Projet Mini-Internet

L. Vanbever, T. Bühler, R. Birkner, T. Holterbach, C. Busse-Grawitz
de l'Institut Fédéral des Technologies de Zurich (ETH-Zurich)
Adapté et traduit par C. Colombo pour Polytech Nancy

5 septembre 2022

Table des matières

1 Introduction

Dans ce projet, vous et les autres groupes allez construire et opérer votre propre Internet. Le but principal est d'établir une connectivité de bout-en-bout à travers des Autonomous Systems (AS) composés de différents équipements réseau. Vous devrez utiliser des techniques classiques de commutation et de routage. Vous ferez face aux défis typiques d'un fournisseur d'accès Internet. Ce projet a été créé par l'ETH-Zurich [1] à travers une initiative Open Source.

Afin d'établir une connectivité complète, autrement dit un Internet fonctionnel, vous devrez configurer votre réseau interne avant de vous connecter à d'autres AS, gérés par d'autres étudiants. Au sein de votre AS, vous utiliserez notamment le Spanning Tree Protocol (STP) et Open Shortest Path First (OSPF). Entre les AS, vous utiliserez le standard d'Internet : Border Gateway Protocol (BGP). À la fin du projet, tous les hôtes devraient pouvoir communiquer, indépendamment de leur AS d'origine.

L'infrastructure du projet est virtuelle, constituée de commutateurs niveau 2 Open vSwitch [2] et de routeurs utilisant la suite logicielle FRRouting [3]. Ces équipements virtuels sont portés par des conteneurs Docker, et déjà connectés entre eux. Vous devrez les configurer en ligne de commande.

Au début du projet, chaque groupe se verra attribuer un numéro, qui servira à identifier sa position dans la topologie globale, et qui servira à définir certains paramètres d'adressage.

La partie 2 présente les consignes générales du projet. Des éléments de cours vous sont présentés dans la partie 3. Vous devrez compléter avec vos propres recherches et observations du projet. La partie 4 présente les différents niveau de topologie utilisés dans le sujet. La partie 5 vous indiquera dans l'ordre les différentes parties du projet et les réalisations attendues. La partie 6 vous donnera les consignes techniques pour accéder à la plateforme, configurer vos équipements, sauvegarder... Enfin, la partie 7 est à destination des instructeurs, contient des informations sur l'installation, la configuration et le débuggage de la plateforme.

2 Consignes

2.1 Livrables attendus

Pour ce projet, vous devez rendre un rapport au format PDF, de maximum 15 pages A4 numérotées, sans annexes, comprenant les différentes captures. Votre fichier devra être nommé "`groupX_rapport_MiniInternet.pdf`", avec X le numéro de votre groupe.

La structure attendue est la suivante :

- 1 page de garde
- Un sommaire et une introduction
- 4 à 6 pages pour la partie Connectivité Intra-domaine
- 4 à 6 pages pour la partie Configuration BGP globale
- 2 à 3 pages pour la partie Policy-routing
- Une conclusion sur le projet, ce que vous en avez retenu
- Une page pour un résumé en Anglais

La notation tiendra compte du contenu, du respect des consignes, de la lisibilité... Vous pouvez utiliser les modèles Polytech.

De plus, vous devrez remettre vos configurations. Un script vous permettra d'exporter vos configurations en un fichier zip, qui devra être nommé "`groupX_configs.zip`", avec X le numéro de votre groupe. Si vos instructeurs divisent le projet en plusieurs périodes, vous devrez remettre un rapport intermédiaire ainsi que vos configurations. Le rapport intermédiaire est une version incomplète du rapport final, il n'est pas nécessaire (ni judicieux) d'y ajouter une conclusion.

2.2 Durées estimées

Le projet est divisé en trois grandes parties, équivalentes en charge de travail, mais de complexité croissante :

5.1 Prise en main de la plateforme, configuration Intra-domaine ;

5.2 Mise en place de la connectivité Internet et découverte du protocole BGP ;

5.3 Mise en place des relations réelles, de la hierarchie des AS et du filtrage via Policy-Routing.

Chaque partie vous prendra une dizaine d'heure de pratique, et deux heures de rédaction du rapport.

2.3 Code de conduite

Vous verrez que certaines parties de vos travaux peuvent être réutilisées par d'autres groupes. Nous attendons de vous que vous ne partagiez pas vos configurations. Vous pouvez bien sûr discuter, vous entraider, mais vous devez travailler par vous même.

Pour le projet, vous avez à votre disposition une infrastructure réseau complète sur laquelle vous êtes libre de configurer vos équipements. Il est interdit de configurer autre chose que ce qui est demandé dans ce document. Étant donné que tous les groupes sont connectés, vos expériences pourraient compromettre le projet pour d'autres groupes. Vous êtes libres de tester différentes configuration, voire certains protocoles, mais vous devez prévenir les instructeurs, et vérifier que vous n'allez pas impacter le projet.

Enfin, gardez à l'esprit que vous n'êtes pas propriétaire du réseau et de la plateforme sur lesquels vous allez travailler. Vous êtes soumis à la loi Française "Loi 88-19 du 5 janvier 1988 relative à la fraude informatique", et au règlement de l'Université de Lorraine et de Polytech Nancy. Toute action, directe ou indirecte, qui préviendrait le fonctionnement du système ou qui modifierait des informations sans autorisation pourrait mener à des actions légales.

3 Élements de cours

3.1 Les Autonomous Systems (AS)

On peut décrire Internet comme un réseau d'accès général à un ensemble de services : Web, Mails, Téléphonie, DNS... Du point de vue utilisateur final, l'accès Internet se présente sous la forme de notre Fournisseur d'Accès Internet (FAI) ou Internet Service Provider (ISP), en ADSL, VDSL, FTTH, 3G/4G/5G, sur un Wi-Fi public... Nous allons ici nous intéresser au fonctionnement du réseau qui permet la connectivité via ces points de présence.

Vous connaissez déjà des protocoles de routage classiques comme OSPF ou RIP. Ce genre de protocoles étaient à l'origine des réseaux, mais avec l'agrandissement d'Internet le nombre de route a explosé. Internet vient à l'origine d'Inter-Network, c'est le réseau qui regroupe tous les réseaux. Une nouvelle architecture à été mise en place : les Autonomous Systems (AS).

Un AS est un ensemble de réseaux informatiques intégrés à Internet. Les ISP sont un exemple typique d'AS. Les AS possèdent un plan de routage interne, qui peut être implémenté via différents protocoles qu'on nomme Interior Gateway Protocol. Il peut s'agir d'OSPF, RIP, IS-IS... Et ils permettent la communication au sein d'un AS. Les AS sont identifiés par un nombre, et portent des préfixes IP, correspondant aux sous-réseau qu'ils contiennent.

Chaque AS dispose d'un numéro, distribué par un Registre Internet Régional (RIR). Tous comme pour les adresses IP publiques ou les noms de domaines c'est l'Internet Assigned Number Authority (IANA) qui est au sommet de la hiérarchie des registres. Les RIR sont des entités qui ont une délégation de l'IANA pour une zone géographique. En Europe, Moyen Orient et Asie du Nord, c'est le RIPE NCC (Réseaux IP Européens Network Coordinaction Center) qui gère les numéros d'AS et les adresses IP publiques.

En 2019, l'IANA enregistre 91 000 AS. De même, la Global Routing Table (GRT), c'est-à-dire l'ensemble des réseaux déclarés sur Internet, contient plus de 850 000 routes IPv4 en 2020. Pour assurer la communication entre les AS, et donc construire l'Internet, il n'est heureusement pas nécessaire de se connecter à chacun des AS ou de connaître toutes les routes.

3.2 La hiérarchie des AS

Internet se base sur une architecture hiérarchique : des AS fournissent un accès à d'autres AS qui connaissent moins de routes. De manière similaire à la passerelle d'un LAN, il suffit de connaître une route vers l'AS qui se trouve au dessus du notre pour pouvoir aller n'importe où sur Internet. Les Tiers Internet décrivent la position d'un AS dans la hiérarchie d'Internet. Il ne s'agit pas de définitions venant d'un standard, mais de la pratique :

- Les AS Tier 1 sont définies comme la colonne vertébrale d'Internet, les points où tous les autres AS se connectent. Ils ne comprennent pas d'utilisateurs, il s'agit de points de transit pour d'autres AS. Ce sont généralement des infrastructures à très large capacité avec d'excellentes performances.
- Les AS Tier 3 sont les AS de bordure d'Internet, qui acheminent le trafic vers les utilisateurs. On les appelle parfois "Stub AS" (en Français : le bout, le talon, le moignon). Aucun trafic ne transite d'un AS vers un autre à travers un Tier 3. Un Tier 3 est toujours source ou destination d'un trafic.
- Les AS Tier 2 sont entre les deux : généralement plus larges qu'un Tier 3, ils autorisent le trafic de transit, et fournissent un accès Internet à des utilisateurs.

Les AS peuvent être connectés entre eux directement, ou à travers un Internet eXchange Point (IXP). Il s'agit de points de rencontre ou de nombreux AS peuvent s'interconnecter. Un sorte de commutateur pour AS. Que ce soit directement ou à travers un IXP, les AS peuvent se connecter de deux manières :

- Les liaisons de peering, sur lesquelles deux AS peuvent échanger uniquement leurs trafics respectifs ;
- Les liaisons de transit aussi appelées Provider/Customer, Fournisseur/Client qui peuvent être utilisées pour des communications directes ou du trafic de transit d'autres AS.

3.3 BGP

Pour interconnecter les AS, et ainsi connecter l'Internet, le Border Gateway Protocol (BGP) a été créé. C'est un protocole de couche 4 d'échange d'informations de routage. Il ne dispose pas de mécanisme d'annonce et de découverte de voisins, comme c'est le cas par exemple dans OSPF. Il faut déclarer tous les voisins manuellement en configuration. En ligne de commande, on rencontre souvent le terme de "neighbor", mais attention, des voisins n'ont pas besoin d'être directement connectés. On parle généralement de "Peer", car le terme est un peu moins trompeur

Une fois un peering déclaré, les peers s'échangent une seule fois un ensemble de route. On peut configurer BGP pour échanger les routes connectées, les routes apprises par un protocole donné, des préfixes spécifiques ou l'intégralité de la Routing Information Base (RIB). Les peers BGP au sein d'un AS ne propagent pas les routes apprises, contrairement aux peering inter-AS.

Lorsque les peers BGP ont échangé les routes souhaitées, ils ne procèdent ensuite que par mise-à-jour. À moins de recharger le peering, les tables complètes ne sont jamais réémises pour économiser l'overhead de communication.

BGP est un protocole dit "Path Vector", c'est-à-dire qu'il propage l'intégralité du détail d'une route (Path), et non pas juste le prochain saut (Vecteur de distance) ou une vision de la topologie (État de lien).

Le routeur utilisant le protocole BGP possède une RIB complète, avec plusieurs routes possibles, mais n'utilise que la meilleure pour chaque réseau dans sa table de routage. La route considérée la meilleure est celle traversant le moins d'AS possible. On parle de "Shortest-AS Path".

On distingue deux utilisations du protocole BGP : External BGP (eBGP) et Internal BGP (iBGP). Il s'agit du même protocole et des mêmes méthodes de configuration. L'eBGP sert à connecter des routeurs d'AS différents, pour échanger de nouvelles routes, alors que l'iBGP sert à connecter des routeurs d'un même AS pour propager ce qui a été appris par les routeurs de bordure en eBGP, généralement vers d'autres routeurs de bordure.

Au delà de la configuration d'un peering BGP, il est souvent nécessaire de filtrer ou de marquer les routes apprises ou envoyées. Le filtrage se fait à l'aide de Route-map/Route-policy, et le marquage à l'aide d'un tag qu'on appelle "Community". Les Route-map/Route-policy peuvent se baser sur l'adresse de la route, la taille de son masque, le peer duquel elle a été apprise, ou encore sa Communauty.

4 Niveaux de topologie réseau

Chaque groupe a sous sa responsabilité un AS, qui contient un LAN représentatif. Chaque nœud d'un AS représente un point de présence de l'opérateur. Pour simplifier l'exercice, seul le LAN de la Suisse contient plusieurs équipements. Les autres LAN comprennent seulement un hôte pour les tests de connectivité.

4.1 Topologie LAN

La topologie LAN de la Suisse a pour but de connecter différents sites universitaires à Internet. Deux types d'utilisateurs sont présents sur ces sites. Chaque site comprendra un hôte "étudiant" et un hôte "personnel" pour représenter les différentes connexions.

La topologie en Figure 1 présente le cablage du LAN, qui relie les trois sites :

- Le Centre Européen de Recherche sur le Nucléaire (CERN) à Genève (GENE)
- L'École Polytechnique Fédérale de Lausanne (EPFL)
- L'Institut Fédéral des Technologies de Zurich (ETHZ)

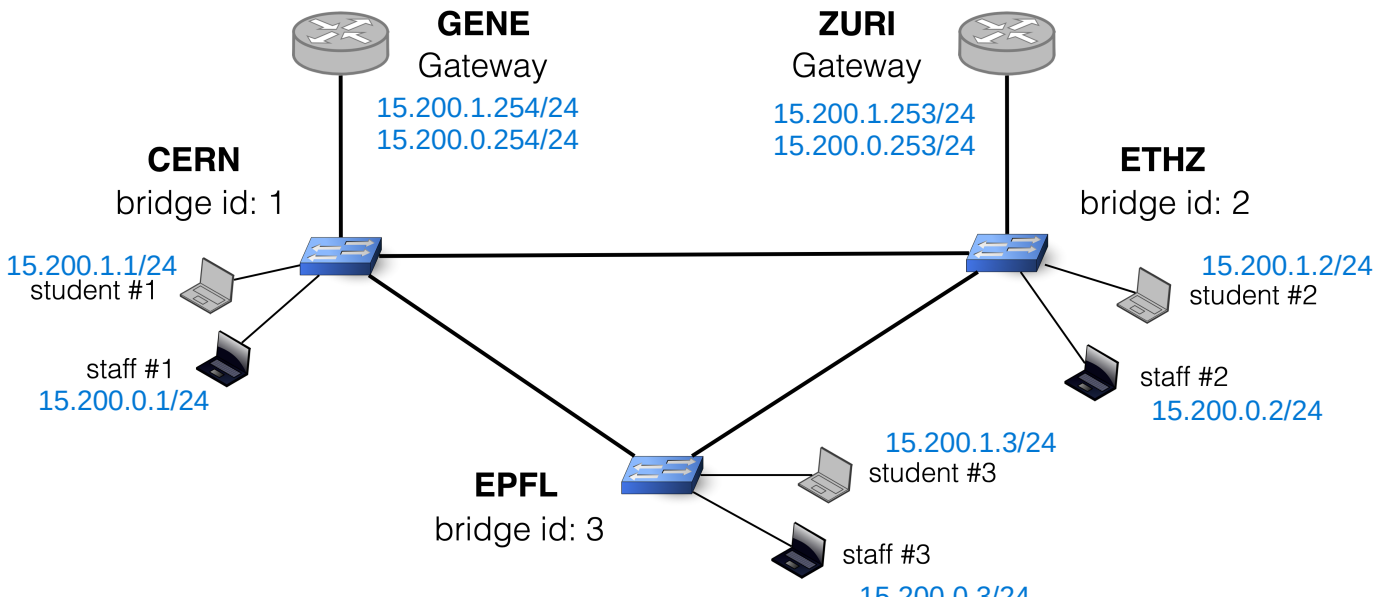

FIGURE 1 – LAN topology

4.2 Topologie AS

Votre LAN fait partie d'un AS qui traverse l'Atlantique : quatre routeurs en Europe et quatre aux États-Unis. Pour faciliter les tests chaque routeur est connecté à un seul hôte, à l'exception de la Suisse.

Le numéro de votre AS est le numéro de votre groupe. Vous disposez d'un ensemble d'adresses X.0.0.0/8, avec X le numéro de votre AS. Vous ne pouvez pas utiliser une adresse en dehors de ce sous-réseau, car elle pourrait appartenir à un autre AS.

La Figure 2 présente la topologie de l'AS, ainsi que l'adressage attendu. Ce plan (ou un plan similaire) doit être complété et apparaître dans le rapport. Les liaisons "Customer", "Provider", "IXP" et "Peer" sont des liaisons externes vers d'autres AS d'Internet. Les liaisons en pointillés représentent les câbles transatlantiques. Ignorez les entités "DNS" et "Measurement", elles servent au bon fonctionnement de la plateforme.

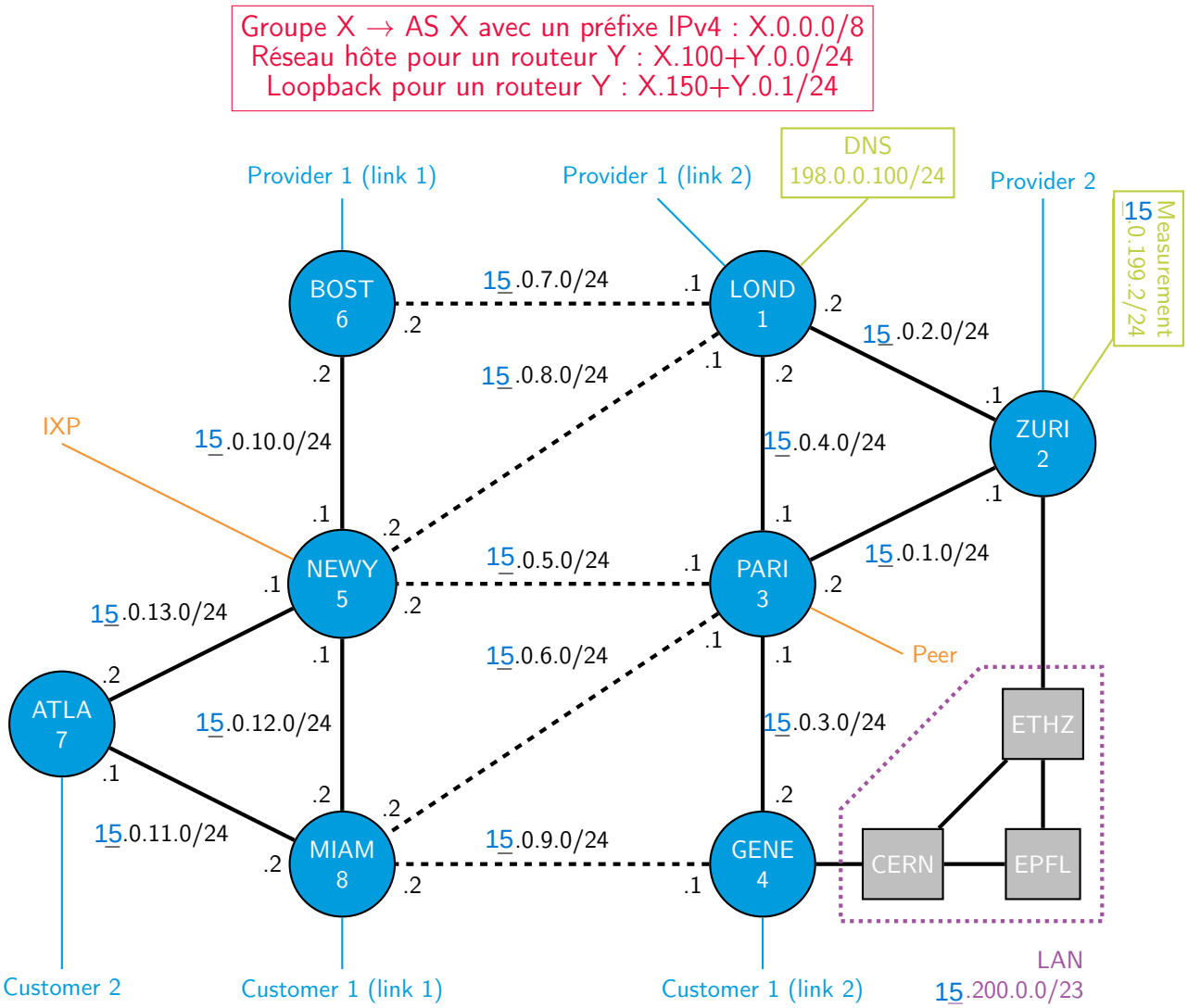

FIGURE 2 – AS topology

4.3 Topologie Internet

Chaque routeur de votre AS est connecté à un voisin Internet. La Figure 3 présente la topologie Internet sur laquelle vous allez travailler. L'AS que vous opérez est un Tier 2, ce qui est le plus courant sur Internet.

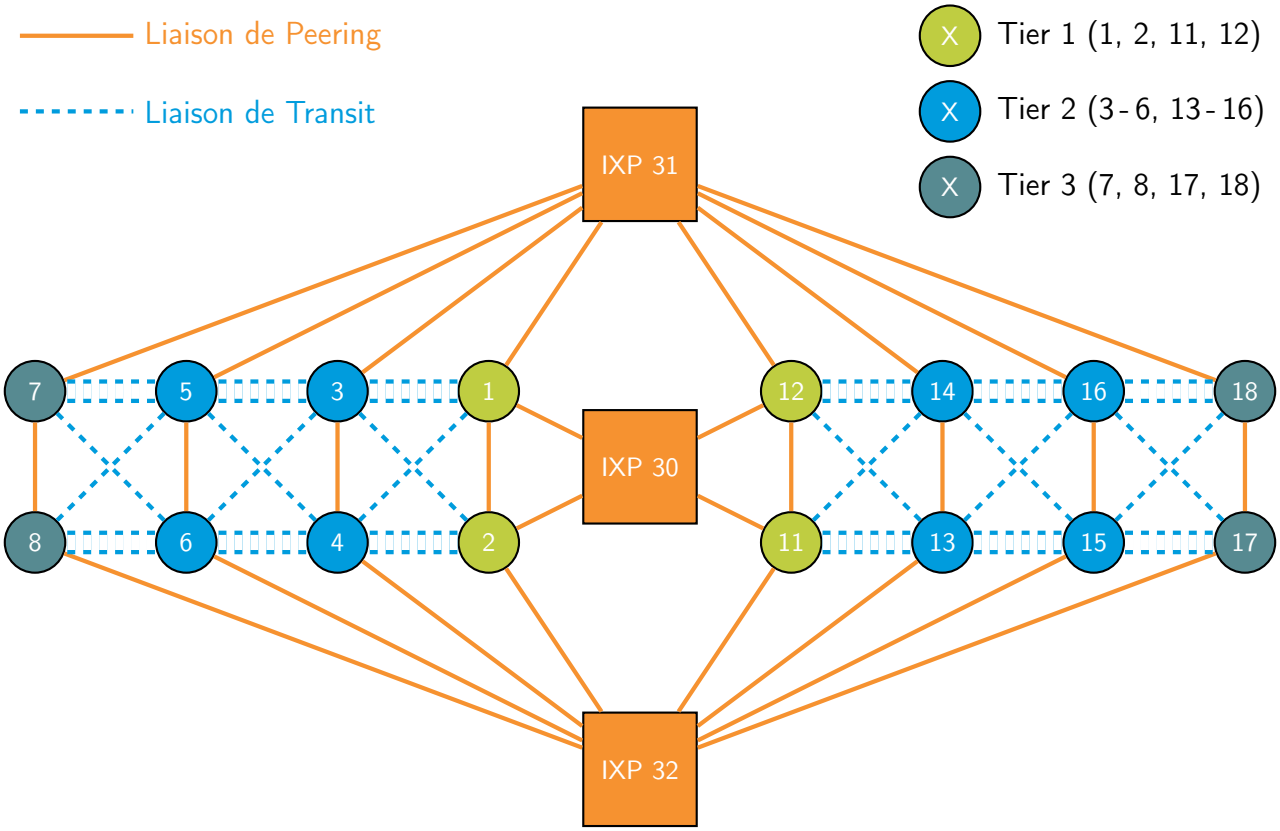

FIGURE 3 – AS-level topology

5 Tâches à réaliser

Pour chaque partie du projet, vous aurez plusieurs tâches à réaliser, et des questions associées. Ces questions sont là pour vous guider dans la rédaction du rapport, mais ne doivent pas être recopiées. Votre rapport ne doit pas être une liste de réponse à ces questions. En tant que futurs ingénieurs, vous devez être capable de rédiger un document technique qui présente le déroulement d'un projet, ses points importants et vos conclusions.

5.1 Connectivité Intra-domaine

5.1.1 Connectivité LAN

Votre première tâche est de permettre aux utilisateurs de se contacter entre eux, et d'accéder à la passerelle. Les étudiants et personnels ne doivent pas se contacter directement, mais à travers leur passerelle.

Vous devez utiliser des adresses appartenant à votre réseau local X.200.0.0/23, avec X le numéro de votre groupe. Les hôtes des sites CERN et EPFL ont pour passerelle GENE, et les hôtes du site ETHZ ont pour passerelle ZURI.

Sur les passerelles, utilisez les interfaces suivantes : GENE-L2.10, GENE-L2.20, ZURI-L2.10 and ZURI-L2.20. Les autres interfaces sont nécessaires dans la suite du projet.

- Quel est votre plan d'adressage ?
- Quel(s) protocole(s) utilisez-vous sur les commutateurs ? spaning tree, SMTP LACP
- Pourquoi ? tempete de broadcast, recuperer les infos de bp etc. doubles liens
- Quels sont les éléments de configuration importants correspondants ? IPv4
- Comment vérifiez-vous la connectivité ? pings/tracrt
- Quel est le résultat d'un traceroute depuis un hôte personnel vers un hôte étudiant ? lien direct par le switch (invisible au traceroute)

5.1.2 Connectivité AS

Votre LAN étant fonctionnel, vous allez maintenant connecter votre AS. Commencez par vous assurer que la connexion entre chaque routeur et son hôte fonctionne. Vous devez utiliser le sous-réseau X.[100+Y].0.0/24 avec X le numéro de groupe, et Y le numéro du routeur, conformément à la Figure 2. L'interface à utiliser sur le routeur est nommée "host", et l'interface sur l'hôte "NAMErouter". Par exemple, l'interface de l'hôte connecté à Miami est nommée "MIAMrouter".

Configurez les autres interfaces des routeurs avec les adresses indiquées Figure 2. Vous devez également configurer les interfaces de Loopback X.[150+Y].0.1/24 avec X le numéro de groupe, et Y le numéro du routeur.

Important : ne modifiez pas les interfaces "`dns-interface`" sur LOND, "`measurement-interface`" sur ZURI, et "`matrix-interface`" sur PARI. Elles sont nécessaires au bon fonctionnement de la plateforme.

Une fois que vous avez validé votre adressage, vous devez activer le routage OSPF au sein de votre AS. Assurez-vous que les réseaux associés au DNS (198.0.0.0/24) et Measurement (X.0.199.0/24) sont également visibles dans le plan de routage.

Vous pouvez maintenant valider votre routage depuis les hôtes, qui peuvent utiliser le serveur DNS (contrairement aux routeurs).

- Vérifiez la connectivité entre tous les hôtes de votre AS.
- Documentez votre plan d'adressage.
- Comment avez-vous configuré OSPF ?
- Quel est le but d'une interface Loopback ?
- Quel est le résultat d'un traceroute entre l'hôte de Paris et l'hôte d'Atlanta ?

5.1.3 Bases de traffic-engineering

En tant qu'opérateur réseau, votre but est de fournir des performances optimales à vos clients. Pour cela, vous allez devoir définir plus finement votre configuration OSPF.

Les liens continentaux disposent tous d'une bande passante de 25 Mb/s [1]. Les liens du LAN supportent 10 Mb/s. Concernant les liens transatlantiques, votre AS peut présenter l'une des quatre configuration illustrées en Figure 4. Vous devez avant tout identifier votre situation à l'aide de l'outil `iperf`.

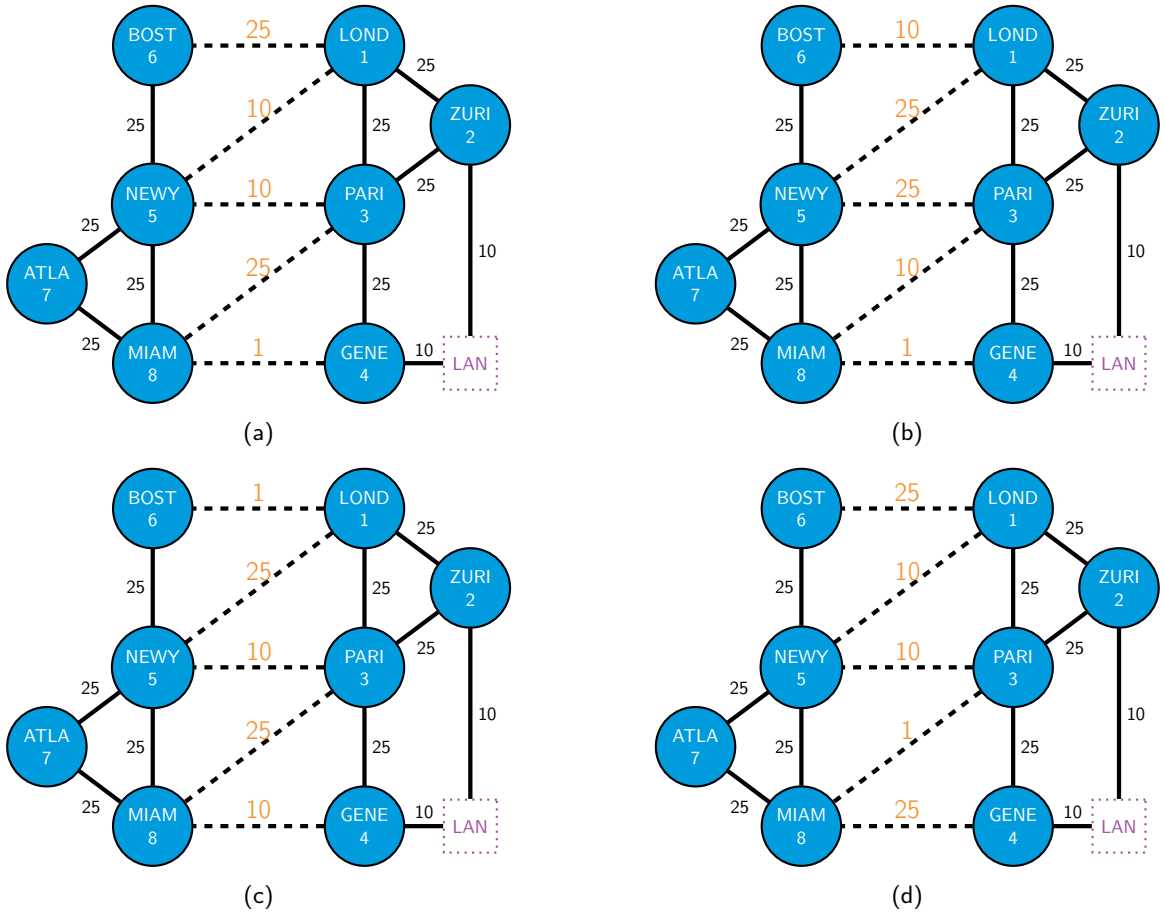

FIGURE 4 – Four possible submarine links configurations (Bandwidth in Mbps)

1. En pratique, vous pourrez observez que ces liens supportent plus que 25 Mb/s, mais vous devez limiter vos tests pour ne pas surcharger la plateforme.

Le protocole de routage OSPF calcule, à l'aide de l'algorithme de Dijkstra, le chemin le plus court vers chaque réseau. Par "plus court", on entend en fait "moins coûteux". Le coût d'un chemin est la somme du coût de chacune des liaisons empruntées. Vous devez donc définir un coût OSPF par lien, de sorte que :

1. Votre priorité est de minimiser la latence, il ne faut donc pas qu'un même trafic traverse deux fois des liens transatlantiques (en pointillés dans la Figure 2). Autrement dit, tout trafic local à un continent ne doit pas en sortir.
2. De plus, vous devez minimisez les risques de congestion en vous assurant d'utiliser les liens de plus grande bande-passante en priorité pour les trafics intercontinentaux.
3. De plus, vous devez assurer de la répartition de charge. Pour cela, vous devez définir des chemins qui ont le même coût :
   a. Tout trafic entre MIAM et NEWY est réparti sur les deux chemins MIAM-NEWY et MIAM-ATLA-NEWY ;
   b. Tout trafic entre ZURI et LOND est réparti sur les deux chemins ZURI-LOND et ZURI-PARI-LOND ;
   c. Tout trafic entre ATLA et ZURI est réparti sur les deux liens transatlantiques à forte bande-passante.

Une fois que vous avez défini le comportement souhaité sur votre réseau, vous devez configurer les coûts OSPF appropriés. Utilisez la commande `maximum-paths` pour permettre au routage OSPF d'utiliser plusieurs chemins de même coût.

- Quelle est votre situation en bande-passante ?
- Quels coûts OSPF avez-vous défini ?
- Vérifiez la répartition de charge en effectuant un traceroute de l'hôte d'ATLA vers l'interface de Loopback de ZURI.
- Pourquoi effectuer ce traceroute vers l'interface de Loopback ?
- Qu'observerait-on en utilisant un hôte du LAN comme destination, ou l'une des interfaces de ZURI ?

Le LAN dispose d'une bande-passante plus faible. Vous devez vous assurez qu'aucun trafic ne transite par le LAN, entre GENE et ZURI. Le sous-réseau du LAN doit être annoncé par OSPF, mais le seul trafic qui doit passer par ces interfaces est le trafic ayant pour source ou destination l'un des hôtes du LAN.

- Quelle technique utilisez-vous ?
- Quel est le résultat d'un traceroute de ETHZ-staff vers l'hôte de PARI ?

5.2 Configuration BGP globale

5.2.1 Intra-domaine : iBGP

Configurez des sessions BGP internes (iBGP) entre toutes les paires de routeurs de votre AS, pas uniquement ceux directement connectés. Par exemple, BOST doit avoir une session BGP établie avec MIAM. On parle de full-mesh. Vérifiez que chacun de vos routeurs dispose d'une session BGP vers tous les autres routeurs de votre AS. Utilisez les adresses de Loopback plutôt que les interfaces physique pour établir les sessions. Vous aurez besoin de la commande `update-source`.

Pour l'instant, vos sessions BGP n'ont pas besoin d'annoncer de routes. Au sein de votre AS, les routeurs connaissent déjà les routes OSPF. Le but d'iBGP est de propager les routes apprises de l'extérieur par vos routeurs connectés à d'autres AS.

Important : dans la configuration BGP, vous devez spécifiez les voisins dans la configuration "`address-family ipv4 unicast`". En effet, il est possible d'établir des sessions BGP pour d'autres types d'adresses, notamment IPv6 ou Anycast. Nous travaillerons uniquement en IPv4 Unicast

- Comment avez-vous configuré iBGP ?
- Comment vérifiez-vous l'établissement des sessions iBGP ?
- Pourquoi utiliser les interfaces de Loopback ? Pensez aux cas de panne.

5.2.2 Inter-domaine : eBGP

Configurez les sessions External BGP (eBGP) avec les AS voisins. Vous devez négocier les adresses utilisées par chacun. Les informations concernant les connexions sont rappelées dans les tableaux page 15 et 16. Cette fois-ci, utilisez les interfaces physiques, et pas les interfaces de Loopback. Attention, rappelez-vous que les sous-réseaux d'interconnexion n'appartiennent à aucun des deux AS, et ne doivent donc pas être déclarés dans OSPF.

Configurez également les sessions eBGP à travers les IXP. Pour cela, vous devez utiliser une adresse du sous-réseau de l'IXP : 180.Y.0.0/24, avec Y le numéro de l'IXP. L'adresse du Route Server, autrement dit le peer BGP, est 180.Y.0.Y. Votre adresse doit être 180.Y.0.X, avec X le numéro de groupe.

- Quelles adresses avez-vous défini avec vos voisins ?
- Comment avez-vous configuré BGP ?
- Pourquoi ne pas utiliser les interfaces de Loopback pour ces liaisons ? Pensez aux cas de panne.

Maintenant que vos sessions eBGP sont établies, vous allez définir les préfixes (autrement dit les sous-réseaux) qui vont être annoncés à vos pairs. Dans un premier temps, vous devez annoncer les adresses du /8 qui vous a été attribué ainsi que les /8 dont vous avez connaissance.

Par défaut, un routeur ne vous laissera pas annoncer un préfixe injoignable : en effet, seuls vos /24 existent dans la table de routage. Si vous utilisez par exemple la redistribution OSPF dans BGP, vous aller annoncer chacun de vos /24, mais cela surchargerait très rapidement les tables BGP de tous les participants. Vous devez donc configurer une route statique vers le /8, dont le next-hop est "null". Il s'agit d'une route vide, mais qui vous permettra de déclarer le /8 dans BGP. Rassurez-vous, la route nulle ne sera jamais utilisée dans le plan de routage : les IGP utilisent toujours en priorité la route la plus précise, donc plutôt les routes vers les /24 apprises par OSPF que la route statique vers le /8.

Pour cette partie, vous aurez besoin de la commande "`next-hop-self`". Lorsqu'un routeur de bordure apprend une route via eBGP, le next-hop de cette route est l'adresse d'un routeur appartenant à un autre AS. Lorsque cette route est propagée via iBGP au sein de votre AS, le next-hop est toujours une adresse appartenant à un autre réseau IP. Elle n'est donc pas joignable par votre plan de routage OSPF. Grâce à la commande "`next-hop-self`", le routeur de bordure remplace le next-hop de la route propagée en interne par sa propre adresse, qui est bien joignable au sein de l'AS.

- À l'aide de la commande "`show ip bgp`" vous devriez voir les préfixes annoncés par les AS voisins, montrant que vos sessions eBGP sont bien établies, et que les sessions iBGP propagent bien les routes apprises.
- À l'aide du Looking Glass (voir 6.7), vérifiez que vos voisins reçoivent bien vos annonces.
- Que se passerait-il sans la commande `next-hop-self` si votre hôte de ZURI tentait d'envoyer un ping vers l'hôte de ZURI de votre voisin ?
- Quel est le résultat d'un traceroute de votre hôte de ZURI vers l'hôte de ZURI de votre voisin ?
- Quel est l'état de la matrix de connectivité (voir 6.8) ?

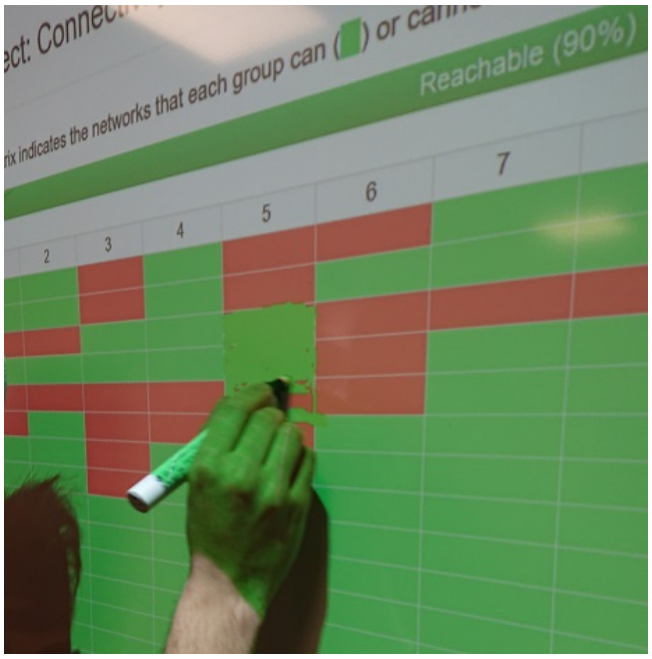

FIGURE 5 – Méthode de remplissage non-autorisée de la matrice, également appelée "Technique de Goldstein"

AS 3			Neighbor AS			
Router	**Role**	**IP**	**AS**	**Router**	**Role**	**IP**
BOST	Customer		1	ZURI	Provider	179.0.3.1/24
LOND	Customer		1	ZURI	Provider	179.0.4.1/24
ZURI	Customer		2	ZURI	Provider	179.0.8.1/24
MIAM	Provider		5	BOST	Customer	
GENE	Provider		5	LOND	Customer	
ATLA	Provider		6	ZURI	Customer	
PARI	Peer		4	PARI	Peer	
NEWY	Peer		IXP 31		Peer	

AS 4			Neighbor AS			
Router	**Role**	**IP**	**AS**	**Router**	**Role**	**IP**
BOST	Customer		2	ZURI	Provider	179.0.6.1/24
LOND	Customer		2	ZURI	Provider	179.0.7.1/24
ZURI	Customer		1	ZURI	Provider	179.0.5.1/24
MIAM	Provider		6	BOST	Customer	
GENE	Provider		6	LOND	Customer	
ATLA	Provider		5	ZURI	Customer	
PARI	Peer		3	PARI	Peer	
NEWY	Peer		IXP 32		Peer	

AS 5			Neighbor AS			
Router	**Role**	**IP**	**AS**	**Router**	**Role**	**IP**
BOST	Customer		3	MIAM	Provider	
LOND	Customer		3	GENE	Provider	
ZURI	Customer		4	ATLA	Provider	
MIAM	Provider		7	ZURI	Customer	179.0.24.2/24
GENE	Provider		7	ZURI	Customer	179.0.25.2/24
ATLA	Provider		8	ZURI	Customer	179.0.26.2/24
PARI	Peer		6	PARI	Peer	
NEWY	Peer		IXP 31		Peer	

AS 6			Neighbor AS			
Router	**Role**	**IP**	**AS**	**Router**	**Role**	**IP**
BOST	Customer		4	MIAM	Provider	
LOND	Customer		4	GENE	Provider	
ZURI	Customer		3	ATLA	Provider	
MIAM	Provider		8	ZURI	Customer	179.0.28.2/24
GENE	Provider		8	ZURI	Customer	179.0.29.2/24
ATLA	Provider		7	ZURI	Customer	179.0.30.2/24
PARI	Peer		5	PARI	Peer	
NEWY	Peer		IXP 32		Peer	

AS 13			Neighbor AS			
Router	**Role**	**IP**	**AS**	**Router**	**Role**	**IP**
BOST	Customer		11	ZURI	Provider	179.0.11.1/24
LOND	Customer		11	ZURI	Provider	179.0.12.1/24
ZURI	Customer		12	ZURI	Provider	179.0.16.1/24
MIAM	Provider		15	BOST	Customer	
GENE	Provider		15	LOND	Customer	
ATLA	Provider		16	ZURI	Customer	
PARI	Peer		14	PARI	Peer	
NEWY	Peer		IXP 32		Peer	

AS 14			Neighbor AS			
Router	**Role**	**IP**	**AS**	**Router**	**Role**	**IP**
BOST	Customer		12	ZURI	Provider	179.0.14.1/24
LOND	Customer		12	ZURI	Provider	179.0.15.1/24
ZURI	Customer		11	ZURI	Provider	179.0.13.1/24
MIAM	Provider		16	BOST	Customer	
GENE	Provider		16	LOND	Customer	
ATLA	Provider		15	ZURI	Customer	
PARI	Peer		13	PARI	Peer	
NEWY	Peer		IXP 31		Peer	

AS 15			Neighbor AS			
Router	**Role**	**IP**	**AS**	**Router**	**Role**	**IP**
BOST	Customer	13.208.0.2	13	MIAM	Provider	13.208.0.1
LOND	Customer	13.204.0.2	13	GENE	Provider	13.204.0.1
ZURI	Customer	14.207.0.2	14	ATLA	Provider	14.207.0.1
MIAM	Provider	179.0.38.1	17	ZURI	Customer	179.0.38.2/24
GENE	Provider	179.0.39.1	17	ZURI	Customer	179.0.39.2/24
ATLA	Provider	179.0.40.1	18	ZURI	Customer	179.0.40.2/24
PARI	Peer	179.0.41.1	16	PARI	Peer	179.0.41.2
NEWY	Peer	180.32.0.15	IXP 32		Peer	180.32.0.32

/24

/30

AS 16			Neighbor AS			
Router	**Role**	**IP**	**AS**	**Router**	**Role**	**IP**
BOST	Customer		14	MIAM	Provider	
LOND	Customer		14	GENE	Provider	
ZURI	Customer		13	ATLA	Provider	
MIAM	Provider		18	ZURI	Customer	179.0.42.2/24
GENE	Provider		18	ZURI	Customer	179.0.43.2/24
ATLA	Provider		17	ZURI	Customer	179.0.44.2/24
PARI	Peer		15	PARI	Peer	
NEWY	Peer		IXP 31		Peer	

14.

5.3 Policy-routing

Grâce à la configuration précédente vous annoncez votre préfixe ainsi que tous les préfixes que vous apprenez. Vous imaginez bien qu'en réalité, une telle situation est impossible à l'échelle d'Internet, qui comporte plusieurs dizaines de milliers d'AS. De plus, une telle architecture serait vulnérable à de nombreuses attaques d'un AS malveillant. En pratique, un opérateur utilise du Policy-routing pour filtrer les routes apprises et émises.

5.3.1 Relations commerciales : BGP Communities

Vous allez maintenant implémenter les comportements correspondant aux relations que vous avez avec vos voisins : client (customer), fournisseur (provider) ou peer. Référez-vous à la Figure 3 pour les relations :

- Vos voisins plus proches du Tier 1 sont vos fournisseurs et vous êtes leur client ;
- Vos voisins plus proches du Tier 3 sont vos clients et vous êtes leur fournisseur ;
- Vos voisins au même niveau sont des peers (comme indiqué par le type de liaison) ;
- Vos voisins à travers les IXP sont également des peers.

Par exemple, l'AS 3 a pour fournisseur 1 et 2, pour client 5 et 6, et pour peer 4 et la liaison vers l'IXP 31.

Dans une relation customer/provider, le provider exporte toutes les routes à sa connaissance (la GRT) pour fournir un accès Internet à son customer qui lui n'émet que son propre préfixe (et celui de ses propre customers). Ainsi, si le client souhaite accéder à d'autres AS, il passe par son fournisseur d'accès. Dans le cas d'un AS Tier 2 comme le votre, vous propagez alors cet accès Internet à vos propres clients.

Dans une relation peer-to-peer, les deux peers envoient leur propre préfixe (et celui de ses customers). Les peers (et leurs clients) peuvent ainsi s'échanger directement du trafic, sans passer par un fournisseur d'accès. Il s'agit généralement d'arrangement commerciaux entre deux AS qui échangent régulièrement du trafic, et qui souhaitent économiser l'achat de la bande-passante à un fournisseur.

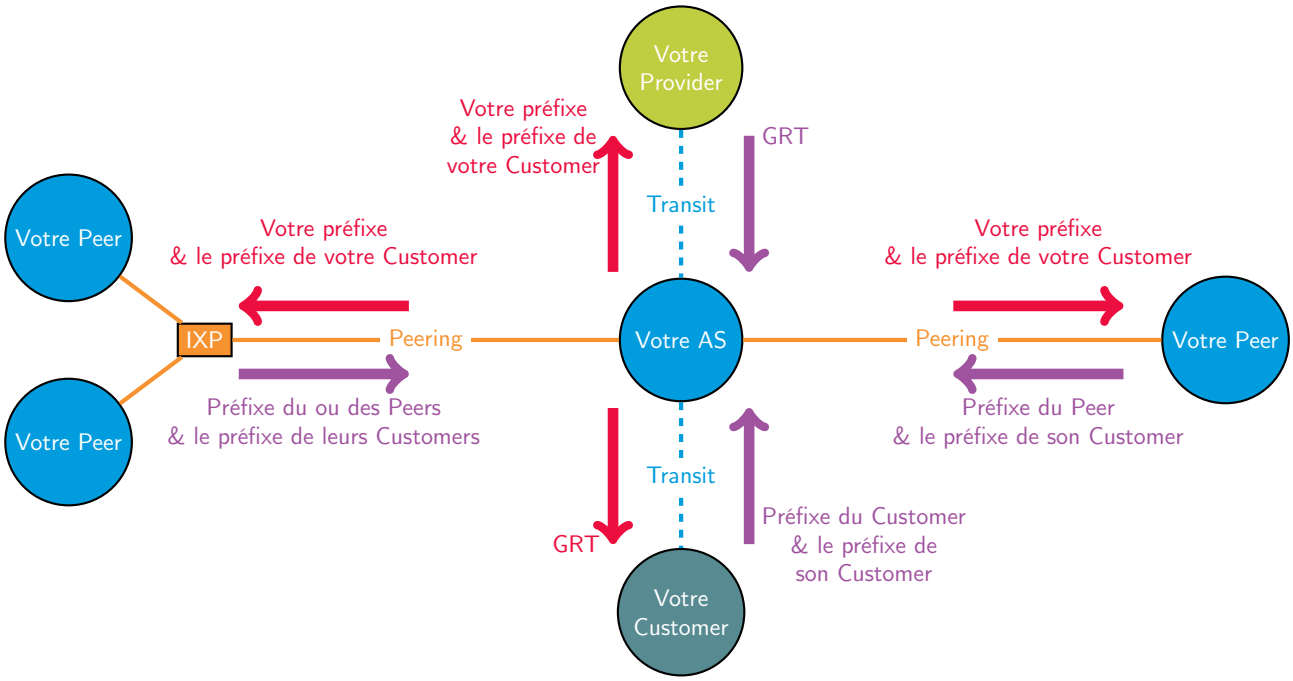

FIGURE 6 – Illustration des relations BGP

Pour configurer les règles d'exportation vous devez marquer les routes que vous apprenez à l'aide de Communities pour retenir d'où vous les avez apprises : s'agit-il de routes de vos clients, de vos fournisseurs ou de vos peers ? À l'aide du marquage que mis en place, vous pourrez définir quelles routes sont annoncées à vos clients, fournisseurs ou peers.

Important : commencez par configurer vos relations customer/provider, et vos peer-to-peer directs. Vous configurerez la liaison par l'IXP dans la suite.

Vous aurez besoin de Route-map pour marquer les routes entrantes et filtrer les routes sortantes suivant ce marquage. Une Route-map :

1. S'applique à un peer BGP dans une direction (in ou out) ;
2. Est de type *permit* ou *deny*. Vous n'aurez besoin que du type *permit*, le *deny* sera implicite ;
3. Est composée de *match* et de *set* :
   a. Les *match* spécifient les critères qui identifient une route, par exemple sa source. Ils s'appliquent suivent un ET logique, c'est-à-dire que la Route-map identifie uniquement les routes qui correspondent à tous les critères. Pour faire un OU logique, vous devez faire plusieurs Route-map. L'absence de *match* implique que la Route-map s'applique à toutes les routes (apprises si appliquée en in, émises si appliquée en out) ;
   b. Les *set* correspondent aux attributs que vous allez modifier (en l'occurence la Community). L'absence de *set* indique que toutes les routes identifiées par le *match* seront apprises ou émises sur le voisinage BGP suivant la direction. Il s'agit alors uniquement de filtrage.

Vérifiez à l'aide du Looking Glass et de traceroutes que les chemins utilisés respectent les relations que vous avez implémenté. Gardez à l'esprit que le Looking Glass peut mettre quelques minutes à se mettre à jour.

- Quelles communautés avez-vous utilisé ? En avez-vous créé une par catégorie ou une par voisin, et pourquoi ?
- Expliquez une Route-map entrante et une Route-map sortante.
- Montrez à l'aide du Looking Glass que vos clients reçoivent bien la GRT de votre part.
- Vérifiez vos relations peer-to-peer à l'aide d'un traceroute. Le trafic ne doit pas passer par votre provider.

Par défaut, les IXP sont configurés pour ne pas relayer d'annonces BGP. Pour annoncer un préfixe à un peer, vous devez utiliser une Community BGP, suivant la politique définie par l'IXP. Une route est transmise à un peer X par l'IXP N si la route est marquée avec une Community N :X. Par exemple, si vous êtes l'AS 5, et que vous voulez annoncer un préfixe à l'AS 7 via l'IXP 31, vous devez marquer votre annonce avec la Community 31 :7.

La Figure 2 présente deux régions, gauche et droite, reliées uniquement par des IXP. Vous devez créer des relations de peering via les IXP avec les AS de la région opposée uniquement. Vous devez donc refuser toute annonce de route venant d'un peer de votre région. Vous aurez cette fois-ci besoin de route-map de type *deny*.

Pour que vous puissiez confirmer votre configuration, les AS Tier 3 ont volontairement été mal configurées : elles annoncent leur préfixe à tout le monde via l'IXP.

- Décrivez un exemple de Route-map que vous avez utilisé.
- À l'aide du Looking Glass, vérifiez que votre préfixe a été enregistré à travers l'IXP.
- Utiliser la commande `show ip bgp` pour montrer que vous refusez bien les annonces du Tier 3 de votre région connecté à l'IXP.
- À l'inverse, montrez que cet AS Tier 3 ne reçoit pas d'annonce de votre part.

5.3.2 Définir la sortie du trafic : Local preference

La "*local preference*" est un paramètre qui permet de contourner la sélection automatique de route. Par défaut, BGP choisira toujours le chemin qui comporte le moins de sauts d'AS, autrement dit l'AS-path le plus court. La "*local preference*" permet de désigner une route favorite. Ce paramètre n'est pas transmis aux peers eBGP, mais est propagée en iBGP. Une valeur plus élevée indique une route préférée. La valeur par défaut est généralement 100, assurez-vous d'utiliser des valeurs supérieures.

Sachant cela, configurez vos Route-map entrantes de sorte à toujours préférer les routes apprises des AS customers, puis les préfixes annoncés par vos peers, puis ceux annoncés par vos AS providers. En pratique, cela évite par exemple qu'un trafic destiné à un client ne repasse par votre provider.

Dans notre topologie, la longueur des AS-Path ne pose généralement pas ce problème, mais vous devez tout de même réaliser cette partie.

- Expliquez une Route-map que vous avez utilisé.

5.3.3 Définir l'entrée du trafic : Traffic-engineering via prepending

Dans cette partie, vous devez faire en sorte de diriger le trafic entrant sur les liaison de votre choix. Votre provider 1 doit servir au trafic de transit, alors que le provider 2 doit servir au trafic qui vous est destiné. Vous allez avoir besoin d'une technique appelée "AS prepending".

Vous devez faire en sorte que le trafic à destination de votre préfixe arrive en priorité par votre liaison avec le provider 2, autrement dit connecté à ZURI. De plus, tout trafic de transit (donc à destination d'un autre préfixe que le votre) doit passer en priorité par les liaisons du provider 1, en préférant la liaison 1 arrivant à BOST.

Vous aurez besoin de la commande "`set as-path prepend`" au sein d'une ou plusieurs Route-maps.

- Expliquez la technique de l'AS Prepending.
- Décrivez les Route-map que vous avez utilisé.
- À l'aide du Looking Glass sur vos deux providers, montrez que votre configuration fonctionne.

6 Informations techniques utiles

6.1 Sauvegarder votre travail

Vous avez à votre disposition un script "save_configs.sh" qui sauvegarde automatiquement touts vos configurations. Le script génère un dossier et le zip correspondant, nommé "configs_[date]_[time]". Vous pouvez alors télécharger le fichier zip sur votre machine (pas depuis votre conteneur Docker principal). Par défaut il est conseillé d'utiliser SCP pour récupérer le fichier :

```
> scp -P 2000+X root@<IP_totoro>:configs_[date]_[time].zip configs_[date]_[time].zip
```

avec X le numéro de votre groupe, et IP_totoro l'adresse du serveur *totoro* qui vous sera donnée par l'instructeur. Par exemple, si vous êtes le groupe 7 et que *totoro* a pour adresse 192.168.2.91/24 :

```
> scp -P 2007 root@192.168.2.91:configs_[date]_[time].zip configs_[date]_[time].zip
```

Sauvegardez votre travail à chaque session : en cas de redémarrage du serveur, de panne, ou encore de coupure de courant, tous les équipements seront réinitialisés.

6.2 Accéder à votre conteneur Docker

Chaque AS est un ensemble de conteneurs auxquels vous allez accéder via SSH. Vous aller d'abord vous connecter à un conteneur principal qui vous redirigera au besoin vers les équipements. Vous devez utiliser un port 2000+X, avec X le numéro de votre groupe. Vous aurez également besoin d'un mot de passe qui vous sera donné par l'instructeur. En cas de redémarrage de la plateforme, ce mot de passe sera automatiquement modifié et l'instructeur vous donnera le nouveau. Utilisez la commande suivante pour vous connecter :

```
> ssh -p 2000+X root@<IP_totoro>          192.168.2.191
```

6.3 Accéder à vos équipements

Depuis votre conteneur Docker principal, vous pouvez utiliser le script "goto.sh" pour vous connecter à vos routeurs, commutateurs ou hôtes.

Pour accéder à un routeur, vous devez utiliser son nom suivi de "router". Vous accédez alors au CLI FRRouting (voir 6.4.1).

```
> ./goto.sh NEWY router
```

Pour accéder à un hôte lié à un routeur, vous devez utiliser le nom du routeur suivi de "host". Vous êtes alors sur l'hôte Linux (voir 6.4.3).

```
> ./goto.sh NEWY host
```

Pour accéder à un commutateur du LAN Suisse, vous devez utiliser l'argument "UNIV" suivi du nom du site. Contrairement à FRRouting, Open vSwitch ne dispose pas d'un CLI classique. Vous devrez utiliser des commandes depuis le CLI Linux du conteneur (voir 6.4.2).

```
> ./goto.sh UNIV CERN
```

Pour accéder à un hôte étudiant ou personnel du LAN Suisse, vous devez utiliser l'argument "UNIV" suivi du type d'utilisateur ("student" ou "staff") suivi de son numéro.

```
> ./goto.sh UNIV student 3
```

6.4 Configurer vos équipements

6.4.1 Configurer un routeur FRRouting

Le CLI FRRouting est très proche du CLI Cisco IOS. Utilisez vos connaissances et la documentation.

Chaque routeur possède des interfaces vers ses routeurs voisins dont le nom est toujours "`port VOISIN`". Par exemple, l'interface de NEWY vers ATLA est nommée "`port ATLA`". De plus, le routeur possède une interface "`host`" vers son hôte, et "`lo`" la Loopback. Les interfaces d'un routeur connecté à un autre AS suivent la convention "`ext ASNUMBER ROUTERNAME`". Par exemple, l'interface de NEWY de l'AS 81 connecté à ZURI de l'AS 82 se nomme "`ext 82 ZURI`".

6.4.2 Configurer un commutateur Open vSwitch

Sur chaque commutateur, les ports associés au hôtes étudiants et personnels sont nommés "`X-student i`" et "`X-staff i`", avec X le numéro de l'AS. Les ports vers d'autres commutateurs sont nommés "`X-SWITCHNAME`", et les ports vers des routeurs sont nommés "`ROUTERNAMErouter`".

Pour afficher un résumé de l'état du commutateur et de la configuration VLAN, utilisez la commande :

```
> ovs-vsctl show
```

Pour configurer un VLAN sur un port, utilisez la commande :

```
> ovs-vsctl set port <PORTNAME> tag=10
```

Pour configurer plusieurs VLAN sur un port, utilisez la commande :

```
> ovs-vsctl set port <PORTNAME> trunks=10,20
```

Pour effacer la configuration VLAN d'un port, utilisez la commande :

```
> ovs-vsctl clear port <PORTNAME> tag
OU
> ovs-vsctl clear port <PORTNAME> trunks
```

Sur chaque commutateur, vous trouverez une interface nommée "`br0`" de type "`internal`". C'est un port local utilisé par le conteneur hôte pour contrôler le commutateur. Vous ne devez pas l'utiliser.

Le Spanning-Tree Protocol est activé par défaut sur tous les commutateurs.

6.4.3 Configurer un hôte

Sur chaque hôte lié à un routeur, l'interface est nommée "<ROUTERNAME>router". Par exemple, l'hôte lié à BOST a pour interface "BOSTrouter".

Pour consulter la liste des interfaces, utilisez la commande :

```
> ip address show
```

Pour assigner une adresse IP à une interface, utilisez la commande :

```
> ip address add <IP/MASK> dev <INTERFACE>
```

Par exemple :

```
> ip address add 111.0.222.3/24 dev LONDrouter
```

Pour configurer la passerelle par défaut, utilisez la commande :

```
> ip route add default via <IP>
```

Pour consulter la passerelle configurée, utilisez la commande :

```
> netstat -rn
```

Pour supprimer une passerelle erronée, utilisez la commande :

```
> ip route del default via <IP>
```

6.5 Utiliser iperf3

iperf3 [4] est un programme qui permet de générer du trafic entre deux points, un client et un serveur, en TCP ou en UDP. Il est installé par défaut sur tous les hôtes de la plateforme. Pour faire une mesure, il faut lancer un serveur sur un hôte, et un client sur un autre hôte.

Pour lancer un serveur, utilisez la commande :

```
> iperf3 --server --one-off
```

L'argument `-one-off` permet au serveur de s'éteindre automatiquement après un seul test.

Pour lancer un client, utilisez la commande :

```
> iperf3 --client <SERVER_IP> --time <TIME>
```

avec SERVER_IP l'adresse de l'hôte sur lequel vous avez lancé le serveur, et TIME la durée du test.

Il existe d'autres options, n'hésitez pas à explorer la documentation, notamment pour limiter la bande-passante utilisée par le test.

6.6 Résumé des commandes utiles

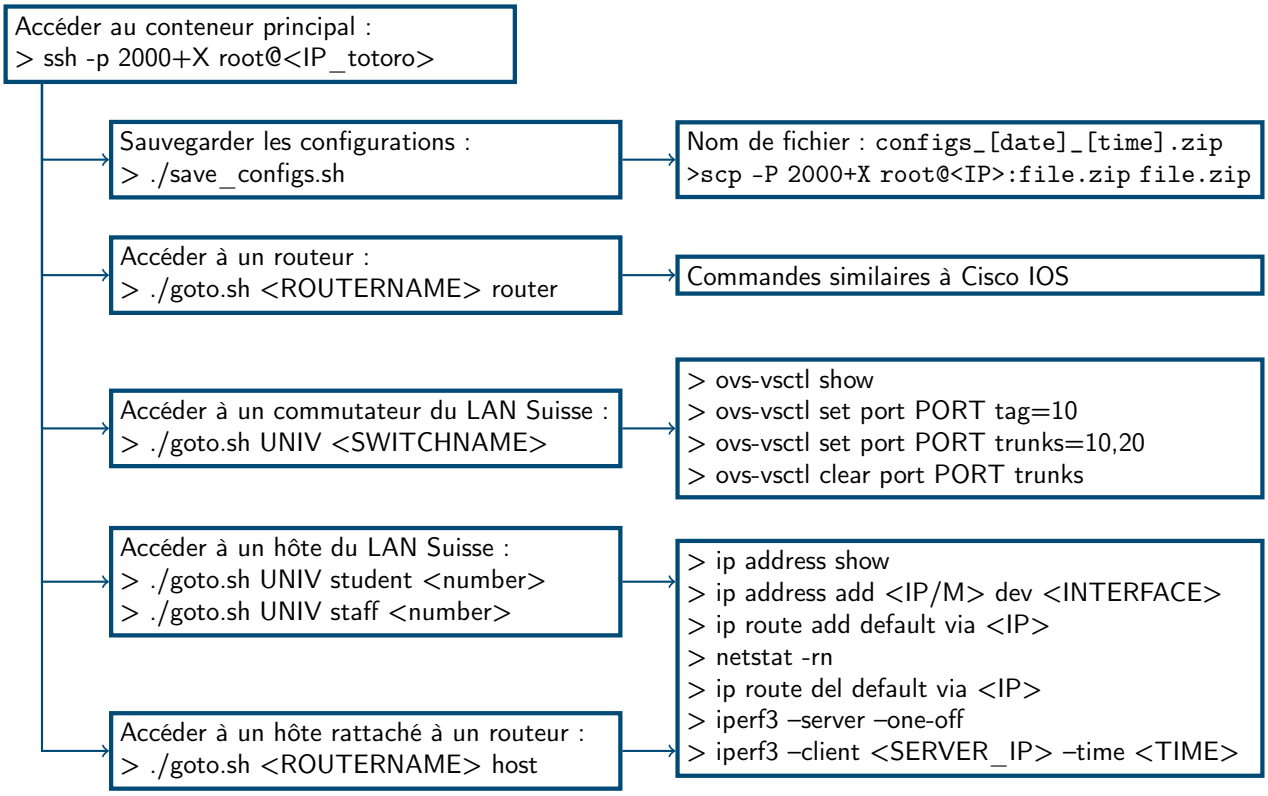

FIGURE 7 – Résumé des commandes utiles

6.7 Looking Glass

Un Looking Glass est un outil fourni par un opérateur à ses voisins pour qu'il puissent consulter les tables BGP des routeurs de bordures. Sur la plateforme, le Looking Glass de chaque AS est géré automatiquement et est disponible à l'URL :

```
http:/<IP_totoro>/looking_glass/
```

Un sous-dossier est associé à chaque groupe. Vous y trouverez des fichiers `.txt` pour chaque routeur, qui correspondent à la sortie d'une commande `show ip bgp`.

6.8 Matrice de connectivité

Pour vérifier la connectivité global d'Internet, vous pouvez consulter l'URL :

```
http:/<IP_totoro>/matrix.html
```

Cette matrice montre le résultat d'une série de pings entre toutes les paires d'AS. Par défaut, si vous avez configuré uniquement le routage interne, la diagonale devrait apparaitre verte (de votre AS vers votre AS), ainsi que les AS auto-configurés, notamment les Tier 1 et Tier 3 qui sont sous la responsabilité de l'instructeur.

7 Administration de la plateforme

7.1 Spécifications du serveur Totoro

- 4 * Intel Xeon CPU E3-1220 v3 @ 3.10GHz
- 4 * 4 Go RAM
- 500 Go HDD
- Ubuntu 20.04 LTS

7.2 Installation

```
sudo snap remove docker

sudo apt-get update
sudo apt-get install apt-transport-https ca-certificates curl gnupg-agent                \
    software-properties-common
curl -fsSL https://download.docker.com/linux/ubuntu/gpg | sudo apt-key add -
sudo add-apt-repository "deb [arch=amd64] https://download.docker.com/linux/ubuntu       \
    $(lsb_release -cs) stable"
sudo apt-get update
sudo apt-get install docker-ce docker-ce-cli containerd.io

sudo apt-get install openvswitch-switch

git clone https://github.com/nsg-ethz/mini_internet_project
```

7.3 Configuration

La configuration de la topologie se trouve dans le dossier `/home/totoro/mini_internet_project/platform/config`. Référez-vous à la documentation de la plateforme pour générer des topologies de votre choix. Les fichiers correspondant à la topologie présentée dans le sujet ont été généré à l'aide du script "`generate_connections.py`" fourni avec la plateforme, avec les paramètres ci-dessous :

```
tier1 = [[1,2],[11,12]]
transit = [[1,2,3,4,5,6,7,8],[11,12,13,14,15,16,17,18]]
ixp_central = 30
ixp_out = [31,32]
```

Important : dans le fichier AS_config.txt, la troisième colonne indique si l'AS doit être préconfiguré ou non. Tous les AS étudiants doivent être paramétrés sur "NoConfig".

AS_config.txt

```
1     AS     Config      router_config_small.txt internal_links_config_small.txt                    \
                         layer2_switches_config_empty.txt layer2_hosts_config_empty.txt             \
                         layer2_links_config_empty.txt
2     AS     Config      router_config_small.txt ...
11    AS     Config      router_config_small.txt ...
12    AS     Config      router_config_small.txt ...
7     AS     Config      router_config_small.txt ...
8     AS     Config      router_config_small.txt ...
17    AS     Config      router_config_small.txt ...
18    AS     Config      router_config_small.txt ...
3     AS     NoConfig    router_config_full.txt internal_links_config.txt layer2_switches_config.txt\
                         layer2_hosts_config.txt layer2_links_config.txt
4     AS     NoConfig    router_config_full.txt ...
5     AS     NoConfig    router_config_full.txt ...
6     AS     NoConfig    router_config_full.txt ...
13    AS     NoConfig    router_config_full.txt ...
14    AS     NoConfig    router_config_full.txt ...
15    AS     NoConfig    router_config_full.txt ...
16    AS     Config      router_config_full.txt ...
30    IXP    Config      N/A N/A N/A N/A N/A
31    IXP    Config      N/A N/A N/A N/A N/A
32    IXP    Config      N/A N/A N/A N/A N/A
```

7.4 Installation du Looking Glass et de la matrice de connectivité

Par défaut, les fichiers du Looking Glass et de la matrice de connectivité ne sont pas disponibles pour les étudiants. Il faut d'abord créer un serveur Web :

```
sudo apt install apache2
sudo systemctl enable apache2.service
sudo ufw allow 80/tcp comment 'accept Apache'
cd /var/www/html/
sudo mkdir css
sudo mkdir looking_glass
cd css
sudo wget https://comm-net.ethz.ch/routing_project/matrix/css/custom.css
sudo wget https://comm-net.ethz.ch/routing_project/matrix/css/bootstrap.min.css
sudo wget https://comm-net.ethz.ch/routing_project/matrix/css/bootstrap-theme.min.css
```

Il faut ensuite modifier deux scripts qui vont copier régulièrement les derniers fichiers dans le serveur Web, afin qu'ils utilisent les chemins absolus du dossier que l'on a créé pour le serveur :

```
cd  /home/totoro/mini_internet_project/platform/utils
sudo nano upload_looking_glass.sh &
sudo nano upload_matrix.sh &
```

upload_looking_glass.sh

```
#!/bin/bash

set -o errexit
set -o pipefail
set -o nounset

readarray groups < /home/totoro/mini_internet_project/platform/config/AS_config.txt
group_numbers=${#groups[@]}

while true
do
  for ((k=0;k<group_numbers;k++)); do
      group_k=(${groups[$k]})
      group_number="${group_k[0]}"
      group_as="${group_k[1]}"
      group_config="${group_k[2]}"
      group_router_config="${group_k[3]}"
      if [ "${group_as}" != "IXP" ];then
          readarray routers < /home/totoro/mini_internet_project/platform/config/$group_router_config
          n_routers=${#routers[@]}
          mkdir G$group_number
          for ((i=0;i<n_routers;i++)); do
              router_i=(${routers[$i]})
              rname="${router_i[0]}"
              property1="${router_i[1]}"
              property2="${router_i[2]}"
              cp /home/totoro/mini_internet_project/platform/groups/g${group_number}/${rname}/      \
                                                looking_glass.txt G$group_number/${rname}.txt
              echo $group_number $rname
          done
          cp -r G$group_number /var/www/html/looking_glass/
          rm -r G$group_number
          echo $group_number done
      fi
  done
  sleep 10
done
```

upload_matrix.sh

```
#!/bin/bash

while true
dohttps://fr.overleaf.com/project/5f0c64ec66a9760001168380
    docker cp MATRIX:/home/matrix.html /var/www/html/matrix.html
    echo 'matrix sent'
    sleep 20
done
```

Enfin, il faut s'assurer que ces deux scripts sont lancés en tâche de fond :

```
cd  /home/totoro/mini_internet_project/platform/utils
sudo nohup ./upload_looking_glass.sh &
sudo nohup ./upload_matrix.sh &
```

7.5 Connexion des étudiants à leur conteneur principal

Il faut commencer par modifier les paramètres du serveur SSH :

```
sudo nano /etc/ssh/sshd_config
```

Les trois paramètres suivants sont nécessaires :

```
GatewayPorts yes
PasswordAuthentication yes
AllowTcpForwarding yes
```

Vous pouvez maintenant redémarrer le serveur SSH et rediriger les ports nécessaires à l'aide du script fourni :

```
sudo service ssh restart
sudo /home/totoro/mini_internet_project/platform/portforwarding.sh
```

Les mots de passe des différents groupes se trouvent dans le fichier :
`/home/totoro/mini_internet_project/platform/groups/ssh_passwords.txt`.

Si vous souhaitez donner un accès à tous les étudiants, il suffit de copier ce fichier contenant tous les mots de passe dans le serveur Web. Si cela facilite l'accès, les étudiants devront faire preuve d'une certaine responsabilité :

```
sudo cp /home/totoro/mini_internet_project/platform/groups/ssh_passwords.txt \
        /var/www/html/ssh_passwords.txt
```

7.6 Démarrage

Pour lancer ou redémarrer la plateforme, utilisez les commandes suivantes :

```
cd mini_internet_project/platform
sudo ./cleanup/hard_reset.sh
sudo ./startup.sh
sudo ./portforwarding.sh
sudo nohup ./utils/upload_looking_glass.sh &
sudo nohup ./utils/upload_matrix.sh &
#Pour chaque IXP :
sudo docker exec -it 30_IXP bash
/etc/init.d/quagga restart
exit
sudo docker exec -it 31_IXP bash
/etc/init.d/quagga restart
exit
sudo docker exec -it 32_IXP bash
/etc/init.d/quagga restart
exit
```

Les mots de passe sont régénérés à chaque redémarrage de la plateforme. Si vous devez relancer la plateforme (coupure de courant, erreur de manipulation...), pensez à donner les nouveaux mots de passe aux étudiants. Pour rappel, les mots de passe des différents groupes se trouvent dans le fichier :
`/home/totoro/mini_internet_project/platform/groups/ssh_passwords.txt`.

7.7 Accès administrateur

Le serveur dispose d'un accès SSH administrateur : Depuis le serveur, pour accéder au CLI d'un routeur sur l'AS X :

```
sudo docker exec -it X_ROUTERNAMErouter bash
vtysh
```

Depuis le serveur, pour accéder au CLI d'un commutateur sur l'AS X :

```
sudo docker exec -it X_L2_UNIV_SWITCHNAME bash
```

7.8 Débuggage

Depuis le serveur, pour obtenir la liste de tous les conteneurs Docker :

```
sudo docker ps
```

Pour redémarrer un conteneur :

```
docker kill CONTAINER_NAME
docker start CONTAINER_NAME
./groups/restart_container.sh CONTAINER_NAME
```

Références

[1] T. Holterbach, T. Bü, T. Rellstab, and L. Vanbever, "An open platform to teach how the internet practically works," *SIGCOMM Comput. Commun. Rev.*, 2020.

[2] B. Pfaff, J. Pettit, T. Koponen, E. J. Jackson, A. Zhou, J. Rajahalme, J. Gross, A. Wang, J. Stringer, P. Shelar, K. Amidon, and M. Casado, "The design and implementation of open vswitch," in *Proceedings of the 12th USENIX Conference on Networked Systems Design and Implementation*, NSDI'15, (USA), p. 117–130, USENIX Association, 2015.

[3] Linux Foundation, "Frrouting." `https://frrouting.org/`.

[4] ESnet / Lawrence Berkeley National Laboratory, "iperf3." `https://iperf.fr/`.