- TP -

Réseau d'opérateur IGP / EGP et raccordement à un IXP

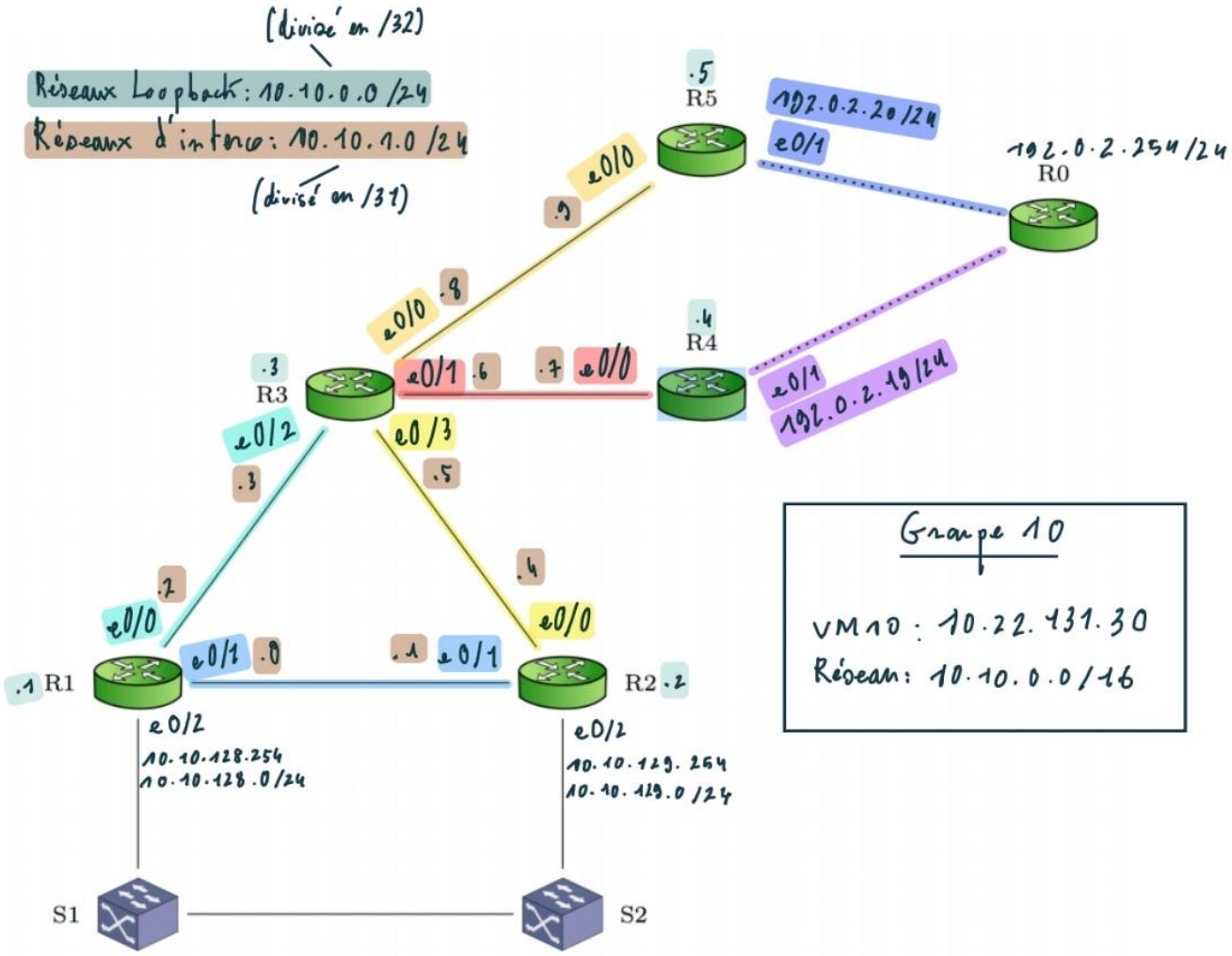
Résumé :

Ce TP a pour but de mettre en place un protocole de routage IGP (OSPF ou IS-IS) entre les routeurs de votre baie, au sein d'un même AS. Vous utiliserez le protocole BGP afin d'échanger vos routes avec les AS voisins sur le point d'échange.

1/ Rappel de l'architecture

La figure ci-dessous rappelle l'architecture d'une baie sous la responsabilité du groupe pour le TP. L'ensemble des commandes se limitera sur les équipements nommés : R1, R2, R3, R4, R5. Le routeur R0 est sous la responsabilité de l'encadrant du TP. R4 et R5 seront des routeurs de bordure (R0 est un switch de l'IXP connecté à des routeurs d'autres AS).

Dans le cadre de ce TP, je dispose de la **VM10** (10.22.131.30) et du réseau **10.10.0.0/16** :



Tobias Favraud

2/ Mise en place de la topologie

1. En premier lieu, modifier le hostname de chaque équipement pour que ces derniers correspondent à ceux représentés sur le schéma.

La commande suivante nous permet de modifier le nom de nos équipements :
hostname R1

2. Faites votre plan d'adressage en découpant des blocs dans le réseau qui a été attribué à votre groupe. Par exemple, réserver un /24 pour les loopbacks, un /24 pour les intercos, etc…

Je dispose du réseau **10.10.0.0/16**. On peut le découper de la façon suivante :

- **10.10.0.0/17** : réseau réservé à un usage interne
  - **10.10.0.0/24** : Réseau pour les loopbacks des routeurs
    - 10.10.0.1/32 : Loopback de R1
    - 10.10.0.2/32 : Loopback de R2
    - 10.10.0.3/32 : Loopback de R3
    - 10.10.0.4/32 : Loopback de R4
    - 10.10.0.5/32 : Loopback de R5
  - **10.10.1.0/24** : Réseau pour les interconnexions entre routeurs
    - 10.10.0.0/31 : Interco entre R1 et R2
    - 10.10.1.2/31 : Interco entre R1 et R3
    - etc.
- **10.10.128.0/17** : réseau réservé aux clients
  - **10.10.128.0/24** : réseau d'un client A
  - **10.10.129.0/24** : réseau d'un client B

3. Identifier les interfaces interconnectant chacun des équipements afin de pouvoir configurer les interfaces IP, et remplir le tableau ci-dessous.

En suivant le plan d'adressage ci-dessus, on subdivise le réseau **10.10.1.0/24** en plusieurs /31 afin de créer les réseaux interconnectant nos routeurs :

Routeur	Interface	En face	IP	Netmask	configuré ?
R1	e0/1	R2	.0	/31	✓
R1	e0/0	R3	.2	/31	✓
R2	e0/1	R1	.1	/31	✓
R2	e0/0	R3	.4	/31	✓
R3	e0/2	R1	.3	/31	✓
R3	e0/3	R2	.5	/31	✓
R3	e0/1	R4	.6	/31	✓
R3	e0/0	R5	.8	/31	✓
R4	e0/1	R0	192.0.2.X.10	/24	✓
R4	e0/0	R3	.7	/31	✓
R5	e0/1	R0	192.0.2.Y.20	/24	✓
R5	e0/0	R3	.9	/31	✓

4. À partir du tableau, configurer sur chacune des interfaces de R1, R2, R3, R4, R5 :
- les adresses IP sur les interfaces physiques.
- ajouter en description de l'interface l'équipement situé en face via la commande : *description CORE : equipement_face (interface_equipement_face)*
  ex : sur R1 interface en face de R2, *description CORE : R2 (s1/0/0)*
- vérifier la connectivité IP de toutes les interfaces IP configurées.

Exemple de configuration sur R1 :

```
int e0/0
        ip address 10.10.1.2 255.255.255.254
        description R1 vers R3 (e0/2)
        no shutdown

int e0/1
        ip address 10.10.1.0 255.255.255.254
        description R1 vers R2 (e0/1)
        no shutdown
```

1. Quel netmask avez-vous utilisé pour vos réseaux d'interco ? Avez-vous essayé en /31 ?

Il est très intéressant d'utiliser le **masque /31** dans le cadre de réseaux d'interco car il permet d'héberger **un maximum de 2 IP**. C'est exactement le nombre requis pour un réseau d'interco, permettant de relier deux routeurs entre eux (**Liaison point à point**), il n'y a donc pas de perte d'adresse IP. Grâce à ce masque, **on optimise au maximum l'utilisation de nos adresses IP**. De plus, la RFC 3021 nous spécifie qu'il n'y a aucun problème à utiliser un /31 avec OSPF, IS-IS ou BGP dans le cadre d'un réseau d'interco (Point à point).

1/1

2. Pouvez-vous joindre n'importe quelle ip configurée depuis n'importe quel routeur ?

Non, ce n'est pas encore possible à ce stade du TP.

3. Pourquoi ? Que manque-t-il ?

Il est impossible de joindre n'importe quelle IP configurée depuis n'importe quel routeur car aucun routage n'est actuellement opérationnel au sein de notre AS. **Il faut mettre en place un routage IGP**, tel qu'OSPF ou IS-IS afin d'annoncer les différents réseaux et permettre aux routeurs de connaître la topologie de notre infrastructure.

4. Une fois la connectivité IP vérifiée, il convient de configurer le protocole de routage de type IGP (choisir OSPF ou IS-IS) sur les équipements :

J'ai fait le choix d'utiliser **OSPF** comme protocole de routage IGP. Voici un exemple de configuration OSPF avec celle présente sur le routeur R3 :

Configuration OSPF sur R3 :

```
int loopback 0
ip ospf 10 area 0

router ospf 10
passive-interface default
no passive-interface e0/0
no passive-interface e0/1
no passive-interface e0/2
no passive-interface e0/3

int e0/0
ip ospf network point-to-point
ip ospf 10 area 0

int e0/1
ip ospf network point-to-point
ip ospf 10 area 0

int e0/2
ip ospf network point-to-point
ip ospf 10 area 0

int e0/3
ip ospf network point-to-point
ip ospf 10 area 0
```

5. Afin de compléter la configuration de l'IGP, chaque équipement de la zone OSPF/IS-IS doit avoir une interface loopback0 configurée :

Routeur	Interface Loopback	IP Loopback	Netmask	configuré ?
R1	lo0	10.10.0.1	/32	✓
R2	lo0	10.10.0.2	/32	✓
R3	lo0	10.10.0.3	/32	✓
R4	lo0	10.10.0.4	/32	✓
R5	lo0	10.10.0.5	/32	✓

Quel netmask avez-vous utilisé pour vos loopbacks ? Est-ce optimum ?

J'ai utilisé **un masque /32** pour mes loopbacks afin d'optimiser l'utilisation de mes adresses IP. En effet, on ne peut attribuer qu'une adresse IP par /32 mais c'est tout ce dont on a besoin pour configurer l'adresse de loopback d'un routeur. Comme **il n'y a pas de perte d'adresse IP**, on peut considérer que **c'est le choix optimum pour notre plan d'adressage**.

Quelle commande rend les interfaces loopback joignables depuis chacun des routeurs ?

J'ai choisi d'utiliser **OSPF** pour faire le routage interne de mon AS. Je peux donc l'utiliser pour **annoncer l'interface loopback de chaque routeur**. Pour ce faire, on utilise la commande suivante sur chaque routeur :

1/1

```
int loopback 0
ip ospf 10 area 0
```

Quelle commande permet à R3 d'annoncer une route par défaut à R1 et R2 ?

Il est possible d'annoncer une route par défaut à R1 et R2 via R3 à l'aide d'OSPF. La commande suivante permet cette annonce :

```
router ospf 10
    default-information originate
```

Quel est la conséquence/risque pour R4 et R5 ?

Le problème de cette commande est qu'elle annonce une route par défaut à tous les membres OSPF, en l'occurrence, R1 et R2 mais aussi R4 et R5 qui sont connectés à l'IXP. R3 étant au centre de notre AS, on risque de rencontrer des boucles de routage.

1/1 Pourrait-on, à la place, configurer une route par défaut statique sur R1 et R2 ? Vers quelle IP ? Avec quelle commande ?

On pourrait configurer une route par défaut statique sur R1 et R2 en utilisant l'interface de loopback de R3. On utiliserait l'adresse de loopback de R3 afin de **garantir la disponibilité** de la route en cas de panne sur l'interface e0/2 ou e0/3 de R3. Pour ce faire, il faudrait renseigner la commande suivante sur R1 et R2 :

```
ip route 0.0.0.0 0.0.0.0 10.10.0.3
```

3/ Mise en place de l'iBGP

Maintenant que la topologie est en place, la mise en place de l'iBGP peut se faire sur les interfaces loopback.

1. Le protocole BGP doit être configuré sur les routeurs R3, R4 et R5.
   Il est important de ne pas oublier le fait que ce dernier doit être full-mesh.

Voici la configuration iBGP de mes routeurs R3, R4 et R5 :

R3 :
```
router bgp 10
    neighbor 10.10.0.4 remote-as 10
    neighbor 10.10.0.4 update-source loopback 0
    neighbor 10.10.0.4 description iBGP Lien vers R4
    neighbor 10.10.0.5 remote-as 10
    neighbor 10.10.0.5 update-source loopback 0
    neighbor 10.10.0.5 description iBGP Lien vers R5
```

R4 :
```
router bgp 10
    neighbor 10.10.0.3 remote-as 10
    neighbor 10.10.0.3 update-source loopback 0
    neighbor 10.10.0.3 description iBGP Lien vers R3
    neighbor 10.10.0.5 remote-as 10
    neighbor 10.10.0.5 update-source loopback 0
    neighbor 10.10.0.5 description iBGP Lien vers R5
```

R5 : router bgp 10
neighbor 10.10.0.3 remote-as 10
neighbor 10.10.0.3 update-source loopback 0
neighbor 10.10.0.3 description iBGP Lien vers R3
neighbor 10.10.0.4 remote-as 10
neighbor 10.10.0.4 update-source loopback 0
neighbor 10.10.0.4 description iBGP Lien vers R4

2. Vérifier que les connexions iBGP sont toutes bien en place et fonctionnelles.

Quelle commande, et quelle(s) partie(s) de cette dernière vous permet de vous en assurer ?

La commande **sh ip bgp summary** permet de vérifier les connexions iBGP entre les routeurs. Dans les informations renvoyées par la commande, on retrouve des informations sur la connectivité avec les voisins :

1/1

```
R3(config)#do sh ip bgp summary
BGP router identifier 10.10.0.3, local AS number 10
BGP table version is 1169, main routing table version 1169
9 network entries using 1332 bytes of memory
13 path entries using 832 bytes of memory
8/8 BGP path/bestpath attribute entries using 1088 bytes of memory
7 BGP AS-PATH entries using 168 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
BGP using 3420 total bytes of memory
BGP activity 227/218 prefixes, 703/690 paths, scan interval 60 secs

Neighbor        V           AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
10.10.0.4       4           10    1878    1850     1169    0    0 1d03h           8
10.10.0.5       4           10    2005    1954     1169    0    0 1d05h           4
```

La colonne Up/Down nous indique que la session est établie depuis 1 jour et 3 heures et la session State/PfxRcd nous indique qu'on reçoit 8 préfixes depuis R4.

3. Nous allons maintenant annoncer notre bloc 10.X.0.0/16 en BGP

Comment annoncer cette route via BGP ?

Il est possible d'annoncer le bloc 10.10.0.0/16 via BGP sur R3 à l'aide de la commande suivante :

router bgp 10
network 10.10.0.0 mask 255.255.0.0

Comment voir sur R3 si vous annoncez cette route à ses voisins ?

On peut vérifier si R3 annonce bien cette route R4 et R5 à l'aide des deux commandes suivantes :

sh ip bgp neighbors 10.10.0.4 advertised-route
sh ip bgp neighbors 10.10.0.5 advertised-route

Comment voir sur R4 et R5 si vous recevez bien la route de R3 en BGP ?

Pour vérifier qu'on reçoit bien la route de R3 en BGP sur R4 et R5, il suffit d'utiliser les commandes suivantes sur R4 et R5 :

2/2

```
router bgp 10
    neighbor 10.10.0.3 soft-reconfiguration inbound

sh ip bgp neighbors 10.10.0.3 received-route
```

Créer une route statique sur R3 :

ip route 10.X.0.0 255.255.0.0 null 0

Pourquoi faut-il créer une route statique vers Null0 pour que cela fonctionne ?

Pour annoncer un réseau via iBGP, il faut l'annoncer dans BGP mais il faut aussi avoir une route vers ce réseau (même préfixe et même sous réseau) dans sa table de routage. C'est pour cette raison que l'on ajoute manuellement une route statique.

Cela pose-t-il un problème que la destination soit Null0 ?

Tout le trafic qui arrive sur l'interface Null0 est jeté. Mais ce n'est pas problématique, au contraire car on annonce un sous réseau en /16 qui est subdivisé en de nombreux sous réseaux. Or, on sait que **les routes plus spécifiques l'emportent toujours sur les routes moins spécifiques** lors du routage.

1/1

Par exemple, si l'on souhaite joindre le réseau 10.10.128.0/24, plus spécifique que 10.10.0.0/16, notre routeur utilisera la route vers 10.10.128.0/24 et le trafic ne sera pas jeté. Si un trafic tente de joindre le réseau 10.10.130.0/24, qui n'existe pas encore au sein de notre AS, il utilisera la route vers 10.10.0.0/16 (car aucune route plus spécifique n'est disponible) et sera jeté. Ainsi, l'interface Null0 permet de filtrer le trafic qui n'a pas une réelle destination au sein de notre AS.

Ici, l'interface Null0 permet aussi d'éviter qu'un trafic en direction d'un sous réseau non existant sur notre /16 se dirige vers la route par défaut, puis revienne, en créant éventuellement des boucles de routage.

Bilan IGP/iBGP

Sur quelle couche le protocole BGP communique-t'il ?

On peut dire que le protocole BGP communique sur **la couche application** car il s'appuie sur TCP (couche transport) pour réaliser ses échanges d'informations de routage (couche réseau).

Quel port/protocole de transport ?

BGP utilise le **port 179** et le protocole de transport **TCP**.

Pourquoi un IGP est-il nécessaire avec une configuration iBGP ?

On utilise un IGP lorsqu'on configure iBGP afin **d'annoncer les loopbacks** des routeurs et **gagner du temps en cas de perte d'un lien** car c'est l'IGP qui recalcule les itinéraires et les temps de convergence sont par défaut plus rapides sur un IGP que sur BGP (à cause du hold time de BGP notamment).

En effet, lorsque l'on configure iBGP au sein de notre AS, il est préférable **d'utiliser les adresses de loopback** des routeurs à la place des interfaces physiques pour configurer les sessions iBGP. Ainsi, si une interface physique est défectueuse, c'est OSPF qui s'occupe de recalculer les routes alternatives pour atteindre les loopbacks mais c'est **transparent pour iBGP**. Effectivement, il n'y a pas de coupure au niveau d'iBGP, **toutes les sessions restent actives car elles s'appuient sur les loopbacks**.

2/2

À quoi sert update-source dans iBGP ?

Lorsqu'un routeur s'associe à son voisin via BGP, il décide de l'interface qu'il utilisera pour maintenir cette session avec ce voisin. **Par défaut, cette interface est l'interface directement connectée au voisin ou celle la plus proche**.

Si l'on souhaite **utiliser une interface spécifique** (comme une loopback) pour maintenir cette session avec le voisin, **on utilise la commande update-source**.

On utilise souvent la commande update-source loopback afin de remplacer l'interface physique directement connectée au voisin par une adresse de loopback et ainsi **éviter de perdre la session iBGP active avec le voisin si cette interface physique est défaillante.**

Depuis R3, comment aurait-on pu annoncer une route par défaut seulement à R1 et R2 en iBGP ?

Depuis R3, on peut annoncer une route par défaut à R1 et R2 via la commande BGP suivante :

```
neighbor 10.10.0.1 default-originate
neighbor 10.10.0.2 default-originate
```

Quel aurait été le problème si on avait fait cela ? / Pourquoi n'a-t-on pas configuré iBGP sur R1 et R2 ?

Pour pouvoir annoncer une route par défaut à R1 et R2 via iBGP depuis R3, **il faudrait configurer iBGP sur ces deux routeurs**. Or, de par son fonctionnement (les routeurs ne réannoncent pas les routes apprises via iBGP aux autres routeurs afin d'éviter les boucles), **iBGP nécessite que chaque routeur dispose d'une connexion directe** (connexion sur le même sous-réseau) **vers tous les autres routeurs iBGP** (Full Mesh), ce qui n'est pas le cas dans notre topologie. C'est pour cette raison que l'on n'a pas configuré iBGP sur R1 et R2.

Quelle aurait été la conséquence ?

- En nombre de sessions à configurer :

Ajouter iBGP sur R1 et R2 nécessiterait de configurer un grand nombre de sessions supplémentaires. En effet, **dès qu'on configure iBGP sur un nouveau routeur, on doit configurer une session iBGP vers chaque routeur déjà connecté en iBGP**. Cela implique aussi de repasser sur tous ces routeurs pour mettre à jour la configuration iBGP et ajouter la session vers ce nouveau routeur, ce qui représente un certain travail.

Le nombre d'interconnexions nécessaires à iBGP Full Mesh est N*(N-1)/2.

R3, R4 et R5 en iBGP : 3*(3-1)/2 = 3
R1, R2, R3, R4 et R5 en iBGP : 5*(5-1)/2 = 10

On passerait donc de 3 à 10 sessions à configurer en ajoutant R1 et R2 à iBGP.

- En termes de ressources (CPU/mémoire) :

Sur un routeur, **l'utilisation du CPU et de la mémoire par iBGP est proportionnelle au nombre de sessions iBGP configurées** car le routeur doit gérer les mises à jour de tous les routeurs avec lesquels il entretient une session iBGP. **Il y aurait donc une forte augmentation des ressources utilisées** par les routeurs si l'on configurait iBGP sur R1 et R2. À partir d'un certain nombre de routeurs, on peut envisager d'utiliser des route reflectors afin de limiter le nombre de sessions et l'utilisation de ressources.

4/ Mise en place de l'eBGP

1. Monter des interconnexions eBGP entre :

- R4 et R0 (AS51706 / 192.0.2.254)
- R5 et R0 (AS51706 / 192.0.2.254)

On monte ces deux interconnexions en renseignant la commande suivante sur R4 et R5 :

```
router bgp 10
    neighbor 192.0.2.254 remote-as 51706
```

Quelle(s) route(s) annoncez-vous à ce voisin ?

La commande **sh ip bgp neighbors 192.0.2.254 advertised-route** nous indique qu'on annonce le réseau 10.10.0.0/16 à R0.

Que différencie une session eBGP d'une session iBGP ?

Dans la configuration (interface / AS):

Une session eBGP est différente d'une session iBGP au niveau de la configuration, **tout d'abord au niveau du numéro d'AS renseigné**. En effet, **iBGP** est utilisé au sein d'un même AS, cela implique donc que le numéro d'AS renseigné dans la configuration de la session iBGP des deux routeurs est le même. **eBGP** est utilisé entre deux AS, le numéro d'AS renseigné dans la configuration de la session eBGP des deux routeurs sera donc différent.

Une autre différence importante entre la configuration d'une session iBGP et eBGP est **l'interface utilisée**. Pour une session **iBGP**, on utilisera l'adresse de loopback des routeurs afin de maintenir la session active en cas de perte du lien physique. Dans le cadre d'une session **eBGP**, on utilisera les interfaces physiques qui connectent les routeurs directement (via le même sous-réseau) entre eux car on souhaite volontairement qu'un routeur termine sa session eBGP avec son voisin si le lien physique qui les connecte est perdu afin qu'il recalcule les routes alternatives via eBGP.

Dans ses effets (ip next-hop, AS_PATH, redistribution):

Il y a une différence importante entre iBGP et eBGP **au niveau du next-hop** car celui-ci
3/3 n'est **pas modifié par iBGP**. En effet, dès lors qu'une route est diffusée par un routeur aux autres routeurs, ce premier routeur qui diffuse la route propage une valeur du next-hop et cette valeur n'est pas modifiée par la suite. Cela peut poser des problèmes si certains routeurs ne connaissent par la route pour atteindre ce next-hop. Il est donc important de bien configurer son routage IGP afin que tous les routeurs soient capables d'atteindre ce next-hop ou d'utiliser la commande next-hop-self dans iBGP.

Contrairement à iBGP, **eBGP modifie la valeur du next-hop**. Quand un routeur annonce une route à son voisin, la valeur du next-hop est l'interface de sortie vers ce voisin. Avec eBGP, on ne retrouve donc pas les problématiques que rencontre iBGP avec la valeur du next-hop.

Il y a aussi une différence entre iBGP et eBGP au niveau de la **redistribution des routes**. Un routeur redistribue toutes les routes eBGP mais ne redistribue pas les routes iBGP qu'il a apprises d'un autre routeur afin d'éviter les boucles.

Enfin, **l'AS_PATH** étant la liste des AS traversés pour atteindre un réseau, il est toujours le même en iBGP. En eBGP, il peut être plus ou moins long selon la localisation du réseau à atteindre mais par défaut, un numéro d'AS ne peut apparaître qu'une fois dans un AS_PATH afin d'éviter les boucles de routage.

2. Monter des interconnexions eBGP entre vos routeurs et ceux des autres AS raccordés au point d'échange.

On monte une interconnexion avec d'autres AS raccordés au point d'échange :

```
router bgp 10
    neighbor 192.0.2.26 remote-as 13
```

Que pouvez-vous observer en regardant toutes les routes apprises via BGP (dans la RIB) ?

On peut remarquer qu'il existe maintenant deux routes pour accéder au réseau de l'AS 13. Le chemin le plus court en termes d'AS_PATH (et celui privilégié, > best) passe maintenant directement par l'AS 13 en évitant l'AS 51706. Le deuxième chemin passe par l'AS 51706 puis par l'AS 13.

Depuis R3, quelles sont les IP next-hop pour les destinations apprises via l'IXP ? Pourquoi ?

Sur R3, on peut s'apercevoir que les IP next-hop pour les destinations apprises via l'IXP sont toujours 192.0.2.254. C'est tout à fait normal car le premier routeur à avoir diffusé ces routes en iBGP est R4 ou R5. Pour ces routeurs, le next-hop vers les destinations apprises via l'IXP est 192.0.2.254 et comme iBGP ne modifie pas le next-hop, on retrouve 192.0.2.254 sur R3.

Quelle(s) route(s) annoncez-vous à ces voisins ? à R0 ?

On peut voir les routes qu'on annonce nos voisins eBGP à l'aide de la commande **ip bgp neighbors X.X.X.X advertised-routes** qui nous indique qu'on annonce en fait à tous nos voisins eBGP (y compris R0) tous les réseaux appris via eBGP, dont un grand nombre ne nous appartient pas. C'est le fonctionnement par défaut de eBGP, il réannonce à tous ses voisins toutes les routes eBGP qu'il connaît :

```
R4>sh ip bgp neighbors 192.0.2.26 advertised-routes
BGP table version is 1164, local router ID is 10.10.0.4
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale, m multipath, b backup-path, f RT-Filter,
              x best-external, a additional-path, c RIB-compressed,
Origin codes: i - IGP, e - EGP, ? - incomplete
RPKI validation codes: V valid, I invalid, N Not found

     Network          Next Hop            Metric LocPrf Weight Path
 *>  1.1.1.1/32       192.0.2.254                            0 51706 6 ?
 *>  2.2.2.2/32       192.0.2.254                            0 51706 6 ?
 *>  3.3.3.0/24       192.0.2.254                            0 51706 6 ?
 *>  3.3.3.3/32       192.0.2.254                            0 51706 6 ?
 *>  4.4.4.0/24       192.0.2.254                            0 51706 6 ?
 *>  4.4.4.4/32       192.0.2.254                            0 51706 6 ?
 *>  5.5.5.0/24       192.0.2.254                            0 51706 6 ?
 *>  5.5.5.5/32       192.0.2.254                            0 51706 6 ?
 *>  10.1.0.0/16      192.0.2.26                             0 13 14 i
 *>  10.4.0.0/16      192.0.2.254                            0 51706 4 i
 *>  10.5.0.0/16      192.0.2.254                            0 51706 5 i
 *>  10.6.0.0/31      192.0.2.254                            0 51706 6 ?
 *>  10.6.0.2/31      192.0.2.254                            0 51706 6 ?
 *>  10.6.0.4/31      192.0.2.254                            0 51706 6 ?
 *>  10.6.0.6/31      192.0.2.254                            0 51706 6 ?
 *>  10.6.0.8/31      192.0.2.254                            0 51706 6 ?
 *>  10.7.0.0/16      192.0.2.254                            0 51706 7 i
 *>  10.8.0.0/16      192.0.2.254                            0 51706 8 i
 *>i 10.10.0.0/16     10.10.0.3                0    100      0 i
 *>  10.13.100.0/24   192.0.2.26                             0 13 i
 *>  10.13.200.0/24   192.0.2.26                             0 13 i
 *>  192.0.0.0/22     192.0.2.254              0             0 51706 i
 r>  192.0.2.0        192.0.2.26                             0 13 7 i

Total number of prefixes 23
```

Est-ce voulu ? Comment feriez-vous pour n'annoncer que votre réseau (/16) ?

Ce n'est pas voulu. En fait, nous voulons annoncer uniquement les réseaux nous appartenant, en l'occurrence le réseau 10.10.0.0/16. Pour annoncer uniquement notre réseau /16, **on réalise une préfix-list en sortie** sur R4 et R5 :

```
router bgp 10
    neighbor 192.0.2.26 prefix-list PFL-AS10-OUT out
    neighbor 192.0.2.254 prefix-list PFL-AS10-OUT out

ip prefix-list PFL-AS10-OUT seq 5 permit 10.10.0.0/16
```

3/3

```
R4#sh ip bgp neighbors 192.0.2.26 policy detail
 Neighbor: 192.0.2.26, Address-Family: IPv4 Unicast
 Locally configured policies:
  prefix-list PFL-AS10-OUT out

 Neighbor: 192.0.2.26, Address-Family: IPv4 Unicast <detail>
 Locally configured policies:
  prefix-list PFL-AS10-OUT out
ip prefix-list PFL-AS10-OUT: 1 entries
   seq 5 permit 10.10.0.0/16
```

On peut maintenant s'assurer qu'on annonce uniquement notre réseau à l'aide de la commande **ip bgp neighbors X.X.X.X advertised-routes** :

```
R4#sh ip bgp neighbors 192.0.2.26 advertised-routes
BGP table version is 1164, local router ID is 10.10.0.4
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale, m multipath, b backup-path, f RT-Filter,
              x best-external, a additional-path, c RIB-compressed,
Origin codes: i - IGP, e - EGP, ? - incomplete
RPKI validation codes: V valid, I invalid, N Not found

     Network          Next Hop            Metric LocPrf Weight Path
 *>i 10.10.0.0/16     10.10.0.3                0    100      0 i

Total number of prefixes 1
```

5/ Mise en place de Filtrage et traffic-shaping

Comment limiter le nombre de routes apprises via une session BGP ?

On peut utiliser la commande suivante pour limiter le nombre de routes apprises via une session BGP, qui permet à notre routeur d'apprendre un maximum de 3000 préfixes via sa session avec R0 :

```
router bgp 10
    neighbor 192.0.2.254 maximum-prefix 3000
```

1/1

La session BGP se coupe quand la limite est atteinte. Il faudra effectuer une commande **clear** sur la session pour pouvoir la relancer.

Comment s'assurer que les routes apprises sont fiables ? Quelle est la configuration ?

On peut déjà s'assurer qu'une entité a le droit d'annoncer une route vers un bloc réseau en vérifiant auprès d'un registre internet régional comme le RIPE ou le ARIN. Ces organismes détiennent des registres de routage internet (**IRR**) permettant de savoir si une entité possède bien un bloc réseau spécifique. On peut ensuite **filtrer les annonces reçues** à l'aide des objets contenus (les route objects comme AUT-NUM, INETNUM) dans ces bases de données.

Pour s'assurer que les routes apprises sont fiables, on peut aussi utiliser avec nos partenaires des **ROA**, ce sont des objets signés et authentifiés par une infrastructure à clés publiques, la RPKI, gérée par l'IANA. Ces objets permettent de valider qu'un AS a bien le droit d'annoncer un préfixe, qu'une société possède un numéro d'AS, etc.

Quelle est la valeur de la "local preference" des routes apprises en BGP ?

La valeur de la local preference des routes apprises en BGP est **100**.

Quelle commande avez-vous utilisée pour la connaître et sur quel équipement ?

Pour connaître la valeur de la local preference, j'ai utilisé la commande sh ip bgp 10.13.100.0 sur R3 :

2/2

```
R3(config)#do sh ip bgp 10.13.100.0
BGP routing table entry for 10.13.100.0/24, version 1243
Paths: (1 available, best #1, table default)
  Not advertised to any peer
  Refresh Epoch 2
  13, (received & used)
    192.0.2.26 (metric 20) from 10.10.0.4 (10.10.0.4)
      Origin IGP, metric 0, localpref 100, valid, internal, best
```

Comment forcer le trafic de son réseau à sortir via R4 vers l'IXP (et via R5 en backup) ?

Pour forcer le trafic de son réseau à sortir via R4 vers l'IXP, on peut augmenter la valeur de la local preference sur R4. La local preference est utilisé par BGP pour choisir le chemin de sortie de l'AS et une haute valeur est toujours préférée à une basse valeur :

```
router bgp 10
        neighbor 192.0.2.254 route-map LOCAL-PREF-500 in

route-map LOCAL-PREF-500 permit 5
        set local-preference 500
```

Comment le voit-on sur R3 ?

On le voit facilement sur R3 à l'aide de la commande **sh ip bgp**. On retrouve la valeur 500 dans **la colonne LocPrf**.

Comment inciter les autres membres de l'IXP à envoyer le trafic (vous étant destiné) vers R4 plutôt que R5 ?

Pour inciter les autres membres de l'IXP à envoyer le trafic vers R4 plutôt que R5, on peut utiliser la technique de **l'AS Path Prepend**, qui vise à **allonger artificiellement la longueur de l'AS Path** sur R5 afin que les autres membres de l'IXP privilégient d'envoyer le trafic vers R4, ayant un plus court AS Path. Voici les commandes pour mettre en place l'AS Path Prepend sur R5 :

```
router bgp 10
    neighbor 192.0.2.254 route-map RTM-IXP-OUT out
    neighbor 192.0.2.26 route-map RTM-IXP-OUT out

route-map RTM-IXP-OUT permit 10
    set as-path prepend 10 10
```

Quelle commande avez-vous utilisée pour vérifier le bon fonctionnement ?
Sur quel équipement ?

Pour vérifier le bon fonctionnement de l'AS Path Prepend, on doit se positionner à **l'extérieur de notre AS**. On peut demander à une personne ayant un accès à un autre AS ou à l'IXP de réaliser un sh ip bgp afin de valider que le numéro d'AS revient plusieurs dans l'AS Path vers R4 :

```
192.0.2.20                                          0 10 10 10 i
```

Quelle est la limite de cette méthode ?

3/3

La problématique de cette méthode est qu'elle se base sur l'AS Path pour privilégier un chemin sur un autre. Or, l'AS Path n'est que le 4ème critère le plus important dans le choix du meilleur chemin. Il y a donc 3 critères, notamment la local preference, que BGP privilégiera sur l'AS Path dans le choix du meilleur chemin.