TP de Réseaux – RICM 5
Le protocole de routage externe BGP
(*Border Gateway Protocol*)

Pascal Sicard – Martin Heusse

1 Introduction

Le protocole de routage BGP (Border Gateway Protocol) est un protocole permettant de communiquer des informations de routages entre différents systèmes autonomes (AS pour *autonomous system*).

Il est dit «externe» aux systèmes autonomes. Il existe d'autres protocoles externes comme EGP mais qui ne sont quasiment plus utilisés.

Contrairement aux protocoles de routages internes (RIP, EIGRP, OSPF…) le problème du routage n'est plus seulement de déterminer le chemin le «plus court». Des contraintes plus strictes peuvent être présentes comme par exemple l'interdiction de traverser un système autonome X pour des raisons de sécurité.

2 Principe du routage externe

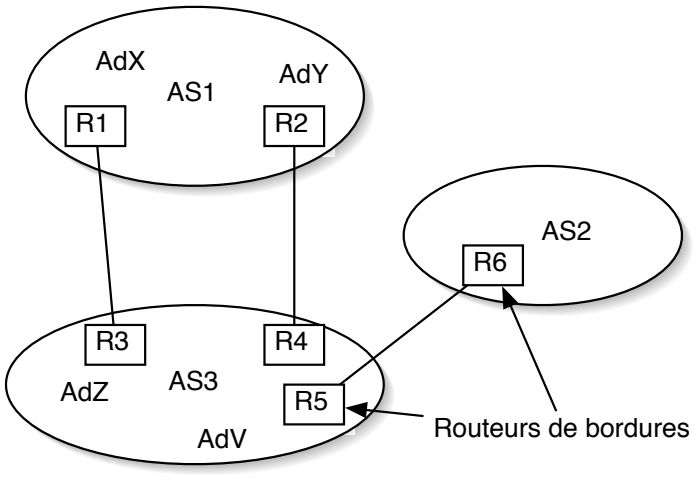

Figure 1 – Routage externe

Dans un protocole de routage externe ce sont les routeurs aux frontières des AS (appelés routeurs de bordures, voir fig. 1) qui s'échangent les informations de routage. Le protocole de

routage externe va permettre l'échange entre ces routeurs de bordure des adresses contenues dans les AS. Il va aussi propager des routes apprises depuis un autre AS.

Par exemple dans la configuration ci dessous AS3 va pouvoir propager des adresses de AS2 vers AS1 et inversement. Les routeurs R4 et R5 vont donc aussi se passer les informations de routages précédemment apprises.

Le passage des informations de routages se fera de routeur de bordure en routeur de bordure et elles seront éventuellement propagées dans les routeurs internes aux AS par une redistribution dans les protocoles de routages internes.

Le but d'un tel protocole est de pouvoir propager (comme les protocoles de routages internes) des routes connues vers d'autres AS mais cela en pouvant appliquer des restrictions décidées par l'administrateur de chaque AS.

Ainsi dans l'exemple ci-dessus on pourra mettre en place ces contraintes :

- L'AS3 pourra décider que pour arriver au réseau d'adresse AdV depuis l'extérieur il faut passer forcément par R4.
- L'AS3 pourra décider que pour aller du réseau d'adresse AdX à celui d'adresse AdY il n'y a pas de possibilité de passage par lui.
- L'AS3 pourra décider que tous les paquets venant de AS1 à destination de l'AS2 passe par R4.
- L'AS3 pourra décider que tous les paquets à destination de AS1 venant de l'AS2 passent par R3.

On voit donc qu'il va falloir faire la distinction entre les routes apprises de façon internes et celles apprises depuis l'extérieur des AS dans ce type de protocole.

3 Le protocole BGP

Le protocole BGP repose sur TCP (port 179). Les échanges se font toujours entre 2 routeurs.

3.1 Format des messages

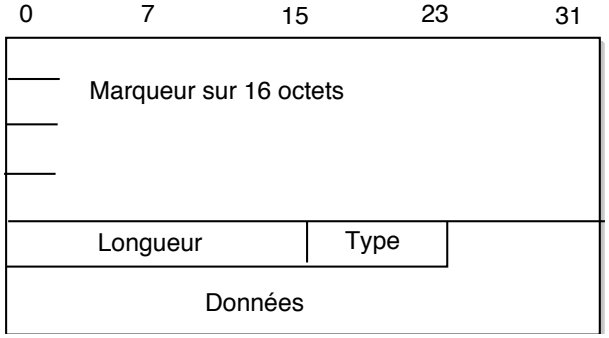

Figure 2 – Format des paquets BGP

Champs du paquet dans l'ordre (voir fig. 2) :

- Marqueur (sur 16 octets)
- Longueur (sur 2 octets) : longueur du paquet BGP qui peut être de taille variable suivant le type (de 19 à 4096 octets).
- Type (sur un octet) :
  - 1 : ouverture de dialogue : émis juste après l'ouverture de connexion TCP
  - 2 : mise à jour des tables de routage BGP
  - 3 : notification d'erreur
  - 4 : sonde : émis périodiquement pour tester l'état du lien et du routeur
- Données de 0 à 4077 octets.

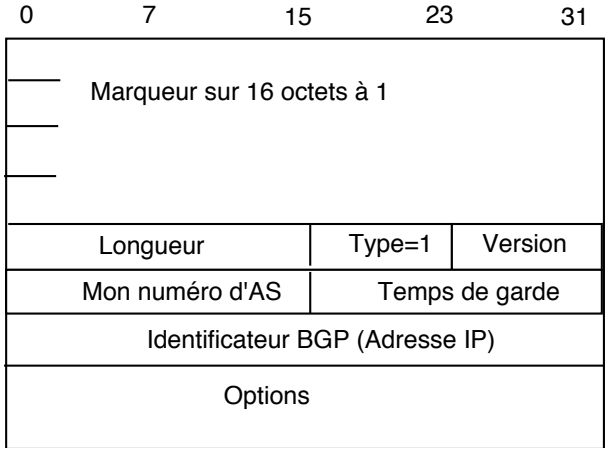

Figure 3 – Format des paquets d'ouverture

Format des données suivant le type :

- Ouverture de dialogue :
  Le marqueur contient des 1.
  - Version du protocole BGP (1 octet)
  - Numéro de mon système autonome (2 octets)
  - Temps maximum en secondes entre deux paquets de sonde (2 octets)
  - Identificateur (adresse) du routeur BGP émetteur (4 octets)
  - Option d'authentification pour la sécurité

- Mise à jour :
  Contient 3 listes : adresses à supprimer, attributs, adresses (voir fig. 4)
  - Adresses à supprimer
    - Longueur des données contenant des routes à supprimer (2 octets)
    - Liste : [Longueur en bits de la partie réseau de l'adresse, partie réseau de l'adresse IP (préfixe)] (nombre d'octets variable)

  - Attributs
    - Longueur totale des attributs.

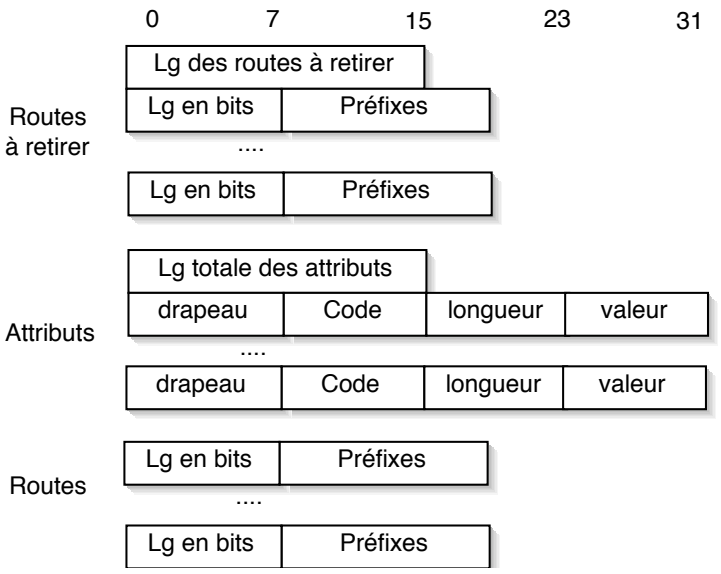

Figure 4 – Format des paquets de mise à jour

— Suite d'attributs [drapeau (1 octet), code (1 octet), longueur de la valeur (1octet), valeur de l'attribut (variable).
Le drapeau permet de spécifier le type d'attribut : Optionnel , Transitif, Partiel (à déjà traversé un routeur) : 3 bits de poids forts du drapeau.

Les principaux attributs :

1. ORIGIN : valeurs :
   — (1) adresse apprise à l'aide d'un protocole interne
   — (2) adresse apprise depuis l'extérieur (eBGP)
   — (3) inconnue : utilisé pour les routes statiques
2. AS_PATH : valeur : suite des numéros d'AS ajouté par chaque routeur traversé cet attribut permet de vérifier que l'information n'a pas fait un tour de boucle.
3. NEXT_HOP : valeur : adresse du prochain routeur à atteindre pour parvenir à une adresse.
4. MULTI_EXIT_DISCR (MED) : valeur : métrique associée aux adresses.
5. LOCAL_PREF : valeur : préférence associée au routeur émetteur comme entrée /sortie de l'AS (utilisé entre routeurs d'un même AS par iBGP).

◦ Adresses
— Listes des adresses : [Longueur en bits de la partie réseau de l'adresse, partie réseau de l'adresse IP (préfixe)] (nombre d'octets variable).

- Notification : Code d'erreur sur un octet.
- Sonde : Pas de donnée

3.2 Fonctionnement du protocole BGP

On peut distinguer 2 types de dialogue :

- Entre deux routeurs de bordure de deux AS différents, dénommé eBGP (external BGP).
- Entre les routeurs d'un même AS dénommé iBGP (internal BGP).

Pour qu'un dialogue BGP s'établisse entre deux routeurs, on les déclarera «voisins» (au sens BGP). Deux voisins d'AS différents sont forcément sur le même réseau local. Deux voisins du même AS peuvent être «éloignés». C'est le protocole de routage interne qui maintient leur connectivité.

On peut filtrer à volonté les routes à diffuser à l'extérieur.

Les routeurs BGP vont prendre leur décision de routage au vue des attributs des adresses qu'ils auront pu recevoir de divers AS et des restrictions/préférences locales. Ces attributs vont spécifier pour une adresse destination donnée @ :

- le prochain routeur à qui envoyer (Next hop) pour atteindre @
- l'origine de l'apprentissage de cet @ (interne, externe ou statique)
- des préférences locales de poids affectés au entrées/sorties d'un AS
- des métriques associées aux adresses
- ...

Important : pour qu'une route vers un préfixe interne à un AS soit propagée, il faut qu'elle soit publiée (commande `network`) mais aussi que le réseau en question apparaisse dans la table de routage IP. Cette vérification évite que le routeur de bordure reçoive du trafic dont il ne saurait pas quoi faire.
Pour qu'une route vers un préfixe externe soit re-publiée, il faut avoir une route vers le `NEXT_HOP`.

Pour visualiser la table de routage BGP, on utilise la commande :
`show ip bgp`
alors que la table de routage IP est consultée par :
`show ip route`
De même, on peut vérifier que la connexion avec les voisins fonctionne par `show ip bgp neighbors`

4 Déroulement du TP

Avant de commencer, il peut être judicieux d'effacer les configurations des routeurs. Pour cela, tapez `erase startup-config`, puis redémarrez le routeur (`reload`). Attention, n'effacez pas le système d'exploitation qui est en mémoire flash !

4.1 Configuration du réseau

Le réseau comporte trois systèmes autonomes (10, 12 et 14). On imagine que le système que nous administrons est l'AS 12. L'AS 10 et 14 sont les systèmes autonomes qui nous permettent de nous relier «au reste du monde». La station R3 sera utilisée comme routeur (sous

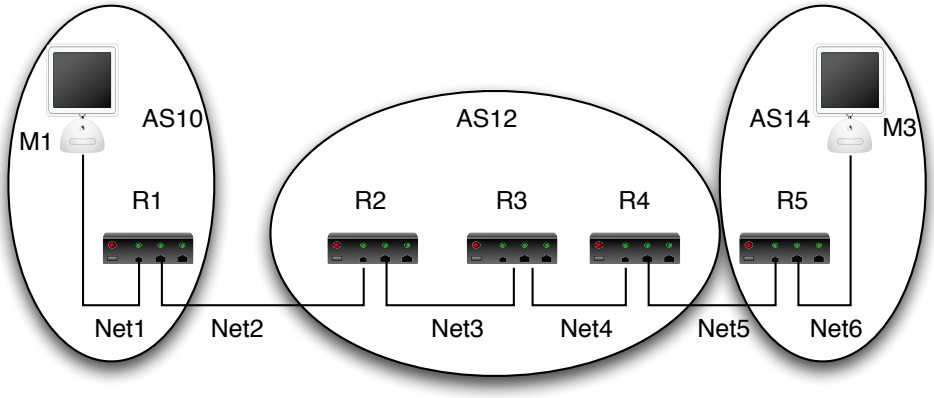

Figure 5 – Réseau de travail

l'environnement `zebra`, voir la documentation sur les routeurs Cisco). Une quatrième station peut être utilisée pour capturer des paquets sur les liens inter-AS.

On choisira pour les adresses des réseaux : Net1 : 1.0.0.0/8, Net2 : 2.0.0.0/8 , ...

4.2 Plan d'adressage

Attribuer une adresse à chaque interface, noter soigneusement le plan d'adressage et configurer les cinq routeurs et les machines.
Commandes (sous `configure terminal`) : `interface ethernet` *numero_interface* puis `ip address` *adresses_internet netmask*.

On ne changera pas les netmasks standards.

On peut changer le nom des routeurs grâce à la commande : `hostname` (sous `configure terminal`). On vérifie par la commande `show configuration` qu'aucun protocole de routage ne tourne déjà [1]. On peut les arrêter par la commande : `no router` *algo_routage*.

4.2.1 Routage interne dans l'AS 12

Nous allons utiliser comme protocole de routage interne OSPF (voir TP deuxième année) :

- Mettre en place le protocole de routage interne OSPF sur les routeurs de l'AS 12.
  - Commandes (sous `configure terminal`) :
  - `router ospf` *ProcessId*
  - `network` *adresse_réseau_interface wildcard* `area 0` [2]

La commande `network` est à faire pour chaque interface sur laquelle on veut que OSPF soit activé. le paramètre `wildcard` doit être égal au complément booléen du netmask du réseau de l'interface. Il n'y a ici qu'une seule aire OSPF de numéro 0.

- Vérifier que les tables de routages des routeurs R2, R3, R4 sont à jour. (`show ip route`)

1. Pour que ce fichier reflète l'état courant du routeur, il faut avoir entré la commande `write` auparavant. Sinon on peut aussi consulter `show running-config`.
2. Ces directives sont légèrement différentes sur zebra.

- La base de données de routage de OSPF est accessible avec `show ip ospf database network`.
- Vérifier que OSPF ne fonctionne effectivement pas sur les liens qui relient deux AS différents (sur ces liens, c'est eBGP qui prend le relais).

4.3 Routage externe eBGP

4.3.1 Échange d'information externe

On va mettre en place BGP sur R1 et R2 et faire en sorte que les adresses de l'AS 12 soient apprises dans l'AS 10 et réciproquement.

- Lancer une capture de paquet sur le réseau net2.
- Lancer BGP sur les routeurs R1 et R2. Commande : `router bgp` *numéro_AS*
- Déclarer R1 et R2 voisins :
  Commande (sous `router`) :
  `neighbor` *adresse_voisin* `remote-as` *Numéro_AS_du_voisin*
- Vérifier si des paquets BGP ont été émis sur le réseau net2 ? Relancer la capture
- «Annoncer» vers l'extérieur l'adresse net1 de l'AS 10 dans R1 : Commande (sous `router`) : `network` *réseau_a_annoncer*
  Remarques : Attention la commande `network` *a ici une signification légèrement différente de celle qu'elle a dans le contexte de RIP ou OSPF (lancement de ces protocoles sur l'interface spécifiée). Pour annoncer une adresse un routeur doit bien entendu avoir dans sa table de routage cette adresse sinon il ne pourrait pas ensuite réexpédier les paquets venant de l'extérieur et à destination de cette adresse.*
- Noter et expliquer la table de routage BGP de R1 et R2 `show ip bgp`
- Analyser le paquet BGP émis par R1 vers R2. Retrouver dans le paquet l'annonce de la route et ses attributs.
- Est ce que les routeurs R3 et R4 de l'AS 12 connaissent net1 ? Pourquoi ?

4.3.2 Connaissance de la route externe net1 dans l'AS 12

On peut redistribuer les adresses apprises par BGP dans le protocole interne OSPF. L'ensemble des machines d'un AS pourra ainsi connaître des routes apprises depuis l'extérieur.

Commande (sous `router ospf` *numéro_de_processus_OSPF*) :
`redistribute bgp` *numéro_AS* `subnets` (le mot-clé `subnets` évite les soucis si vous utilisez des sous-réseaux d'une classe d'adresses).
Vérifier que R3 et R4 connaissent maintenant net1.
Expliquer les informations apparaissant dans la table de routage de ces routeurs.

4.3.3 Diffusion automatique des adresses de l'AS 12 dans l'AS10

Il y a deux façon d'annoncer des adresses à l'extérieur d'un AS. Soit en les annonçant à la main comme précédemment (commande network), soit en redistribuant les adresses connues grâce au protocole de routage interne (OSPF ici) dans BGP. (commande —sous `router bgp`— `redistribute ospf` *numéro_AS*).

Cette dernière méthode n'est pas conseillée car dans ce cas BGP n'est pas sûr que ces adresses soient dans son système autonome (elles peuvent venir d'un autre AS et avoir été

introduites dans le protocole de routage interne par ailleurs). D'autre part, une telle redistribution tend à répercuter vers l'extérieur les évolutions (ou fluctuations) du routage interne, alors que la plus grande stabilité est recherchée au niveau de BGP.

4.3.4 Diffusion des adresses par la commande `network`

C'est la méthode à utiliser de préférence pour publier des préfixes dans BGP. *Enlever, le cas échéant, les redistributions de l'IGP dans BGP.*

- Lancer une capture sur net2
- Dans R2 annoncer les adresses net3 et net4 de l'AS12 (`network`).
- Analyser les paquets BGP émis entre R1 et R2
- Vérifier que R1 connaît maintenant net3 et net4
- Noter la table de routage BGP de R1.

4.4 Routage interne iBGP

On veut maintenant que les adresses de l'AS 12 soient aussi diffusées dans l'AS 14. On peut refaire la même manipulation que précédemment entre les routeurs R4 et R5.

On peut aussi configurer R2 de façon à ce qu'il passe ses informations à R4 pour que celui-ci les diffuse à l'extérieur. Pour cela il faut déclarer R2 et R4 voisins.

- Déclarer R2 et R4 voisins (`neighbor`)
  Vérifier que R4 a appris – via iBGP – les informations de routage BGP de R2
- Déclarer R4 et R5 voisins
- Noter et expliquer le contenu de la table BGP et de la table de routage des routeurs R4 et R5. Pourquoi le réseau net1 n'apparaît pas dans la table de routage de R5 ?

Pourtant net1 apparaît dans la table de routage de R4 avec comme routeur d'accès (next_hop) R1(sur net2). Le problème c'est qu'il n'a pas net2 dans sa table de routage. Si R4 diffusait net1 à R5, R5 lui passerait des paquets à destination de net1 qu'il ne saurait pas réexpédier. Il faut donc que R4 sache comment accéder à net2.

Il faut donc que net2 soit distribué par OSPF et appris via OSPF en R4. Attention il faut que l'interface externe de R2 soit passive pour OSPF (c'est à dire que des HELLOs ne sont pas émis vers l'extérieur !). On peut aussi (en plus) publier le préfixe de net2 par BGP, ce qui peut être fait par l'un ou l'autre des AS.

Important : La conclusion de cette manipulation, c'est que les liens externes doivent être connus du routage interne. Autrement dit, le périmètre du routage interne inclut les premières interfaces des AS voisins, mais il faut bien prendre garde de ne pas émettre le moindre paquet IGP vers l'extérieur !

Essayer et vérifier que R5 connaît bien net1.
Quel est le chemin associé à net1 pour R5 ?
Essayer un ping de R4 vers R1 et de R5 vers R1 ?Pourquoi le deuxième ne fonctionne pas ?
Résoudre le problème.

Utilisation des interfaces *loopback*

Il est d'usage d'utiliser les interfaces `lo` (*loopback*) (ou *discard*, pour des versions plus récentes de l'IOS) comme interface de communication entre les routeurs BGP *d'un même AS*.

En effet, cette interface est toujours ac tive (*UP*), ce qui permet aux communications entre routeurs de bordure d'un même AS de ne pas dépendre de l'état d'une interface précise. Les connexions TCP entre routeurs d'un même AS peuvent donc s'adapter aux changements de topologies au sein du système autonome grâce à la réactivité de l'IGP.

Mise en œuvre :

```
interface loopback 0
```

Configuration de l'interface : on lui associe une nouvelle adresse IP.

Faire en sorte que le voisinage entre R2 et R4 soit établi entre leurs interfaces *loopback* (ne pas oublier de supprimer le voisinage avec les interfaces ethernet).

Il faut également spécifier que les paquets de mise à jour doivent avoir pour origine l'interface `loopback`, de façon à ce qu'ils soient acceptés par le voisin.

```
neighbor Adresse_Internet update-source loopback 0
```

En utilisant la topologie de la figure 6, donner un scénario qui montre l'intérêt de l'utilisation de l'interface *loopback*, si la liaison directe entre R2 et R4 disparaît.

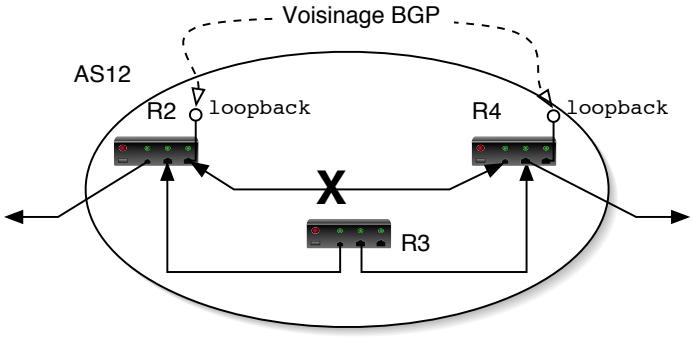

Figure 6 – Utilisation de l'interface *loopback*

Pourquoi cette méthode n'est pas utilisée pour les connexions entre routeurs voisins dans deux AS différents ?

Pourquoi les paquets BGP émis vers un voisin situé dans un AS différent ont un TTL de 1(champ de l'entête IP) ?

4.5 Sauvegarde des configurations

On peut sauvegarder ou restaurer des configurations à l'aide de fichiers sur les routeurs Cisco. Cela va nous permettre de ne pas refaire les configurations à la main sur les routeurs lors de séances de TP successives.

Utilisation de TFTP pour sauvegarder et modifier la configuration des routeurs CISCO TFTP (*trivial file transfer protocol*) est un protocole d'échange de fichiers similaire à FTP, mais qui met en œuvre le dialogue le plus simple possible entre l'émetteur et le récepteur. TFTP repose sur UDP, à la différence de FTP. Aucune session (login) n'est ouverte entre le client et le serveur. TFTP est utilisé en général pour configurer des machines à l'initialisation...

Avant toute chose il faut que la configuration soit écrite dans le fichier `startup-config` sur le routeur. Pour cela il suffit d'exécuter la commande `write`.

1. Configuration du serveur : le démon `tftpd` qui est le serveur du protocole TFTP doit être mis en route. En pratique, il suffit généralement d'ajouter («décommenter», en fait) une ligne du fichier `/etc/inetd.conf`, ceci afin que `inetd` démarre `tftpd`.

   L'option `-s` de `tftpd` permet de spécifier le répertoire racine des fichiers demandés ou passés au serveur. En général, c'est `/tftpboot` qui est utilisé... On peut utiliser `/tmp` si on veut.

   Il faut ensuite tuer `inetd` et le relancer (`inetd -wW`) afin qu'il prenne en compte les nouvelles directives lues dans `/etc/inetd.conf`.
2. Permettre l'upload d'un fichier Comme il n'y a pas de session ouverte par TFTP, il est nécessaire pour qu'un fichier puisse être «*uploadé*» qu'un fichier du même nom soit présent dans le répertoire de travail de `tftpd`. (Avec les droits en écriture pour tout le monde)
3. Copie routeur vers ordinateur :
   `ROUTER# copy startup-config tftp:` [le routeur pose ensuite les bonnes questions]

   Copie ordinateur vers routeur :
   `ROUTER# copy tftp startup-config`

Réaliser les sauvegardes des configurations des différents routeurs dans des fichiers. Sauvegarder ces fichiers sur votre compte de l'UFR IMA.

Il est possible de modifier la configuration de chaque routeur en éditant ces fichiers avec un simple éditeur de texte. Une fois la configuration rechargée sur le routeur, la commande `reload` permet de redémarrer le routeur en la prenant en compte.

4.6 Mise en place de filtres

Dans BGP il faut pouvoir filtrer à volonté des propagations de route. On veut par exemple ne pas vouloir propager vers un AS une route apprise depuis un AS précis. Ou bien encore on veut interdire à un AS de propager une route qu'on lui a passée.

Il existe pour cela trois méthodes de filtrage dans BGP :

- Par route(ou adresse) : on interdit la propagation par BGP d'une adresse ou d'un ensemble d'adresses.
- Par chemin : on interdit la propagation par BGP de l'ensemble des routes apprises depuis un AS ou une suite d'AS
- Par communauté : on interdit à un voisin de propager certaines routes qu'on lui a diffusées. Il faut alors avoir toute confiance en lui.

4.6.1 Filtrage par route

On peut affecter à chaque voisin une liste de permission / autorisation d'apprentissage / divulgation d'adresse.

La commande suivante permet d'affecter la liste d'accès de numéro *No* au voisin d'adresse IP_adresse et cela soit en entrée (apprentissage depuis ce voisin), soit en sortie (divulgation d'information vers ce voisin) : `neighbor` *IP_adresse* `distribute_list` *No* `in/out`

Les listes d'accès sont ensuite définies par la commande :
`acces-list` *No* `permit/deny` *adresse_IP bits_non_significatifs*
No est le numéro de la liste, *adresse_IP* est l'adresse à interdire/autoriser,

bits_non_significatifs permet de spécifier les octets représentatifs de l'adresse (à l'inverse des *netmask*, ici les bits indiqués sont ceux qui sont *non significatifs*.).

Par exemple :

```
acces_list 1 deny 160.10.0.0 0.0.255.255
```

Cette commande définit la liste d'accès numéro 1 qui interdit les adresses 160.10.255.255. On devra lui ajouter une autorisation de toutes les autres adresses par la commande :

```
acces_list 1 permit 0.0.0.0 255.255.255.255
```

À l'aide de ces commandes faire en sorte que l'AS 12 ne divulgue pas à l'AS10 l'adresse net6. Vérifiez que ce filtrage a bien eu lieu par des pings et la visualisation des tables de routage et tables BGP.

Interdire ensuite à R1 d'apprendre l'adresse net4 diffusée par R2.

Pour accélérer la prise en compte de ces suppressions de route, on peut utiliser la commande `clear ip bgp *`. On peut visualiser les listes d'accès par `show access-list` *No*

4.6.2 Filtrage par AS ou suite d'AS (*path*)

On peut définir un tel filtre grâce à la commande : `ip as-path access-list` *numéro* `deny/permit` *expression-regulière*

numéro est le numéro de la l iste d'accès.

expression-régulière permet de spécifier l'AS ou la suite d'AS. Elle se compose de numéro d'AS et de caractères spéciaux aux significations suivantes :

`^` : début de chemin

`$` : fin de chemin

`.` : n'importe quel caractère

`*` : un nombre quelconque de fois

On peut vérifier que l'expression est bonne grâce à la commande `show ip bgp regexp` *expression*.

Exemples :

```
ip as-path access-list 1 deny ^200$
ip as-path access-list 1 permit .*
```

`^200$` spécifie toutes les adresses venant directement de l'AS 200

`.*` spécifie tout AS (`.` : n'importe quel caractère, `*` : un nombre quelconque de fois)

`^200 300$` spécifie le chemin AS200 puis AS300 (source de l'annonce).

`^200.*` spécifie toute route dont le premier *hop* est l'AS 200 mais dont le chemin ultérieur peut être quelconque.

Supprimer les listes d'accès précédentes par `no neighbor` *IP_adresse* `distribute_list`.

Activer la liste de filtrage :

`neighbor` *IP_adresse* `filter-list` *No* `in/out`

A l'aide d'un filtrage par AS faire en sorte que R1 ne prenne pas en compte les adresses venant de l'AS12 mais qu'il prenne en compte celle venant de l'AS 14.

4.7 Choix entre des routes multiples

Dans le cas de routes multiples, on peut les pondérer de diverses manières afin de déterminer laquelle sera mise dans la table de routage par BGP. Cette pondération peut être locale à un serveur, local à un AS ou diffusée d'un AS à l'autre. Pour les diffusions de ces pondérations entre routeur BGP des attributs particuliers sont associées aux adresses transmises

dans les paquets BGP.

Le choix d'une route se fait suivant l'ordre des critères suivant :

1. Poids : cet attribut permet de spécifier vers quel voisin envoyer le trafic. Il est donc local au routeur.
2. Préférence locale (à un AS) : cet attribut est transporté par iBGP. Il permet de préférer tel ou tel routeur pour sortir d'un AS.
3. Longueur du chemin d'AS : on préfère utiliser le chemin le plus court en nombre d'AS traversés.
4. Origine : protocole interne préféré à un protocole externe : on ne connaît pas vraiment la longueur d'une route ne commençant pas par «i».
5. Métrique de BGP : cette métrique est communiquée avec le chemin d'AS, même aux voisins externes. Elle n'est rien de plus qu'une indication de la route à préférer, étant donné sa place assez basse dans la présente liste.
6. Métrique du protocole interne vers le Next hop

1. Informations locales à un routeur
   On peut associer un poids à un voisin par la commande
   `neighbor` *IP_adresse* `weight` *poids*
   Dans le cas de routes multiples le passage par le voisin de poids le plus élevé sera utilisé. Attention ce poids est une information qui n'est pas transmise de routeur en routeur. Elle sert à sélectionner les routes au niveau d'un routeur donné. À l'opposé, les méthodes de sélection suivantes (préférence et métrique) font partie du standard BGP et sont transportées par [i]BGP.

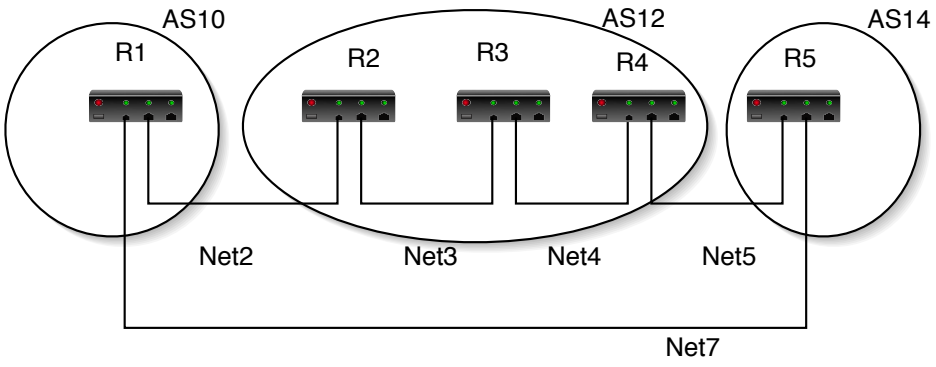

Figure 7 – Mise en place du réseau net7

Supprimer les listes précédentes.
Connecter les routeurs R1 et R5 par un réseau net7 d'adresse 7.0.0.0/8. Mettre en route le routage BGP sur ce lien.
Déclarer le réseau net7 par une commande `network` en R1 **et** R5. Regarder les tables de routages et les tables bgp des routeurs R2 , R3 e t R4.

Faire en sorte que le routeur 5 accède à net2 par le routeur R1 puis R4 si net3 est déconnecté par exemple.

2. Préférences locales à un AS

3. Informations entre AS
   Un AS va pouvoir influer sur les choix de ses voisins par la pondération des routes qu'il leur diffuse. C'est l'attribut METRIC qui permet de diffuser cette pondération

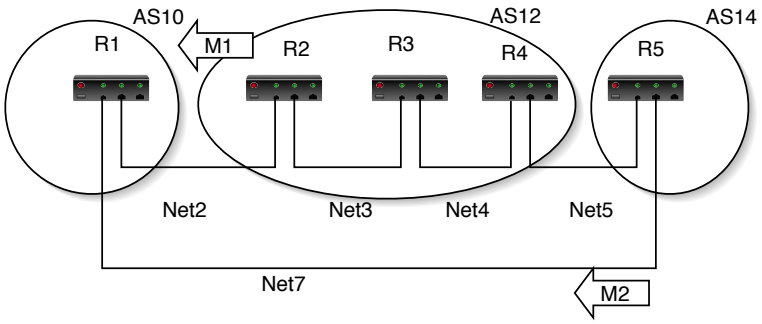

Figure 8 – Métrique BGP

entre AS. Il est appelé MED (Multi_Exit_Discriminator) dans BGP version 4 et INTER_AS dans BGP 3 (code 3). Cet attribut n'est pas transitif, il n'est pas propagé : l'indication n'est donc valable que pour les routeurs qui sont immédiatement connectés à un AS. Il permet à un AS d'associer une métrique à une destination qu'il diffuse à un autre AS. Un routeur qui reçoit différentes possibilités pour accéder une destination pren dra celle de métrique la plus faible. Un AS peut donc décider de la pondération qu'il associe à sa traversée par exemple. Les commandes suivantes permettent de spécifier cette pondération (pour toutes les adresses émises) :
`neighbor` *AS_voisin* `route-map` *ma_route-map* `out`
`route-map` *ma_route-map* `permit 10`
`set metric` *M1*
Faire en sorte que R2 et R5 annoncent des métriques différentes à R1 (métrique plus grande pour R2). Vérifiez que ces métriques sont respectées pour l'accès à net5 par exemple (il faudra pour cela qu'il existe deux chemins de même longueur, c'est à dire que net5 devra être publié par l'AS 12 et l'AS 14).

Attention : normalement les attributs METRIC ne sont comparés que s'ils proviennent d'un même AS (car il n'y a pas de raison *a priori* pour que deux AS se mettent d'accord sur une échelle de métriques). Pour que les métriques soient prises en compte, il faut donc spécifier `bgp always-compare-med`.

Dernière configuration :
Faire en sorte que les paquets émis depuis l'AS12 à destination de net7 passent par R5 et que les paquets en provenance de net7 à destination de AS12 passe par R2. En d'autres termes on voudrait que tous les paquets rentrent par R2 dans AS12 et sortent de l'AS12 par R5.
Vérifiez que cela fonctionne sur R2, R3 et R4.
Comment R3 a t-il appris ces contraintes BGP ?

BGP en vrai :

Le site de RIPE (Réseaux IP Européens) (adresse : http ://www.ripe.net/perl/whois) gère une base de donnée (appelée whois) qui donne pour chaque AS : les AS qui fournissent des routes et les AS auxquels sont fournies des routes. Aller consulter cette base de donnée avec AS2200 qui est le numéro d'AS de RENATER.

On a utilisé les numéros d'AS 10,12 et 14, mais les numéros pour usage privé sont de 64512 à 65534.