UNIVERSITÉ CAEN NORMANDIE

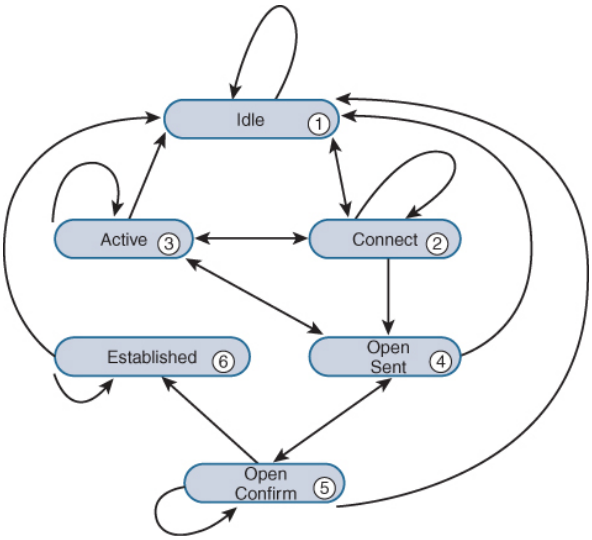
.....BGP & Peering, le routage d'Internet.....20.02.2023

The protocol that makes the Internet work;-)

Je distribue des routes qui n'en veut, on partage ?

Informe et redistribue

Auteur : Pascal Fougeray



Source : http://www.ciscopress.com/articles/article.asp?p=2756480

BGP au 20ième siècle

MP-BGP au 21ième siècle

Préambule

Savez-vous vraiment, comment les fournisseurs d'Accès à Internet s'échangent leurs routes ?
Savez-vous comment sont choisies les routes et quelle route est prioritaire ?

Si OUI alors le cours est fini, si NON alors on continue ☺

Si vous désirez comprendre les ***Bonnes pratiques de configuration de BGP*** alors je vous invite à lire un excellent document : http://www.ssi.gouv.fr/uploads/IMG/pdf/guide_configuration_BGP.pdf

Ce cours n'est pas un cours exhaustif sur BGP, il n'a pas cette prétention pour diverses raisons, BGP c'est très compliqué et il y a bien trop de possibilités, le temps... et d'exemples.

Seules les personnes travaillant chez un ISP ont besoin de bien comprendre ce protocole de routage et surtout bien le sécuriser !

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 20ième 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).

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.

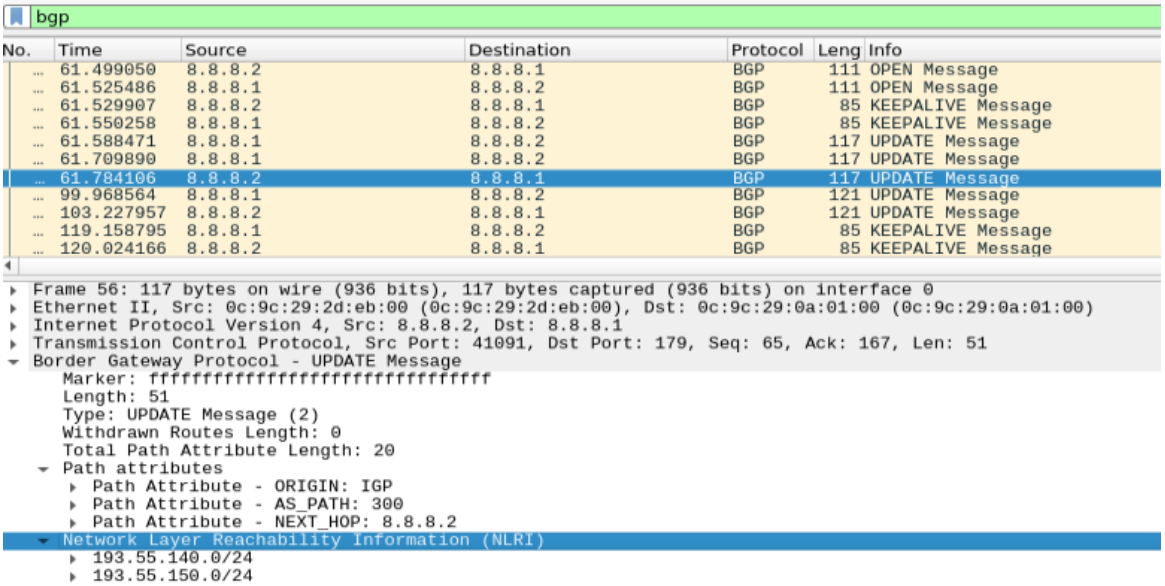
BGP est donc **le protocole de routage** de l'Internet.

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.

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**



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.lookinglass.org/** ou **http://www.bgp4.as/looking-glasses**

Pour connaitre 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 31 janvier 2023, à comparer avec celles de juin 2014 passé de 500 000 à presque 1 000 000 soit presque +100% en 9 ans !

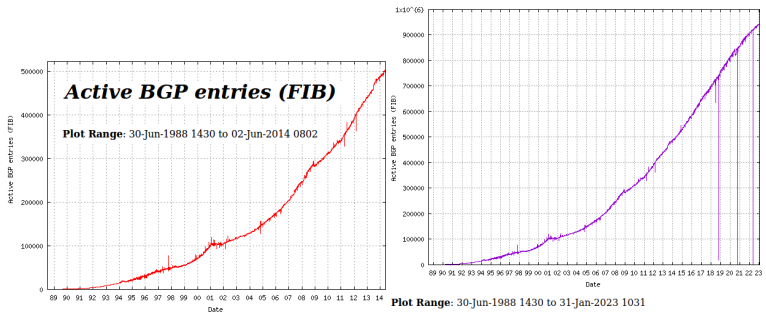


Figure 1 – **Évolution table de routage BGP en juin 2014 et janvier 2023**

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 :

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.

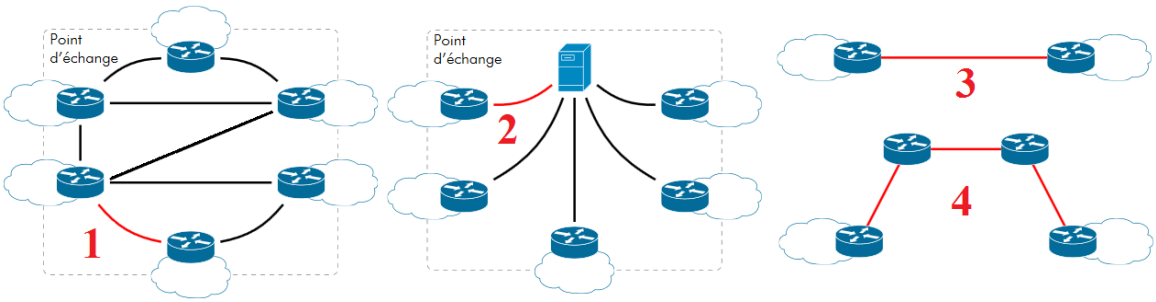


Figure 2 – **Types d'interconnexions BGP**

4 Types de relations entre AS

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

1. **Transitaire / client** « feuille » . Existe entre un AS transitaire et un AS « 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.

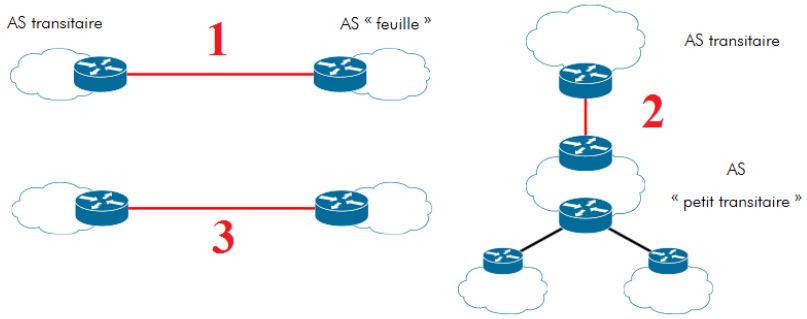


Figure 3 – Types de relations entre AS

5 Le Routage à travers l'Internet

Le routage à travers l'Internet est de 2 types, Intra ou Inter domaine(s)
La partie Intra Domaine a été traitée dans le cours précédent. Voir OSPF

5.1 Intra-domaine

- 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***.
- Les performances est une question essentielle, meilleur chemin.
  Mais qu'est-ce que le meilleur chemin ?

5.2 Inter-domaineS

- 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

6 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

6.1 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, comme le montre les lignes suivantes que vous verrez en TP.

R3# BGPSSA ssacount is 0

****Jun 19 15 :39 :48.131 : BGP(0) : 1.3.0.0 rcv UPDATE about 30.0.0.0/8 -- DENIED due to : AS-PATH contains our own AS ;***

****Jun 19 15 :39 :48.131 : BGP(0) : 1.3.0.0 rcv UPDATE about 31.0.0.0/8 -- DENIED due to : AS-PATH contains our own AS ;***

****Jun 19 15 :39 :48.131 : BGP(0) : 1.3.0.0 rcv UPDATE about 32.0.0.0/8 -- DENIED due to : AS-PATH contains our own AS ;***

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

****Jun 19 16 :56 :55.415 : BGP(0) : Revise route installing 1 of 1 routes for 20.0.0.0/8 -> 2.4.0.0(global) to main IP table***

****Jun 19 16 :56 :55.415 : BGP(0) : Revise route installing 1 of 1 routes for 21.0.0.0/8 -> 2.4.0.0(global) to main IP table***

****Jun 19 16 :56 :55.419 : BGP(0) : Revise route installing 1 of 1 routes for 22.0.0.0/8 -> 2.4.0.0(global) to main IP table***

(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.

   Il est possible de modifier cette valeur : ***neighbor @IPduVoisin timers 70 130 100,*** 70 étant le ***keepalive*** (60 normalement), 130 le ***holdtime*** (180 normalement), 100 le ***minholdtime*** (doit être inférieur au *holdtime*)

6.2 Annonce 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 !

6.3 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 ;

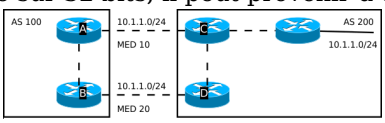
— ***Optional Nontransitive*** (ON) : pas nécessairement pris en charge ni propagés, peuvent être complètement ignorés s'ils ne sont pas pris en charge.

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 *Network*, *Aggregate* et *Redistribute*
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 quand une route est redistribuée dans BGP
6	**MED**	ON	Le plus bas	Permet d'influencer le choix du routeur pour entre 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

Préfix	***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)

6.4 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-sur 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 cisco est : ***neighbor 3.3.3.3 password UnJoliMdp***
La commande chez Mikrotik : ***routing bgp peer tcp-md5-key***
Si les 2 mots de passe (secret) divergent alors vous obtiendrez le message suivant :

Jul 2 09 :48 :32.043 : %TCP-6-BADAUTH : **Invalid MD5 digest from 1.1.1.1(47788) to 3.3.3.3(179) tableid - 0*

6.5 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.

6.5.1 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 denier 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***... ou ***bogons*** : 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 ethttp://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 sur 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-lis**t* **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.

6.5.2 En sortie

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

7 Le réflecteur de route

Voir la RFC : https://tools.ietf.org/html/rfc1966

Nous venons de voir comment les AS s'échangent leurs tables de routage à l'aide dur protocole de routage BGP.

Les routes n'étant pas transitives, une route reçue d'un voisin iBGP n'est pas transmise aux autres voisins iBGP à l'intérieur d'un AS ! ! !

Pour que les routes soient connues de tous les routeurs d'un AS, il y a :

— L'établissement de connexions entre eux dans un maillage complet (***full mesh***), ce qui peut engendrer un très grand nombre de connexions quand ces routeurs de bordure sont nombreux,

— Le problème que le nombre de connexions ***Nbr*** augmente comme le carré du nombre de routeurs ***n*** : ***Nbr = n(n-1)***

— Obligation de modifier la configuration de tous les routeurs BGP de l'AS, si on ajoute un nouveau routeur.

Imaginons la situation suivante, un ISP connecté, donc proposant du peering, avec 12 autres ISP. Cet ISP a donc 12 routeurs de bordure et ses 12 routeurs de bordures doivent s'échanger leurs tables de routages apprises via BGP.

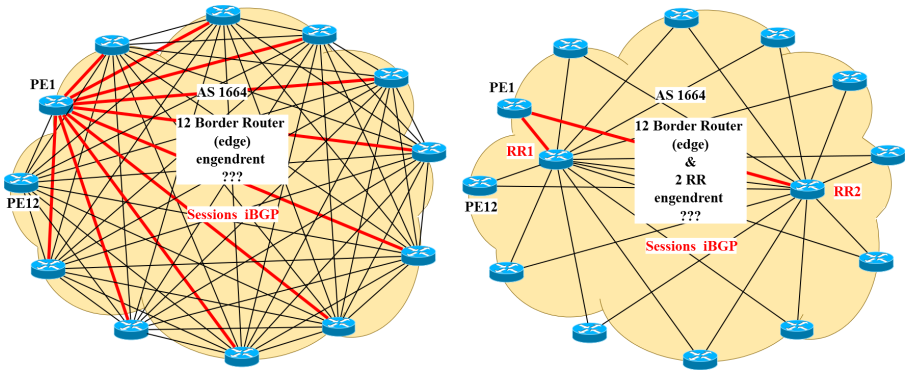


Figure 4 – RR pour ISP avec 12 BR

Le route reflector permet de diminuer cette contrainte : il redistribue les routes apprises par iBGP à des pairs iBGP appelés clients. Ces clients n'ont besoin que d'établir des sessions iBGP qu'avec le route reflector.

Des précautions sont prises via les attributs BGP optionnels non-transitifs ORIGINATOR_ID et CLUSTER_LIST pour éviter le bouclage dans l'annonce de routes.

En général on utilise au moins **2 RR** pour assurer la **redondance** en cas de défaillance d'un RR.

Le route reflector est fréquemment utilisé dans les réseaux MPLS. Il est généralement réservé à cet usage et **surtout il n'est pas employé pour le transit du trafic**.

8 MP-BGP

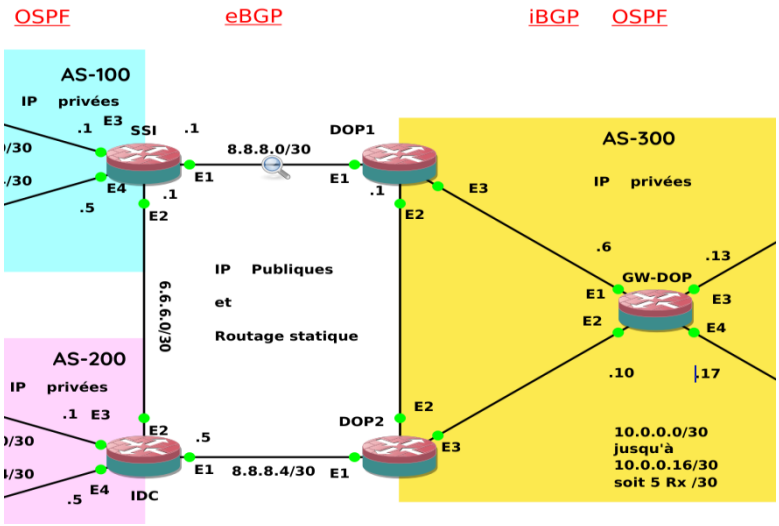
Le protocole MP-BGP est une extension du protocole BGP 4. Il permet d'échanger des routes de tous types :

— Unicast IPv4 et IPv6
— Multicast
— des routes VPNv4 et VPNv6
— des routes l2vpn pour VPLS, les VFI.
— des routes VRF etc...
— EVPN

MP-BGP adopte une terminologie similaire à BGP concernant le peering, vous verrez peut-être cela plus en détails dans un cours intitulé MPLS et les suivants...

9 Exemples de configuration chez Mikrotik

Ce sont les exemples du TP



— Pour SSI

```
/routing bgp instance
set default as=100 router-id=6.6.6.1
/routing bgp network
add network=193.55.110.0/24 synchronize=no
add network=193.55.120.0/24 synchronize=no
/routing bgp peer
add name=IDC remote-address=6.6.6.2 remote-as=200
add name=DOP1 remote-address=8.8.8.2 remote-as=300
```

— Pour IDC

```
/routing bgp instance
set default as=100 router-id=6.6.6.2
/routing bgp network
add network=193.55.110.0/24 synchronize=no
add network=193.55.120.0/24 synchronize=no
/routing bgp peer
add name=IDC remote-address=6.6.6.1 remote-as=200
add name=DOP1 remote-address=8.8.8.5 remote-as=300
```

— Pour DOP1 et DOP2

DOP1

```
/routing bgp instance
set default as=300 router-id=1.1.1.1
/routing bgp network
RIEN !!!!
/routing bgp peer
add name=SSI remote-address=8.8.8.1 remote-as=100
```

```
add name=DOP2 remote-address=10.0.0.2 remote-as=300
add name=GW-DOP remote-address=10.0.0.6 remote-as=300

DOP2
/routing bgp instance
set default as=300 router-id=2.2.2.2
/routing bgp network
RIEN !!!!
/routing bgp peer
add name=SSI remote-address=8.8.8.5 remote-as=200
add name=DOP2 remote-address=10.0.0.1 remote-as=300
add name=GW-DOP remote-address=10.0.0.10 remote-as=300
```

— Pour GW-DOP

```
/routing bgp instance
set default as=300 router-id=4.4.4.4
/routing bgp network
add network=193.55.140.0/24 synchronize=no
add network=193.55.150.0/24 synchronize=no
/routing bgp peer
add name=DOP1 remote-address=10.0.0.5 remote-as=300
add name=DOP2 remote-address=10.0.0.9 remote-as=300
```

En examinant les 5 configurations on peut voir que c'est toujours pareil ou presque !

1. **Déclarer** l'instance : ***/routing bgp instance set default as=300 router-id=4.4.4.4***
2. **Déclarer** les Rx à partager : ***/routing bgp network add network=193.55.140.0/24 synchronize=no***
3. **Déclarer** ses voisins : ***/routing bgp peer add name=DOP1 remote-address=10.0.0.5 remote-as=***

Et ça fonctionne !

Si on regarde la table de routage ensuite on récupère quelque chose comme

```
[admin@DOP1] /ip route print where bgp
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 ADb  193.55.100.0/24                    8.8.8.5                 200
 1  Db  193.55.100.0/24                    8.8.8.1                  20
 2 ADb  193.55.110.0/24                    8.8.8.1                  20
 3 ADb  193.55.120.0/24                    8.8.8.1                  20
 4 ADb  193.55.130.0/24                    8.8.8.5                 200
 5  Db  193.55.130.0/24                    8.8.8.1                  20
 6 ADb  193.55.140.0/24                    10.0.0.6                200
 7 ADb  193.55.150.0/24                    10.0.0.6                200
[admin@DOP1]
```

```
[admin@GW-DOP] > /ip route print where bgp
Flags: X - disabled, A - active, D - dynamic, C - connect, S - static, r -
b - bgp, o - ospf, m - mme, B - blackhole, U - unreachable, P - prohibit
 #      DST-ADDRESS        PREF-SRC        GATEWAY            DISTANCE
 0 ADb  193.55.100.0/24                    8.8.8.5                 200
 1 ADb  193.55.110.0/24                    8.8.8.1                 200
 2 ADb  193.55.120.0/24                    8.8.8.1                 200
 3 ADb  193.55.130.0/24                    8.8.8.5                 200
[admin@GW-DOP] >
```

À expliquer en TD et TP !

10 Conclusion

BGP est LE protocole de routage d'Internet, il est le seul ! Si vous travaillez chez un ISP vous êtes obligé de le connaître.

Si vous faites administrateur système dans une société et gérer des comptes utilisateurs, alors aucun intérêt ou presque ☺

Nous ferons UN seul TP sur BGP qui vous montrera les grands principes.

Et surtout comment fonctionne INTERNET