TP BGP

Objectifs du TP	
1	Comprendre le fonctionnement de BGP
2	Comprendre une configuration simple de BGP pour un AS de transit
3	Comprendre une configuration simple de BGP pour un AS souche

1 Présentation du TP

Ce TP a pour but d'illustrer le fonctionnement de BGP dans un cas simple mais néanmoins réaliste. Afin de créer un topologie intéressante et de permettre à chacun de manipuler et d'obtenir la maitrise de la configuration du protocole, nous avons fait le choix d'utiliser des machines virtuelles pour ce TP. Ces machines, routeurs et hôtes, seront *émulées* au moyen du logiciel *Marionnet* qui permet de définir une topologie réseau, constitué de machines Linux.

Chaque machine est constitué d'un noyau Linux UML * et d'un système de fichier. Les routeurs que nous utiliseront seront donc des machines Linux avec plusieurs interfaces et faisant tourner le logiciel *Quagga*, qui permet de configurer et d'administrer les protocoles de routage BGP, OSPF, RIP et IS-IS. *Quagga* a l'avantage de présenter une interface de configuration proche des routeurs CISCO via un shell nommé *vtysh*.

Dans le cadre de ce TP, la topologie du réseau a été crée pour vous sous forme d'un projet *Marionnet* que vous chargerez puis configurerez selon les besoins avant de démarrer les machines virtuelles.

1.1 Topologie

Chaque binôme administrera deux AS, l'un sera un AS de transit offrant une connectivité à l'autre AS, qui sera donc un AS souche. La figure 1 montre la topologie du réseau dont vous serez les administrateurs. Les deux AS sont délimités par les marques en pointillé. La prise Ethernet représenté à gauche de la figure représente la liaison entre l'AS de transit et un point de peering. Dans les faits, cette prise sera relié à un VLAN du réseau réel de la salle et vous permettra de vous interconnecter avec les AS des autres binômes.

∗. UML : User Mode Linux, un mode de compilation du noyau Linux qui permet de lancer un noyau complet comme un processus utilisateur

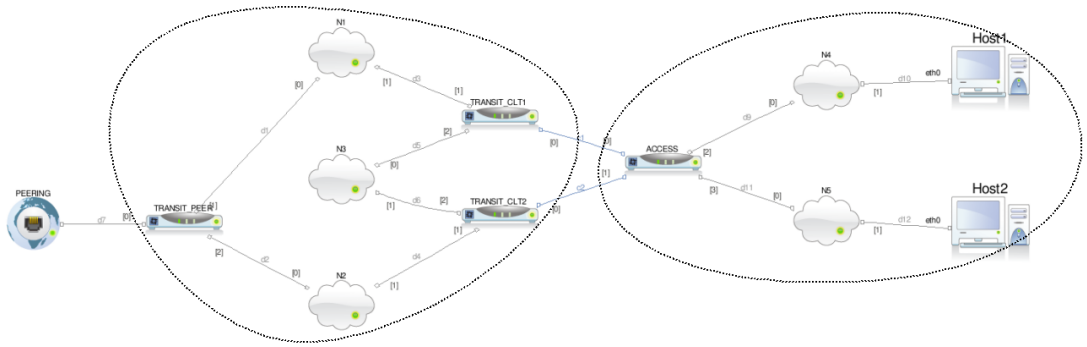

FIGURE 1: Topologie du réseau

2 Mise en place

Avant de commencer à manipuler les routeurs, vous devrez mettre en place l'environnement d'émulation puis réaliser un plan d'adressage et configurer *Marionnet* en conséquence.

2.1 Lancement de *Marionnet*

Pour lancer *Marionnet* utilisez l'icône (main qui tient des ficelles de marionnette) dans la barre de lancement en haut de l'écran.

Copiez tout d'abord le fichier `/home/marionnet/TP_BGP/TP_BGP.mar` sur votre compte. Vous pouvez maintenant charger le projet utilisé dans ce TP en utilisant le menu fichier→ouvrir.

2.2 Adressage

Pour réaliser ce TP, il vous faudra définir un plan d'adressage pour vos AS. Afin de synchroniser tout le monde et d'éviter d'avoir plusieurs adressages qui se chevauchent, nous simulerons une autorité de distribution des numéros et adresses (similaire à l'IANA et au différents RIRs ... en plus petit et avec moins de paperasse). Vous devrez donc aller faire enregistrer vos numéros d'AS et vos préfixes d'adresses auprès des professeurs AVANT de définir le plan d'adressage détaillé.

Chaque binôme disposera d'un préfixe de longueur 8 pour son réseau de transit et d'un préfixe de longueur 16 pour son réseau client. Utilisez les nombreuses adresses à votre disposition afin de simplifier la tâche de définition du plan d'adressage (en d'autres termes, inutile de créer des sous-réseaux dimensionnés au plus juste, utilisez des préfixes de longueur multiple de 8).

Une fois les préfixes d'adresse et vos numéros d'AS enregistrés, réalisez un plan d'adressage complet de votre réseau.

Dessinez (ou copiez) la topologie de votre réseau avec les informations d'adressage, les numéros d'AS, ainsi que les numéros d'interfaces des machines.

Point de vérification 1

Configurez ensuite les adresses de vos machines dans l'onglet **interfaces** de *Marionnet*. Pensez à renseigner les adresses de broadcast et les netmask.

Dans le cas des routeurs *TRANSIT_PEER* qui seront reliés les uns aux autres via in vlan du réseau réel, *Marionnet* leur attribue une adresse MAC de façon automatique. Cependant cette

adresse sera la même pour tous les routeurs, ce qui pose problème. Il vous faudra donc modifier votre adresse de façon à ce qu'elle soit unique sur ce réseau de peering.

2.3 Lancement des machines

Vous pouvez maintenant démarrer toutes vos machines en cliquant sur **Démarrer tout** dans *Marionnet*. Pensez à laisser le temps à tout les systèmes de démarrer avant de continuer.

3 Manipulations

Une fois l'environnement d'émulation configuré et les machines lancées, vous pourrez interagir avec chacune au moyen d'une connexion `ssh`. Si vous devez relancer une machine utilisez les options de démarrage et d'arrêt de *Marionnet* (demandez à un professeur).

Les manipulations se dérouleront en plusieurs parties. Le but final étant d'avoir une interconnexion entre tous les binômes reliés à un point de peering, vous veillerez à vérifier l'état d'avancement des autre binômes reliés au même réseau de *peering* que vous, et à vous synchroniser entre chaque étape afin que tout le monde puisse avancer au même rythme.

3.1 Configuration de l'AS de transit

Vous commencerez par configurer BGP dans votre AS de transit. Pour cela, lancez l'interpréteur de commandes de *Quagga* : `vtysh`.

Une fois dans ce shell, vous pouvez utiliser la plupart des commandes *CISCO* (`show run`, `show ip route`, ...). Vous disposerez aussi de l'aide en ligne (`?`) et de la complétion automatique (touche `<tab>`).

Commencez par attribuer un identifiant unique à chacun de vos routeurs (en prenant une de leurs adresses IP) avec la commande **router-id**. Pensez à passer en mode configuration avant (**configure terminal**).

Vous pourrez maintenant passer à la configuration de BGP. Les commandes utiles sont :

— `router bgp <numero d'as du routeur local>` – Passer en mode configuration de BGP
— `neighbor <adresse ip du voisin> remote-as <numéro d'as du voisin>` – Déclarer un voisin BGP du routeur, à répéter pour chaque voisin
— `network <préfixe à annoncer en notation CIDR>` – Déclarer un réseau via BGP

Configurez vos routeurs de façon à ce qu'ils connaissent leurs voisins et qu'ils annoncent leur réseau (le /8 de votre AS de transit). Chaque routeur du réseau de transit sera voisin de tous les routeurs auxquels il est directement rattaché (y compris en interne). Le routeur TRANSIT_PEER sera notamment voisin des deux routeurs TRANSIT_CLT et des routeurs TRANSIT_PEER des AS voisins.

3.1.1 Vérification de la configuration BGP

Afin de vérifier que la configuration est correcte, vous utiliserez les commandes `show ip route`, `show ip bgp`, `show ip bgp neighbors` et `show ip bgp <préfixe CIDR>` (ces commandes sont disponibles hors du mode config). Vous répondrez ensuite aux questions suivantes.

Quels sont les prefixes BGP annoncés par les autres routeurs au routeur TRANSIT_PEER ?

Point de vérification 2

Pour un préfixe annoncé par plusieurs voisins, expliquez le choix fait par BGP pour sélectionner la route à placer dans la Loc-RIB.

Point de vérification 3

Notez vous un problème dans la diffusion des préfixes vers les routeurs TRANSIT_CLT ? Décrivez le et expliquez sa cause.

Point de vérification 4

3.2 Distribution des routes par un IGP

Afin de résoudre le problème précédent, nous allons déployer le protocole OSPF dans le réseau de transit. Les routeurs utiliseront OSPF pour annoncer les routes directement rattachées sur chacun des réseaux internes.

La configuration d'OSPF se fera en recopiant et modifiant les lignes suivantes (vous remplacerez les réseaux par les réseaux internes rattachés à votre routeur) :

```
router ospf
redistribute connected
network 153.0.1.0/24 area 0
network 153.0.3.0/24 area 0
```

Configuration 1: Activation d'OSPF dans les routeurs de l'AS de transit

Vérifiez à nouveau la configuration de BGP sur tous les routeurs. Le problème est il résolu ?

Point de vérification 5

3.3 Configuration de l'AS client

Réalisez maintenant la configuration BGP du routeur de l'AS client avec les mêmes commandes que pour les routeurs de l'AS de transit.

Vous penserez à donner un identifiant unique à votre routeur.

Est il nécessaire d'activer OSPF dans cet AS ? Pourquoi ?

Point de vérification 6

De quelles pannes BGP protège t'il l'AS client ?

Point de vérification 7

Testez maintenant la connectivité de bout en bout avec les commandes *ping* et **traceroute** lancées depuis les machines terminales.

Cela fonctionne t'il ? Pourquoi ?

Point de vérification 8

Résolvez éventuellement le problème puis vérifiez le bon fonctionnement.

3.4 Filtrage des annonces de routes BGP (optionnel)

Nous allons maintenant voir les mécanismes de filtrage d'annonce des routes offert par BGP. Cette fonctionnalité est très puissante et nécessaire dans l'Internet tant pour des raisons de performance que de sécurité.

Dans ce TP nous ne verront qu'une partie de cette fonctionnalités, notez toutefois que l'on peut filtrer les routes annoncées par leur préfixe en entrée comme en sortie et que les possibilités de cet outil sont dictées par l'implémentation de BGP utilisée.

Notez vous sur les routeurs TRANSIT_PEER des routes annoncées qui ne sont issues de votre réseau ? Peuvent elles poser problème ?

Point de vérification 9

Nous allons filtrer les routes annoncées par le routeur TRANSIT_PEER afin de n'annoncer que les réseaux de l'AS de transit et de son client. Pour cela il vous faudra définir un filtre de préfixe puis l'associer aux annonces vers les voisins externes à l'AS.

La définition d'un filtre de préfixe se fait grâce à la commande `ip prefix-list`. Chaque nouvelle règle ajouté à un même filtre sera exécuté dans l'ordre jusqu'à déclenchement d'un règle.

Vous autoriserez donc d'abord l'annonce de vos préfixes (2 règles) puis vous interdirez toutes les autres annonces.

Pour associer ce filtre aux annonces faites à vos voisins, dans la configuration du routeur BGP, utilisez la commande `neighbor <adresse IP du voisin> prefix-list <nom du filtre> out`.

Notez et expliquez les commandes de définition du filtre de préfixe. Que signifie *out* dans la ligne de commande d'association du filtre avec le voisin ?

Point de vérification 10

Vérifiez avec les AS voisins le bon fonctionnement du filtre.

Point de vérification 11