



.....Le routage : réseau Opérateur..... 12.11.2019

l'ancêtre du GPS®

Non, l'autre droite....

Auteur : Pascal Fougeray



source : <http://www.dudelire.com/nimportekoi/circulation-anglaise,37.html>

1 Introduction

Le routage est aux réseaux ce que les processus sont au processeur... Bon ça ne veut rien dire.

Le routage c'est se poser la question suivante : **Par où je passe pour aller là ?**

Bon ce n'est pas encore terrible mais ça s'améliore, non ?

Comme nous l'avons vu dans le cours intitulé Internet, les réseaux contiennent des adresses et à ces adresses se trouvent des entités.

Le souci c'est qu'il existe des dizaines, que dis-je des centaines, que dis-je des milliers, que dis-je beaucoup de routes possibles pour y aller.

Alors laquelle prendre ?

réponse : ça dépend...

Elle est nulle l'introduction du prof, on a rien compris.

Rassurez vous le prof non plus et comment introduire le routage ?

Internet ce sont des milliers de réseaux (Backbone) et chaque réseau contient plein de routes et de routeurs !

Entre 2 routes se trouve un routeur et entre 2 routeurs se trouve un réseau !

Les réseaux sont comme des boîtes qui contiennent des boîtes, un réseau contient des réseaux, un réseau contient des routeurs et ce que vous n'avez pas encore vu, c'est qu'un routeur peut contenir des routeurs... virtuels...



2 Le Routage à travers l'Internet

Le routage à travers l'Internet est de 2 types, Intra ou Inter domaine(s)

1. La partie Intra Domaine sera traitée dans les parties RIP et OSPF
2. La partie Inter Domaine sera traitée dans la partie BGP

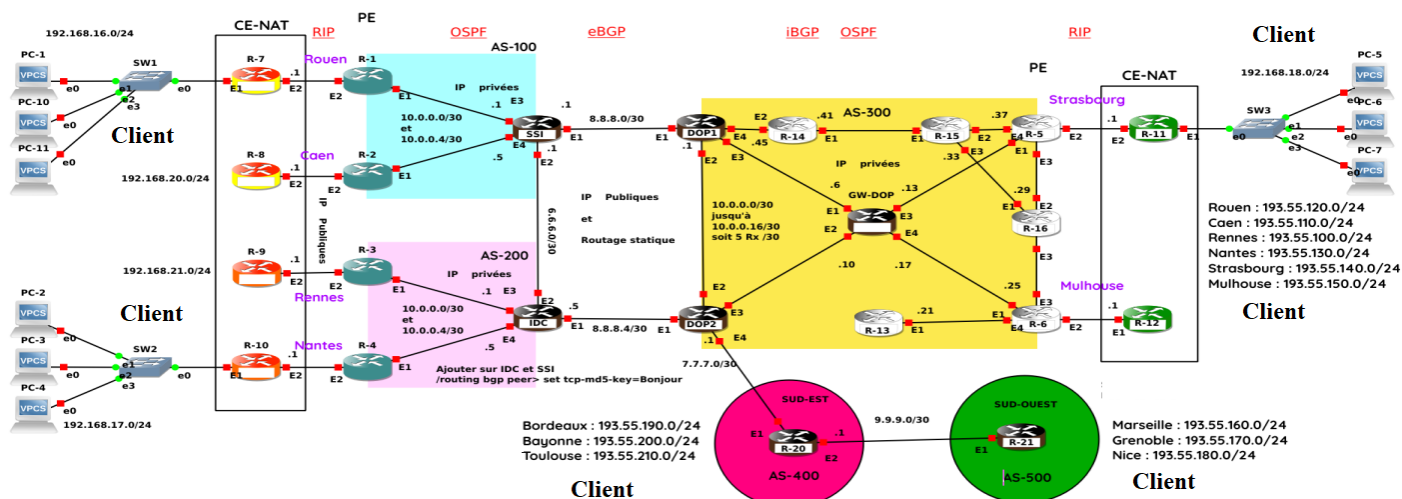
Nous allons juste voir rapidement des définitions !

Voici un exemple (Celui du TP 1 sur le routage)

On a :

- 5 domaines : Appelés AS-100 à AS-500
- Les clients (Les villes)

Ici on a 12 clients qui sont représentés par des villes mais qui sont aussi des noms de sociétés etc !



2.1 Intra-domaine

1 AS - 1 Domaine - IGP - Un seul Opérateur ou ISP ou FAI

On parle de réseau d'opérateur

Dans un réseau d'opérateur on utilise le **routage dynamique** !

Il existe 4 protocoles de routage dynamique qui ont chacun leur intérêt. En TP nous en verrons deux RIP et OSPF Pourquoi ? Parce que pas le temps et que le but est de comprendre les principes et l'intérêt du routage dynamique ! Ce seront RIP et OSPF, pourquoi ?

Parce que ...

Pas les meilleurs, le meilleur c'est... aucune idée...

- RIPv2 qui est généralement utilisé entre le CE (**Customer Edge**) et le PE (**Provider Edge**)
 - OSPF dans l'AS lui même, la Backbone !
 - Un AS détermine le chemin d'un paquet à l'intérieur de son domaine, **il applique la politique qu'il veut** !
 - Il utilise un protocole de routage à état des liens, **IGP, Interior Gateway Protocols**, tels IS-IS, OSPF, RIP. Cet IGP trouve le "**meilleur**" chemin à travers un AS. Il est possible d'avoir des chemins explicites quand on applique une politique de **Trafic Ingénierie**.
 - La performance est une question essentielle, meilleur chemin.
- Mais qu'est-ce que le meilleur chemin ?**

2.2 Inter-domaines

n AS - n Domaines - EGP - Plusieurs Opérateurs ou ISP ou FAI

On parle d'un réseau de réseaux d'opérateurs

Nous avons vu que les opérateurs possèdent chacun un **Backbone**.

Si on relie ces Backbones entre eux cela forme Internet !

Le protocole de routage utilisé par les opérateurs pour s'échanger les routes d'un backbone à l'autre se nomme BGP

Nous reviendrons sur ce protocole lors du cours sur BGP



- Les AS s'échangent des informations "d'**atteignabilité**"
- Basé sur des politiques entre eux.
 - la politique n'est pas obligatoirement la même entre
 - un AS A et un AS B que celle entre
 - ce même AS A et un autre AS C
- Pas nécessairement le plus court chemin, **mais le plus court est-il le meilleur?**
- Ils utilisent un protocole de routage de type EGP **Exterior Gateway Protocols (BGP)**.
Cet EGP définit des règles de relations entre AS

3 Routage

Le routage est le mécanisme par lequel des chemins sont sélectionnés dans un réseau pour acheminer les données d'un expéditeur jusqu'à un ou plusieurs destinataires.

C'est une tâche (processus?) exécutée dans les réseaux, tels que

- les réseaux **téléphoniques**,
- le réseau **Internet**,
- et les réseaux de **transports**.

Chaque entité ou agent dans le monde du réseau possède une table de routage !

Que ce soit un **routeur** ou un **ordinateur**

3.1 Table de routage

que l'on peut voir à l'aide des commandes suivantes :

- Sous **Linux** : **ip route ls**

```
$ ip route ls
default via 10.38.16.1 dev eth0
10.38.16.0/22 dev eth0 proto kernel scope link src 10.38.19.111
169.254.0.0/16 dev eth0 scope link metric 1000
172.17.0.0/16 dev docker0 proto kernel scope link src 172.17.0.1 linkdown
192.168.56.0/24 dev vboxnet0 proto kernel scope link src 192.168.56.1 linkdown
fougeray@C304L-159C00:~$
```
- Sous windows : **route PRINT -4 ou netstat -r**

```
C:\WINDOWS\system32>route PRINT -4
```

Liste d'Interfaces

```
25...c8 d3 ff 1f 67 40 .....Intel(R) Ethernet Connection (2) I219-LM
7...0a 00 27 00 00 07 .....Npcap Loopback Adapter
17...0a 00 27 00 00 11 .....VirtualBox Host-Only Ethernet Adapter #3
16...e4 a7 a0 6c 02 56 .....Microsoft Wi-Fi Direct Virtual Adapter #4
14...e6 a7 a0 6c 02 55 .....Microsoft Wi-Fi Direct Virtual Adapter #5
20...00 50 56 c0 00 01 .....VMware Virtual Ethernet Adapter for VMnet1
23...00 50 56 c0 00 08 .....VMware Virtual Ethernet Adapter for VMnet8
26...e4 a7 a0 6c 02 55 .....Intel(R) Dual Band Wireless-AC 8260
1.....Software Loopback Interface 1
```

IPv4 Table de routage

Itinéraires actifs :

Destination réseau	Masque réseau	Adr. passerelle	Adr. interface	Métrique
0.0.0.0	0.0.0.0	192.168.1.254	192.168.1.18	25
127.0.0.0	255.0.0.0	On-link	127.0.0.1	331
127.0.0.1	255.255.255.255	On-link	127.0.0.1	331
127.255.255.255	255.255.255.255	On-link	127.0.0.1	331
192.168.1.0	255.255.255.0	On-link	192.168.1.18	281
192.168.1.18	255.255.255.255	On-link	192.168.1.18	281
192.168.1.255	255.255.255.255	On-link	192.168.1.18	281
192.168.56.0	255.255.255.0	On-link	192.168.56.1	281
192.168.56.1	255.255.255.255	On-link	192.168.56.1	281
192.168.56.255	255.255.255.255	On-link	192.168.56.1	281
192.168.83.0	255.255.255.0	On-link	192.168.83.1	291
192.168.83.1	255.255.255.255	On-link	192.168.83.1	291
192.168.83.255	255.255.255.255	On-link	192.168.83.1	291
192.168.109.0	255.255.255.0	On-link	192.168.109.1	281
192.168.109.1	255.255.255.255	On-link	192.168.109.1	281
192.168.109.255	255.255.255.255	On-link	192.168.109.1	281
192.168.203.0	255.255.255.0	On-link	192.168.203.1	291
192.168.203.1	255.255.255.255	On-link	192.168.203.1	291
192.168.203.255	255.255.255.255	On-link	192.168.203.1	291
224.0.0.0	240.0.0.0	On-link	127.0.0.1	331
224.0.0.0	240.0.0.0	On-link	192.168.109.1	281
224.0.0.0	240.0.0.0	On-link	192.168.56.1	281
224.0.0.0	240.0.0.0	On-link	192.168.1.18	281
224.0.0.0	240.0.0.0	On-link	192.168.203.1	291
224.0.0.0	240.0.0.0	On-link	192.168.83.1	291
255.255.255.255	255.255.255.255	On-link	127.0.0.1	331
255.255.255.255	255.255.255.255	On-link	192.168.109.1	281

— Routeurs Mikrotik : **ip route print**

```
[admin@OSPF-BGP] /ip route> print
Flags: X - disabled, A - active, D - dynamic,
C - connect, S - static, r - rip, b - bgp, o - ospf, m - mme,
B - blackhole, U - unreachable, P - prohibit
```

#	ADo	DST-ADDRESS	PREF-SRC	GATEWAY	DISTANCE
0	ADo	1.1.1.1/32		10.0.0.21	110
1	ADo	2.2.2.2/32		10.0.0.21	110
2	ADo	3.3.3.3/32		10.0.0.21	110
3	ADo	4.4.4.4/32		10.0.0.21	110
4	ADo	5.5.5.5/32		10.0.0.21	110
5	ADo	6.6.6.6/32		10.0.0.21	110
6	ADC	7.7.7.7/32	7.7.7.7	lo	0
7	A S	8.8.8.8/32		193.55.130.2	1
8	ADo	10.0.0.0/30		10.0.0.21	110
9	ADo	10.0.0.4/30		10.0.0.21	110
10	ADo	10.0.0.8/30		10.0.0.21	110
11	ADo	10.0.0.12/30		10.0.0.21	110
12	ADo	10.0.0.16/30		10.0.0.21	110
13	ADC	10.0.0.20/30	10.0.0.22	ether2	0
14	ADb	11.0.0.0/27		193.55.130.2	20
15	ADo	192.168.1.0/24		10.0.0.21	110
16	ADo	192.168.2.0/24		10.0.0.21	110
17	ADo	192.168.17.0/24		10.0.0.21	110
18	ADo	192.168.18.0/24		10.0.0.21	110

```
[admin@OSPF-BGP] /ip route> □
```

— Routeurs Cisco : **show ip route**

```

R1#show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area

Gateway of last resort is not set

    10.0.0.0/8 is variably subnetted, 13 subnets, 2 masks
C       10.12.0.2/31 is directly connected, GigabitEthernet4/0
O       10.2.2.2/32 [110/2] via 10.12.0.2, 00:04:26, GigabitEthernet4/0
O       10.3.3.3/32 [110/3] via 10.12.0.2, 00:04:26, GigabitEthernet4/0
C       10.1.1.1/32 is directly connected, Loopback0
O       10.6.6.6/32 [110/3] via 10.12.0.2, 00:04:26, GigabitEthernet4/0
O       10.4.4.4/32 [110/4] via 10.12.0.2, 00:04:26, GigabitEthernet4/0
O       10.5.5.5/32 [110/5] via 10.12.0.2, 00:04:26, GigabitEthernet4/0
O       10.26.0.2/31 [110/2] via 10.12.0.2, 00:04:26, GigabitEthernet4/0
O       10.23.0.2/31 [110/2] via 10.12.0.2, 00:04:26, GigabitEthernet4/0
O       10.45.0.2/31 [110/4] via 10.12.0.2, 00:04:26, GigabitEthernet4/0
O       10.46.0.2/31 [110/3] via 10.12.0.2, 00:04:26, GigabitEthernet4/0
O       10.34.0.2/31 [110/3] via 10.12.0.2, 00:04:26, GigabitEthernet4/0
O       10.36.0.2/31 [110/3] via 10.12.0.2, 00:04:27, GigabitEthernet4/0
--

```

— Routeurs Juniper : **show route table**

```

user@router> show route

inet.0: 9 destinations, 9 routes (9 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both

10.10.10.91/32      *[Direct/0] 00:09:40
                   > via lo0.0
10.10.10.92/32      *[OSPF/10] 00:01:50, metric 1
                   > to 172.16.1.2 via ge-0/0/2.0
100.100.1.0/24      *[Static/5] 00:01:50
                   Reject
172.16.1.0/24       *[Direct/0] 00:06:09
                   > via ge-0/0/2.0
172.16.1.1/32       *[Local/0] 00:06:09
                   Local via ge-0/0/2.0
192.168.0.0/16      *[Aggregate/130] 00:00:06
                   Reject
192.168.0.0/17      *[Aggregate/130] 00:00:06
                   > to 172.16.1.2 via ge-0/0/2.0
192.168.50.0/24     *[Static/5] 00:00:06
                   > to 172.16.1.2 via ge-0/0/2.0
192.168.51.0/24     *[Static/5] 00:00:06
                   > to 172.16.1.2 via ge-0/0/2.0

```

— etc...

La table de routage contient :

- les adresses du routeur ou de l'ordinateur,
- les adresses des sous-réseaux auxquels le routeur est directement connecté,
- les routes **statiques**, celles configurées **explicitement**,
- les routes **dynamiques**, apprises par des protocoles de routage dynamique tels BGP, OSPF, IS-IS, etc.
- une route par **défaut** !

3.2 Objectifs des protocoles de routage

1. Le rôle principal est de **découvrir dynamiquement** les routes vers les réseaux d'un **inter réseau** et les inscrire dans la **table de routage sur routeur**.
2. S'il existe plus d'une route vers un réseau, inscrire **la meilleure route** dans la table de routage.
3. **Détecter** les routes **invalides** et les **supprimer** de la table de routage.
4. **Ajouter** le plus rapidement possible les **nouvelles** routes ou **remplacer** le plus rapidement les routes **perdues** par **la meilleure route actuellement disponible**.

3.3 Fonctionnement

- Un protocole de routage transporte des informations sur les différentes routes dans l'inter réseau mais aussi **des messages de maintien de relations de voisinage**.
- Chaque routeur reçoit et envoie des informations de routage à ses **voisins** et que ses **voisins!!!**

Mais qu'est-ce qu'un voisin !

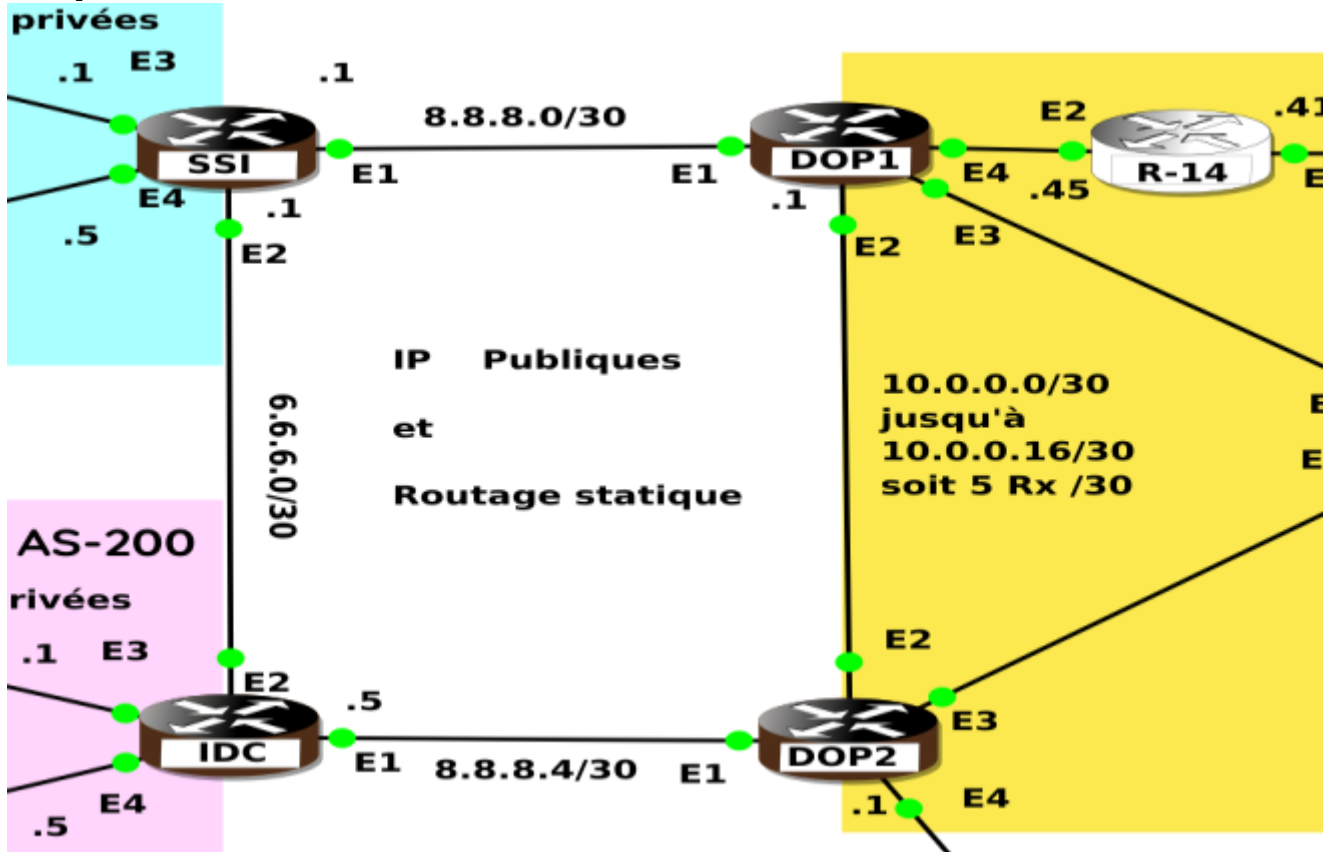
- Pour OSPF et autre c'est le routeur d'à côté physiquement !

Il est appelé **neighbor**

- Pour BGP ce n'est pas vrai !

Il est appelé **peer**

Exemple sur la structure du TP



Le routeur DOP1 à

- 2 voisins OSPF : **Neighbor**, Ici R-14 et DOP2

On peut le voir à l'aide de la commande **/routing ospf neighbor print**

```
[admin@DOP1] /routing ospf> neighbor
find print
[admin@DOP1] /routing ospf> neighbor print
0 instance=default router-id=2.2.2.2 address=10.0.0.2 interface=ether2
priority=1 dr-address=10.0.0.2 backup-dr-address=10.0.0.1 state="Full"
state-changes=6 ls-retransmits=0 ls-requests=0 db-summaries=0
adjacency=2m59s

1 instance=default router-id=4.4.4.4 address=10.0.0.6 interface=ether3
priority=1 dr-address=10.0.0.6 backup-dr-address=10.0.0.5 state="Full"
state-changes=6 ls-retransmits=0 ls-requests=0 db-summaries=0
adjacency=3m1s
[admin@DOP1] /routing ospf> █
```

- 2 voisins BGP : **Peer**, Ici SSI et DOP2

On peut le voir à l'aide de la commande **/routing bgp peer print detail**

```
[admin@DOP1] /routing bgp> peer print detail
Flags: X - disabled, E - established
0 E name="SSI" instance=default remote-address=8.8.8.1 remote-as=100
  tcp-md5-key="" nexthop-choice=default multihop=no route-reflect=no
  hold-time=3m ttl=255 in-filter="" out-filter="" address-families=ip
  default-originate=never remove-private-as=no as-override=no passive=no
  use-bfd=no
1 E name="DOP2" instance=default remote-address=10.0.0.2 remote-as=300
  tcp-md5-key="" nexthop-choice=default multihop=no route-reflect=no
  hold-time=3m ttl=255 in-filter="" out-filter="" address-families=ip
  default-originate=never remove-private-as=no as-override=no passive=no
  use-bfd=no
2 E name="GW-DOP" instance=default remote-address=10.0.0.6 remote-as=300
  tcp-md5-key="" nexthop-choice=default multihop=no route-reflect=no
  hold-time=3m ttl=255 in-filter="" out-filter="" address-families=ip
  default-originate=never remove-private-as=no as-override=no passive=no
  use-bfd=no
[admin@DOP1] /routing bgp>
```

- Il applique un algorithme, par exemple **Dijskra** pour OSPF, qui optimise ces informations en **chemins** cohérents.
Un chemin est un ensemble de routes !

3.4 Routage statique VS routage dynamique

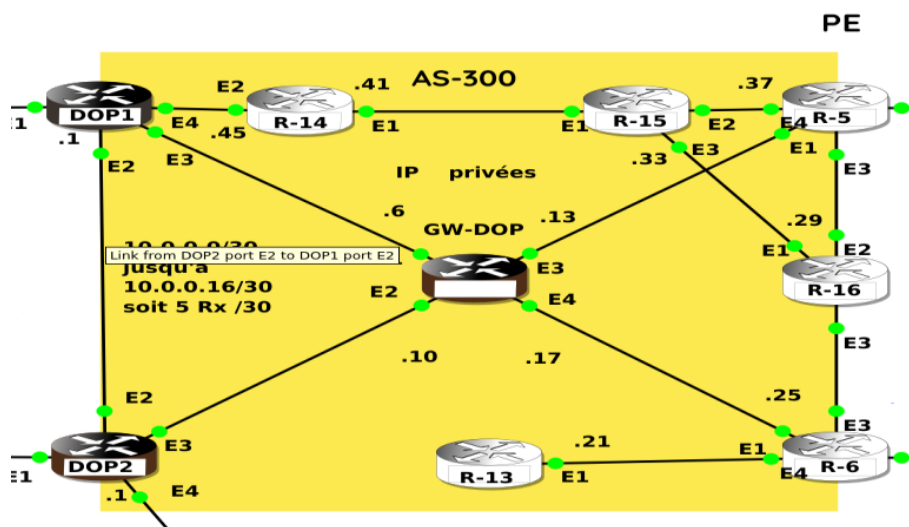
- **Avantages** du routage statique :
 - Il peut servir de mécanisme de backup.
 - Il est facile à configurer.
 - Aucune ressource supplémentaire nécessaire. (Ne prends pas de processus !)
 - Il est plus sécurisé.
- **Désavantages** du routage statique :
 - Chaque changement dans la topologie nécessite une intervention manuelle sur les routeurs de la topologie.
 - Cette méthode ne convient pas pour des réseaux d'opérateurs !!!

3.5 Système autonome (AS)

- Un système autonome (**AS**) est un ensemble de réseaux sous la même **autorité administrative** dans le sens administratif !.
- Au sein d'un système autonome, les routes sont générées par des protocoles de routage intérieurs les **IGP** comme **RIP**, **EIGRP**, **OSPF** ou **ISIS**.
- **Le protocole** (il n'y en a qu'un !) de routage qui permet de connecter les AS entre eux est le protocole de routage extérieur **EGP** comme **BGP**.
- Dans le contexte de l'interconnexion mondiale des réseaux, l'**IANA** (par délégation aux organismes régionaux) attribue les numéros de système autonome (16/32 bits).

Exemple sur la structure du TP nous avons 5 AS

Tous les routeurs de l'AS-300 sont gérés par la même équipe



Nous verrons cela plus en détails dans le cours sur BGP !

3.6 Quelques définitions !

Convergence : c'est le temps nécessaire pour qu'un ensemble de routeurs puissent disposer d'une vision **homogène, complète et efficace** de l'**ensemble des routes d'un inter réseau**.



Le temps de convergence est particulièrement éprouvé lorsqu'il y a des modifications topologiques dans l'inter réseau.

Il est très rapide pour OSPF et très lent pour BGP

Mais qu'est-ce que rapide et lent ?

Métrique : La métrique d'une route est la valeur d'une route en comparaison à d'autres routes apprises par le même protocole de routage.

Plus sa valeur est faible, meilleure est la route.

Chaque protocole dispose de sa méthode de valorisation.

On peut trouver toute une série de composantes de métrique parmi lesquelles :

- le nombre de sauts **RIP**
- la bande passante **EIGRP**
- le délai **EIGRP**
- la charge **EIGRP**
- la fiabilité **EIGRP**
- le coût **OSPF** et **IS-IS**

Distance administrative d'une route : indique la préférence dans une table de routage pour des destinations apprises par un protocole de routage par rapport aux mêmes destinations apprises par un autre protocole de routage. Cette valeur est codée sur 8 bits et va de 0 à 255

Plus la valeur est petite et plus le protocole est préféré.

Par exemple, une route EIGRP sera préférée à une route RIP ;

Une route statique sera préférée à toute autre route dynamique.

Le tableau ci dessous donne les **distances administratives**

Méthode de routage	Distance administrative
Réseau connecté	0
Route statique	1
Ext-BGP	20
Int-EIGRP	90
OSPF	110
IS-IS	115
RIP	120
Int-BGP	200
Inconnu	255

3.7 Protocoles de routage à vecteur de distance

- Un protocole de routage à vecteur de distance utilise un **algorithme de routage additionnant les distances** pour trouver les meilleures routes (**Bellman-Ford**).
- Les routeurs envoient la totalité de leur table de routage aux voisins.
- Ils sont sensibles aux boucles de routage.
- Avec ce type de protocole, aucun routeur ne remplit de fonction particulière. On parle de connaissance "plate" de l'inter réseau ou de routage non-hiérarchique.
- Ils convergent lentement.
- **RIP** et **EIGRP** (Cisco) sont des protocoles à vecteur de distance
- Ils ne sont pas utilisés dans les backbones car MPLS (voir en M1 !) a besoin d'un protocole de routage à état de liens

3.8 Protocoles de routage à état de liens

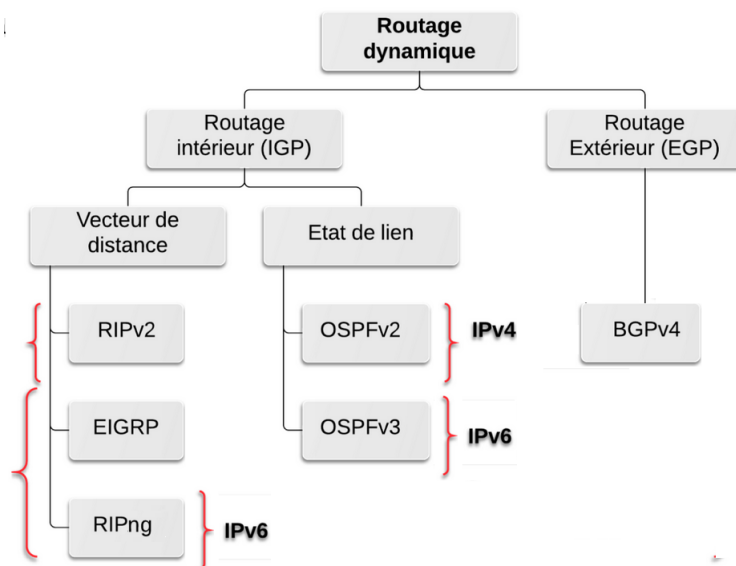
On verra leur étude un peu plus loin dans les parties OSPF et BGP !

- Un protocole de routage à état de liens utilise un algorithme plus efficace (**Dijkstra** ou **Shortest Path First**) mais demande plus de ressources CPU/RAM.
- Les routeurs collectent l'ensemble des **coûts des liens** d'un inter réseau et construisent de leur point de vue l'arbre de tous les chemins possibles.
Les meilleures routes sont alors intégrées à la table de routage.
- On parle de routage hiérarchique.



- Ils convergent très rapidement.
- **OSPF** et IS-IS sont des protocoles de routage à état de liens.
- **Les routeurs entretiennent des relations de voisinage maintenues, ils n'arrêtent pas de dialoguer !**

3.9 Synthèse de protocoles de routage



3.10 Synthèse des IGP

Vecteur de distance	État de liens
Algorithme Bellman-Ford (RIP)	Algorithme Dijkstra (OSPF)
Facile à configurer	Compétences requises
Partage des tables de routage	Partage des liaisons
Réseaux plats	Réseaux organisés en aires
Convergence plus lente	Convergence rapide, répartition de charge
Topologies limitées	Topologies complexes et larges
Gourmand en bande passante	Relativement discret
Peu consommateur en RAM et CPU	Grand consommateur en RAM et CPU
Mises à jour régulière en Broadcast/Multicast	Mises à jour immédiate
Pas de signalisation	Signalisation fiable et en mode connecté (BGP)
RIP v1, v2 et NG (IPv6)	OSPFv2/v3
EIGRP	ISIS

3.11 La route par défaut (Gateway!)

Elle est obligatoire sur chaque entité d'un réseau travaillant sur la couche IP.

C'est la route qui mène à la **passerelle** (*gateway* en anglais!)

Une passerelle est un ordinateur qui fait du routage!

Nous l'avons vu sous Linux en TP

L'image précédente montre que les PC de sciences 3 sous Linux sortent par la passerelle d'@IP 10.38.16.1

```
$ ip route ls
```

```
default via 10.38.16.1 dev eth0
```

```
10.38.16.0/22 dev eth0 proto kernel scope link src 10.38.19.111
```

```
169.254.0.0/16 dev eth0 scope link metric 1000
```

```
172.17.0.0/16 dev docker0 proto kernel scope link src 172.17.0.1 linkdown
```

```
192.168.56.0/24 dev vboxnet0 proto kernel scope link src 192.168.56.1 linkdown
```

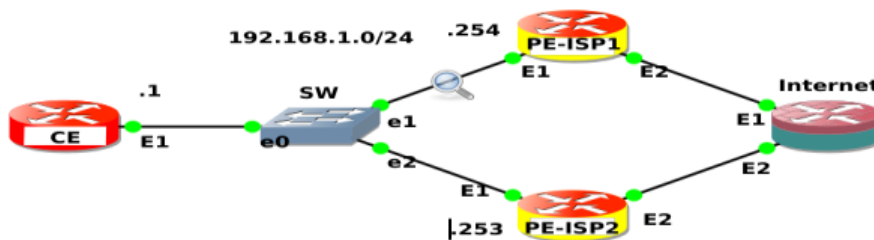
```
fougeray@C304L-159C00:~$
```

```
$
```

3.12 Répartition de charge

Ce que l'on appelle communément "**Load Balancing**" est la capacité pour un routeur de supporter plusieurs chemins à **coût égaux** vers une destination.

- Il en résulte que les paquets vers une même destination sont répartis sur plusieurs interfaces.
- Il existe aussi le **load balancing** pour un client désirant avoir toujours accès à Internet !
- Il a donc **2 passerelles** !
- Prenons l'exemple de la structure suivante :



Un client, ici CE pour **Customer-Edge** est chez 2 ISP différents bien-sur.

Son ISP principal est ISP1, second est alors ISP2 en toute logique.

Voici sa configuration pour son interface de sortie **Ether1**

```
/ip route add gateway=192.168.1.254 check-gateway=ping
/ip route add gateway=192.168.2.253 distance=2
```

Ce routeur a ou aurait ? ainsi 2 routes par défaut, 2 **passerelles, gateway**

1. Une principale représentée par l'@ IP 192.168.1.254
2. Une secondaire représentée par l'@ IP 192.168.1.253

L'image ci-dessous représente comment réactiver rapidement la principale si elle venait à tomber.

Le premier **/ip route print** montre que la route par défaut 0.0.0.0/0 active est la secondaire

On fait un ping volontaire et le second **/ip route print** montre que la route par défaut 0.0.0.0/0 active est la principale

```
[admin@CE] > /ip route print
Flags: X - disabled, A - active, D - dynamic,
C - connect, S - static, r - rip, b - bgp, o - ospf, m - mme,
B - blackhole, U - unreachable, P - prohibit
# DST-ADDRESS PREF-SRC GATEWAY DISTANCE
0 S 0.0.0.0/0 192.168.1.254 1
1 A S 0.0.0.0/0 192.168.1.253 2
2 ADC 192.168.1.0/24 192.168.1.1 ether1 0
[admin@CE] > /ping 192.168.1.254
SEQ HOST SIZE TTL TIME STATUS
0 192.168.1.254 56 64 5ms
1 192.168.1.254 56 64 1ms
sent=2 received=2 packet-loss=0% min-rtt=1ms avg-rtt=3ms max-rtt=5ms
[admin@CE] > /ip route print
Flags: X - disabled, A - active, D - dynamic,
C - connect, S - static, r - rip, b - bgp, o - ospf, m - mme,
B - blackhole, U - unreachable, P - prohibit
# DST-ADDRESS PREF-SRC GATEWAY DISTANCE
0 A S 0.0.0.0/0 192.168.1.254 1
1 S 0.0.0.0/0 192.168.1.253 2
2 ADC 192.168.1.0/24 192.168.1.1 ether1 0
[admin@CE] >
```

Dans la réalité pas besoin faire un ping volontaire. Le routeur CE ping toutes les 10 secondes la passerelle principale.

Si elle ne répond pas il change sa route par défaut !

No.	Time	Source	Destination	Protocol	Leng	Info
...	996.262008	192.168.1.254	192.168.1.1	ICMP	70	Echo (ping) reply id=0xe500, seq=31488/...
...	1006.2722...	192.168.1.1	192.168.1.254	ICMP	70	Echo (ping) request id=0xe500, seq=31744/...
...	1006.2728...	192.168.1.254	192.168.1.1	ICMP	70	Echo (ping) reply id=0xe500, seq=31744/...
...	1016.2786...	192.168.1.1	192.168.1.254	ICMP	70	Echo (ping) request id=0xe500, seq=32000/...
...	1016.2792...	192.168.1.254	192.168.1.1	ICMP	70	Echo (ping) reply id=0xe500, seq=32000/...
...	1026.2821...	192.168.1.1	192.168.1.254	ICMP	70	Echo (ping) request id=0xe500, seq=32256/...
...	1026.2830...	192.168.1.254	192.168.1.1	ICMP	70	Echo (ping) reply id=0xe500, seq=32256/...
...	1036.2982...	192.168.1.1	192.168.1.254	ICMP	70	Echo (ping) request id=0xe500, seq=32512/...
...	1036.2987...	192.168.1.254	192.168.1.1	ICMP	70	Echo (ping) reply id=0xe500, seq=32512/...
...	1046.3024...	192.168.1.1	192.168.1.254	ICMP	70	Echo (ping) request id=0xe500, seq=32768/...
...	1046.3030...	192.168.1.254	192.168.1.1	ICMP	70	Echo (ping) reply id=0xe500, seq=32768/...

Frame 244: 70 bytes on wire (560 bits), 70 bytes captured (560 bits) on interface 0
 Ethernet II, Src: 0c:99:5f:ad:99:00 (0c:99:5f:ad:99:00), Dst: 0c:99:5f:79:9d:00 (0c:99:5f:79:9d:00)
 Internet Protocol Version 4, Src: 192.168.1.1, Dst: 192.168.1.254
 Internet Control Message Protocol

Conclusion : A un temps **t**, il n'y a qu'une seule route par défaut, mais sur une période on peut en avoir plusieurs !

Et c'est même toujours le cas !

3.13 La redistribution

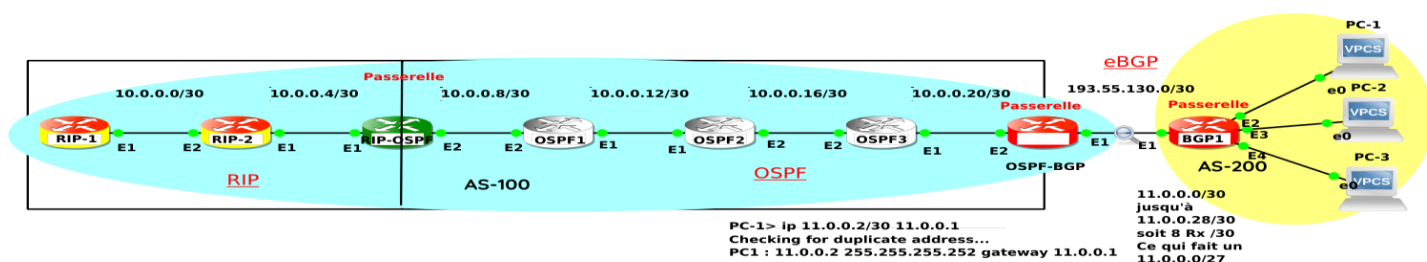
C'est le principe d'échange d'informations entre 2 protocoles de routage différents

Pour gérer efficacement plusieurs protocoles de routage dans le même réseau, l'information de routage doit être partagée entre les protocoles

Par exemple,

- des routes apprises par un processus RIP peuvent être importées par un processus OSPF
- des routes apprises par un processus OSPF peuvent être importées par un processus BGP
- Uniquement les routeurs frontaliers (RIP-OSPF et OSPF-BGP) doivent faire tourner plus d'une instance d'un protocole de routage et cela uniquement si nécessaire
- Chaque processus de routage requiert des quantités importantes de mémoire et CPU
- Un routeur qui utilise plusieurs protocoles peut apprendre le même réseau à partir de différentes sources d'information
- La **Distance Administrative** permet de choisir parmi différentes sources d'information
- Si 2 routes ont les mêmes adresses réseau et masques, le routeur toujours choisit la route dont le protocole de routage a la **plus petite distance administrative**
- Tous les routeurs n'ont pas besoin de connaître toutes les routes d'un réseau ! Mais dans ce cas il leur faut la fameuse route par défaut !

Ce qui est le cas dans la structure suivante :



Exemples de table de routage

— **Rip-1** :

- Il ne connaît pas ce qu'il y a après le routeur de passerelle RIP-OSPF
- Il ne sait faire que du RIP !
- Sa route par défaut lui permet de sortir !

```
[admin@RIP-1] /ip route> print
Flags: X - disabled, A - active, D - dynamic, C - connect, S - static,
r - rip, b - bgp, o - ospf, m - mme, B - blackhole, U - unreachable, P
- prohibit
# DST-ADDRESS      PREF-SRC      GATEWAY      DISTANCE
0 A S 0.0.0.0/0      10.0.0.2      1
1 ADC 1.1.1.1/32     1.1.1.1       0
2 ADr 2.2.2.2/32     10.0.0.2     120
3 ADr 3.3.3.3/32     10.0.0.2     120
4 ADC 10.0.0.0/30     10.0.0.1     0
5 ADr 10.0.0.4/30     10.0.0.2     120
6 ADC 192.168.1.0/24  192.168.1.1   0
7 ADC 192.168.2.0/24  192.168.2.1   0
[admin@RIP-1] /ip route>
```

— RIP-OSPF :

- Il sert de passerelle entre les 2 zones RIP et OSPF
- Il sait faire du RIP et de l'OSPF
- Sa route par défaut lui permet de sortir!

```
[admin@RIP-OSPF] /ip route> print
Flags: X - disabled, A - active, D - dynamic, C - connect, S - static,
r - rip, b - bgp, o - ospf, m - mme, B - blackhole, U - unreachable, P
- prohibit
# DST-ADDRESS      PREF-SRC      GATEWAY      DISTANCE
0 A S 0.0.0.0/0      10.0.0.10     1
1 ADr 1.1.1.1/32     10.0.0.5     120
2 ADr 2.2.2.2/32     10.0.0.5     120
3 ADC 3.3.3.3/32     3.3.3.3       0
4 ADo 4.4.4.4/32     10.0.0.10    110
5 ADo 5.5.5.5/32     10.0.0.10    110
6 ADo 6.6.6.6/32     10.0.0.10    110
7 ADo 7.7.7.7/32     10.0.0.10    110
8 ADr 10.0.0.0/30     10.0.0.5     120
9 ADC 10.0.0.4/30     10.0.0.6     0
10 ADC 10.0.0.8/30    10.0.0.9     0
11 ADo 10.0.0.12/30   10.0.0.10    110
12 ADo 10.0.0.16/30   10.0.0.10    110
13 ADo 10.0.0.20/30   10.0.0.10    110
14 ADr 192.168.1.0/24 10.0.0.5     120
15 ADr 192.168.2.0/24 10.0.0.5     120
16 ADo 192.168.17.0/24 10.0.0.10    110
17 ADo 192.168.18.0/24 10.0.0.10    110
[admin@RIP-OSPF] /ip route>
```

— OSPF2 :

- Il ne sait faire que de l'OSPF
- Il ne connaît pas (11.0.0.0/27) ce qu'il y a après le routeur de passerelle OSPF-BGP
- Sa route par défaut lui permet de sortir!

```
[admin@OSPF2] /ip route> print
Flags: X - disabled, A - active, D - dynamic, C - connect, S - static,
r - rip, b - bgp, o - ospf, m - mme, B - blackhole, U - unreachable, P
- prohibit
# DST-ADDRESS      PREF-SRC      GATEWAY      DISTANCE
0 A S 0.0.0.0/0      10.0.0.18     1
1 ADo 1.1.1.1/32     10.0.0.13    110
2 ADo 2.2.2.2/32     10.0.0.13    110
3 ADo 3.3.3.3/32     10.0.0.13    110
4 ADo 4.4.4.4/32     10.0.0.13    110
5 ADC 5.5.5.5/32     5.5.5.5       0
6 ADo 6.6.6.6/32     10.0.0.18    110
7 ADo 7.7.7.7/32     10.0.0.18    110
8 ADo 10.0.0.0/30     10.0.0.13    110
9 ADo 10.0.0.4/30     10.0.0.13    110
10 ADo 10.0.0.8/30    10.0.0.13    110
11 ADC 10.0.0.12/30   10.0.0.14     0
12 ADC 10.0.0.16/30   10.0.0.17     0
13 ADo 10.0.0.20/30   10.0.0.18    110
14 ADo 192.168.1.0/24 10.0.0.13    110
15 ADo 192.168.2.0/24 10.0.0.13    110
16 ADo 192.168.17.0/24 10.0.0.13    110
17 ADo 192.168.18.0/24 10.0.0.13    110
[admin@OSPF2] /ip route>
```

— OSPF-BGP :

- Il sert de passerelle entre les 2 zones AS100 et AS200
- Il sait faire de l'OSPF et du BGP
- Il est le seul à connaître les 8 réseaux de 11.0.0.0/30 à 11.0.0.28/30
Mais tiens bizarre qu'une seule ligne??? On va voir plus loin pourquoi!
- Pas de route par défaut?
- Pourquoi cette route **static**?

```
[admin@OSPF-BGP] /ip route> print
Flags: X - disabled, A - active, D - dynamic,
C - connect, S - static, r - rip, b - bgp, o - ospf, m - mme,
B - blackhole, U - unreachable, P - prohibit
# DST-ADDRESS      PREF-SRC  GATEWAY      DISTANCE
0 ADo 1.1.1.1/32      10.0.0.21    110
1 ADo 2.2.2.2/32      10.0.0.21    110
2 ADo 3.3.3.3/32      10.0.0.21    110
3 ADo 4.4.4.4/32      10.0.0.21    110
4 ADo 5.5.5.5/32      10.0.0.21    110
5 ADo 6.6.6.6/32      10.0.0.21    110
6 ADC 7.7.7.7/32      7.7.7.7      0
7 AS 8.8.8.8/32      193.55.130.2 1
8 ADo 10.0.0.0/30     10.0.0.21    110
9 ADo 10.0.0.4/30     10.0.0.21    110
10 ADo 10.0.0.8/30     10.0.0.21    110
11 ADo 10.0.0.12/30    10.0.0.21    110
12 ADo 10.0.0.16/30    10.0.0.21    110
13 ADC 10.0.0.20/30     10.0.0.22    0
14 ADb 11.0.0.0/27      193.55.130.2 20
15 ADo 192.168.1.0/24   10.0.0.21    110
16 ADo 192.168.2.0/24   10.0.0.21    110
17 ADo 192.168.17.0/24  10.0.0.21    110
18 ADo 192.168.18.0/24  10.0.0.21    110

[admin@OSPF-BGP] /ip route> 
```

— BGP1 :

- Il sert de passerelle entre les 2 zones AS100 et AS200
- Il sait faire que du BGP mais on aurait pu faire la même structure que pour l'AS 100
- Il est le seul à connaître les 8 réseaux de 11.0.0.0/30 à 11.0.0.28/30 dans son AS !
Mais tiens encore bizarre qu'une seule ligne ??? On va voir plus loin pourquoi !
- Pas de route par défaut ?
- Pourquoi cette route **static** ?

```
[admin@BGP1] /ip route> print
Flags: X - disabled, A - active, D - dynamic,
C - connect, S - static, r - rip, b - bgp, o - ospf, m - mme,
B - blackhole, U - unreachable, P - prohibit
# DST-ADDRESS      PREF-SRC  GATEWAY      DISTANCE
0 AS 7.7.7.7/32      193.55.130.1 1
1 ADC 8.8.8.8/32      8.8.8.8      0
2 ADb 10.0.0.0/27      193.55.130.1 20
3 ADC 11.0.0.0/30      11.0.0.1     0
4 ADC 11.0.0.4/30      11.0.0.5     0
5 ADC 11.0.0.8/30      11.0.0.9     0
6 ADC 193.55.130.0/30  193.55.130.2 0

[admin@BGP1] /ip route> 
```

Avec les routeurs Mikrotik c'est la commande :

- Sur le routeur RIP1
/routing rip set redistribute-connected=yes
- Sur le routeur RIP-OSPF
/routing ospf instance set 0 router-id=3.3.3.3 redistribute-connected=as-type-1 redistribute-rip=as-type-1

RIP

/routing rip set redistribute-connected=yes

RIP-OSPF

/routing ospf instance set 0 router-id=3.3.3.3 redistribute-connected=as-type-1 redistribute-rip=as-type-1

Remarque : Il est possible de faire plein de types de redistribution mais cela dépasse ce cours
Plus d'informations ici : <https://wiki.mikrotik.com/wiki/Manual:Routing/OSPF>

3.14 L'agrégation de routes

Appelé aussi le **résumé de routes**

Cela répond à la question :

- Il est le seul à connaître les 8 réseaux de 11.0.0.0/30 à 11.0.0.28/30 dans son AS !
Mais tiens encore bizarre qu'une seule ligne ??? On va voir plus loin pourquoi



Imaginons le scénario suivant, un routeur doit ajouter dans sa table de routage tout un ensemble de réseaux qui se suivent d'un point de vue plage IP.

N° Rx	@ du Réseau	1er Octet	2ème Octet	3ème Octet	4ème Octet
1	10.0.0.0/30	0000 1010	0000 0000	0000 0000	000 0 0000
2	10.0.0.4/30	0000 1010	0000 0000	0000 0000	000 0 0100
3	10.0.0.8/30	0000 1010	0000 0000	0000 0000	000 0 1000
4	10.0.0.12/30	0000 1010	0000 0000	0000 0000	000 0 1100
5	10.0.0.16/30	0000 1010	0000 0000	0000 0000	000 1 0000
6	10.0.0.20/30	0000 1010	0000 0000	0000 0000	000 1 0100
7	10.0.0.24/30	0000 1010	0000 0000	0000 0000	000 1 1000
8	10.0.0.28/30	0000 1010	0000 0000	0000 0000	000 1 1100

On voit que seuls les 5 derniers bits changent !

Donc on peut ne déclarer qu'un /27 plutôt que 8 /30 non ?

Marrant ou Mathématique : $8 = 2^3$ et $27 + 3 = 30$;)

Bilan :

- Processus de routage plus efficace
- Table de routage moins volumineuse
- Mises à jour plus simples
- Routeur moins gourmand en mémoire et en CPU
- Les fournisseurs d'accès gèrent eux-mêmes l'espace des adresses

Par exemple sur la structure précédente, les routeurs de Bordure en BGP ne déclarent que les réseaux.

10.0.0.0/27 et **11.0.0.0/27**

Au lieu de déclarer les 8 réseaux de /30 de 10.0.0.0 à 10.0.0.28 !

```
[admin@BGP1] /routing bgp network> print
Flags: X - disabled
# NETWORK SYNCHRONIZE
0 11.0.0.0/27 no
[admin@BGP1] /routing bgp network>
```

```
[admin@OSPF-BGP] /routing bgp network> print
Flags: X - disabled
# NETWORK SYNCHRONIZE
0 10.0.0.0/27 no
[admin@OSPF-BGP] /routing bgp network>
```

4 Routage sous Linux

Quand on travaille sur un serveur ou un ordinateur quelconque, ce dernier peut posséder plusieurs interfaces.

Imaginons le scénario suivant :

- Vous avez un ordinateur avec 2 interfaces filaires Eth0 et Eth1, plus une interface Wifi plus une interface 4G, pourquoi pas.
- Vous faites un ping vers une IP très célèbre telle 8.8.8.8, que se passe-t-il ?
- Oui ça répond, mais par où est passée votre packet ICMP Echo Request ?
- Non non ce n'est pas au pif, c'est toujours pareil

Pour le savoir, il suffit de lancer la commande **ip route ls** qui doit vous renvoyer quelque chose comme :

```
$ ip route ls
default via 10.38.16.1 dev eth0
10.38.16.0/22 dev eth0 proto kernel scope link src 10.38.19.111
169.254.0.0/16 dev eth0 scope link metric 1000
172.17.0.0/16 dev docker0 proto kernel scope link src 172.17.0.1 linkdown
192.168.56.0/24 dev vboxnet0 proto kernel scope link src 192.168.56.1 linkdown
fougeray@C304L-159C00:~$
```

\$ □

A la FAC pas chez vous !

Expliquons ce résultat !



Ou faisons un schéma ?
Combien d'interfaces ?

4.1 Qu'est-ce que le réseau 169.254.0.0/16 ?

C'est l'**APIPA (Automatic Private Internet Protocol Addressing)** ou **IPv4LL**.

Un processus qui permet à un OS de s'attribuer automatiquement une adresse IP, lorsque le serveur DHCP est hors service ou injoignable.

APIPA utilise la plage d'adresses IP 169.254.0.0/16, c'est-à-dire la plage dont les adresses vont de 169.254.0.0 à 169.254.255.255.

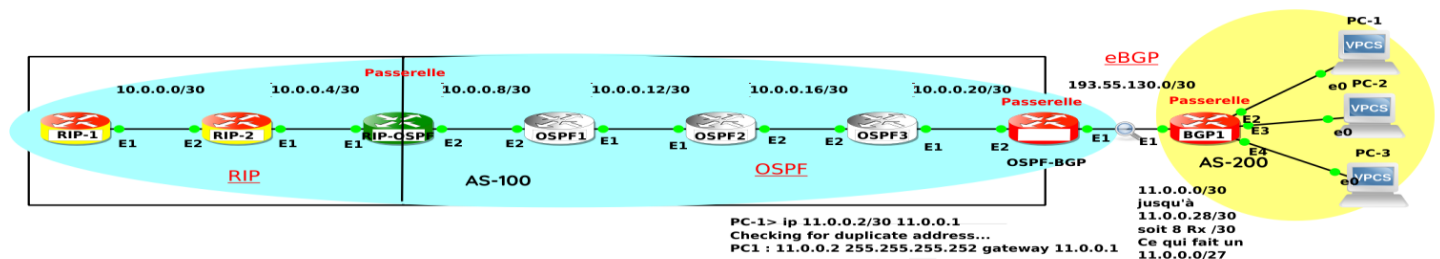
Cette plage est réservée à cet usage auprès de l'IANA.

Et dire que l'on manque d'IPv4 ... Bref

5 Étude de 3 protocoles de routage

Je reprends la structure vue précédemment, pas celle du 1er TP

- On a 3 protocoles de routages utilisés
- 2 en intra domaine : RIP et OSPF
- 1 en inter domaine : BGP



5.1 RIP

C'est un protocole de routage dynamique qui ne sert pas dans les GRANDS réseaux d'opérateurs. Mais en dehors, par exemple les réseaux de collecte.

Il n'est pas compliqué à étudier. Et on ne va pas vraiment l'étudier !

Juste voir qu'il existe !

Vous le verrez un peu en TP.

rip

No.	Time	Source	Destination	Protocol	Leng	Info
...	1.593973	10.0.0.6	224.0.0.9	RIPv2	66	Request
...	1.752940	10.0.0.5	224.0.0.9	RIPv2	66	Request
...	1.767464	10.0.0.6	10.0.0.5	RIPv2	86	Response
...	1.956002	10.0.0.5	224.0.0.9	RIPv2	186	Response
...	3.162650	10.0.0.6	224.0.0.9	RIPv2	186	Response
...	33.299767	10.0.0.5	224.0.0.9	RIPv2	186	Response

▶ Frame 19: 86 bytes on wire (688 bits), 86 bytes captured (688 bits) on interface 0
 ▶ Ethernet II, Src: 0c:99:5f:0b:a7:00 (0c:99:5f:0b:a7:00), Dst: 0c:99:5f:3e:65:00 (0c:99:5f:3e:65:00)
 ▶ Internet Protocol Version 4, Src: 10.0.0.6, Dst: 10.0.0.5
 ▶ User Datagram Protocol, Src Port: 520, Dst Port: 520
 ▼ Routing Information Protocol
 Command: Response (2)
 Version: RIPv2 (2)
 ▼ IP Address: 3.3.3.3, Metric: 1
 Address Family: IP (2)
 Route Tag: 0
 IP Address: 3.3.3.3
 Netmask: 255.255.255.255
 Next Hop: 0.0.0.0
 Metric: 1
 ▼ IP Address: 10.0.0.4, Metric: 16
 Address Family: IP (2)
 Route Tag: 0
 IP Address: 10.0.0.4
 Netmask: 255.255.255.252
 Next Hop: 0.0.0.0
 Metric: 16

Les RX donnés par RIP-OSPF à RIP2.

Sa LoopBack et 10.0.0.4

Pas 10.0.0.8 car pas de RIP Dessus !

Voilà rien de plus ;)

5.2 OSPF

OSPF est un protocole de routage dynamique à état de liens !

Je ne vais pas vous faire un cours complet sur OSPF non juste comprendre les principes !

Si vous voulez devenir expert en OSPF vous pouvez mais pas en 1h...

https://fr.wikipedia.org/wiki/Open_Shortest_Path_First

5.2.1 Fonctionnement général

- Dans OSPF, chaque routeur établit des **relations d'adjacence** avec ses voisins immédiats en envoyant des **messages hello à intervalle régulier**. Chaque routeur communique ensuite la liste des réseaux auxquels il est connecté par des messages **Link-state advertisements (LSA)** propagés de proche en proche à tous les routeurs du réseau.
- L'ensemble des LSA forme une **BDD de l'état des liens Link-State Database (LSDB)** pour chaque aire, qui est identique pour tous les routeurs participants dans cette aire. Chaque routeur utilise ensuite l'algorithme de Dijkstra, Shortest Path First (SPF) pour déterminer la route la plus rapide vers chacun des réseaux connus dans la LSDB.
- Le bon fonctionnement d'OSPF requiert donc une complète cohérence dans le calcul **SPF**, il n'est donc par exemple pas possible de **filtrer des routes** ou de les **résumer à l'intérieur d'une aire**.
- **En cas de changement de topologie, de nouveaux LSA sont propagés de proche en proche, et l'algorithme SPF est exécuté à nouveau sur chaque routeur.**
- Cela va très vite !!!! Vous le verrez en TP !

5.2.2 Les aires

Afin de simplifier les calculs etc..., il est possible même nécessaire de partager ce backbone en aires.

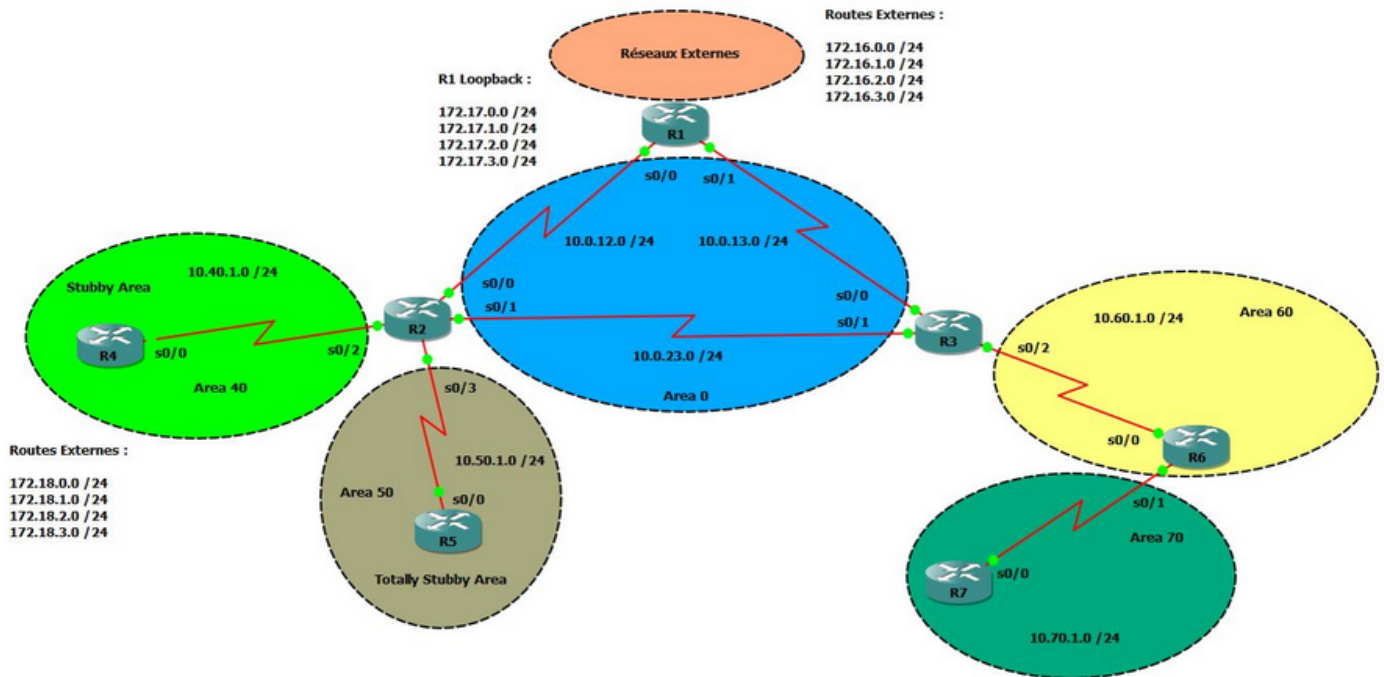


Comme je n'ai pas pour but de faire de vous des experts en OSPF, mais des étudiants qui ont compris le principe, je ne vais pas développer.

Sachez seulement

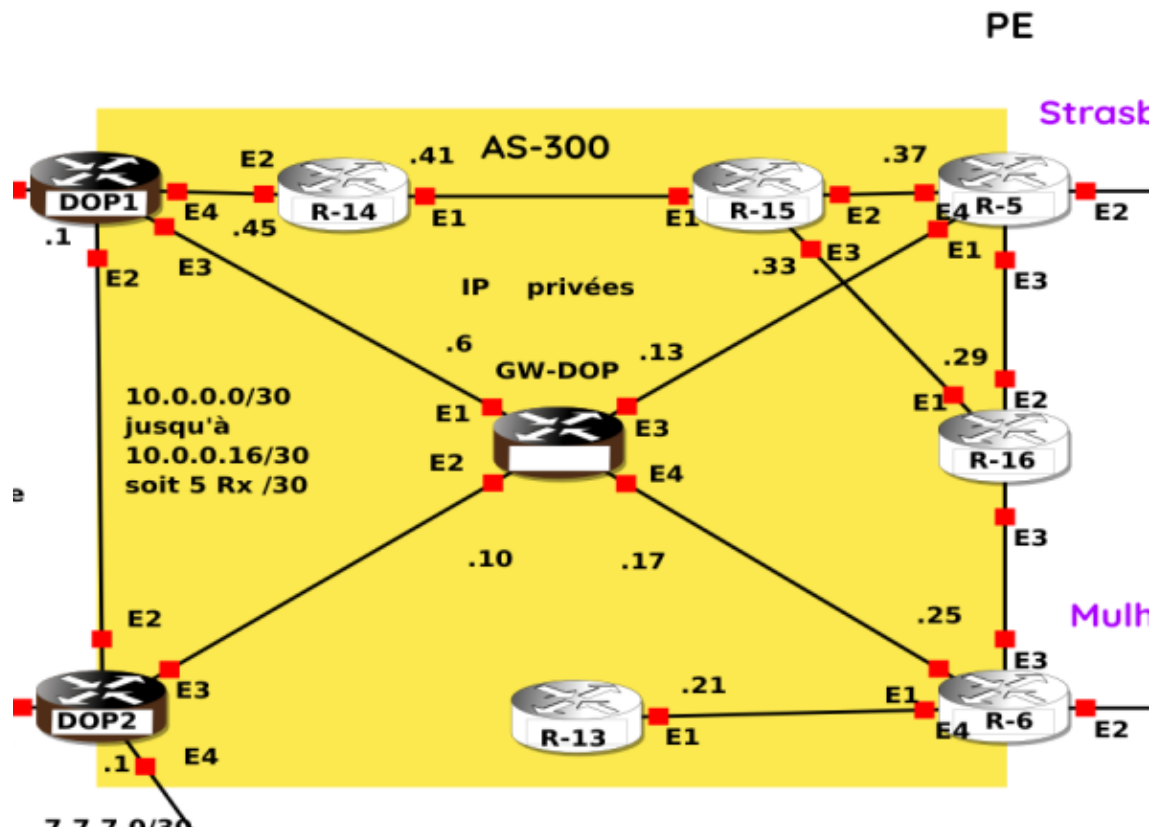
- qu'il existe toujours une **aire principale** appelée **aire 0** appelée Backbone chez Mikrotik. Nous ne ferons pas de Zone en TP !
- Des **stubs** (cul de sac) donc des aires qui n'ont qu'une entrée/sortie et donc tous les routeurs **ont tous la même route par défaut !**

Exemple sur une image prise ici : <https://www.networklab.fr/les-differents-types-de-zones-ospf/>



5.2.3 OSPF en pratique

Au TP 1, vous travaillerez sur la structure suivante, elle représente le réseau d'un opérateur quelconque, vous savez le FAI qui vous permet d'aller sur Internet ☺

iBGP OSPFRIP

Cette structure ou disons ce backbone contient 9 routeurs placés dans des grandes villes...

Vu d'internet c'est un seul réseau, vu de l'intérieur c'est 21 réseaux !

Pourquoi 21 réseaux ?

Et bien si on compte toutes les liaisons entre chaque routeur cela en fait 12 et il y a aussi le réseau des interfaces de **loopbacks** de chaque routeur : $12 + 9 = 21$...

Mais pour simplifier je vous montre la configuration de la structure précédente !

5.2.3.1 La configuration Il n'y a rien de bien compliqué.

1. On déclare une instance ici la ligne :
/routing ospf instance set 0 router-id=5.5.5.5
2. On déclare une zone (pas dans notre cas car une seule zone !)
3. On déclare les réseaux que l'on désire propager à ses voisins ici pour OSPF2 les lignes
/routing ospf network
add area=backbone network=5.5.5.5/32
add area=backbone network=10.0.0.12/30
add area=backbone network=10.0.0.16/30

Vous remarquerez qu'ils sont tous dans la même zone.

5.2.3.2 Le protocole OSPF OSPF est un protocole de routage, donc ça parle ?

Voyons ce qui se passe quand on allume tous les routeurs de l'AS-300 sauf R-13.

Puis on allume R-13 et il va récupérer tous les Réseaux.

Analysons rapidement tout cela !

C'est ce que vous ferez en TP !



No.	Time	Source	Destination	Protocol	Leng	Info
1	0.000000	10.0.0.22	224.0.0.5	OSPF	78	Hello Packet
2	9.998840	10.0.0.22	224.0.0.5	OSPF	78	Hello Packet
3	19.996934	10.0.0.22	224.0.0.5	OSPF	78	Hello Packet
...	28.661129	10.0.0.21	224.0.0.5	OSPF	78	Hello Packet
...	29.996908	10.0.0.22	224.0.0.5	OSPF	82	Hello Packet
...	30.039102	10.0.0.21	10.0.0.22	OSPF	66	DB Description
...	30.045814	10.0.0.22	10.0.0.21	OSPF	66	DB Description
...	30.047537	10.0.0.22	10.0.0.21	OSPF	366	DB Description
...	30.061690	10.0.0.21	10.0.0.22	OSPF	238	LS Request
...	30.063206	10.0.0.22	10.0.0.21	OSPF	810	LS Update
...	30.063494	10.0.0.21	10.0.0.22	OSPF	86	DB Description
...	30.066626	10.0.0.22	10.0.0.21	OSPF	70	LS Request
...	30.067057	10.0.0.22	10.0.0.21	OSPF	66	DB Description
...	30.075773	10.0.0.21	10.0.0.22	OSPF	66	DB Description
...	30.076521	10.0.0.22	10.0.0.21	OSPF	66	DB Description
...	30.079198	10.0.0.21	10.0.0.22	OSPF	110	LS Update
...	30.096222	10.0.0.22	224.0.0.5	OSPF	166	LS Update
...	31.080104	10.0.0.21	224.0.0.5	OSPF	378	LS Acknowledge

Frame 25: 810 bytes on wire (6480 bits), 810 bytes captured (6480 bits) on interface
 Ethernet II, Src: 0c:7a:53:ed:bf:03 (0c:7a:53:ed:bf:03), Dst: 0c:7a:53:96:98:00 (0c:7a:53:96:98:00)
 Internet Protocol Version 4, Src: 10.0.0.22, Dst: 10.0.0.21
 Open Shortest Path First
 OSPF Header
 LS Update Packet
 Number of LSAs: 15
 LSA-type 1 (Router-LSA), len 60
 .000 0000 0100 1101 = LS Age (seconds): 77
 0... .. = Do Not Age Flag: 0
 Options: 0x02, (E) External Routing
 LS Type: Router-LSA (1)
 Link State ID: 1.1.1.1
 Advertising Router: 1.1.1.1
 Sequence Number: 0x80000005
 Checksum: 0x31ae
 Length: 60
 Flags: 0x00
 Number of Links: 3
 Type: Stub ID: 10.0.0.0 Data: 255.255.255.252 Metric: 10
 Type: Transit ID: 10.0.0.6 Data: 10.0.0.5 Metric: 10
 Type: Stub ID: 1.1.1.1 Data: 255.255.255.255 Metric: 10
 LSA-type 1 (Router-LSA), len 84
 LSA-type 1 (Router-LSA), len 72
 LSA-type 1 (Router-LSA), len 72
 LSA-type 1 (Router-LSA), len 60
 LSA-type 1 (Router-LSA), len 72
 LSA-type 1 (Router-LSA), len 72
 LSA-type 2 (Network-LSA), len 32
 LSA-type 2 (Network-LSA), len 32
 LSA-type 2 (Network-LSA), len 32
 LSA-type 2 (Network-LSA), len 32
 LSA-type 2 (Network-LSA), len 32
 LSA-type 2 (Network-LSA), len 32
 LSA-type 2 (Network-LSA), len 32
 LSA-type 2 (Network-LSA), len 32

A EXPLIQUER !!!

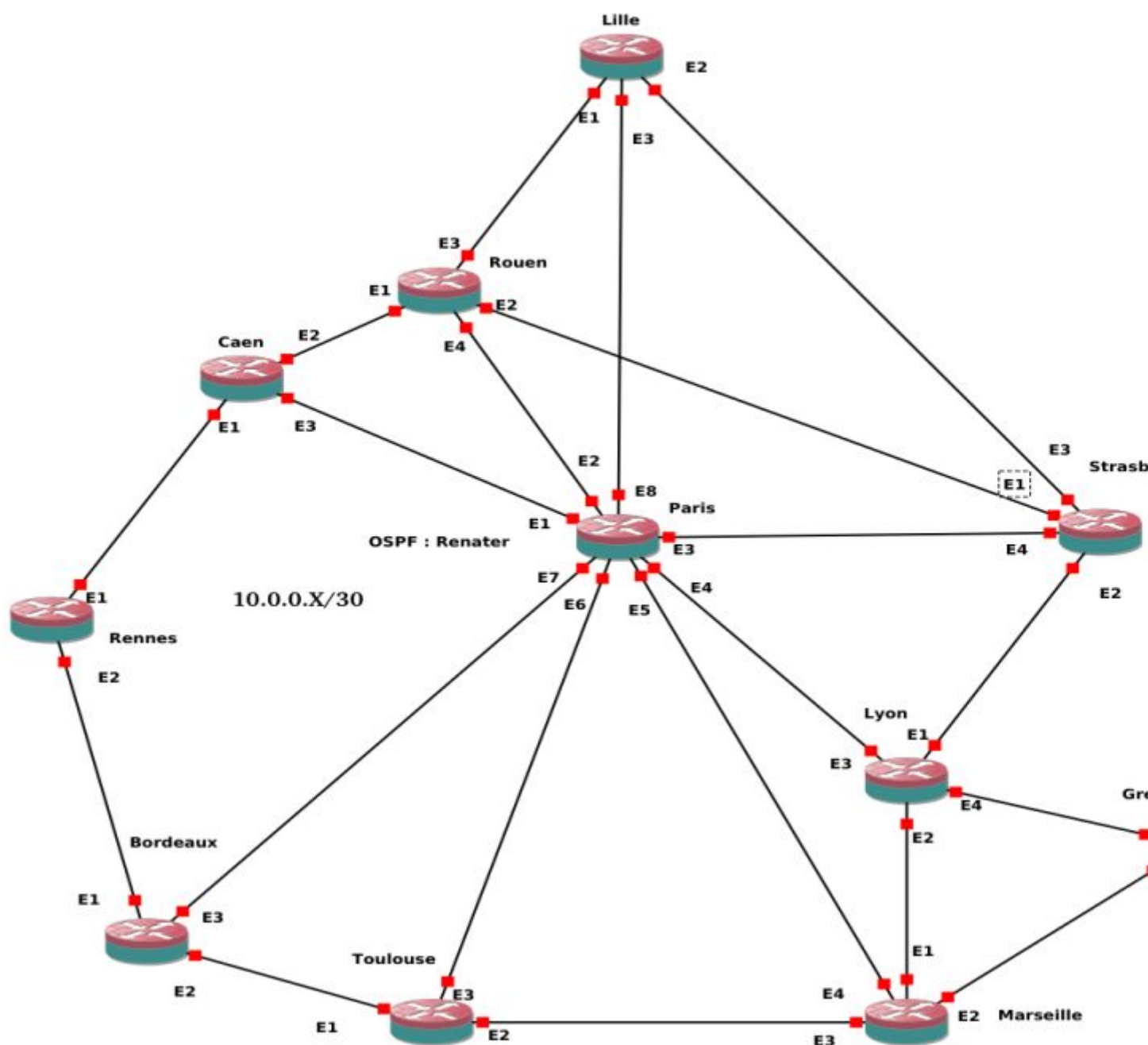
5.2.3.3 Adresses sources et destinations On peut remarquer que les 2 routeurs utilisent les **adresses destination** !

- De leur port Ethernet respectif soient 10.0.0.1/24 et 2 car ils sont sur le réseau 10.0.0.0/30 !
Pour tout ce qui est DB Description et LS Update (pas toujours !)
- De type **multicast 224.0.0.5** pour les paquets de type **Hello Packet** , **LS-Acknowledge** et **LS Update** (pas toujours !)
2 adresses **multicast** sont utilisées
 - 224.0.0.5 et FF02 : :5 (Ipv6) pour tous les routeurs OSPF
 - **224.0.0.6** et FF02 : :6 (Ipv6) pour tous les routeurs OSPF de **bordure** DR/BDR OSPF
C'est le cas du routeur de Caen quand on n'allume que 3 routeurs Caen, Rouen et Lille.
Si vous regardez bien le schéma, dans ce cas Caen est un routeur de Bordure et Lille aussi alors que Rouen non.
 - Rouen utilise 224.0.0.5 et Caen 224.0.0.6 dans ce cas.
 - Si on allume les bretons, le routeur Rennes alors Caen ne serait plus un routeur de Bordure !

Ce qui suit est issu de la structure que vous verrez en Master M1 peut-être

Que voici

Les captures se passent entre Caen et Rouen



5.2.3.4 Les messages Il y a 5 types de messages OSPF !

1. Les **hello packet** : ça semble logique, les routeurs signalent leur présence à leurs voisins.

Il disent salut en n'utilisant pas une adresse IP de type Unicast, mais de type multicast (224.0.0.5 et .6), ça forme un bon groupe un ensemble de routeur qui parle le même protocole !

```

> Frame 394: 82 bytes on wire (656 bits), 82 bytes captured (656 bits) on interface 0
> Ethernet II, Src: 0c:ca:a6:51:cb:00 (0c:ca:a6:51:cb:00), Dst: IPv4mcast_05 (01:00:5e:00:00:05)
> Internet Protocol Version 4, Src: 10.0.0.1, Dst: 224.0.0.5
  > Open Shortest Path First
    > OSPF Header
      Version: 2
      Message Type: Hello Packet (1)
      Packet Length: 48
      Source OSPF Router: 1.1.1.1
      Area ID: 0.0.0.0 (Backbone)
      Checksum: 0xe195 [correct]
      Auth Type: Null (0)
      Auth Data (none): 0000000000000000
    > OSPF Hello Packet
      Network Mask: 255.255.255.252
      Hello Interval [sec]: 10
      Options: 0x02, (E) External Routing
      Router Priority: 1
      Router Dead Interval [sec]: 40
      Designated Router: 10.0.0.2
      Backup Designated Router: 10.0.0.1
      Active Neighbor: 2.2.2.2
  
```

2. Les **DB descption** : Décrit le contenu des bases de données d'état de liens (**link-state database**) des routeurs

OSPF

```

Frame 32: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0
Ethernet II, Src: 0c:ca:a6:51:cb:00 (0c:ca:a6:51:cb:00), Dst: 0c:ca:a6:b0:41:00 (0c:ca:a6:b0:41:00)
Internet Protocol Version 4, Src: 10.0.0.1, Dst: 10.0.0.2
Open Shortest Path First
  OSPF Header
    Version: 2
    Message Type: DB Description (2)
    Packet Length: 32
    Source OSPF Router: 1.1.1.1
    Area ID: 0.0.0.0 (Backbone)
    Checksum: 0xb3f8 [correct]
    Auth Type: Null (0)
    Auth Data (none): 0000000000000000
  OSPF DB Description
    Interface MTU: 1500
    Options: 0x42, 0, (E) External Routing
    DB Description: 0x07, (I) Init, (M) More, (MS) Master
      .... 0... = (R) OOBResync: Not set
      .... .1.. = (I) Init: Set
      .... .1.. = (M) More: Set
      .... .1.. = (MS) Master: Yes
    DD Sequence: 0

```

```

0000  0c ca a6 b0 41 00 0c ca a6 51 cb 00 08 00 45 c0  ....A...Q....E.
0010  00 34 72 51 00 00 01 59 32 5e 0a 00 00 01 0a 00  -4rQ...Y 2^.....
0020  00 02 02 00 20 01 01 01 01 00 00 00 00 b3 f8  ....
0030  00 00 00 00 00 00 00 00 00 00 05 dc 42 07 00 00  ....
0040  00 00

```

3. Les **LS-Update** (LSU) : Transporte les **link-sate advertisements**, les LSA, aux routeurs voisins. En français donne les réseaux qu'il connaît !

```

Frame 412: 226 bytes on wire (1808 bits), 226 bytes captured (1808 bits) on interface 0
Ethernet II, Src: 0c:ca:a6:b0:41:00 (0c:ca:a6:b0:41:00), Dst: IPv4mcast_05 (01:00:5e:00:00:05)
Internet Protocol Version 4, Src: 10.0.0.2, Dst: 224.0.0.5
Open Shortest Path First
  OSPF Header
    Version: 2
    Message Type: LS Update (4)
    Packet Length: 192
    Source OSPF Router: 2.2.2.2
    Area ID: 0.0.0.0 (Backbone)
    Checksum: 0x44e2 [correct]
    Auth Type: Null (0)
    Auth Data (none): 0000000000000000
  LS Update Packet
    Number of LSAs: 3
    LSA-type 1 (Router-LSA), len 84
      .000 0000 0000 0001 = LS Age (seconds): 1
      0... .. = Do Not Age Flag: 0
      Options: 0x02, (E) External Routing
      LS Type: Router-LSA (1)
      Link State ID: 2.2.2.2
      Advertising Router: 2.2.2.2
      Sequence Number: 0x80000004
      Checksum: 0xd373
      Length: 84
      Flags: 0x00
      Number of Links: 5
      Type: Stub ID: 10.0.0.12 Data: 255.255.255.252 Metric: 10
      Type: Transit ID: 10.0.0.21 Data: 10.0.0.21 Metric: 10
      Type: Stub ID: 10.0.0.16 Data: 255.255.255.252 Metric: 10
      Type: Transit ID: 10.0.0.2 Data: 10.0.0.2 Metric: 10
      Type: Stub ID: 2.2.2.2 Data: 255.255.255.255 Metric: 10
    LSA-type 2 (Network-LSA), len 32
      .000 0000 0000 0001 = LS Age (seconds): 1
      0... .. = Do Not Age Flag: 0
      Options: 0x02, (E) External Routing
      LS Type: Network-LSA (2)
      Link State ID: 10.0.0.21
      Advertising Router: 2.2.2.2
      Sequence Number: 0x80000001
      Checksum: 0xb869
      Length: 32
      Netmask: 255.255.255.252
      Attached Router: 2.2.2.2
      Attached Router: 3.3.3.3
    LSA-type 1 (Router-LSA), len 48
      .000 0000 0000 0101 = LS Age (seconds): 5
      0... .. = Do Not Age Flag: 0
      Options: 0x02, (E) External Routing
      LS Type: Router-LSA (1)
      Link State ID: 3.3.3.3
      Advertising Router: 3.3.3.3
      Sequence Number: 0x80000002
      Checksum: 0x11dd
      Length: 48
      Flags: 0x00
      Number of Links: 2
      Type: Stub ID: 10.0.0.20 Data: 255.255.255.252 Metric: 10

```

Stub ?
Transit ?

Lille est dénoncé à
Caen par Rouen ;)

4. Les **LS-Acknowledge** (LSAk) : Accusés de réception des LSA des voisins.

```

Frame 53: 78 bytes on wire (624 bits), 78 bytes captured (624 bits) on interface 0
Ethernet II, Src: 0c:ca:a6:b0:41:00 (0c:ca:a6:b0:41:00), Dst: IPv4mcast_05 (01:00:5e:00:00:05)
Internet Protocol Version 4, Src: 10.0.0.2, Dst: 224.0.0.5
Open Shortest Path First
  OSPF Header
    Version: 2
    Message Type: LS Acknowledge (5)
    Packet Length: 44
    Source OSPF Router: 2.2.2.2
    Area ID: 0.0.0.0 (Backbone)
    Checksum: 0xea03 [correct]
    Auth Type: Null (0)
    Auth Data (none): 0000000000000000
  LSA-type 1 (Router-LSA), len 72
    000 0000 0011 0100 = LS Age (seconds): 52
    0 . . . . . = Do Not Age Flag: 0
    Options: 0x02, (E) External Routing
    LS Type: Router-LSA (1)
    Link State ID: 1.1.1.1
    Advertising Router: 1.1.1.1
    Sequence Number: 0x80000002
    Checksum: 0x8943
    Length: 72
0000 01 00 5e 00 00 05 0c ca a6 b0 41 00 08 00 45 c0 ..A...A..E-
0010 00 40 72 68 00 00 01 59 5c 36 0a 00 00 02 e0 00 .@rh...Y\6....
0020 00 05 02 05 00 2c 02 02 02 02 00 00 00 00 ea 03 .....4...
0030 00 00 00 00 00 00 00 00 00 00 00 34 02 01 01 01 .....4...
0040 01 01 01 01 01 01 80 00 00 02 89 43 00 48 .....C-H

```

5.2.3.5 La table de routage avec 3 routeurs allumés ! On voit que les réseaux connus par Lille, par exemple 10.0.0.28 (la ligne 10) entre Lille et Strasbourg est connu de Caen.

Lille l'a dit à Rouen qui l'a dit à Caen ...

Pour preuve, voyons la table de routage de Caen : **ip route print**...(tiens c'était **ip route ls** sous Linux ^^) renvoie

```

[admin@Caen] > ip route print
Flags: X - disabled, A - active, D - dynamic,
C - connect, S - static, r - rip, b - bgp, o - ospf, m - mme,
B - blackhole, U - unreachable, P - prohibit
#    DST-ADDRESS      PREF-SRC  GATEWAY          DISTANCE
0    ADC 1.1.1.1/32      1.1.1.1      10              0
1    ADo 2.2.2.2/32      10.0.0.2     10.0.0.2         110
2    ADo 3.3.3.3/32      10.0.0.2     10.0.0.2         110
3    ADC 10.0.0.0/30     10.0.0.1     ether1            0
4    ADC 10.0.0.4/30     10.0.0.5     ether2            0
5    ADC 10.0.0.8/30     10.0.0.9     ether3            0
6    ADo 10.0.0.12/30    10.0.0.2     10.0.0.2         110
7    ADo 10.0.0.16/30    10.0.0.2     10.0.0.2         110
8    ADo 10.0.0.20/30    10.0.0.2     10.0.0.2         110
9    ADo 10.0.0.24/30    10.0.0.2     10.0.0.2         110
10   ADo 10.0.0.28/30    10.0.0.2     10.0.0.2         110

```

5.2.3.6 La table de routage avec tous les routeurs allumés ! Voici la table de routage complète sur le routeur de Caen quand tous les routeurs du Backbone sont allumés !

```

[admin@Caen] > ip route print
Flags: X - disabled, A - active, D - dynamic,
C - connect, S - static, r - rip, b - bgp, o - ospf, m - mme,
B - blackhole, U - unreachable, P - prohibit
#    DST-ADDRESS      PREF-SRC  GATEWAY          DISTANCE
0    ADC 1.1.1.1/32      1.1.1.1      10              0
1    ADo 2.2.2.2/32      10.0.0.2     10.0.0.2         110
2    ADo 3.3.3.3/32      10.0.0.2     10.0.0.2         110
3    ADo 4.4.4.4/32      10.0.0.2     10.0.0.10        110
4    ADo 5.5.5.5/32      10.0.0.10    10.0.0.10        110
5    ADo 6.6.6.6/32      10.0.0.10    10.0.0.10        110
6    ADo 7.7.7.7/32      10.0.0.10    10.0.0.10        110
7    ADo 8.8.8.8/32      10.0.0.6     10.0.0.6          110
8    ADo 9.9.9.9/32      10.0.0.6     10.0.0.6          110
9    ADC 10.0.0.0/30     10.0.0.1     ether1            0
10   ADC 10.0.0.4/30     10.0.0.5     ether2            0
11   ADC 10.0.0.8/30     10.0.0.9     ether3            0
12   ADo 10.0.0.12/30    10.0.0.2     10.0.0.2         110
13   ADo 10.0.0.16/30    10.0.0.2     10.0.0.2         110
14   ADo 10.0.0.20/30    10.0.0.2     10.0.0.2         110
15   ADo 10.0.0.24/30    10.0.0.10    10.0.0.10        110
16   ADo 10.0.0.28/30    10.0.0.2     10.0.0.2         110
17   ADo 10.0.0.32/30    10.0.0.10    10.0.0.10        110
18   ADo 10.0.0.36/30    10.0.0.2     10.0.0.2         110
19   ADo 10.0.0.40/30    10.0.0.10    10.0.0.10        110
20   ADo 10.0.0.44/30    10.0.0.10    10.0.0.10        110
21   ADo 10.0.0.48/30    10.0.0.10    10.0.0.10        110
22   ADo 10.0.0.52/30    10.0.0.10    10.0.0.10        110
23   ADo 10.0.0.56/30    10.0.0.10    10.0.0.10        110
24   ADo 10.0.0.60/30    10.0.0.10    10.0.0.10        110
25   ADo 10.0.0.64/30    10.0.0.10    10.0.0.10        110
26   ADo 10.0.0.68/30    10.0.0.6     10.0.0.6          110
27   ADo 10.0.0.72/30    10.0.0.10    10.0.0.10        110
28   ADo 10.0.0.76/30    10.0.0.6     10.0.0.6          110
29   ADo 10.0.0.80/30    10.0.0.10    10.0.0.10        110
30   ADo 11.11.11.11/32  10.0.0.10    10.0.0.10        110

```

On voit bien les 31 réseaux eux non 33, Ah oui c'est vrai Genève n'est pas configuré...

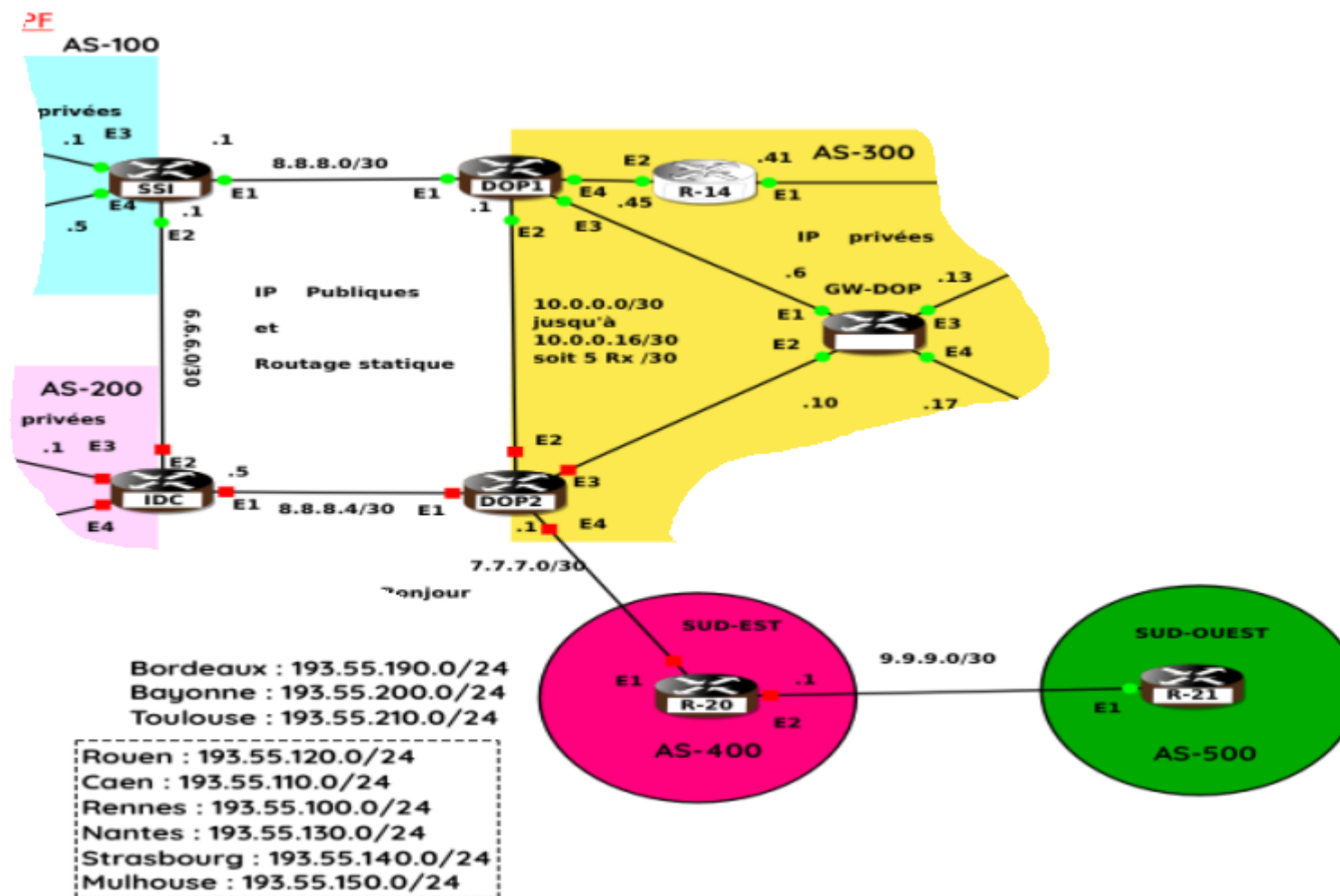
Allez en TP vous annexe la Suisse et vous y mettez vos sous euh non la bonne configuration en vous inspirant de la configuration d'un autre routeur!☺

5.3 BGP

C'est le protocole de Routage d'Internet entre les AS !

Par exemple sur l'image





5.3.1 Historique

Internet ce n'est pas vieux, juste un peu plus que vous ☺

Au début d'Internet, BGP était utilisé que par un petit nombre de gros ISP.

Ce n'est qu'en 1995, vous me direz au 20^{ème} siècle..., avec le début du Web chez les particuliers que le nombre d'ISP utilisant BGP a sérieusement augmenté.

L'introduction du CIDR (**Classless Inter-Domain Routing**) y est aussi pour beaucoup.

Actuellement vouloir ne pas utiliser BGP pour un ISP est comme vouloir ne pas utiliser Internet... ou le téléphone portable... pour un(e) étudiant(e).

5.3.2 Introduction

Voir la RFC : <https://www.ietf.org/rfc/rfc4271.txt>

Pour s'échanger des paquets, les AS utilisent des machines spécialisées, des routeurs appelés **routeurs de bordure** (**Border Routers edge**), qui font circuler l'information (pas vos données, **les tables de routage**) dans le réseau, en utilisant le protocole **BGP, Border Gateway Protocol**, signifiant **protocole de passerelle** ou **de frontière**.

Les règles de ce protocole permettent à chaque routeur d'annoncer à ses voisins s'ils peuvent accéder à une adresse IP en passant l'AS à laquelle il est rattaché.

BGP est donc le protocole de routage de l'Internet.

La façon dont on l'utilise, conditionne le bon ou le mauvais fonctionnement des réseaux sur Internet.

Contrairement aux protocoles conçus pour les réseaux internes que vous connaissez (**RIP, IS-IS, OSPF, etc...**), BGP fonctionne en **mode connecté** et se base sur **TCP** sur le **port 179**, il est le seul protocole de routage fonctionnant sur TCP.

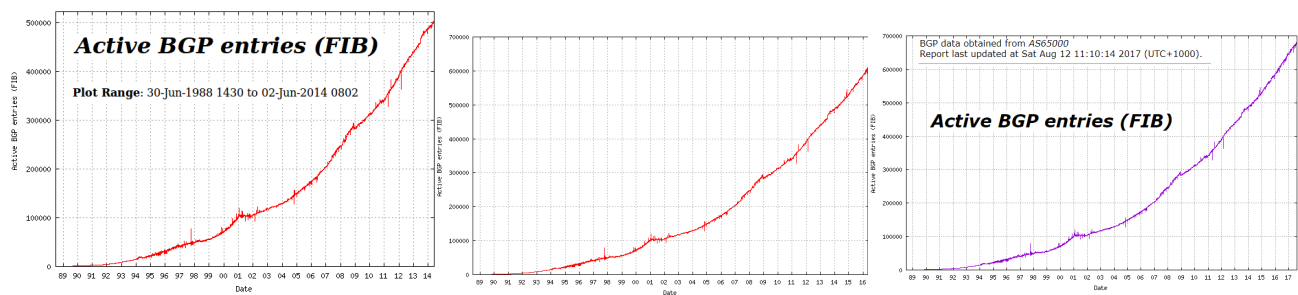


Figure 1 – Évolution table de routage BGP en juin 2014 et aout 2017

Pour rappel les autres protocoles de routage interne utilisent les adresses **multicast** de lien local ! **224.0.0.0/24** et non 239.0.0.0/24

- **224.0.0.4** et ff02 : :5 (SPF) et ff02 : :6 (DR) pour **OSPF**
- **224.0.0.9** et ff02 : :9 pour **RIP**
- **224.0.0.19-21** et ff02 : :8 pour **IS-IS**

bgp						
No.	Time	Source	Destination	Protocol	Leng	Info
...	61.499050	8.8.8.2	8.8.8.1	BGP	111	OPEN Message
...	61.525486	8.8.8.1	8.8.8.2	BGP	111	OPEN Message
...	61.529907	8.8.8.2	8.8.8.1	BGP	85	KEEPALIVE Message
...	61.550258	8.8.8.1	8.8.8.2	BGP	85	KEEPALIVE Message
...	61.588471	8.8.8.1	8.8.8.2	BGP	117	UPDATE Message
...	61.709890	8.8.8.1	8.8.8.2	BGP	117	UPDATE Message
...	61.784106	8.8.8.2	8.8.8.1	BGP	117	UPDATE Message
...	99.968564	8.8.8.1	8.8.8.2	BGP	121	UPDATE Message
...	103.227957	8.8.8.2	8.8.8.1	BGP	121	UPDATE Message
...	119.158795	8.8.8.1	8.8.8.2	BGP	85	KEEPALIVE Message
...	120.024166	8.8.8.2	8.8.8.1	BGP	85	KEEPALIVE Message

<p>Frame 56: 117 bytes on wire (936 bits), 117 bytes captured (936 bits) on interface 0</p> <p>Ethernet II, Src: 0c:9c:29:2d:eb:00 (0c:9c:29:2d:eb:00), Dst: 0c:9c:29:0a:01:00 (0c:9c:29:0a:01:00)</p> <p>Internet Protocol Version 4, Src: 8.8.8.2, Dst: 8.8.8.1</p> <p>Transmission Control Protocol, Src Port: 41091, Dst Port: 179, Seq: 65, Ack: 167, Len: 51</p> <p>Border Gateway Protocol - UPDATE Message</p> <p>Marker: ffffffffffffffffffffffffffffffffff</p> <p>Length: 51</p> <p>Type: UPDATE Message (2)</p> <p>Withdrawn Routes Length: 0</p> <p>Total Path Attribute Length: 20</p> <p>Path attributes</p> <ul style="list-style-type: none"> Path Attribute - ORIGIN: IGP Path Attribute - AS_PATH: 300 Path Attribute - NEXT_HOP: 8.8.8.2 <p>Network Layer Reachability Information (NLRI)</p> <ul style="list-style-type: none"> 193.55.140.0/24 193.55.150.0/24
--

La connexion d'un routeur donné avec son voisin se fait **manuellement**, ces routeurs sont appelés **routeurs de bordure**

Une interconnexion BGP consiste en l'échange, entre 2 AS, de préfixes IP.

Chaque AS informe son interlocuteur, qu'il a la possibilité d'acheminer le trafic à destination de ces préfixes.

Il est possible de voir les tables de routages des routeurs d'Internet.

Pour cela on va sur des sites tels <http://www.lookingglass.org/> ou <http://www.bgp4.as/looking-glasses>

Pour connaître le nombre @IP (préfixes) dans les routeurs BGP d'Internet, donc les tables de routage :

<http://bgp.potaroo.net/as2.0/bgp-active.html> ,

Le 12 aout 2017, à comparer avec celles de juin 2014 et mai 2016, passé de 500000 à plus de 600000 puis presque 700000 soit +40% en 3 ans !

5.3.3 Types d'interconnexions BGP

Les ISP sont interconnectés entre eux afin de s'échanger des routes via BGP et ainsi permettre aux données de passer d'un point A à un point B au travers des backbones des ISP.

Il existe 4 types d'interconnexions :



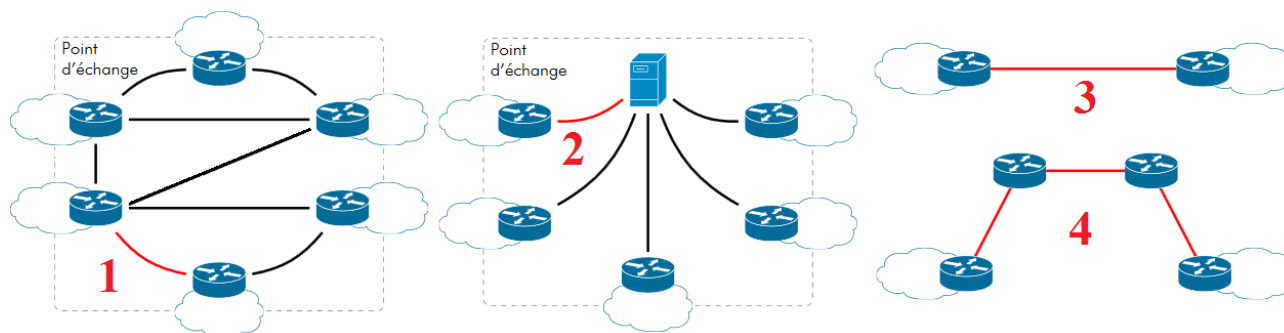


Figure 2 – Types d'interconnexions BGP

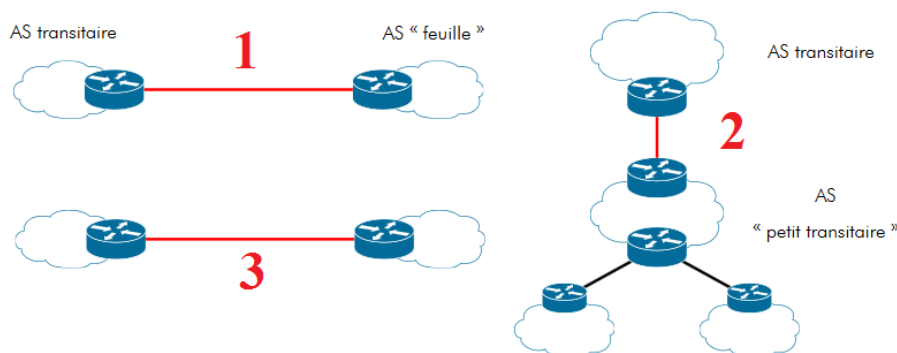


Figure 3 – Types de relations entre AS

1. Peering bilatéral dans un **GIX** (point d'échanges) .
2. Peering à l'aide d'un serveur de routes dans un GIX.
3. Peering privé entre 2 AS dans un **Network Access Point**, ou interconnexion dans une salle
4. Session établie en **multi-hop** : L'interconnexion entre les routeurs BGP n'est pas directe.

5.3.4 Types de relations entre AS

Les Systèmes Autonomes (AS) peuvent avoir entre eux 3 types de relations.

1. **Transitaire / client** à **feuille** : Existe entre un AS transitaire et un AS à feuille n'offrant pas de service de transit.
2. **Transitaire / petit transitaire** : Existe entre un transitaire et un AS client, ce dernier étant également ISP pour un ou plusieurs autres AS.
3. **Peering** : Existe entre 2 AS s'échangeant des préfixes, sans que l'un de ces AS ne fournisse à l'autre un service de transit.

5.3.4.1 BGP plus en détails

Plus en détails mais pas trop, je n'ai pas le temps et de toute manière vous n'allez pas le retenir

Et si vous en voulez plus : https://fr.wikipedia.org/wiki/Border_Gateway_Protocol ou bien un livre :
ou bien une doc *cisco* en français canadien ☺ :
http://www.cisco.com/cisco/web/support/CA/fr/109/1094/1094968_bgp-toc.pdf

Les 4 messages de base de BGP

1. **Open** : établit une session BGP utilisant le port TCP 179, donc une meilleure fiabilité, en mode connecté.
2. **Notification** : Informe son voisin d'un problème. La relation BGP est stoppée, ainsi que la session TCP, et le routeur repasse en mode **Idle** (au repos).

3. **Update** : Permet d'annoncer de nouvelles routes, ou d'en retirer. Quand on annonce une nouvelle route, l'**AS Path** est donné avec. Il s'agit du chemin que va emprunter le paquet pour arriver à destination.

Si le routeur qui reçoit la route pour une destination voit son propre AS dans l'AS Path, il refusera la route, sinon il y aurait une boucle de routage

- (a) Informe un voisin de nouvelles routes devenues **actives**
 (b) Informe un voisin de nouvelles routes devenues **inactives**

4. **Keepalive** : Informe un voisin que la connexion est toujours valide.

Par défaut le message **Keepalive** est envoyé toutes les 30 secondes.

Passé un délai de 90 secondes sans message **Update** ni **Keepalive** reçu entraîne la fermeture de la session TCP

Annnonce d'un préfixe Quand un routeur annonce un préfixe à l'un de ses voisins BGP,

- L'information est valide jusqu'à ce qu'un routeur annonce explicitement qu'elle n'est plus valide
- BGP ne nécessite pas le rafraîchissement de l'information.
- Si le nœud A annonce un chemin pour un préfixe au nœud B, alors B peut être sûr que A lui-même utilise ce chemin pour atteindre la destination !

Les 4 types d'un Attribut d'un chemin Quand un routeur reçoit une route, il regarde tous les **tags** ou **attributs** la constituant, et en déduit (après un algorithme que je ne vais pas vous détailler...) la meilleure route...

- **Well-Known Mandatory** (WM) : doivent être pris en charge et propagés, ils doivent être inclus dans l'**Update** ;
- **Well-Known Discretionary** (WD) : doivent être pris en charge, la propagation est optionnelle, par déduction ne sont pas forcément envoyés dans les **Update** ;
- **Optional Transitive** (OT) : pas nécessairement pris en charge mais propagés, les **Non-Transitive** quand ils sont annoncés, ne sortent pas de l'AS ;
- **Optional Nontransitive** (ON) : pas nécessairement pris en charge ni propagés, peuvent être complètement ignorés s'ils ne sont pas pris en charge.

Mais pour bien compléter le tout et cela va vous montrer que connaître BGP en détails c'est.... impossible dans notre cours..., **ces différentes catégories d'attributs peuvent se cumuler** :

N°	Attribut	Type	Préférence	Description
0	Next-Hop	WM		Ignorer les routes ayant un next-hop inaccessible
1	Weight	OT	Le plus haut	Permet de favoriser un voisin. Configuré en local, n'est pas annoncé
2	LOCAL_PREF	WD	Le plus haut	Métrique appliquée sur une route annoncée dans l'AS (pour les voisins iBGP)
3	Self Originated			Favoriser les routes annoncées par le routeur lui-même via les commandes <i>Network</i> , <i>Aggregate</i> et <i>Redistribute</i>
4	AS Path	WM	Le plus court	Choisir la route passant par le moins d'AS
5	Origin	WM	IGP < EGP < Inconnue	Préférer une route IGP par rapport à une eBGP. Le type inconnu survient quand une route est redistribuée dans BGP
6	MED	ON	Le plus bas	Permet d'influencer le choix du routeur pour entrer dans l'AS
7	BGP AD		eBGP	Préférer une route apprise par eBGP
8	IGP Cost		La plus basse	Choisir la route avec une métrique iBGP
9	Multipath			Déterminer si plusieurs routes doivent être installées pour faire du Multipath
10	Age		La plus ancienne	Ne pas remplacer une route par une nouvelle route qui arrive à égalité N°9 Multipath (même si elle est meilleure sur les N° 11, 12 et 13 suivants)
11	Router ID	ON	Le plus bas	Choisir la route venant du routeur d'ID le + bas
12	Originator ID	ON		Le routeur ignore la route si l'Originator ID est son propre ID
13	Neighbor Address		La plus basse	Choisir la route venant du voisin avec l'IP la plus faible

— AS-PATH

Liste des AS au travers desquels l'annonce pour un préfixe est passée.

Chaque AS ajoute son N° d'AS à l'attribut **AS Path** lors de la transmission d'une annonce

Permettant ainsi de détecter et prévenir les boucles

Préfixe Next Hop AS PATH

123.234.111.12/22 231.111.124.13 1664 33 51

— MED Multi-Exit Discriminator

— Utilisé quand 2 AS sont reliés par 2 liens. Il permet à un AS d'indiquer un lien préféré.

— Le MED est un cout codé sur 32 bits, il peut provenir d'un protocole de routage interne.





image prise sur wikipédia :

— NEXT HOP

- Pour un préfixe annoncé à un voisin eBGP, Next Hop représente l'adresse IP de sortie vers ce voisin.
- Cet attribut n'est pas altéré quand il est transmis aux voisins iBGP, ceci implique que la route vers l'adresse IP du voisin eBGP est connue en utilisant un IGP.
- Si ce n'est pas le cas, la route BGP est marquée comme inutilisable.

— ORIGIN

- Qui est à l'origine de l'annonce ? Où un préfixe a-il été injecté dans BGP ?
- IGP, EGP ou Incomplète (souvent utilisé pour les routes statiques)

La sécurité des sessions Plus d'informations ici : https://fr.wikipedia.org/wiki/Sécurité_du_Border_Gateway_Protocol

Les spécifications de BGP4 ne définissent pas de mécanisme permettant de protéger les sessions.

BGP s'appuie sur TCP, il est donc possible de mettre fin aux sessions en envoyant des paquets TCP RST.

Un attaquant peut ainsi réaliser un DOS (**Deni Of Service**).

Bien-sûr cela n'est pas donné à tout le monde, mais la menace est bien réelle, il existe une solution pour se protéger c'est l'authentification des messages avec TCP MD5 décrit dans la RFC 2385 .

Ce mécanisme est disponible.

Il permet d'assurer l'**intégrité** et l'**authenticité** des messages TCP en incluant un MAC **Message Authentication Code** calculé à l'aide de la fonction de hachage MD5.

Il va de soit, qu'un secret différent doit être configuré pour chaque interconnexion.

Le secret utilisé doit être fort, sinon le mécanisme fourni par TCP MD5 ne présente plus d'intérêt. La force du secret dépend de sa longueur et des classes de caractères qui le composent. Dans le cas du TP le secret est mal choisi mais ce n'est qu'un TP.

La commande chez Mikrotik : **routing bgp peer tcp-md5-key**

Si les 2 mots de passe (secret) divergent alors pas de connexion !

Le filtrage des préfixes BGP Le protocole BGP ne fournit pas de mécanisme permettant de valider les annonces de préfixes.

Un AS peut donc annoncer n'importe quel préfixe et c'est pas bien....

Il peut s'agir de :

- préfixes non gérés par l'AS, c'est ce que l'on appelle une usurpation de préfixes
- préfixes ne devant pas être annoncés au sein de l'Internet.

Il existe différentes méthodes de filtrage des préfixes permettant de contrôler l'envoi et la réception des mises à jour BGP entre 2 voisins.

Pour rappel un voisin peut récupérer tous les préfixes appris par un autre voisin.

Sachant qu'actuellement il y a plus de 700 000 routes (préfixes) sur Internet...

Il y a méthodes de filtrages des mises à jour BGP.

En entrée En entrée, il faut filtrer les annonces BGP qui portent sur :

- des préfixes réservés (qui ne doivent donc pas être présents sur Internet) que l'on nomme **martians** ;
- les préfixes supérieurs à /8, ils n'ont jamais été alloués et inférieurs à /24, pour ce dernier c'est un consensus centre ISP afin de ne pas saturer la table de routage BGP ;
- un chemin d'AS trop long ;
- un **next-hop** ou un AS pair avec lequel vous n'avez aucune session BGP ;
- nos préfixes (ils nous ont été alloués, personne d'autre ne doit les annoncer) ;
- un trop grand nombre de préfixes, ce qui signifie que le pair a fait une erreur comme désagréger les préfixes.

1. **Filtrer** les préfixes réservés, les **martians**... : https://en.wikipedia.org/wiki/Martian_packet

Pour rappel : https://fr.wikipedia.org/wiki/Adresse_IP

Exemples :

- 0.0.0.0/8,
- 127.0.0.0/8 Loopbacks,
- Les réseaux privés 10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16
- 100.64.0.0/10 https://fr.wikipedia.org/wiki/Carrier-grade_NAT et <http://www.bortzmeyer.org/6598.html>
- Multicast 224.0.0.0/24

— etc...

2. **Filtrer** les informations de route, (ACL), nous pourrions le faire en TP, pas le temps...

exemple : R1, AS100 ne distribue pas les routes provenant de R5, AS500 à R3

```
access-list 13 deny 50.0.0.0 0.255.255.255
```

```
access-list 13 deny 51.0.0.0 0.255.255.255
```

```
access-list 13 deny 52.0.0.0 0.255.255.255
```

```
access-list 13 permit any
```

```
router bgp 100
```

```
neighbor 3.3.3.3 distribute-list 13 out
```

3. **Filtrer** sur le nombre de routes reçues, il est possible de limiter le nombre de préfixes reçus, surtout en **peering** !
Pour se protéger d'un routage anormal, on repère un nombre inhabituel de routes reçus sur un **peering** (via un peer). On peut ainsi rapidement repérer quand un **peer censé (supposé)** nous annoncer uniquement ses routes commence à envoyer toute la table Internet qu'il apprend par ailleurs. On configure des seuils sur chaque **peering** pour recevoir une alarme (voir les logs ou **trap snmp**) et ensuite couper le **peering** quand la quantité de routes est devenue anormale et bien sûr discuter avec l'autre AS !
4. **Filtrer** les informations de chemin ou Filtrage sur l'**AS_PATH** des routes annoncées par les pairs. par exemple, AS100 peut accepter ce qui arrive de AS200 via AS300 mais pas via AS400.
commandes : **ip as-path access-list access-list-number { permit | deny } as-regular-expression**
et dans router bgp XXX : **neighbor {ip-address | peer-group-name} filter-list access-list-number {in | out}**
5. **Filtrer** les communautés comme base.
Pas trop le temps d'en parler et cela devient très complexe... il faudrait avant étudier les communautés dans BGP... pas le temps...

Toutes les méthodes permettent d'obtenir les mêmes résultats. Le choix d'une méthode plutôt qu'une autre dépend de la configuration du réseau spécifique.

En sortie Une seule règle simple : ne pas annoncer autre chose que les préfixes qui vous ont été alloués !

Utilisation de la journalisation Les routeurs proposent de nombreuses fonctions de journalisation, vous étudierez cela plus en détails en M1 avec Mr Fougeray.

La journalisation permet de déceler des problèmes de stabilité et est utile lors d'une intervention suite à un incident.

Les enregistrements permettent d'identifier l'équipement à l'origine de l'entrée de journal, la session concernée, la cause et l'horodatage précis de l'incident en utilisant le protocole NTP.

Pour le cas de BGP, et sur les routeurs Cisco et Juniper, les événements de changements d'adjacence **ne sont pas journalisés par défaut**.

Ces événements correspondent aux changements d'état des sessions, ils doivent donc être journalisés. Les routeurs offrent également des fonctions de journalisation plus avancées, permettant d'enregistrer le contenu des messages échangés. Ces fonctions sont très utiles pour le débogage.

6 Conclusion

Le routage dynamique n'a rien de difficile, ça marche sans problème !

Mais heureusement que l'on utilise pas que cela sur Internet sinon on ne ferait pas le dixième de ce que l'on y fait.

Le routage est un mécanisme du 20^{ième} siècle au millénaire dernier.

Depuis on a installé des mécanismes s'appuyant sur le routage et qui permettent qu'il n'y ai pas de bouchons !

Et oui, c'est bien de tous prendre la route la plus rapide, mais cette route devient la plus lente... surtout aux heures de travail...

Le pont de **Cadix** ☹

