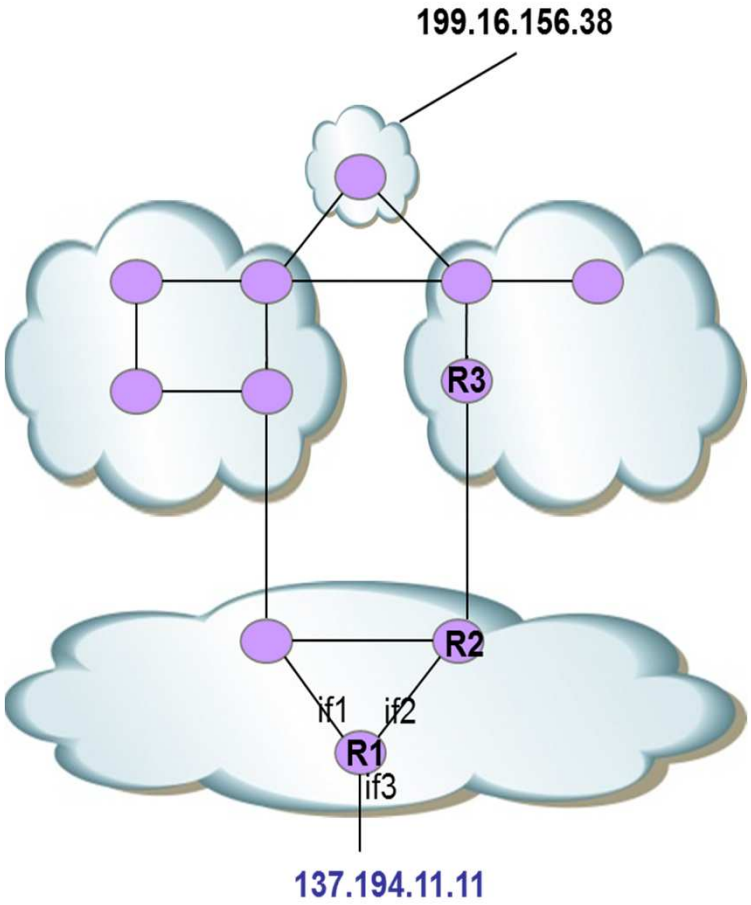
BGP
et l’interconnexion de réseaux

Sarah Nataf

IEUFI – Institut Mines-Telecom – 23 mai 2014
sarah.nataf@gmail.com

Qu’est-ce que BGP ?

- BGP est un protocole de routage IP dynamique
  - pour l'aiguillage des datagrammes IP
  - acheminement « hop-by-hop »
- Comment fonctionnent les routeurs IP ?
  - ont plusieurs « pattes » ou interfaces
  - utilisent l’adresse IP destination des paquets
  - résolvent cette adresse dans la table pour en déduire l’interface de sortie du paquet
- Comment peupler les tables de routage des routeurs IP ?
  - Les protocoles de routage IP transportent des infos de routes ou chemin vers des blocs d’@ IP pour calculer les meilleurs chemins



- **BGP est LE protocole de routage dynamique sur l’Internet**

Sommaire

BGP et l'Internet

Grands principes du routage BGP

Relations de peering vs client/transitaire

Politique de routage

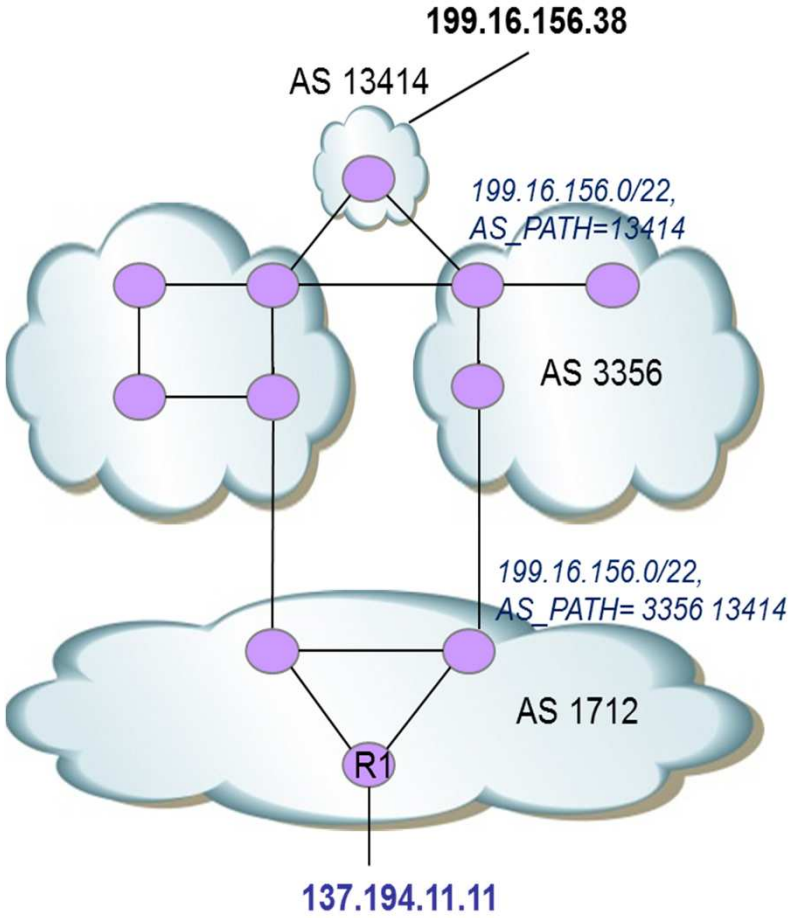
Un peu de protocole

Exemples de configuration

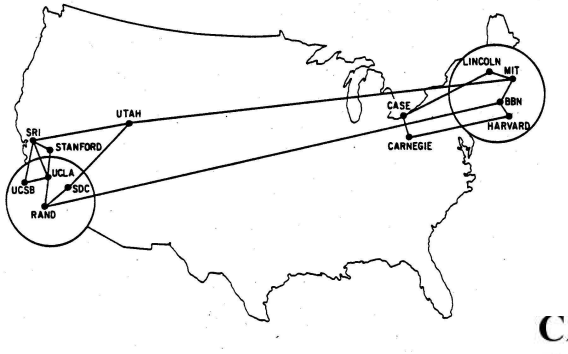
Comprendre les incidents BGP les plus célèbres

1. BGP et l'Internet

- Un peu de vocabulaire
  - AS
  - RIR / LIR
  - préfixe IP (e.g. 192.0.2.0/24, 2001:db8:abcd::/56)
  - voisin BGP
  - route BGP
  - attribut BGP (métriques, marqueurs, next-hop, etc)
  - AS_PATH
- Un protocole à vecteur de chemin (path vector) : décisions locales pour des chemins de bout en bout
- Un protocole robuste…

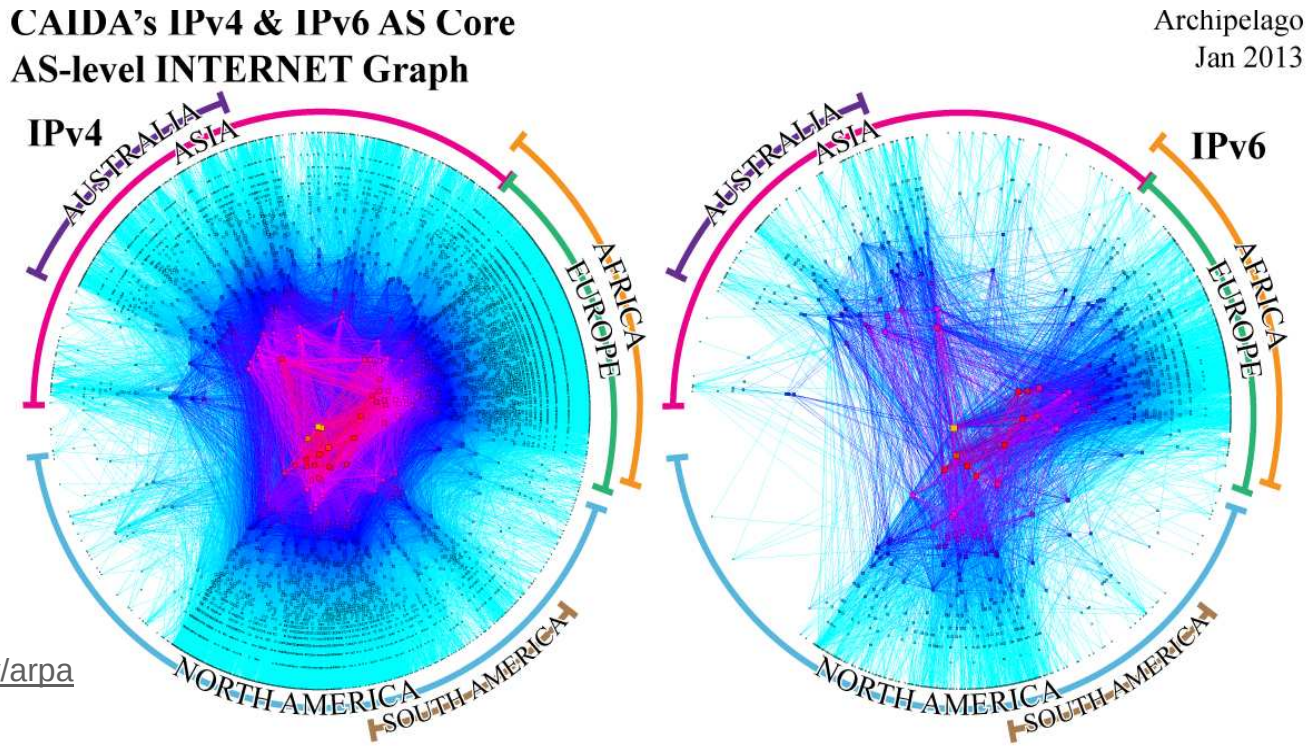


1. BGP et l'Internet



Arpanet - 1970

EGP : début 80's
BGP-1 : fin 80's
BGP-4 : 1995



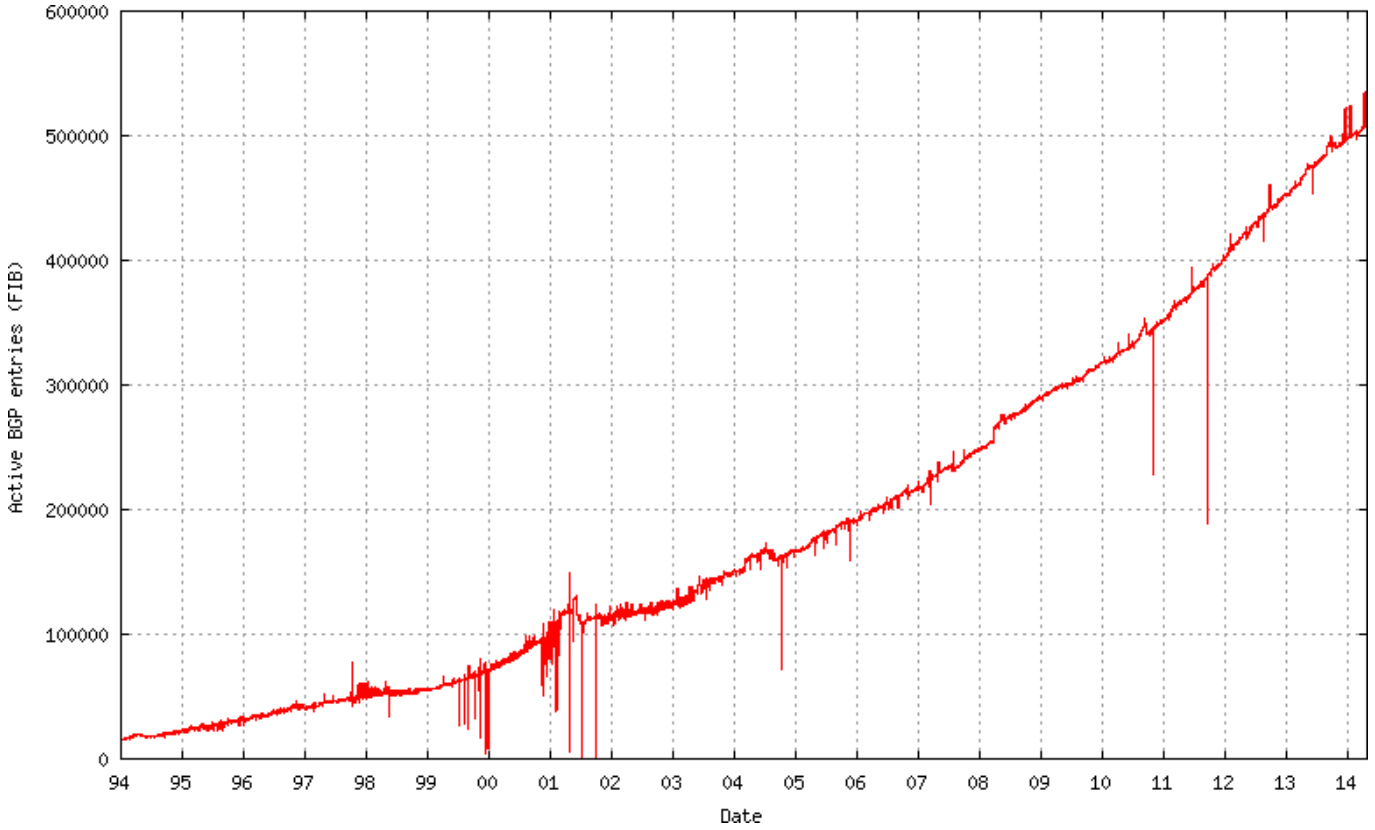
sources des illustrations:

http://som.csudh.edu/fac/lpress/history/arpamaps/

CAIDA : http://www.caida.org/home/

1. BGP et l'Internet

Évolution de la table IPv4 (source: potaroo.net)
vue de l'AS 6447 / Route-views Oregon IX

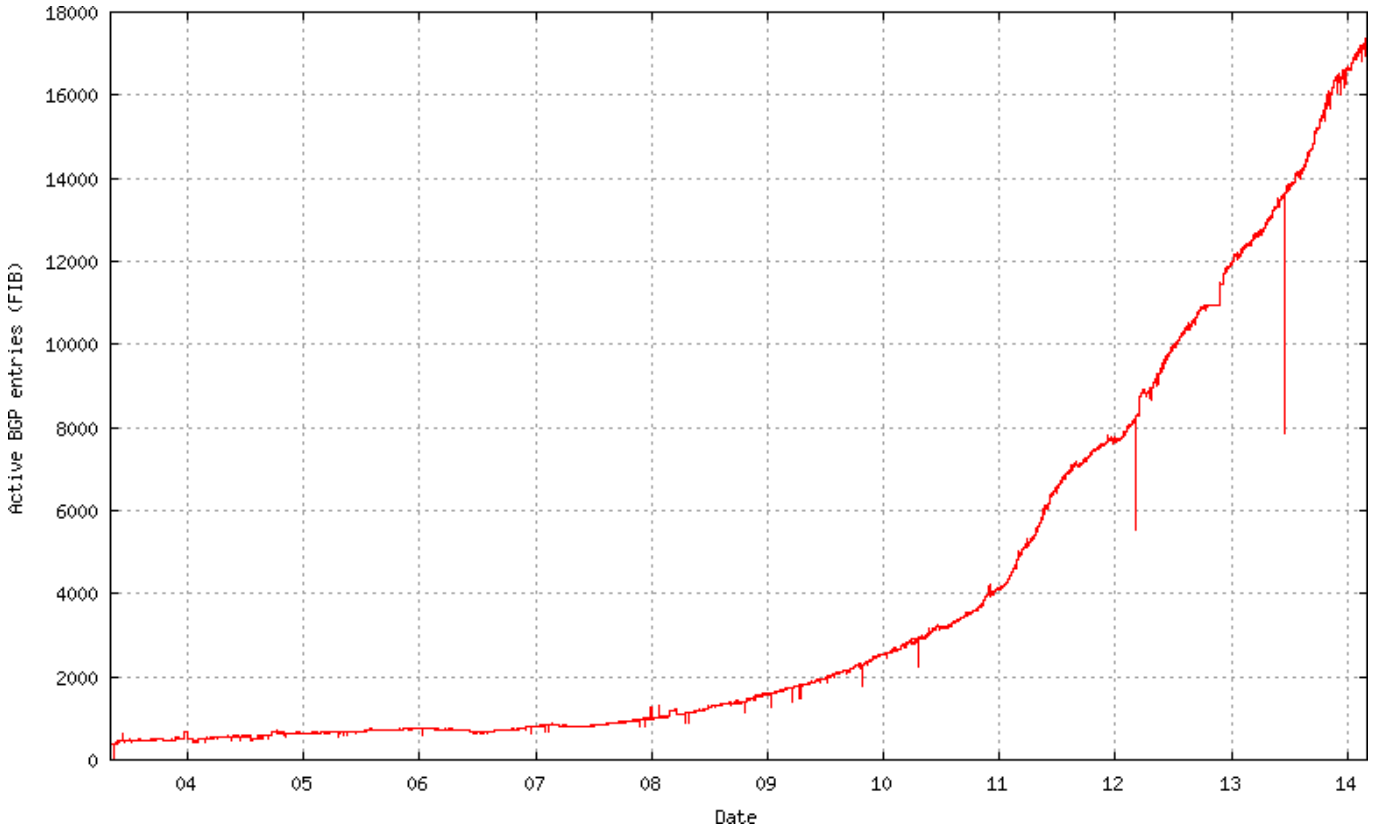


Chiffres clefs

505 000	nombre de routes IPv4
47 000	nombre d’AS
268 000	nombre de /24 dans la DFZ
53%	% d’adresses à 2 AS de distance de l’AS 6447
17 500	nombre de routes IPv6

1. BGP et l'Internet

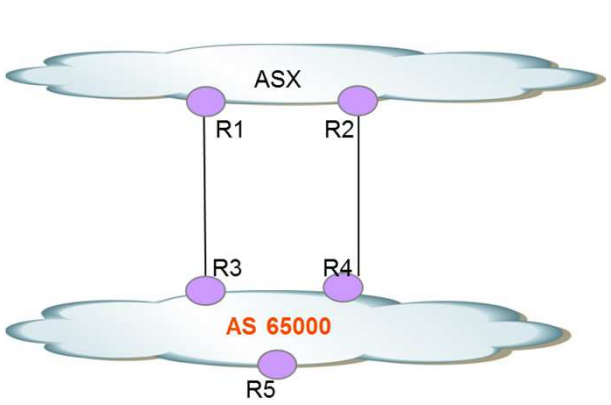
Évolution de la table IPv6 (source: potaroo.net)
vue de l'AS 6447 / Route-views Oregon IX

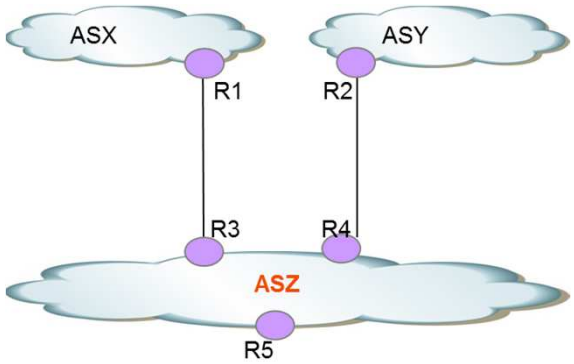


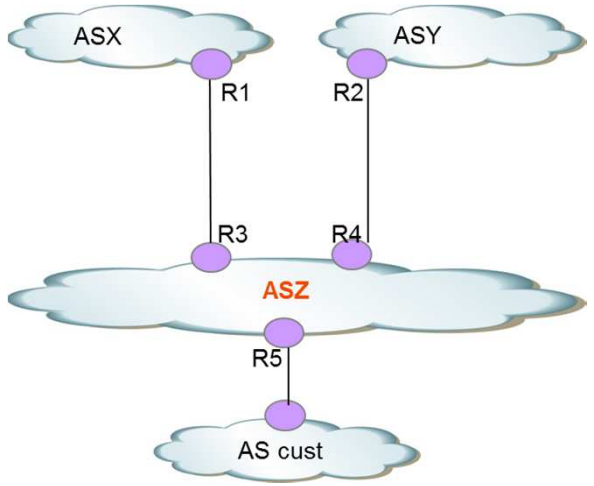
2. Grands principes du routage BGP

Pourquoi choisir d'activer une session BGP ?

- Utiliser BGP n'est pas une obligation pour se raccorder au reste du monde : il est possible par exemple d'utiliser une route par défaut statique.
- Cas d'usage classique : AS multihomé avec des besoins d'ingénierie de trafic particuliers
  - remarque : un tel AS peut très bien ne recevoir de ses transitaires qu'une route par défaut et non pas le full-routing.
  - remarque bis : un opérateur multihomé vers un unique autre opérateur peut utiliser BGP avec un numéro d'AS privé.



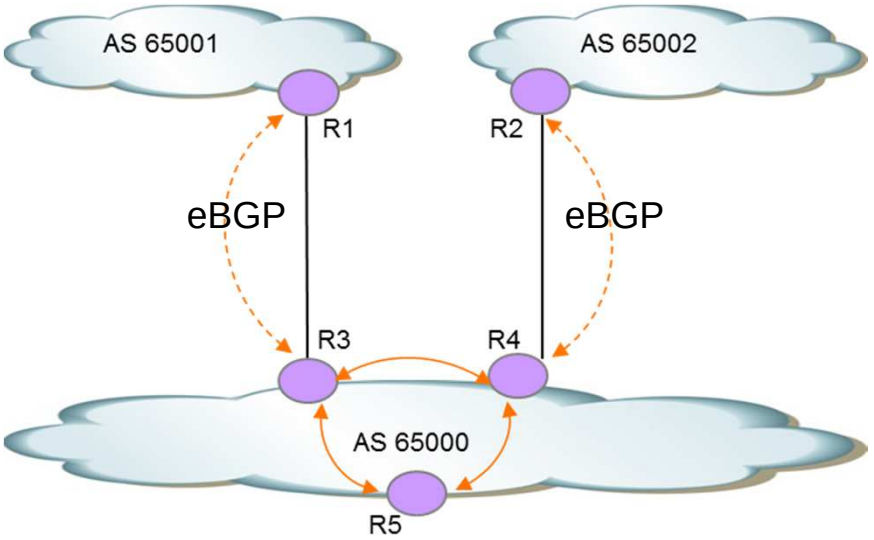




2. Grands principes du routage BGP
Établissement des sessions BGP

- Une session BGP s'établit entre 2 routeurs (ou voisins BGP) sur le port TCP/179
  - eBGP entre deux AS
  - iBGP au sein d'un AS
    - en full-mesh

- Par défaut, les sessions eBGP sont construites sur des liens directs (session monohop)
  - sinon configurer la session en multihop ;
  - optionnellement, possibilité de configurer une authentification.

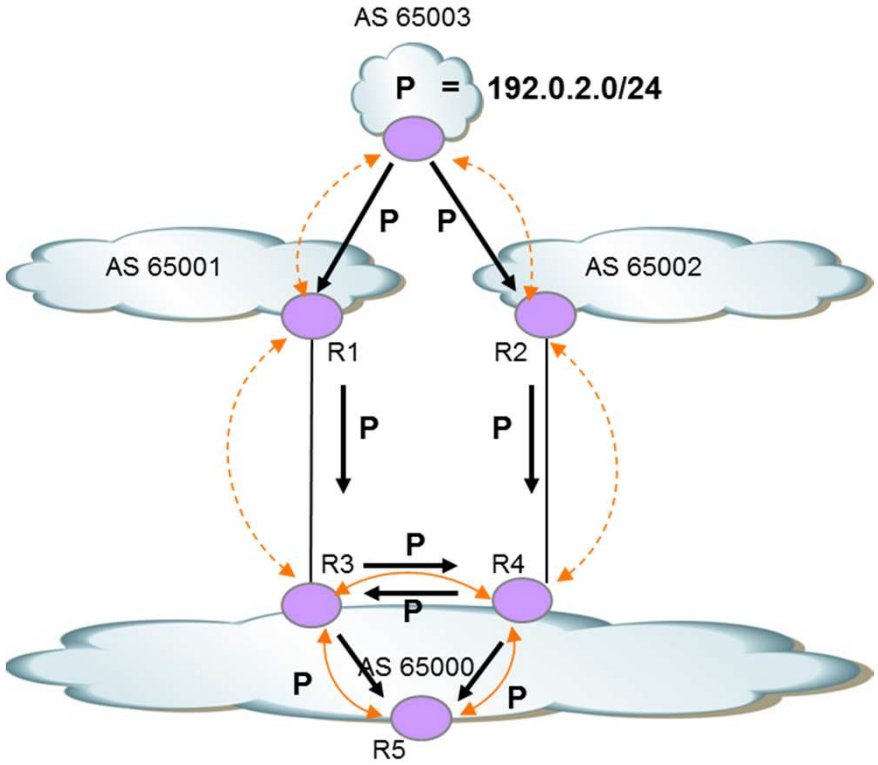


L'AS 65000 est multihomé.

2. Grands principes du routage BGP

Annonce d'une route BGP sur l'Internet

- Par défaut,
  - un routeur recevant une route via eBGP la réannonce à ses voisins iBGP ;
  - une route apprise via iBGP n'est pas réannoncée aux autres voisins iBGP.
- Le routeur construit sa table de routage BGP et réannonce sa "BEST"(*)
  - selon la politique de routage configurée ;
  - si pour une même destination plusieurs routes sont en concurrence, l'algorithme de sélection des meilleures routes s'applique.



Dans cet exemple, R3, R4 et R5 connaissent chacun 2 routes distinctes pour le préfixe P.

(*) en l'absence de fonctions type add-path

4. Politique de routage BGP

Attributs BGP

- 4 types d'attributs

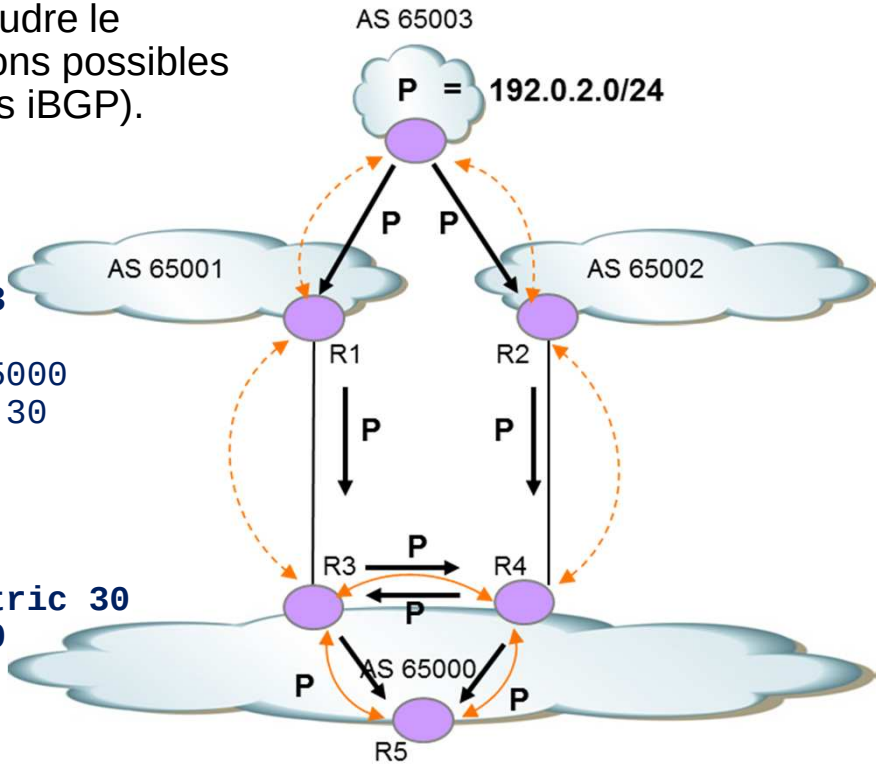
Well-known mandatory (reconnus, propagés et obligatoires) - AS_PATH - Next-Hop - Origin	**Optional Transitive** (transmis au voisin, optionnels) - Community - Aggregator
Well-known discretionnary (reconnus, propagés, présence facultative) - Local Preference - Atomic Aggregate	**Optional non-transitive** (optionnels et non retransmis) - MED (Multi-exit Discriminator)

source: APNIC elearning « BGP attributes »

2. Grands principes du routage BGP

Annonce d'une route BGP sur l'Internet

- Interaction entre BGP et l'IGP:
  - résolution des points de montage des sessions
  - c'est aussi l'IGP qui permet à R5 de résoudre le « next-hop » de la route (plusieurs solutions possibles lors des réannonces de routes eBGP vers iBGP).




```
sna@R5> show route 192.0.2.1 detail
192.0.2.0/24 (2 entries, 1 announced)
        *BGP    Preference: 170/-101
                Protocol next hop: 10.0.0.3
                State: <Active Int Ext>
                Local AS: 65000 Peer AS: 65000
                Age: 2w5d 5:41:32 Metric2: 30
                (…)
        BGP     Preference: 170/-101
                (…)
sna@R5> show route 10.0.0.3
10.0.0.3/32  *[IS-IS/18] 4w6d 07:29:03, metric 30
                     > to 10.5.3.3 via ae3.0


sna@R5> show route 192.0.2.1
192.0.2.0/24        *[BGP/170] 2w5d 06:00:31, localpref 100, from 10.0.0.3
                      AS path: 65001 65003 I, validation-state: unverified
                    > to 10.5.3.3 via ae3.0
                    [BGP/170] 2w5d 06:00:31, localpref 100, from 10.0.0.4
                      AS path: 65002 65003 I, validation-state: unverified
                    > to 10.5.4.4 via ae4.0
```

2. Grands principes du routage BGP

Exemples extraits de looking-glass

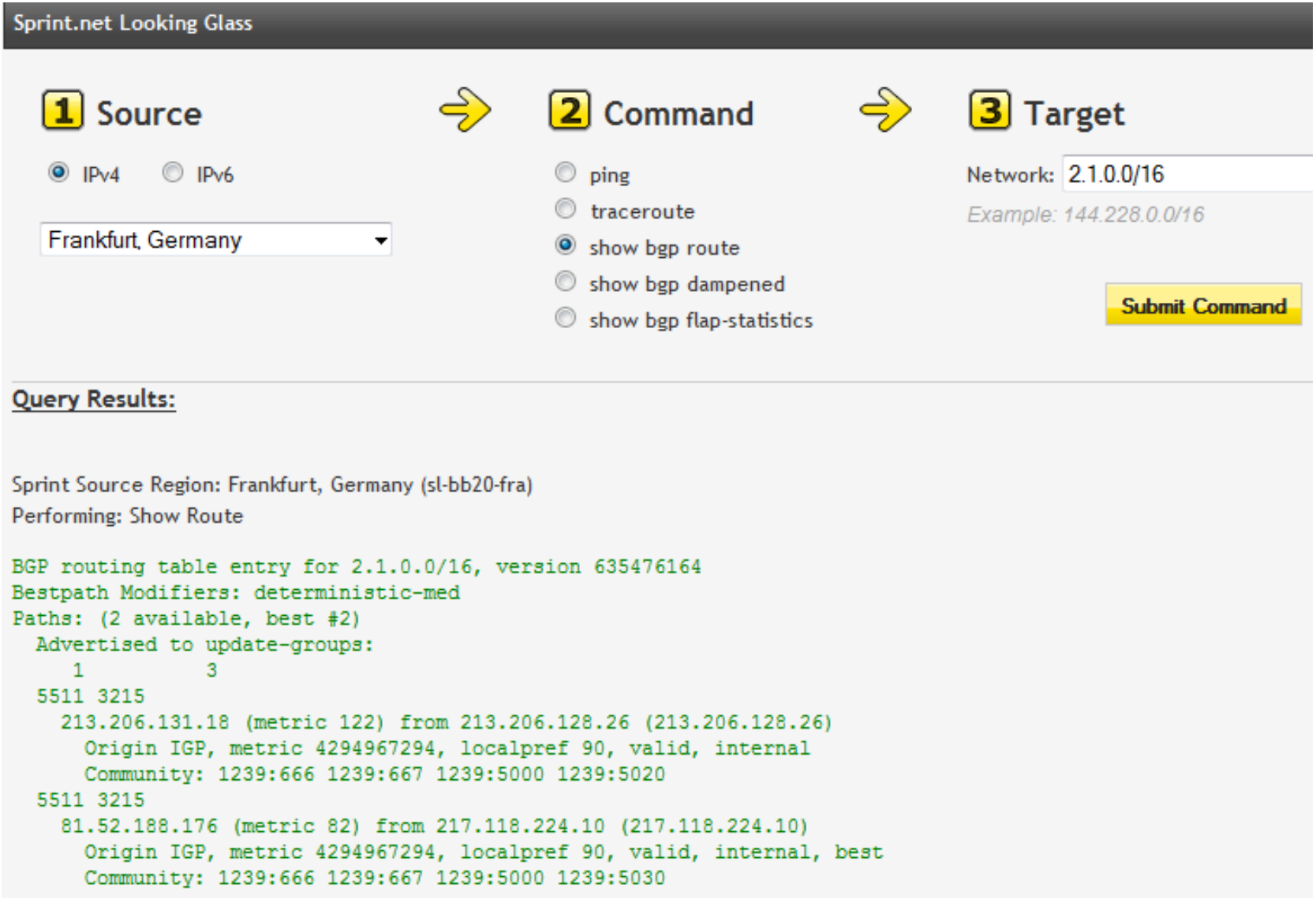
Test	Router Location	Hostname / IP Address	
BGP	DE - Frankfurt	2.1.0.0/16	Go!

```
BGP routing table entry for 2.1.0.0/16, version 203962045
Paths: (1 available, best #1, table Default-IP-Routing-Table)
  5511 3215
    130.117.15.2 (metric 10102022) from 38.28.1.137 (38.28.1.137)
      Origin IGP, metric 4294967294, localpref 100, valid, internal, best
      Community: 174:11401 174:20666 174:21100 174:22005
      Originator: 38.28.1.42, Cluster list: 38.28.1.137, 38.28.1.250, 38.28.1.30
```

Test	Router Location	Hostname / IP Address	
BGP	US - Washington, DC	2.1.0.0/16	Go!

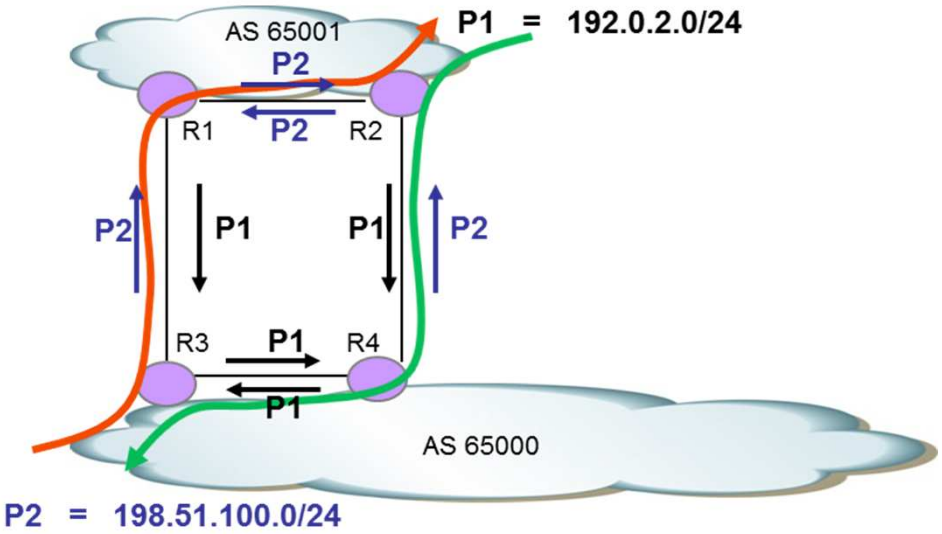
```
BGP routing table entry for 2.1.0.0/16, version 2246453881
Paths: (1 available, best #1, table Default-IP-Routing-Table)
  5511 3215
    154.54.10.14 (metric 10102021) from 154.54.66.76 (154.54.66.76)
      Origin IGP, metric 4294967294, localpref 100, valid, internal, best
      Community: 174:10031 174:20666 174:21000 174:22013
      Originator: 66.28.1.9, Cluster list: 154.54.66.76, 66.28.1.69, 66.28.1.89
```

2. Grands principes du routage BGP



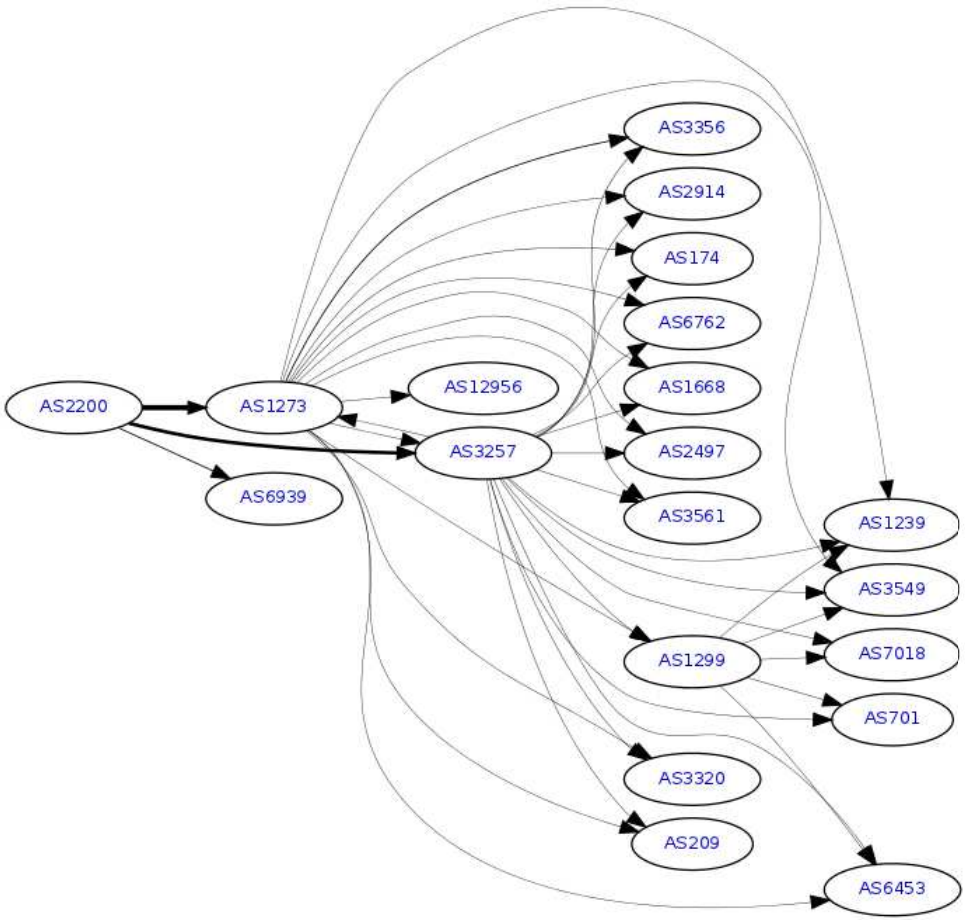
2. Grands principes du routage BGP
Principe de la patate chaude

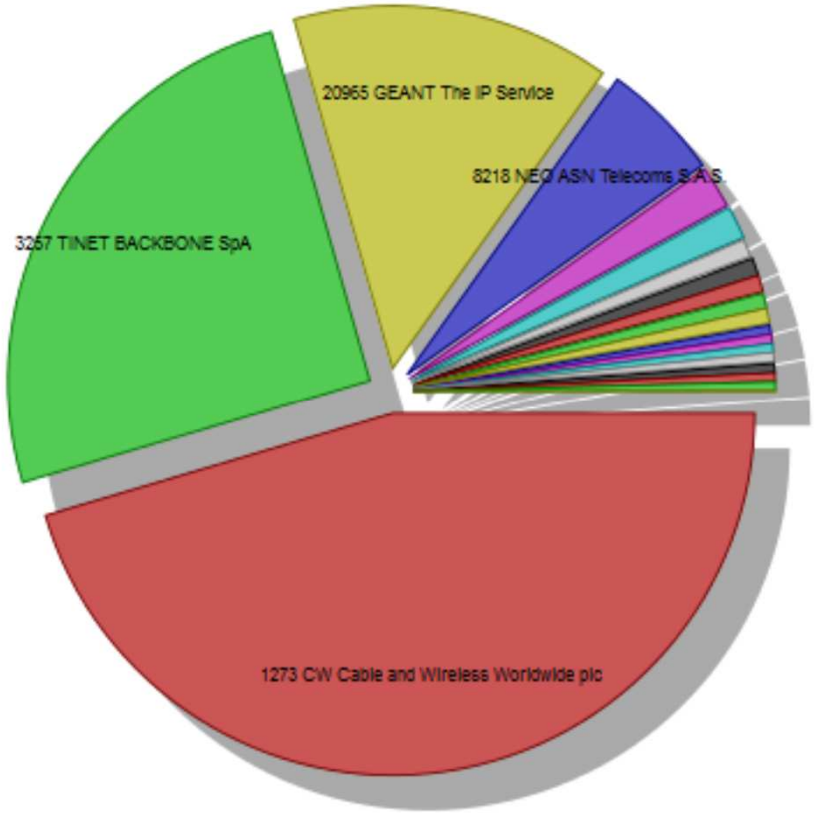
- Routage « hot potato »
  - en l'absence de politique de routage contraire, pour un même préfixe et à égalité de certains critères (e.g. même longueur d'AS_PATH etc), une route apprise via eBGP est préférée à une route apprise via iBGP



3. Relations entre AS

Exemple : graphe de connexion IPv4 pour l'AS 2200 (Renater) tel que vu par HE et par Robtex





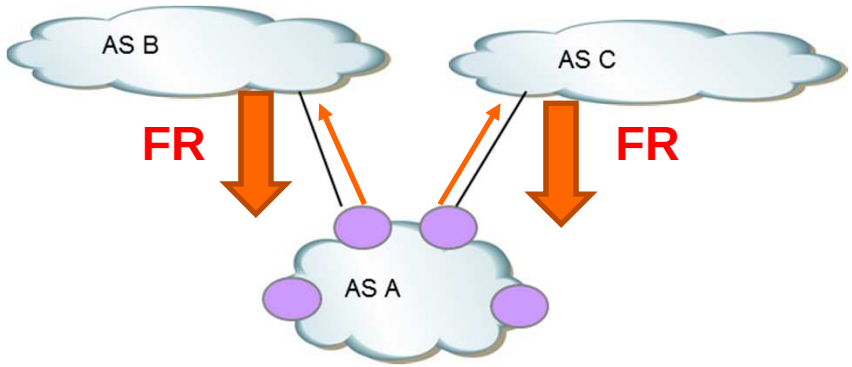
3. Relations entre AS

La relation client / transitaire

- A annonce toutes ses routes à B (ainsi que celles de ses éventuels clients).
- B annonce la full-routing Internet à A.

- A utilise B pour l'évasion de son trafic vers le reste de l'Internet, et réciproquement reçoit le trafic Internet via son transitaire B.

- Attention : A n'envoie pas la full-routing à B !



A est client de B,
B est transitaire de A

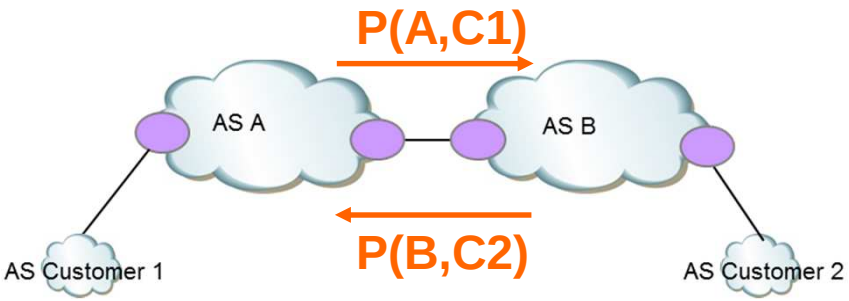
3. Relations entre AS

La relation de peering

- A annonce toutes ses routes à B ainsi que celles de ses éventuels clients
- B annonce toutes ses routes à A ainsi que celles de ses éventuels clients

- Le trafic entre clients de A et de B passe par le lien de peering et n'utilise pas les réseaux des transitaires
  - coûts (opérateurs ☺) et performances (utilisateurs ☺)

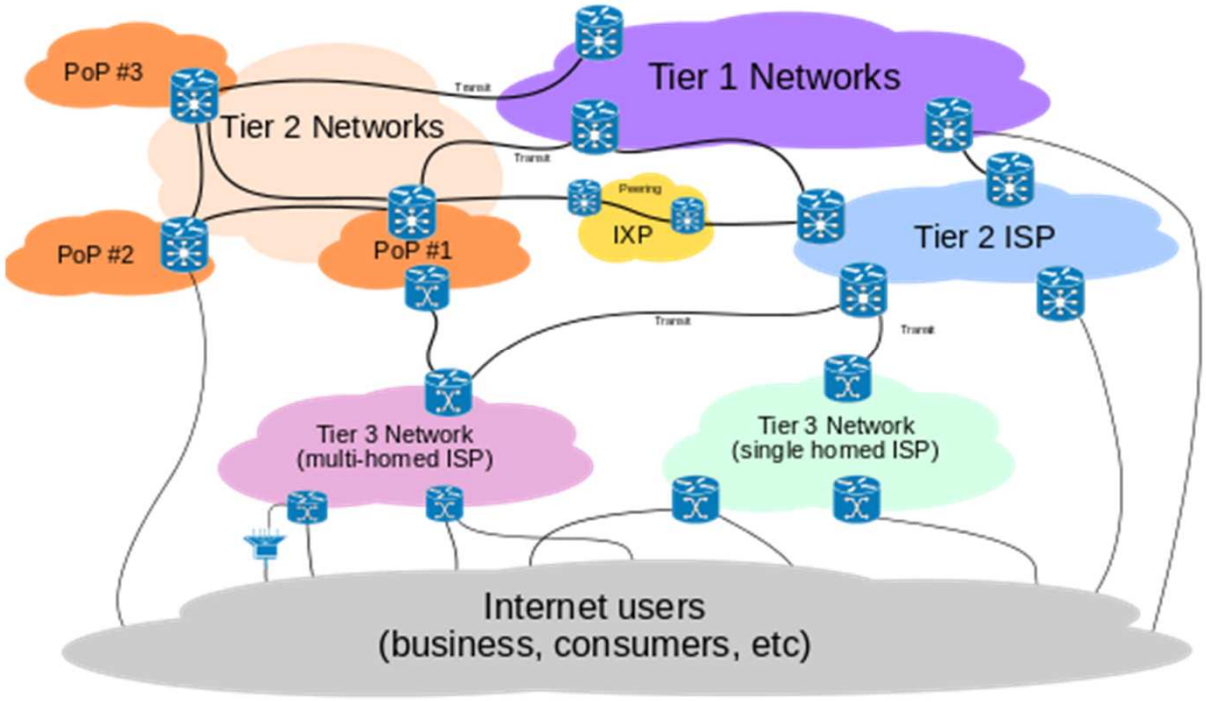
- Attention : A n'annonce pas la full-routing à B ni des routes reçues de ses peers ! (et réciproquement)



A et B sont peers

3. Relations entre AS

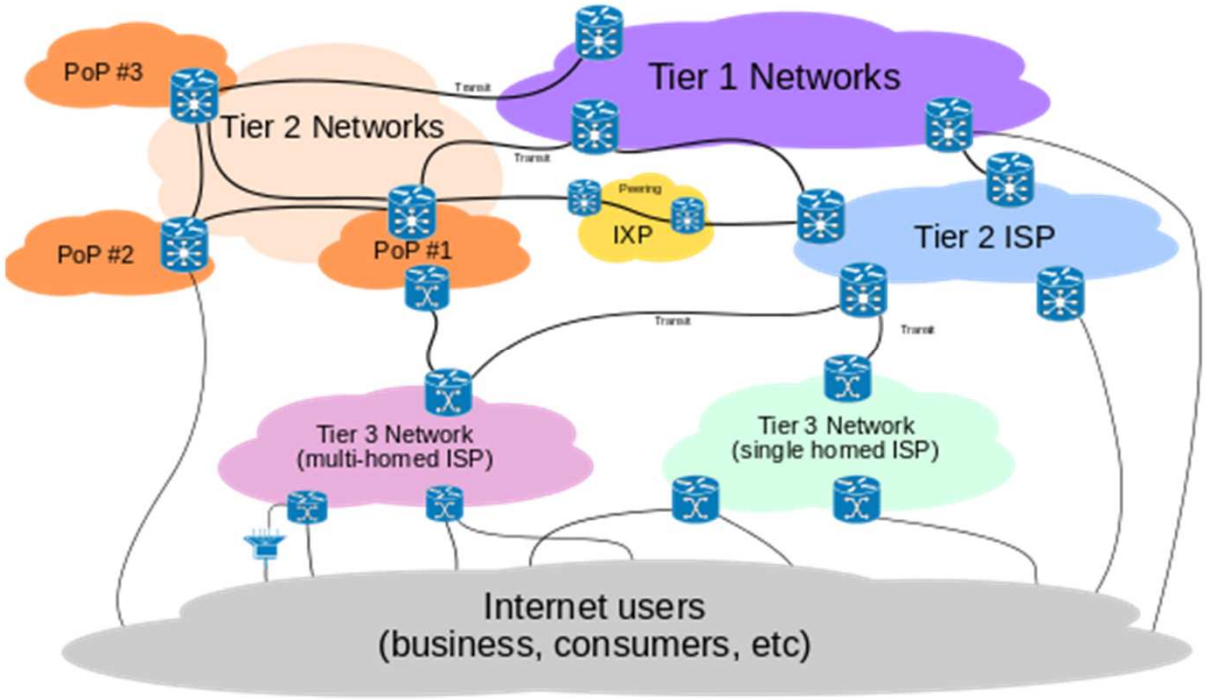
Tier-1, Tier-2, etc



source: Wikipedia

- Est dit « Tier-1 » un AS qui ne paie aucun transitaire pour joindre la totalité des destinations de l'Internet :
  - il n'a que des relations de peering,
  - et est lui-même transitaire pour certains clients.
- Cartel des Tier-1 (liste extraite de http://en.wikipedia.org/wiki/Tier_1_network) : AT&T, CenturyLink, DT, XO, GTT (ex-Tinet), Verizon, Sprint, Telia, NTT, L3, Tata, AboveNet, Cogent, Seabone

3. Relations entre AS
architectures d'interconnexion

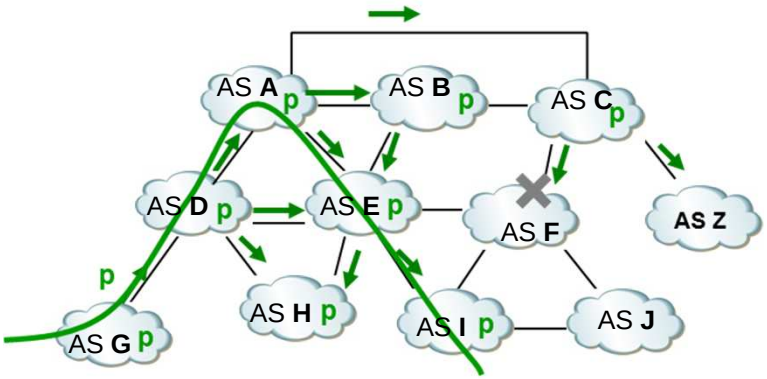


source: Wikipedia

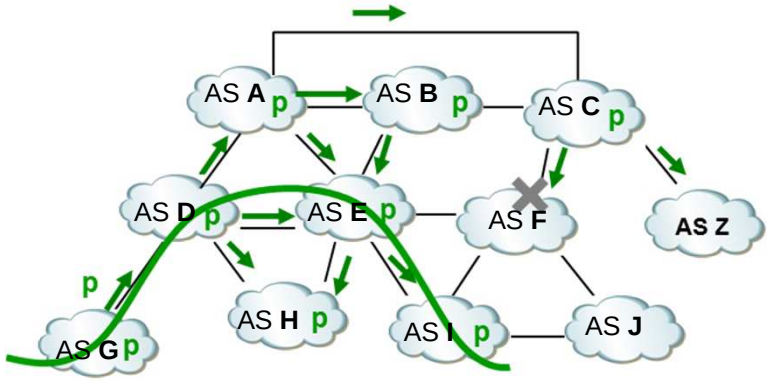
- sur les POP (Point of Presence)
- en direct
- via un IXP ou point d'échange
  - en direct (vlan privé)
  - sur le vlan public, optionnellement via un route-server

3. Relations entre AS

Graphe des relations entre AS



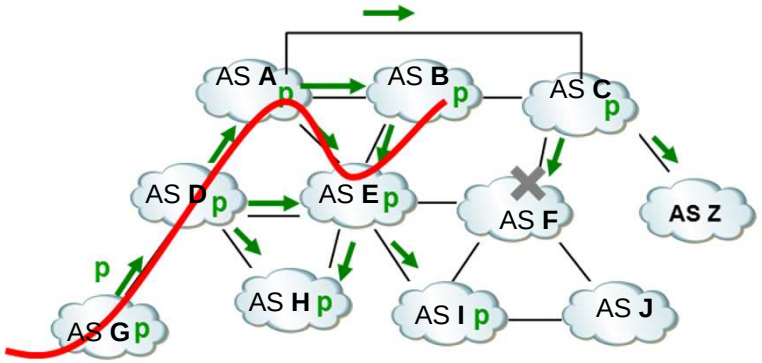
OK



OK

Ce chemin d'annonce du préfixe p est anormal car un client ne réannonce pas à un transitaire une route reçue d'un autre transitaire.

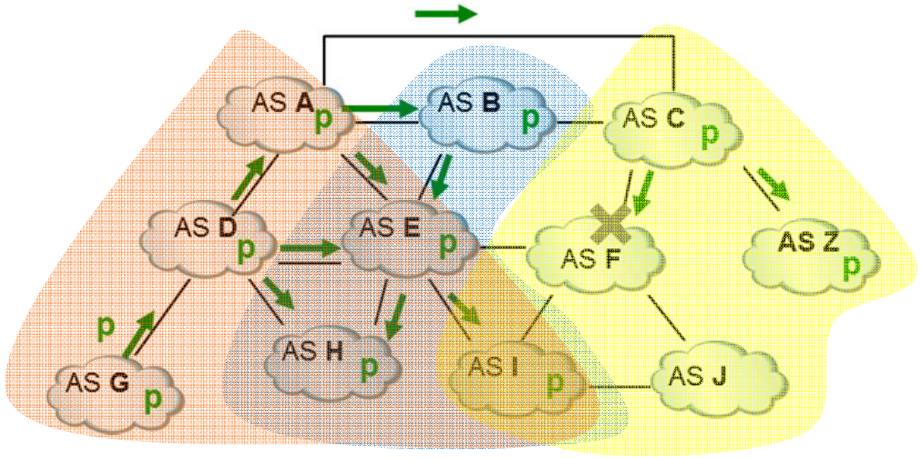
NB : les moteurs d'inférences de relations utilisent un autre modèle (composé) = transit mutuel ("sibling").



NOK

3. Relations entre AS

Propagation d'une annonce BGP



- Sur l'Internet, les tables de routage de chaque routeur diffèrent du fait des politiques de routage implémentées dans les AS :
  - Un routeur BGP ne réannonce que sa BEST à ses voisins.
  - selon les filtres, certains préfixes peuvent même ne pas être reçus par certains AS : connectivité (graphe) n'implique pas joignabilité.
- Exemple de « depeering » : Cogent/Telia en 2008 (théorie des petits mondes)

4. Politique de routage BGP

Généralités

- La politique de routage BGP est propre à un AS
  - « autonome » : chaque AS fait ce qu'il veut sur son réseau,
  - la cohérence est à la charge à de l'ingénierie et des choix d'implémentation.
- La politique de routage BGP traduit les accords économiques entre AS et les choix d'ingénierie de trafic, par exemple
  - 1. pour une destination donnée préférer un écoulement via un client, sinon via un peer, sinon via un transitaire ;
  - 2. connexions nominale / backup vers 2 transitaires
  - 3. connexions en partage de charge vers 2 transitaires
  - 4. préférer le routage « cold potato » pour des raisons de qualité de service,
  - 5. favoriser le trafic local, etc
- Attention, BGP assure le contrôle de la sortie du trafic de l'AS mais ne peut contrôler à 100% comment il entre dans le réseau.
- Critères de sélection des meilleures routes : la politique de routage utilise les attributs des routes BGP.

4. Politique de routage BGP

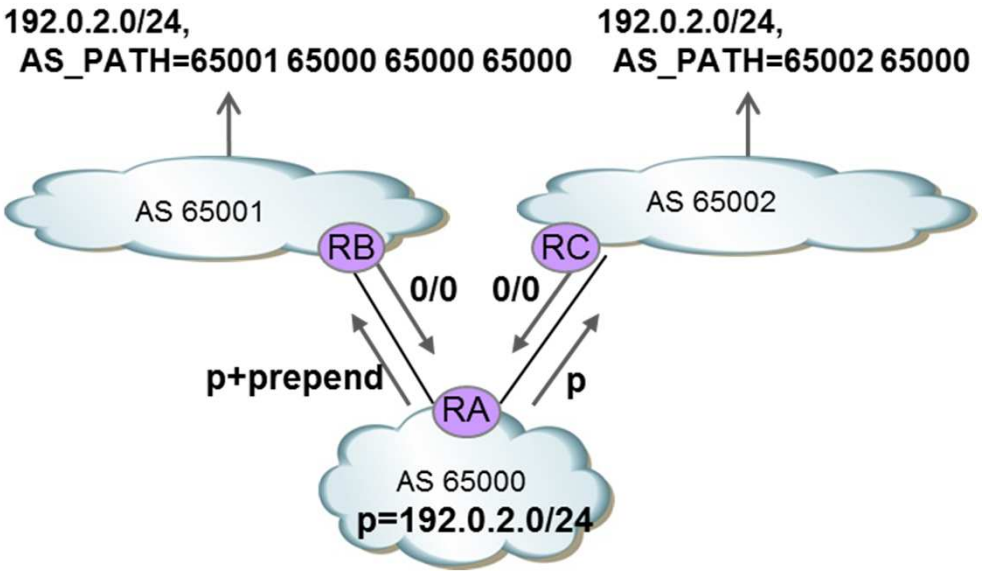
Élection du meilleur chemin

- Chaque vendeur a son propre algorithme de sélection des meilleurs chemins !
- Exemple d'algorithme (simplifié) sur les routeurs Cisco :
  1. Prefer the path with the highest WEIGHT.
  2. Prefer the path with the highest LOCAL_PREF.
  3. Prefer the path that was locally originated via a network or aggregate BGP subcommand or through redistribution from an IGP.
  4. Prefer the path with the shortest AS_PATH.
  5. Prefer the path with the lowest origin type.
  6. Prefer the path with the lowest multi-exit discriminator (MED).
  7. Prefer eBGP over iBGP paths.
  8. Prefer the path with the lowest IGP metric to the BGP next hop.
  9. Determine if multiple paths require installation in the routing table for BGP Multipath.
  10. When both paths are external, prefer the path that was received first (the oldest one).
  11. Prefer the route that comes from the BGP router with the lowest router ID.
  12. If the originator or router ID is the same for multiple paths, prefer the path with the minimum cluster list length.
  13. Prefer the path that comes from the lowest neighbor address.

4. Politique de routage BGP

Application : interco nominale/backup grâce au prepending de préfixe + local pref

```
hostname RA
!
router bgp 65000
 no synchronization
 bgp log-neighbor-changes
 network 192.0.2.0
 neighbor 10.10.1.1 remote-as 65001
 neighbor 10.10.1.1 route-map RB-OUT out
 neighbor 10.10.2.1 remote-as 65002
 neighbor 10.10.2.1 route-map RC-IN in
 maximum-paths 2
 no auto-summary
!
access-list 1 permit 192.0.2.0
ip as-path access-list 2 permit ^65002$
route-map RB-OUT permit 10
 match ip address 1
 set as-path prepend 65000 65000
!
route-map RC-IN permit 10
match as-path 2
 set local-preference 200
```



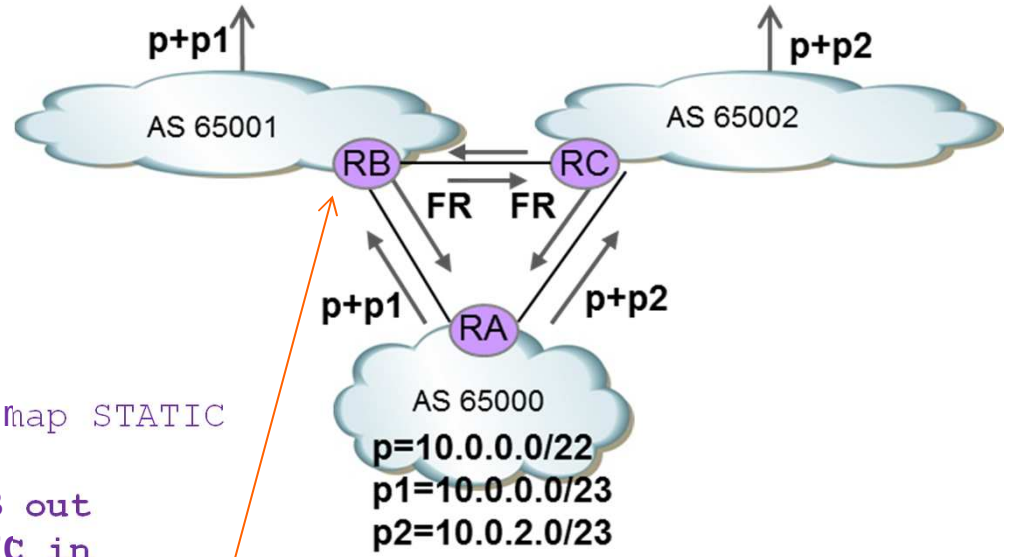
Résultat sur RA (extraits) :

```
RA# show ip bgp
Status codes: s suppressed, d damped, h history,
* valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network   Next Hop   LocPrf Weight Path
*  0.0.0.0   10.10.1.1     100      0 65001 i
*>i          10.10.2.1     200      0 65002 i
```

4. Politique de routage BGP

Application : multihoming avec partage de charge




```
hostname RA
!
router bgp 65000
 no synchronization
 bgp log-neighbor-changes
 redistribute static metric 0 route-map STATIC
 neighbor 10.10.1.1 remote-as 65001
 neighbor 10.10.1.1 prefix-list toRB out
 neighbor 10.10.1.1 route-map GENERIC in
 neighbor 10.10.2.1 remote-as 65002
 neighbor 10.10.2.1 prefix-list toRC out
 neighbor 10.10.2.1 route-map GENERIC in
 maximum-paths 2
 no auto-summary
!
ip prefix-list toRB permit 10.0.0.0/22
ip prefix-list toRB permit 10.0.0.0/23
ip prefix-list toRC permit 10.0.0.0/22
ip prefix-list toRC permit 10.0.2.0/23
ip route 10.0.0.0 255.255.252.0 null0
```

Dans la RIB :
10.0.0.0/22, AS_PATH = 65000
10.0.0.0/23, AS_PATH = 65000
10.0.2.0/23, AS_PATH = 65002 65000
Dans la FIB :
10.0.0.0/23 : if-TO-RB
10.0.2.0/23 : if-TO-RC

D'où désagrégation : propagation de 3 routes pour l'AS 65000 au lieu de 1. Et en fonction de la charge, on adapte les annonces pour répartir le trafic (e.g. ajout d'un /24, etc),

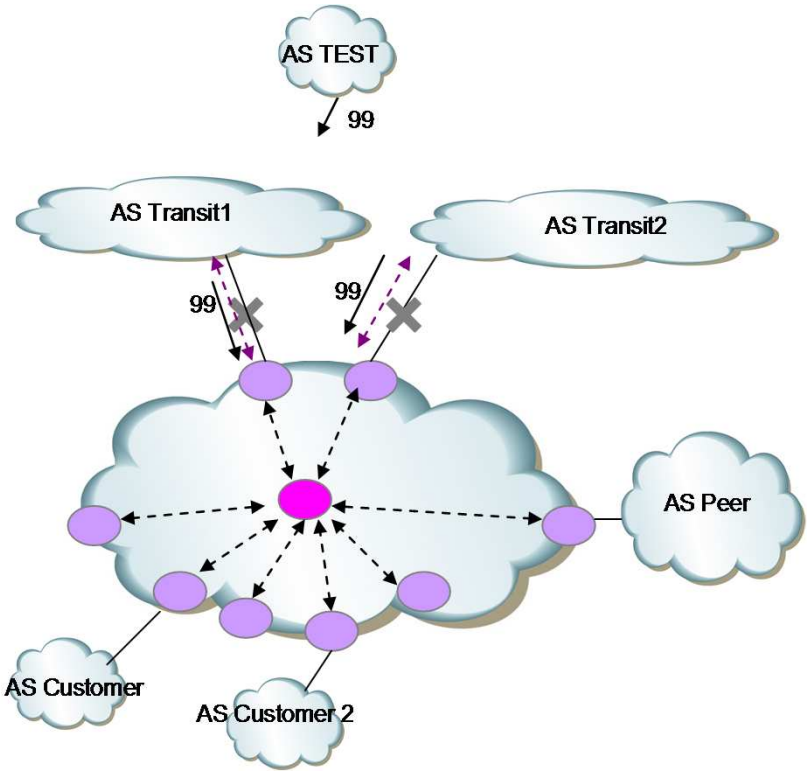
5. Protocole BGP
Spécifications

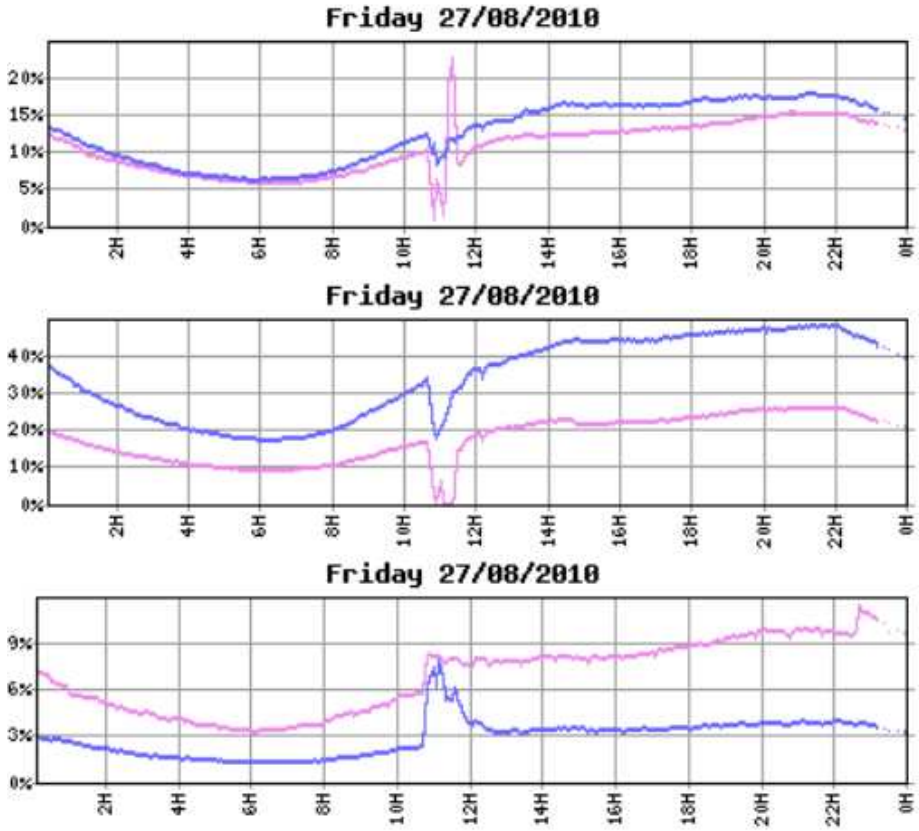
- Normalisé principalement dans le RFC 4271 (2006), qui définit entre autre
  - les 4 types de messages : OPEN, UPDATE, KEEP ALIVE, NOTIFICATIONS ;
  - la machine à états pour l'établissement, le maintien et la fermeture de session ;
  - les opérations de maintenance des tables utilisées par BGP (Adj-RIB-in etc), d'émission de nouvelle annonce ou suppression de chemin pour un préfixe donné.
- RFC4271 définit également les attributs et leur utilisation
  - ceci pour les routes IPv4 unicast.
- D'autres RFC définissent les solutions de réflexion de routes ou confédération au sein d'un AS, ou encore des extensions BGP pour d'autres AFI/SAFI, des mécanismes de haute disponibilité, etc.
  - Les routeurs annoncent leur compatibilité avec ces extensions dans les messages OPEN.

5. Protocole BGP

jouer avec le protocole BGP…

- incident « BGP option 99 » - 27 août 2010
  - révélation d'un bug lors de tests préliminaires de secure BGP





5. Protocole BGP
jouer avec le protocole BGP…

- Incident « Mikrotik » :
  - Révélation d'un bug sur le traitement d'UPDATE BGP contenant un préfixe avec un AS_PATH trop long

- Pour remédier à ces incidents,
  - pour le BGP 99 : une optimisation protocolaire a été proposée pour tenter de maintenir une session BGP établie lorsque seuls certains messages UPDATE (NLRI avec attribut malformés) sont malformés au lieu de systématiquement clore les sessions ;
  - pour le mikrotik : déployer un filtre sur la longueur de l'attribut AS_PATH a été recommandé, filtre toujours présent sur nombre de configurations.

6. Configuration et commandes BGP

```
*A:ALU>config>router>bgp# info
    remove-private
    router-id 10.10.10.5
    enable-peer-tracking
    rapid-withdrawal
    group "GROUPE-iBGP"
        family ipv4 ipv6 vpn-ipv4 flow-ipv4
        type internal
        export "STATIC2BGP" "IBGP-OUT"
        local-address 10.10.10.5
        neighbor 10.10.10.3
            description "R3"
        exit
        neighbor 10.10.10.4
            description "R4"
        exit
    exit
    group "Transit1"
        family ipv4
        type external
        local-address 10.1.1.1
        import "GENERIC-IN" "Transit1-IN"
        export "Transit1-OUT"
        neighbor 10.1.1.2
            description "R1-Transit1-10GE"
            peer-as 65501
            prefix-limit 50
        exit
    exit
    group "Transit1-v6"
        family ipv6
        type external
        local-address 2001:db8::5
        import "GENERIC-IN" "Transit1-IN"
        export "Transit1-OUT"
        neighbor 2001:db8::4
            peer-as 65501
            prefix-limit 10
        exit
    exit
    no shutdown
```

6. Configuration et commandes BGP

```
Looking Glass Query results

BGP router identifier 195.66.232.254, local AS number 5459
BGP table version is 291365610, main routing table version 291365610
415496 network entries using 56507456 bytes of memory
2765936 path entries using 154892416 bytes of memory
505220/72867 BGP path/bestpath attribute entries using 64668160 bytes of memory
261900 BGP AS-PATH entries using 9691704 bytes of memory
25409 BGP community entries using 1291898 bytes of memory
92 BGP extended community entries using 2794 bytes of memory
16 BGP route-map cache entries using 576 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
BGP using 287055004 total bytes of memory
1273432 received paths for inbound soft reconfiguration
BGP activity 26805232/26294225 prefixes, 733136865/730230610 paths, scan
interval 60 secs

Neighbor           AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
195.66.224.1     6412  134810  140418 291365610    0    0 6w2d          214
195.66.224.2    51823   70833   70874 291365610    0    0 6w2d            1
195.66.224.13   47541       0       0        1    0    0 4w1d     Idle
195.66.224.21    6939  479147   70853 291365610    0    0 6w2d        56483
195.66.224.50   39792       0       0        1    0    0 1y13w    Active
195.66.224.52  132591   29310   32260 291365610    0    0 2w6d            1
```

6. Configuration et commandes BGP

```
R1#sh ip bgp neighbors aaa.bbb.ccc.ddd
BGP neighbor is aaa.bbb.ccc.ddd,  remote AS 3215, internal link
 Description: R1
 Member of peer-group ROUTEURS-IBGP for session parameters
  BGP version 4, remote router ID aaa.bbb.xxx.yyy
  BGP state = Established, up for 1w0d
  Last read 00:00:06, last write 00:00:24, hold time is 90,
keepalive interval is 30 seconds
  Neighbor sessions:
    1 active, is not multisession capable
  Neighbor capabilities:
    Route refresh: advertised and received(new)
    Four-octets ASN Capability: advertised and received
    Address family IPv4 Unicast: advertised and received
    Graceful Restart Capability: received
      Remote Restart timer is 120 seconds
      Address families advertised by peer:
        none
    Multisession Capability: advertised
                         Sent       Rcvd
    Opens:                  1          1
    Notifications:          0          0
    Updates:             3914     156187
    Keepalives:         21990      22409
    Route Refresh:          0          0
    Total:              25905     178597
  Default minimum time between advertisement runs is 0 seconds
```

7. Incidents BGP

Ré-annonces de tables de routage Internet

- La plus ancienne occurrence : AS 7007
  - réannonce de la FR dans l'IGP lui-même réannoncé en BGP
- De nombreuses occurrences de cet incident, ayant des retombées diverses sur le trafic.

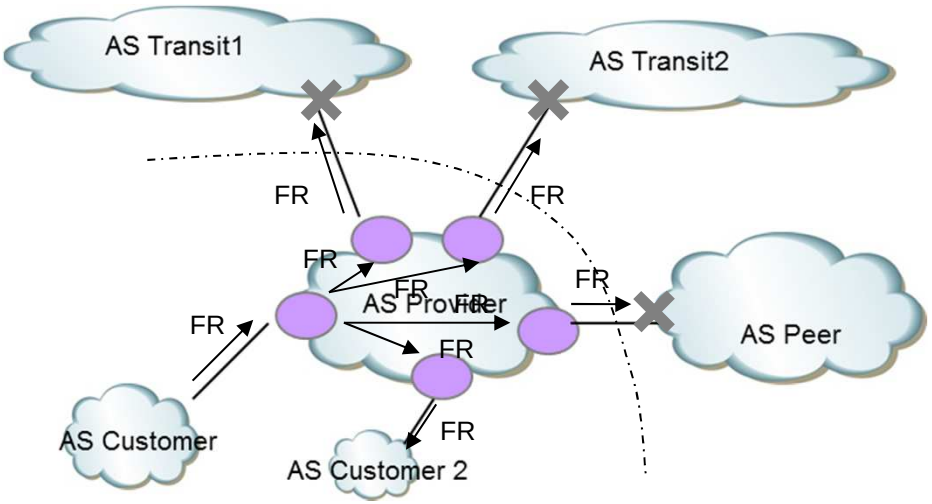
- Pour s'en prémunir, des filtres sont positionnées en IN sur les sessions eBGP (entre peers, entre clients/transitaires) :
  - filtres en exact-match sur les préfixes
  - les filtres sur l'AS_PATH ne suffisent en général pas si l'AS fautif a modifié les AS origines

    ex de filtre :

    ```
    as-path access-list xx permit ^(_2200)+(_1712)*(_64497)$
    ```
  - limitation sur le nombre de route annoncées : cf. slide 31

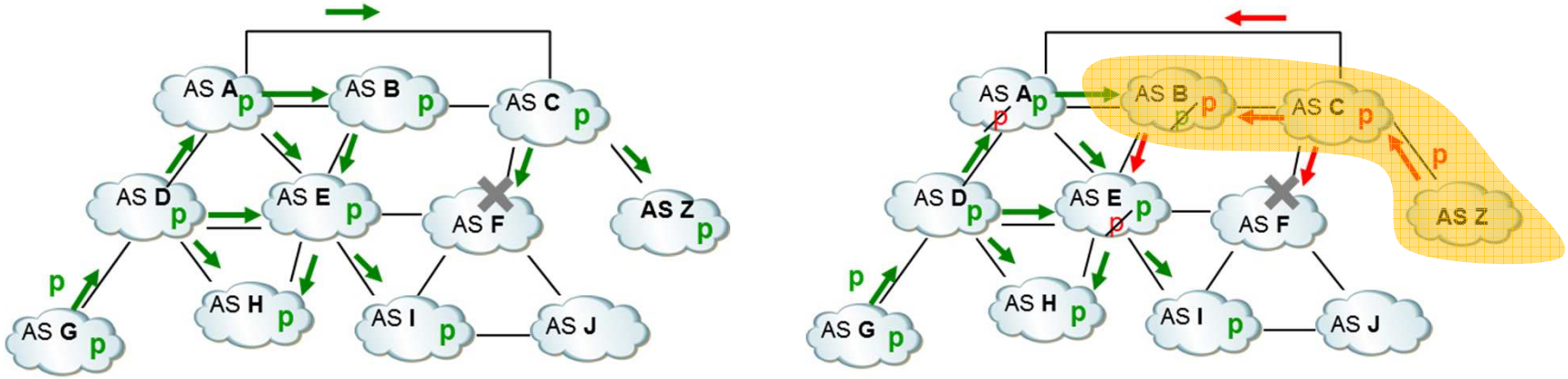
7. Incidents BGP

Ré-annonces de tables de routage Internet : un exemple de février 2012



7. Incidents BGP

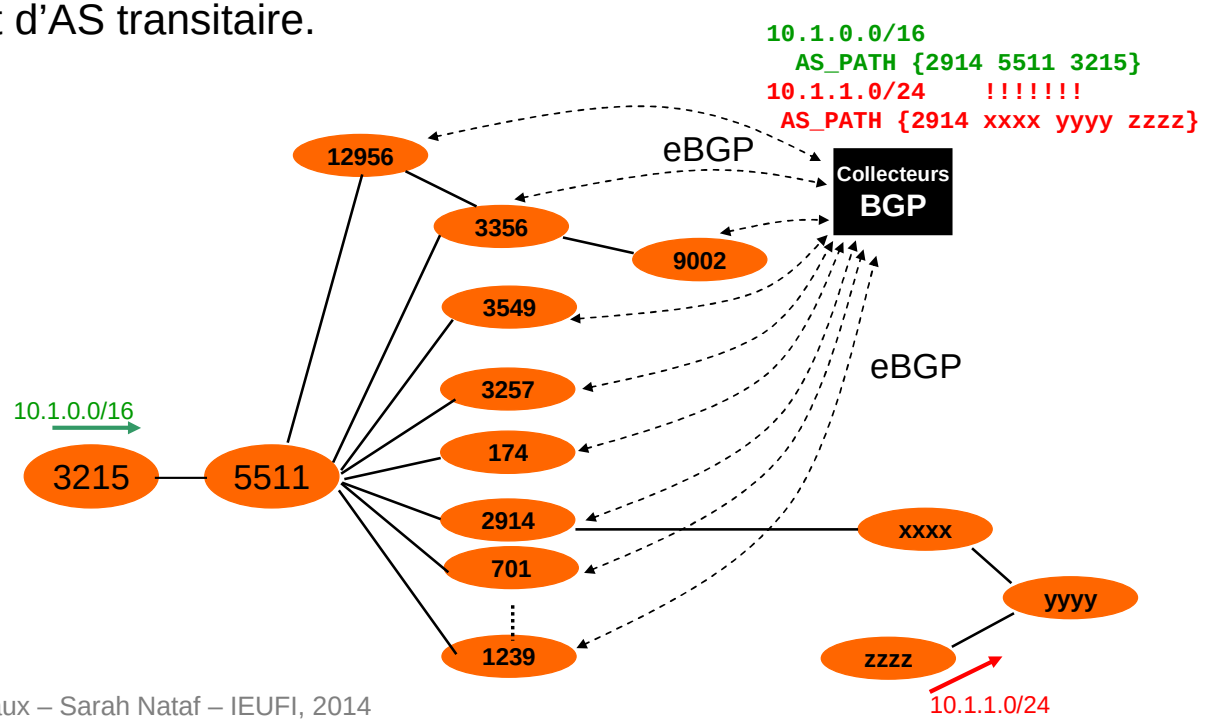
Usurpation de préfixes ou BGP hijacking



- Lorsqu'un préfixe p est usurpé par l'AS Z, il est fréquent que seule une partie de l'Internet converge sur la nouvelle route.
  - l'impact dépend du degré de connectivité des AS légitime et usurpateur du préfixe ainsi que des filtres.
- Si un AS Z annonce un préfixe p' plus spécifique, la zone de pollution est souvent bien plus importante.

7. Incidents BGP
Monitoring BGP sur l'Internet

- Outils construits autour de sondes BGP qui traitent les tables de routage ou les UPDATES BGP et détectent les anomalies :
  - disparition d'un préfixe ;
  - nouveau préfixe pour un AS donné ;
  - préfixe identique annoncé par un autre AS ;
  - préfixe plus spécifique (e.g. un /24 appartenant à un /16) ;
  - changement d'AS transitaire.



7. Incidents BGP

Retour d'expérience sur l'usurpation de préfixes

- De rares incidents en 2009 et 2010
  - Exemple : Annonce d'un préfixe plus spécifique

```
==========================================================
Possible Prefix Hijack (Code: 10)
==========================================================
Your prefix:          92.142.0.0/16:
Update time:          2010-06-03 11:15 (UTC)
Detected by #peers:   56
Detected prefix:      92.142.8.0/22
Announced by:         AS1257 (TELE2)
Upstream AS:          AS2119 (TELENOR-NEXTEL T.net)
ASpath:               2119 1257

AS 1257 is now announcing 92.142.8.0/22 which is a sub-
   prefix of 92.142.0.0/16.  92.142.0.0/16 is
   historically announced by ASes: 3215.
   Time: Thu Jun  3 05:15:44 2010 GMT
   Observed path: 812 1257
```

- Cas similaire à l'incident Youtube/Pakistan Telecom de 2008

http://www.ripe.net/internet-coordination/news/industry-developments/youtube-hijacking-a-ripe-ncc-ris-case-study

  - Malheureusement pour Youtube, l'AS 17557 annonçait un /24

- Accélération des usurpations depuis début 2011 pour l'AS 3215

7. Incidents BGP

Retour d'expérience sur l'usurpation de préfixes : historique du préfixe 2.0.0.0/12

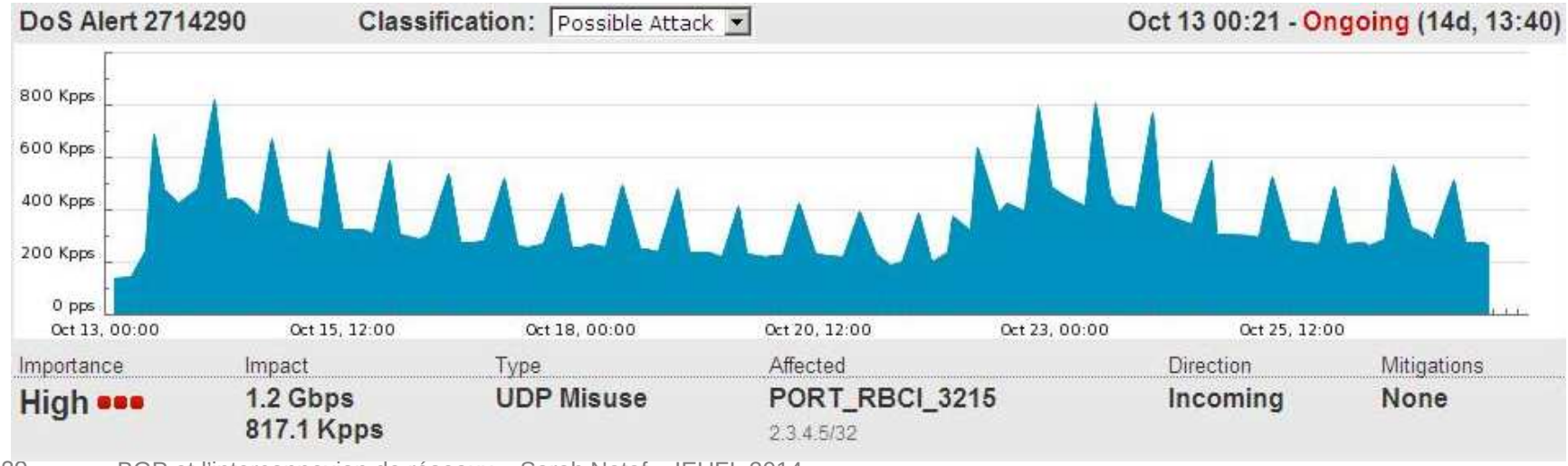
- Avant le déploiement :
  - Historique des annonces BGP

3 entries found for 2.3.0.0/16 related prefixes

This group of prefixes was last seen by RIS on **2011-02-10 10:15:16 UTC**.

Prefix	Origin AS	First seen	Last seen
2.3.0.0/16	4761	2011-01-14 12:19:09 UTC	2011-01-14 12:20:54 UTC
2.3.0.0/16	3215	2011-01-13 14:16:37 UTC	2011-02-10 10:15:16 UTC
2.3.4.0/24	6503	2011-01-20 19:52:09 UTC	2011-01-20 20:05:36 UTC

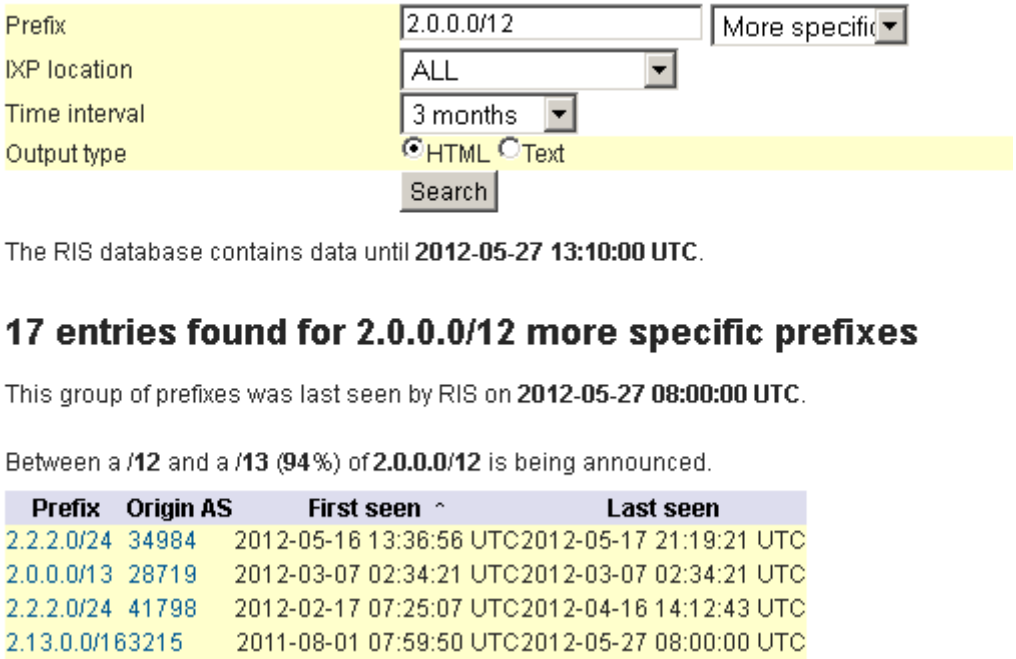
- Au déploiement des 2.2.0.0/16 et 2.3.0.0/16 :
  - Recrudescence des attaques DoS vers l'AS 3215



7. Incidents BGP

Retour d'expérience sur l'usurpation de préfixes : cas du 2.0.0.0/12

- Depuis la mise en service de ce pool, une trentaine d'occurrences d'usurpation :
  - des /30, des /24, en particulier le 2.2.2.0/24;
  - avec ou non impact sur le trafic client
- Utilisation de BGPmon pour la surveillance et les alertes
- Des initiatives pour sécuriser les annonces BGP (e.g. RPKI)



Prefix 2.0.0.0/12 More specific
IXP location ALL
Time interval 3 months
Output type HTML Text
Search

The RIS database contains data until **2012-05-27 13:10:00 UTC**.

17 entries found for 2.0.0.0/12 more specific prefixes

This group of prefixes was last seen by RIS on **2012-05-27 08:00:00 UTC**.

Between a **/12** and a **/13** (**94%**) of **2.0.0.0/12** is being announced.

Prefix	Origin AS	First seen	Last seen
2.2.2.0/24	34984	2012-05-16 13:36:56 UTC	2012-05-17 21:19:21 UTC
2.0.0.0/13	28719	2012-03-07 02:34:21 UTC	2012-03-07 02:34:21 UTC
2.2.2.0/24	41798	2012-02-17 07:25:07 UTC	2012-04-16 14:12:43 UTC
2.13.0.0/16	3215	2011-08-01 07:59:50 UTC	2012-05-27 08:00:00 UTC

En bref

- Les politiques de routage BGP traduisent les besoins de SLA et les accords économiques ; elles sont très souples. Mais l'interconnexion entre deux AS reste surtout affaire de négociations.

- BGP est un protocole éprouvé et robuste. La robustesse d'Internet repose également sur la confiance mutuelle entre opérateurs et leur coopération en cas d'incidents.
  - Ce sont les bonnes pratiques qui résolvent la plupart des incidents.
  - Le monitoring est important pour le diagnostic.

- Parmi les évolutions de BGP ou ses autres fonctionnalités, on aurait pu également citer (impossible faute de temps) :
  - les architectures RR et confédérations ;
  - les évolutions des implémentations avec corrections de bugs et les optimisations de gestion des erreurs, pour améliorer la stabilité ;
  - les formats de routes (nouvelles AFI/SAFI par exemple) pour porter de nouveaux services :
    - pour des architectures de type VPN, datacenter ;
    - Flowspec pour la diffusion de filtres et policers ;
  - les outils pour la lutte contre l'usurpation de préfixes à travers RPKI (ou d'autres mécanismes en cours de normalisation reposant sur des mécanismes cryptographiques).

Quelques pointeurs

- BGP & l'Internet :
  - blogs de BGPmon, Potaroo, Renesys
  - site de Dr Peering
  - site de Stéphane Bortzmeyer
- Outils de supervision / visualisation des préfixes ou Updates BGP :
  - Robtex, HE, RIPE-NCC, Routeviews
- Configuration et exemples :
  - les documentations de votre(vos) constructeur(s) préféré(s)
  - les tutoriels de peering lors des différents NOG (e.g. Nanog, Apricot)
  - les documentations de votre(vos) constructeur(s) préféré(s) !
  - Guide des bonnes pratiques de configuration sécurité BGP par l'ANSSI
  - les documentations de votre(vos) constructeur(s) préféré(s) !!
- Et bien sûr les RFC IETF http://tools.ietf.org/