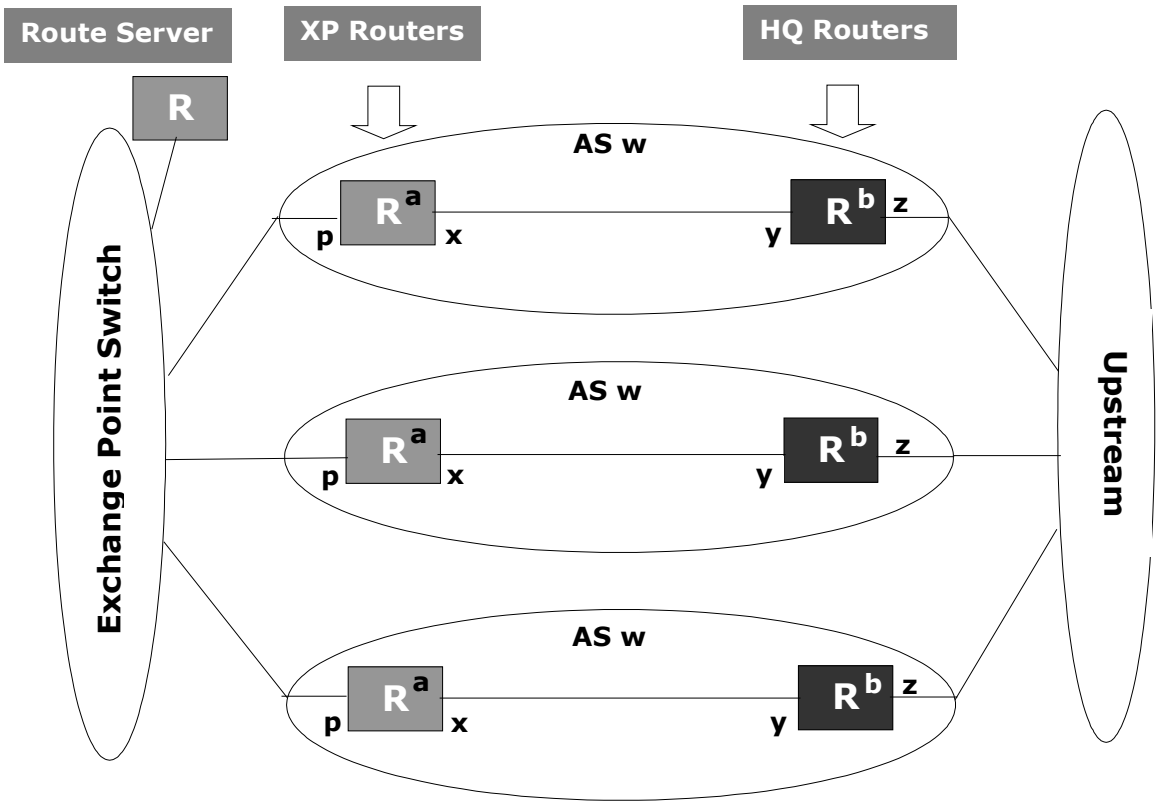
8. Pour chaque pair au point d'échange, ajouter les commandes BGP "neighbor" pour leur parler. Dans chaque cas, utiliser un filtre de sortie « outgoing » qui permet vos routes et refuser les autres, et utiliser un filtre entrant qui permet les routes de ce pair particulier et refuse les autres.

```
router bgp 100                          ! Votre nombre AS
  neighbor p.p.p.p remote-as 200        ! Son adresse IP et son nombre AS
  neighbor p.p.p.p description Expert Networks, phone 123-4567
  neighbor p.p.p.p next-hop-self
  neighbor p.p.p.p soft-reconfiguration inbound
  neighbor p.p.p.p prefix-list my-routes out
  neighbor p.p.p.p prefix-list peer-AS200 in
  neighbor p.p.p.p maximum-prefix 100
```

9. Vérifier en utilisant "show ip bgp summary", "show ip bgp", "show ip bgp neighbor", "show ip route", "ping", et "traceroute".

Exercice 3 : Modèle multilatéral / serveur des routes

À la fin de l'exercice 1, nous avons plusieurs FAIs chacun avec un routeur au point d'échange, mais le point d'échange ne fonctionne pas encore. Dans l'exercice 3, nous faisons le point d'échange en utilisant un modèle de serveur de route. Vous pouvez faire l'exercice 3 au lieu de l'exercice 2, ou même les deux, selon le temps disponible.



1. Commencer avec tout installé comme à la fin de l'exercice 1. Si vous aviez sauté l'exercice 2, alors vos routeurs devraient déjà être installés correctement. Si vous n'aviez pas sauté l'exercice 2, alors vous devriez commencer par défaire toutes les commandes BGP "neighbor" que vous aviez ajoutées dans l'exercice 2. (ne pas s'inquiéter de ne pas défaire le reste des commandes que vous aviez ajoutées dans l'exercice 2.)

```
router bgp 100                ! votre nombre AS
  no neighbor p.p.p.p   ! defaire tout lien avec le voisin
  no neighbor q.q.q.q   ! enlever aussi les autres voisins
```

2. Les formateurs actionneront le serveur des routes, qui est relié à l'Ethernet du point d'échange. Ils vous donneront le nombre AS et les adresse IP du serveur d'itinéraire.
3. Procéder exactement comme dans l'exercice 2, excepté que, quand vous devrez ajouter les commandes BGP "neighbor", n'ajoutez aucune session BGP avec n'importe quel autre FAI. Au lieu de cela, ajouter une session BGP (commandes) "neighbor" pour le pair serveur des routes. Utiliser un filtre sortant qui permet vos routes et refuse toute autre route. Utiliser un filtre entrant qui permet toutes les routes excepté les fausses routes.

(noter que les filtres étaient plus strictes dans l'exercice 2, mais sont plus facile dans cet exercice.)

```
router bgp 100                          ! votre nombre AS
  neighbor s.s.s.s remote-as ssss       ! adresse IP et AS du serveur des
routes
  neighbor s.s.s.s description Serveur des Routes au PE
  neighbor s.s.s.s prefix-list no-bogons in
  neighbor s.s.s.s prefix-list my-routes out
  neighbor s.s.s.s next-hop-self
  neighbor s.s.s.s soft-reconfiguration inbound
  neighbor s.s.s.s maximum-prefix 2000
```

4. Vérifier en utilisant "show ip bgp summary", "show ip bgp", "show ip bgp neighbor", "show ip route", "ping", et "traceroute".