Groupe 15 - Rapport du Projet Mini-Internet

Juliette Bluem, Antoine Laguette & Guillaume Tisserand

16 octobre 2022

Table des matières

Partie I : Introduction

A l'issue de ces 2 années d'études IA2R nous avons développé les connaissances et les compétences nécessaires à la réalisation d'un projet à grande échelle comme la réalisation de notre propre réseau internet.

Ce projet va nous permettre de mettre en application et surtout corréler tout ce que nous avons pu apprendre précédemment. Cependant, la principale différence et difficulté résidera dans la syntaxe des commandes de configuration saisies. en effet, le projet mini internet est trop gros pour être modélisé physiquement avec de vrais équipements. De ce fait, tout est virtualisé via FRRouting et OpenVSwitch, deux solutions de virtualisation réseau.

Plusieurs étapes sont nécessaires pour mener à bien ce projet, la première consiste à réaliser la configuration de base de notre mini internet. C'est à dire créer un réseau local, le connecter à un AS (Autonomous System) puis de faire en sorte que tous les hôtes du réseau configuré puissent se contacter. Cette configuration de base va passer par la mise en place de l'adressage, de VLAN, routage OSPF mais également de l'analyse de lien ou traffic-engineering.

Les autres groupes doivent effectuer la même configuration mais avec un adressage différent puis on passera à la seconde étape, l'élaboration d'une configuration BGP Globale avec iBGP et eBGP.

Enfin nous verrons comment mettre en place une police de management pour administrer et gérer notre mini internet.

Partie II : Connectivité Intra-domaine

Comme énoncé dans l'introduction, cette première partie a pour vocation la configuration de base de notre réseau afin que les autres équipes puissent faire de même pour inter-connecter tous les réseaux configurés. Cette partie n'est pas négligeable dans le sens où si nous manquons la moindre configuration d'une adresse IP ou d'un protocole cela peut avoir un impact extrêmement important sur le bon fonctionnement de notre mini internet.

1 Connectivité LAN

On commence par configurer le réseau LAN. C'est une étape que nous maîtrisons car nous avons toujours débuté par cette étape en TP et dans n'importe quelle autre configuration de réseau. On adresse les interfaces des hôtes staff et student respectivement au plan d'adressage donné :

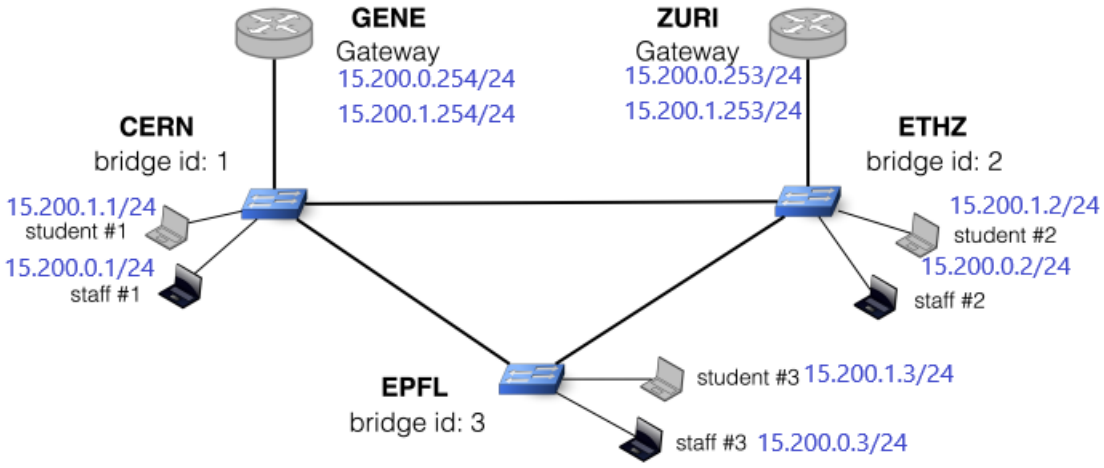

FIGURE 1 – Plan d'adressage

Une fois ce plan respecté nous mettons en place des VLAN pour que les étudiants ne puissent pas contacter le staff et inversement.
En nous intéressant plus aux routeurs, on adresse les interfaces puis on applique un routage dynamique OSPF en l'activant et en déclarant les réseaux voisins de chaque routeur

Après cela nous mettons en place le protocole STP qui nous permettra de conserver un lien de secours automatique si un des liens venait à se couper entre les commutateurs. Plus tard nous pourrions nous intéresser au protocole SNMP dans le cadre de la management policy.

Afin de nous assurer que tout le monde monde puisse maintenant communiquer et que nos règles de séparation Staff et Student soient bien en place, on effectue de simples ping.
Pour avoir plus de détails sur le trajet qu'empruntent nos données, nous effectuons des traceroute pour observer que toutes les données ne transitent pas que par un seul et unique trajet ou équipement.
De notre côté, tout fonctionne (évidemment). Par exemple si on réalise un traceroute entre Staff#2 et Student#1 on peut observer que les données transitent jusqu'au routeur puis redescendent vers les destinations car student et staff ne sont pas dans le même vlan donc ne peuvent pas communiquer via les commutateurs mais les routes réseaux sont configurées donc ils peuvent communiquer par réseau interposé grâce à l'OSPF configuré.

2 Connectivité AS

De la même manière que pour le LAN nous configurons toutes les interfaces de tous les routeurs de notre AS. C'est une partie qui demande beaucoup de minutie car ils y a un gros volume d'adressage à faire. Ainsi, nous respectons le schéma suivant :

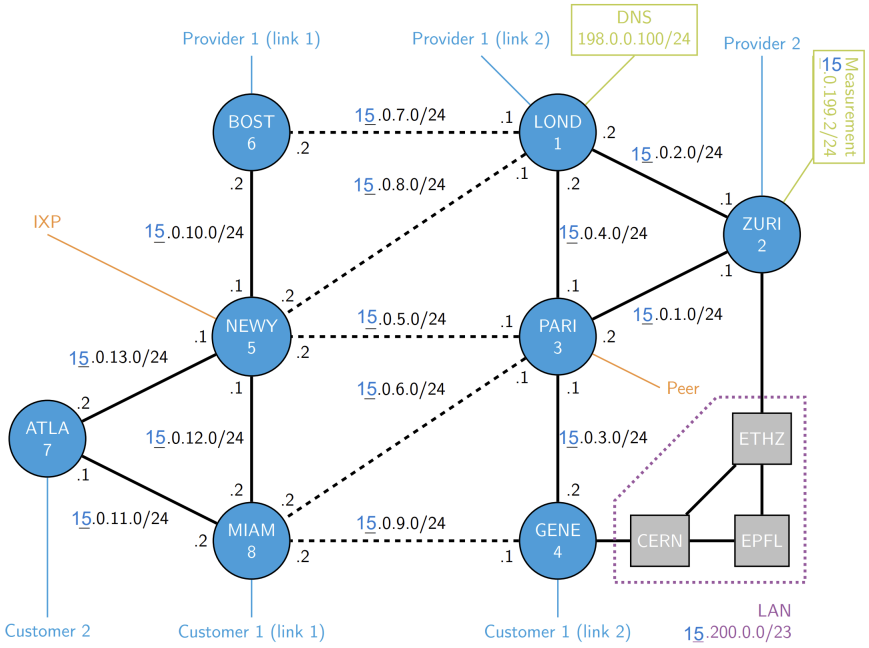

FIGURE 2 – Plan d'adressage

Nous avons configuré notre OSPF afin d'avoir un routage dynamique. Sa configuration est exactement la même que pour que notre LAN, c'est à dire en déclarant nos réseaux voisins sur chaque routeur. Ainsi, chaque hôte va pouvoir communiquer avec les autres.

Également, il ne faut pas oublier d'adresser les hôtes des routeurs de notre AS et les interfaces de loopback. Les interfaces de loopback vont nous servir par la suite pour la configuration de l'iBGP car iBGP établit des connexions TCP/IP grâce à ces interfaces. de même que pour le réseau LAN nous effectuons des ping et traceroute pour observer par où transitent nos données comme ci-dessous avec un traceroute entre l'hôte de Paris et l'hôte d'Atlanta

```
root@staff_2:~# traceroute 15.103.0.1
traceroute to 15.103.0.1 (15.103.0.1), 30 hops max, 60 byte packets
 1  15.200.0.253 (15.200.0.253)  2.714 ms  2.682 ms  2.667 ms
 2  PARI-GENE.group15 (15.0.3.1)  3.757 ms  3.654 ms PARI-ZURI.group15 (15.0.1.2)
2.675 ms
 3  host-PARI.group15 (15.103.0.1)  3.713 ms  3.622 ms  3.601 ms
```

FIGURE 3 – Traceroute hôte Paris vers hôte Atlanta

3 Traffic-engineering

En tant qu'opérateur réseau, notre but est de fournir des performances optimales à nos clients.
Pour cela, nous allons devoir définir plus finement notre configuration OSPF.

Les liens continentaux disposent tous d'une bande passante de 25 Mb/s. Les liens du LAN supportent 10 Mb/s. Concernant les liens transatlantiques, notre AS peut présenter une configuration parmi quatre. Nous devons donc bien sûr la connaître afin d'être certain de ce que nous proposons au client et de l'optimiser le mieux possible.

Afin d'identifier cette topologie, nous effectuons ce que nous appelons du traffic-engineering. Ce principe est basé sur l'étude des équipements et des liens qui composent notre réseau.

Via un outil appelé IPerf nous pouvons réaliser cette identification. En effet IPerf nous permet de faire une état des lieux de notre bande réseau afin d'en déterminer les limites.

Pour trouver la configuration des liens transatlantiques nous allons tester deux liens :
BOST – LOND

```
root@LOND_host:~# iperf3 -c 15.106.0.1 -b 25M
Connecting to host 15.106.0.1, port 5201
[  4] local 15.101.0.1 port 55666 connected to 15.106.0.1 port 5201
[ ID] Interval           Transfer     Bandwidth       Retr  Cwnd
[  4]   0.00-1.00   sec  2.82 MBytes  23.7 Mbits/sec    0    105 KBytes
[  4]   1.00-2.00   sec  3.00 MBytes  25.2 Mbits/sec    0    105 KBytes
[  4]   2.00-3.00   sec  3.00 MBytes  25.2 Mbits/sec    0    105 KBytes
[  4]   3.00-4.00   sec  3.00 MBytes  25.2 Mbits/sec    0    105 KBytes
[  4]   4.00-5.00   sec  3.00 MBytes  25.2 Mbits/sec    0    105 KBytes
[  4]   5.00-6.00   sec  3.00 MBytes  25.2 Mbits/sec    0    105 KBytes
[  4]   6.00-7.00   sec  2.88 MBytes  24.1 Mbits/sec    0    105 KBytes
[  4]   7.00-8.00   sec  3.00 MBytes  25.2 Mbits/sec    0    105 KBytes
[  4]   8.00-9.00   sec  3.00 MBytes  25.2 Mbits/sec    0    105 KBytes
[  4]   9.00-10.00  sec  3.00 MBytes  25.2 Mbits/sec    0    105 KBytes
- - - - - - - - - - - - - - - - - - - - - - - - -
[ ID] Interval           Transfer     Bandwidth       Retr
[  4]   0.00-10.00  sec  29.7 MBytes  24.9 Mbits/sec    0             sender
[  4]   0.00-10.00  sec  29.5 MBytes  24.7 Mbits/sec                  receiver
```

FIGURE 4 – Resultat Iperf entre Boston et London

Nous observons que le lien BOST – LOND peut supporter des échanges à 25Mb/s.
Sur nos quatre configurations d'AS possibles, seules deux ont cette capacité sur ce lien.

Nous voulons donc les différencier par le lien MIAM-PARI qui sera soit à 1Mb/s si nous sommes dans la configuration D, soit 25Mb/s dans le cas A.

* PARI – MIAM

```
Connecting to host 15.108.0.1, port 5201
[  4] local 15.103.0.1 port 47292 connected to 15.108.0.1 port 5201
[ ID] Interval           Transfer     Bandwidth       Retr  Cwnd
[  4]   0.00-1.00   sec  1.27 MBytes  10.7 Mbits/sec   17   1.41 KBytes
[  4]   1.00-2.00   sec  63.6 KBytes   521 Kbits/sec   16   2.83 KBytes
[  4]   2.00-3.00   sec   191 KBytes  1.56 Mbits/sec   17   1.41 KBytes
[  4]   3.00-4.00   sec  63.6 KBytes   521 Kbits/sec   14   1.41 KBytes
[  4]   4.00-5.00   sec   127 KBytes  1.04 Mbits/sec   14   1.41 KBytes
[  4]   5.00-6.00   sec   127 KBytes  1.04 Mbits/sec   13   1.41 KBytes
[  4]   6.00-7.00   sec   127 KBytes  1.04 Mbits/sec   18   2.83 KBytes
[  4]   7.00-8.00   sec   127 KBytes  1.04 Mbits/sec   14   2.83 KBytes
[  4]   8.00-9.00   sec  63.6 KBytes   521 Kbits/sec   19   2.83 KBytes
[  4]   9.00-10.00  sec   127 KBytes  1.04 Mbits/sec   15   1.41 KBytes
- - - - - - - - - - - - - - - - - - - - - - - - -
[ ID] Interval           Transfer     Bandwidth       Retr
[  4]   0.00-10.00  sec  2.27 MBytes  1.90 Mbits/sec  157             sender
[  4]   0.00-10.00  sec  2.10 MBytes  1.76 Mbits/sec                  receiver

iperf Done.
```

FIGURE 5 – Résultat Iperf entre Miami et Paris

Le lien PARI – MIAM est visiblement limité à 1Mb/s.
Nous éliminons donc la configuration A et pouvons conclure que nous sommes dans la configuration suivante :

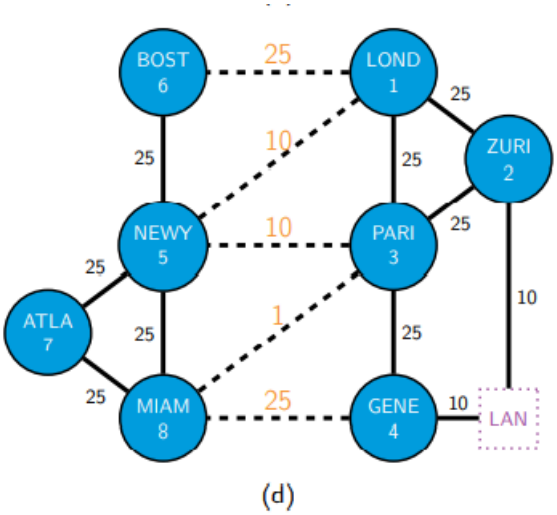

FIGURE 6 – Configuration D

Maintenant que nous avons parfaitement connaissance de la capacité des liens de notre AS, nous allons définir les coûts OSPF afin de privilégier certains liens selon des règles bien précises.

Nous choisissons dans un premier temps d'attribuer tous les liens 25Mb/s à un cout de 1, ceux de 10Mb/s, un cout de 10 et ceux de 1Mb/s, un cout de 100.
De cette façon, nous nous assurons de respecter les règles suivantes :

1. Aucun trafic ne traverse des liens transatlantiques deux fois
2. Les liens de plus forte bande passante sont utilisés en priorité pour les trafic intercontinentaux

Nous voulons maintenant modifier notre règle afin d'assurer une répartition de charge entre plusieurs chemins.

Tout trafic entre MIAM et NEWY doit être réparti sur deux chemins de même coût, le direct et celui passant uniquement par ATLA.
De la même façon, le trafic entre ZURI et LOND sera reparti entre deux chemins, le direct et celui passant par PARI. Pour cela, nous passons simplement le coût des liens directs à 2 au lieu de 1.

Enfin, nous devons nous assurer que le trafic entre ATLA et ZURI est réparti sur les deux liens transatlantiques à forte bande-passante. C'est le cas avec notre architecture actuelle.

Ci-dessous, un schémas récapitulatif de nos choix de coûts sur notre réseau :

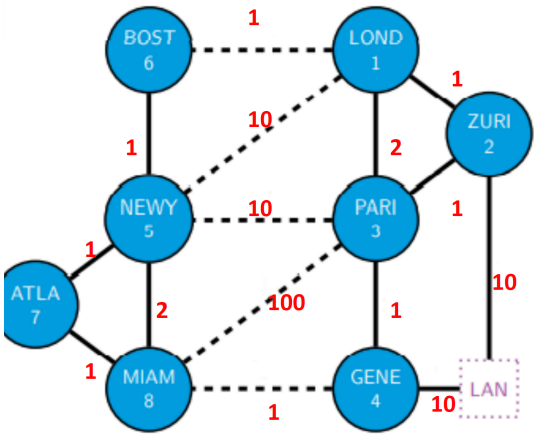

FIGURE 7 – Coûts des liens de notre AS

Nous mettons donc en place sur nos routeurs cette configuration de coût OSPF. Notons qu'ils faut absolument indiquer aux routeurs qu'ils ont le droit d'utiliser plusieurs chemins de même coûts.

Partie III : Configuration BGP globale

1 iBGP

Dans cette partie nous configurons des sessions BGP sur l'ensemble de nos routeurs et non pas uniquement ceux directement connectés.

Cette étape a pour objectif de créer un réseau dit full-mesh (ou maillé), permettant de garder les connexions fonctionnelles, et ce même si un ou plusieurs routeurs tombent en panne.

Nous configurons chaque routeur de la manière suivante :

```
X_router# conf t
X_router(config)# router bgp 15

X_router(config-router)# address-family ipv4 unicast
X_router(config-router-af)# exit

X_router(config-router)#neighbor 15.X.0.1 remote-as 15
X_router(config-router)#neighbor 15.X.0.1 update-source lo
```

On configure alors l'ensemble des adresses loopback de chaque routeur présent au seins de l'AS 15 en répétant ces deux dernières commandes.

On utilise ces adresses car si nous utilisons une adresse IP d'interface, et que celle-ci tombe en panne, la relation BGP disparaît.
Bien sûr, cela ne fait sens qu'uniquement si notre réseau dispose de liens redondants vers ce voisin.

Pour vérifier que les sessions BGP sont établies nous utilisons la commande suivante.

```
router# show ip bgp summary
```

```
PARI_router# sh ip bgp summary

IPv4 Unicast Summary:
BGP router identifier 15.153.0.1, local AS number 15 vrf-id 0
BGP table version 5
RIB entries 9, using 1656 bytes of memory
Peers 8, using 163 KiB of memory

Neighbor        V         AS MsgRcvd MsgSent   TblVer  InQ OutQ  Up/Down State/PfxRcd
15.151.0.1      4         15     394     399        0    0    0 06:31:18            0
15.152.0.1      4         15     396     401        0    0    0 06:33:09            0
15.154.0.1      4         15     397     402        0    0    0 06:33:37            1
15.155.0.1      4         15     396     399        0    0    0 06:31:06            2
15.156.0.1      4         15     393     398        0    0    0 06:30:13            0
15.157.0.1      4         15     403     409        0    0    0 06:34:15            1
15.158.0.1      4         15     396     400        0    0    0 06:32:40            1
179.0.41.2      4         16     339     341        0    0    0 05:33:55            3

Total number of neighbors 8
```

FIGURE 8 – Session BGP du router PARI

On vérifie ainsi que l'ensemble de notre AS est bien connectée selon le maillage mis en place.

Cela termine la partie de configuration du BGP interne.

2 eBGP

La configuration de BGP externe se fait en coordination avec les autres AS.

Durant cette première période, tous les groupes (représentant chacun une AS) n'étant pas prêts, la configuration du BGP externe sera réalisée lors de la prochaine période de travail.

Nous avons tout de même réussi à nous organiser avec nos voisins directs afin de déterminer les adresses et réseaux de liaison entre les AS.

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

FIGURE 9 – Tableau des voisins

Nous avons donc configuré nos routeurs en suivant ce tableau et nous nous tenons prêts pour la suite du projet.