Mini Projet - Réseaux Avancés

Routage extérieur : BGP

Travail à réaliser :

Vous devrez rédiger un compte-rendu, qui contiendra :

- Des extraits pertinents des running-configuration des routeurs ou listings des commandes IOS utilisées
- Des extraits des tables de routage intra- (sh ip route) et inter- (sh ip bgp) domaines pertinentes
- Des extraits pertinents des captures de trames prises par wireshark
- Des sorties des commandes ping et traceroute

Principes de fonctionnement du protocole :

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. Dans un protocole de routage externe ce sont les routeurs aux frontières des AS, appelés routeurs de bordure, qui s'échangent les informations de routage. Le protocole de routage externe va permettre l'échange des adresses contenues dans les AS entre ces routeurs de bordure. Il va aussi propager des routes apprises de puis un autre AS. Le passage des informations de routage 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 en pouvant appliquer des restrictions décidées par l'administrateur de chaque AS. 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. Le protocole BGP repose sur TCP (port 179). Les échanges se font toujours entre 2 routeurs.

On peut distinguer 2 types de dialogue BGP :

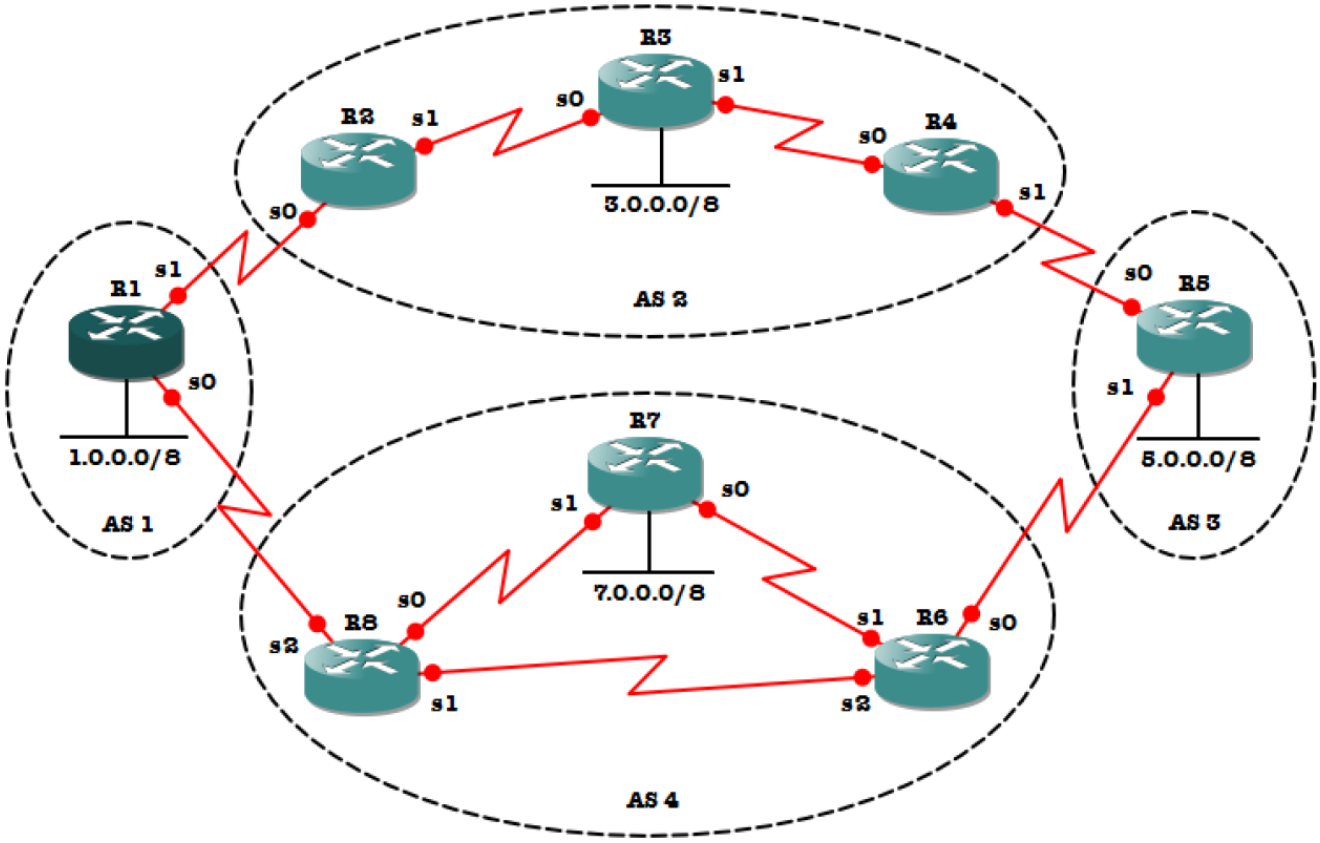
- Entre deux routeurs de bordure de deux AS différents, dénommé eBGP (external BGP).
- Entre les routeurs d'un même AS dénommé iBGP (internal BGP).

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 sur des réseaux différents. 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, ...

La topologie étudiée :

Avec GNS3, créez un nouveau réseau pour qu'il soit identique à la figure suivante :



La topologie est constituée de 4 Systèmes Autonomes (AS 1 à 4). Les routeurs R1, R2, R4, R5, R6 et R8 étant des routeurs de bordure qui devront prendre en charge le routage BGP. Chaque AS comporte un réseau interne (Un seul PC par réseau interne suffit pour la simulation) qui devra être rendu accessible de l'extérieur par le protocole BGP.

Pour faciliter la mise en œuvre, tous les réseaux (Ethernet ou lien entre routeurs) ont un masque de /8 (classe A) et doivent êtres configurés selon l'adressage mnémotechnique suivant :

- 1.0.0.0/8 sur l'interface Ethernet de R1 (préfixe réseau 1 noté **LAN1**)
- 12.0.0.0/8 entre R1 et R2
- 18.0.0.0/8 entre R1 et R8
- 23.0.0.0/8 entre R2 et R3
- 3.0.0.0/8 sur l'interface Ethernet de R3 (préfixe réseau 3 noté **LAN3**)
- 34.0.0.0/8 entre R3 et R4
- 45.0.0.0/8 entre R4 et R5
- 5.0.0.0/8 sur l'interface Ethernet de R5 (préfixe réseau 5 noté **LAN5**)
- 56.0.0.0/8 entre R5 et R6
- 67.0.0.0/8 entre R6 et R7
- 68.0.0.0/8 entre R6 et R8
- 7.0.0.0/8 sur l'interface Ethernet R7 (préfixe réseau 7 noté **LAN7**)
- 78.0.0.0/8 entre R7 et R8

Pour simplifier, les interfaces (séries ou Ethernet) d'un routeur Ri doivent êtres configurées avec la terminaison .0.0.i. Par exemple, le routeur R5 a 3 interfaces actives : L'interface Ethernet, d'adresse IP 5.0.0.5 sur le réseau 5.0.0.0/8 Serial0, d'adresse IP 45.0.0.5 sur le réseau 45.0.0.0/8 Serial1, d'adresse IP 56.0.0.5 sur le réseau 56.0.0.0/8

Sauvegarder la configuration de chaque routeur avec *copy run start*. Ensuite dans GNS3 sauvegardez votre projet complet.

Démarrez Wireshark sur les liens R1-R2, R1-R8, R6-R8 et R7-R8 pour observer les paquets échangés (encapsulation HDCL)

I – Configuration du routage dynamique intérieur dans les AS 2 et AS 4

1. Configurez un routage intra domaine dynamique en utilisant RIPv2 dans l'AS 2 et OSPF dans l'AS 4 (une seule aire). Pensez à déclarez au besoin les réseaux Ethernet et également les réseaux sortant vers les autres AS (interface passive).
2. Vérifiez vos configurations en contrôlant les tables de routages des routeurs de l'AS 2 et l'AS 4.

II – Configuration du routage BGP intérieur dans les AS2 et AS4

1. Activez BGP sur les routeurs R2 et R4 de l'AS 2 avec *(config) router bgp* et configurez R2 et R4 comme voisins intra-AS avec *(config-router) neighbor*.
2. Annoncez en BGP sur R2 le réseau 3.0.0.0 interne à l'AS 2 avec *(config-router) network*
3. Affichez la table BGP de R2 avec *show ip bgp*. Que valent les attributs *Weight* et *LocPrf* pour la route vers ce réseau ? Expliquez.
4. Affichez après mise à jour la table BGP de R4. Comment apprend-il la route BGP vers le réseau 3.0.0.0 ?
5. Que valent les attributs *Weight* et *LocPrf* pour la route BGP sur R4 vers le réseau 3.0.0.0 ? Expliquez.
6. Annoncez en BGP sur R4 le réseau 3.0.0.0 et réinitialisez sa table BGP avec la commande *clear ip bgp* *
7. Réaffichez la table BGP de R4. Que constate-t-on ? Pourquoi a-t-on deux routes vers le réseau 3.0.0.0 ? Commentez les attributs de chacune des routes et le choix de la route principale.
8. Réaffichez ensuite la table BGP de R2 et commentez également les informations de chacune vers le réseau 3.0.0.0.
9. Activez BGP sur les routeurs R6 et R8 de l'AS 4, configurez-les comme voisins intra-AS et annoncez-y le réseau 7.0.0.0
10. Vérifiez au bout de quelques instants la présence de routes dans les tables BGP de R6 et R8 et commentez-les.

III – Configuration du routage extérieur BGP (inter-AS)

1. Activez BGP sur les routeurs R1 et R5 des l'AS 1 et 3. Déclarez tous les voisins inter-AS nécessaires sur toute la topologie.
2. Annoncez en BGP sur R1 le réseau 1.0.0.0 interne à l'AS 1 et sur R5 le réseau 5.0.0.0 interne à l'AS 3.
3. Observez les échanges de messages avec Wireshark et suivez les évolutions des tables de routage internes (*show ip route*) et externes (*show ip bgp*) sur tous les routeurs BGP jusqu'à leur stabilisation.
4. Répertoriez alors toutes les routes existantes vers les différents LANs depuis les différents routeurs BGP. Y-a-t-il des routes manquantes ? sur quels AS est en direction de quels LANSs ?
5. Effectuez une recherche sur Internet pour expliquer les absences de routes précédentes.
6. Apportez les modifications nécessaires aux routeurs R2, R4, R6 et R8 et vérifiez l'apparition des routes manquantes.
7. Quel est alors le chemin pour atteindre LAN5 à partir de LAN1 ?
8. R3 et R7 connaissent-il des routes vers les réseaux LAN1, LAN3, LAN5 et LAN7 (vérifiez avec show ip route) ? Pourquoi ?
9. Redistribuez les routes BGP vers OSPF dans l'AS 4 sur R6 et R8 : *(router-ospf) redistribute bgp num_AS*

10. Redistribuez les routes BGP vers RIP dans l'AS 2 sur R2 et R4 : *(router-rip) redistribute bgp num_AS (router-rip) default metric 15*
11. Observez les résultats sur R3 et R7 avec *show ip route*
12. Vérifiez que vous pouvez pingez le réseau LAN5 depuis le réseau LAN1 (tapez sur R1 la commande *ping* sans argument et donnez comme adresse de destination l'adresse de loopback de R5 et comme adresse source l'adresse de loopback de R1)

IV – Détermination de nouveaux chemins

1. Désactivez le lien R5-R6 et observez les échanges de messages avec Wireshark et l'évolution des tables de routage.
2. Pingez LAN5 à partir de R1 par leurs adresses de loopback . Combien de temps faut-il pour récupérer la connectivité ?
3. Quel est le nouveau chemin pour atteindre LAN5 à partir de LAN1 ? (analysez les messages Update BGP sous Wireshark)
4. Même questions en réactivant le lien R5-R6 (attendre le rétablissement) et en désactivant le lien R6-R8.
5. Désactivez le réseau loopback LAN5 et observez les échanges de messages avec wireshark et l'évolution des tables de routage.

V – Configuration de politique de routage BGP

Filtrage par route :

On peut affecter à chaque voisin une liste de permission d'apprentissage ou divulgation de préfixes. On peut affecter la liste d'accès de numéro *num* au voisin d'adresse *IP@* et cela soit en entrée (apprentissage depuis ce voisin), soit en sortie (divulgation d'information vers ce voisin) avec *neighbor IP@ distribute-list num in/out*

Les listes d'accès sont ensuite définies par *access-list num permit/deny IP@ wild_card_mask*. Par exemple *access-list 1 deny 160.10.0.0 0.0.255.255*.

On devra lui ajouter une autorisation de toutes les autres adresses par la commande *access-list 1 permit 0.0.0.0 255.255.255.255.*

Pour accélérer la prise en compte de ces suppressions de route, on peut nettoyer les tables avec *clear ip bgp* *. On peut visualiser les listes d'accès avec *show access-list num*

Filtrage par AS ou AS path :

On peut filtrer la propagation par BGP de l'ensemble des routes apprises depuis un AS ou une suite d'AS avec *ip as-path access-list num deny/permit regu-expr* où « *regu-expr* » (expression régulière) permet de spécifier un AS ou un chemin d'AS. Elle se compose de numéros 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 avec *show ip bgp regexp regu-expr*.

Exemples :

- ^200$ (toutes les adresses venant directement de l'AS 200)
- .* (spécifie tout AS)

- ^200 300$ (spécifie le chemin AS300 (source) puis AS200)
- ^200.* (spécifie toute route passant en dernier lieu par l'AS 200 mais dont le chemin antérieur peut être quelconque)

Gestion 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, locale 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
2) Préférence locale (à un AS)
3) Longueur du chemin d'AS
4) Origine : protocole interne préféré à un protocole externe
5) Métrique de BGP
6) Métrique du protocole interne vers le next hop

Poids : Informations locales à un routeur

On peut associer un poids à un voisin avec *neighbor IP@ weight wgt*

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) sont transportées par BGP.

Préférences locales : à un AS Cette information est stockée dans les messages dans l'attribut LOCAL PREF des paquets BGP, son code est 5. Par défaut cet attribut vaut 100. Un routeur diffusant l'attribut LOCAL PREF le plus grand pour une destination sera choisi pour l'atteindre. Il permet ainsi de privilégier une entrée/sortie d'un AS par rapport à une autre.

La commande *bgp default local-preference value* peut être utilisée pour changer cet attribut pour toutes les adresses diffusées depuis un routeur. D'autres commandes permettent de spécifier cet attribut seulement pour certaines routes en utilisant des listes d'accès.

Métrique de BGP : 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 entre AS. Il est appelé MED (Multi Exit Discriminator).

Métrique du protocole interne vers le next hop : 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 prendra 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 IP@ route-map my-route-map out
route-map my-route-map permit 10
set metric m1

Réseau avec chemins multiples et routage politique :

1. On considère le réseau avec tous les liens opérationnels. Implémentez un filtrage par route sur les préfixes LAN3 et LAN7 afin qu'ils ne soient pas connus des AS 1 et 3. Vérifiez que ce filtrage a bien eu lieu par des pings et la visualisation des tables de routage et tables BGP.

2. Supprimez les listes d'accès précédentes par *no neighbor IP@ distribute-list*. Activer la liste de filtrage par AS avec *neighbor IP@ filter-list num in/out*. Définissez un filtrage par AS dans l'AS 3 afin que R5 ne prenne pas en compte les adresses venant de l'AS 2 mais qu'il prenne en compte celle venant de l'AS 4. Est-ce que LAN1 est visible dans R5 ?

3. Supprimez le filtrage précédent. L'AS 3 souhaite que le trafic avec l'AS 1 passe (dans les deux sens) de préférence par l'AS 2 mais en gardant la connectivité par l'AS 4 en cas de coupure avec l'AS 2. Configurez la politique de routage de l'AS 3 en conséquence et vérifier son bon fonctionnement dans tous les cas.

4. Modifiez maintenant la politique de l'AS 3 afin que le trafic sortant à destination du réseau LAN1 passe via l'AS 2 et que le trafic entrant en provenance du LAN1 passe via l'AS 4. Comment R3 et R7 ont-ils appris ces contraintes BGP ? Vérifiez le bon fonctionnement de la politique de routage dans tous les cas et si besoin corrigez la configuration.

5. Configurez 2 préfixes supplémentaires LAN11 et LAN12 dans l'AS 1 et modifiez la politique de l'AS 3 afin que le préfixe LAN11 soit accessible de préférence via l'AS 2, le préfixe LAN12 de préférence via l'AS 4, et le préfixe LAN1 uniquement par l'AS 4. Vérifiez le bon fonctionnement de la politique de routage dans tous les cas et si besoin corrigez la configuration.