

# Laboratoire de téléinformatique



## BGP Multihoming

Auteurs : Gilles-Etienne Vallat, Alexandre Délez

Professeur : Fabien Bruchez

Version : 1.5 05/11/2009

Groupe No : \_\_\_\_\_

Elèves : \_\_\_\_\_  
\_\_\_\_\_



heig-vd

Haute Ecole d'Ingénierie et de Gestion  
du Canton de Vaud

## ***Table des matières***

---

Table des matières .....	2
Introduction.....	2
Matériel.....	3
Structure du laboratoire et BGP en 2 mots.....	3
Présentation.....	3
Configuration (exemples de cas) .....	4
Manipulations .....	10
Préparation .....	10
Configuration de base des routeurs.....	10
1. Liens iBGP et eBGP .....	11
1.1) Etablir le lien iBGP entre ROUTER RX1 et le ROUTER RX2.....	11
1.2) Etablir le lien eBGP entre le ROUTER RX2 et le ISP2 .....	12
1.3) Etablir le lien eBGP entre le ROUTER RX1 et le ISP1 .....	12
2. Envoyez votre réseau à vos ISP.....	13
3. Configuration du « Multihoming » sans trafic de transit.....	14
4. Ajustement Avancé de votre routage BGP .....	16
4.1) Activez la fonction de reconfiguration douce.....	16
4.2) Nouvelle DMZ à injecter dans votre AS .....	16
4.3a) Restriction d'exportation de routes pour ISP2 .....	17
4.3b) Indiquez votre ISP de préférence pour un réseau .....	18
5. Redondance Interne pour le Poste Utilisateur .....	19
5.1) Passerelle redondante .....	19
5.2) Indiquez votre routeur de préférence pour certains réseaux .....	20
Règles de Notation pour le laboratoire .....	20

## ***Introduction***

---

Le but de ce travail est de mettre en évidence l'aspect architectural de BGP (eBGP, iBGP) et la situation de « multihoming ».

Le laboratoire va permettre à l'étudiant de se familiariser avec tous les aspects de BGP de manière à mieux comprendre la théorie. Ces aspects sont :

- Etablissement de « peering » eBGP et iBGP
- Pratique du mode eBGP « multi hop »
- Contrôle de table BGP et résolution de problèmes IGP
- Injection de Route BGP depuis son AS
- Configuration d'un AS « multihomed » (pas de trafic en transit)
- Filtrage de routes et ajustement des différents attributs BGP pour :
  - o Préférer un ISP pour certaines routes
  - o Indiquer aux autres AS qu'un des deux liens est meilleur
- Recherche de panne avec « debug » Cisco
- Capture des échanges de messages BGP entre les différents « peers »
- Etc ...

## **Matériel**

---

Chaque poste de travail est composé des éléments suivants :

- 2 clients Windows XP (PCX1 et PCX2) avec:
  - Un analyseur réseau Wireshark (au minimum la version 0.10.x)
  - Un serveur TFTP
  - Accès sur la machine avec : compte: **labo**, mot de passe: **labo**
- 2 routeurs CISCO (modèles 2811 et 2821)
- Un Petit HUB
- Bornier : prises vertes et prises HUB salle (prises 7 et 8)

## **Structure du laboratoire et BGP en 2 mots**

---

### **Présentation**

Le cœur du réseau Internet utilise le protocole de routage BGP pour l'échange des routes (~200'000 à l'heure actuelle) entre les AS. En effet, BGP est le seul protocole EGP (Exterior Gateway Protocol) capable de gérer efficacement ce volume d'information.

BGP est un « path vector protocol », ce qui signifie qu'il échange des chemins (suite de numéros d'AS « Autonomous System » traversées) pour sélectionner le meilleur afin qu'un routeur puisse atteindre un réseau donné. Il est extrêmement paramétrable, ce qui permet de préférer facilement un chemin.

L'échange de ces informations se fait entre deux routeurs selon un lien configuré manuellement. Ce lien doit donc exister avant le moindre échange d'information de routage. Le « peering » peut se faire avec autant de routeur que l'on souhaite. Cela peut être utile pour des questions de redondances ou de taille des chemins échangés.

Dans BGP, le fait d'établir un « peering » ne suffit pas pour échanger nos informations de routage. Il faut annoncer les réseaux que l'on veut transmettre à l'extérieur en prenant garde, dans le cas du « Multihoming », de ne pas laisser nos liens servir comme réseau de transit.

Dans le cas d'une « Stub area », BGP ne servira que si l'on veut avoir dans le futur de la redondance avec un deuxième ISP (Multihoming). En effet, si nous nous contentons d'un seul ISP, il est nettement préférable d'utiliser une route par défaut vers notre ISP.

BGP utilisant TCP pour ses échanges, il a besoin de disposer d'un IGP (« Interior Gateway Protocol ») afin de pouvoir créer un lien entre deux routeurs. Ceci peut prendre la forme d'une route statique, d'un protocole de routage comme OSPF ou d'un lien directement connecté.

Il existe deux façons de transférer ses informations : eBGP et iBGP. eBGP est utilisé sur un lien entre deux routeurs ne faisant pas partie du même AS. iBGP en revanche ne communique que dans un AS unique.

Les informations échangées dans BGP peuvent être diverses. Il échange des NLRI « Network Layer Reachability Information ». Par défaut sur des routeurs CISCO, l'échange utilise des adresses IPv4.

## Configuration (exemples de cas)

Etablissement d'un lien iBGP (soit RTA et RTB dans l'AS100):

```
RTA#  
router bgp 100  
neighbor ip_address_de_RTB remote-as 100
```

Etablissement d'un lien eBGP (soit RTA dans l'AS100, ISP dans l'AS200):

```
RTA#  
router bgp 100  
neighbor ip_address_de_ISP remote-as 200
```

Etablissement d'un lien eBGP vers une adresse d'un sous-réseau atteignable via un autre sous-réseau intermédiaire (RTA dans l'AS100, vers ISP dans l'AS200):

```
RTA#  
router bgp 100  
neighbor ip_address_de_ISP remote-as 200  
neighbor ip_address_de_ISP ebgp-multihop
```

Etablissement d'un lien eBGP (à adapter pour iBGP) à partir d'une interface spécifique de notre routeur (RTA dans l'AS100, vers ISP dans l'AS200):

```
RTA#  
router bgp 100  
neighbor ip_address_de_ISP remote-as 200  
neighbor ip_address_de_ISP update-source loopback0
```

Pour que les changements apportés à BGP soient pris en compte sur les liens actifs, nous devons réinitialiser les liens (réinitialisation à partir de RTA, connecté à ISP):

Réinitialisation d'un lien:

```
RTA#  
clear ip bgp address_de_ISP
```

Réinitialisation de tous les liens:

```
RTA#  
clear ip bgp *
```

Permettre de recalculer les changements effectués, sans perdre la connexion (réinitialisation à partir de RTA dans l'AS100, connecté à ISP dans l'AS200):

```
RTA#  
router bgp 100  
  neighbor ip_address_de_ISP remote-as 200  
  neighbor ip_address_de_ISP soft-reconfiguration inbound
```

La commande de réinitialisation à utiliser dans ce cas:

```
RTA#  
clear ip bgp ip_address_de_neighbor soft in
```

Renvoyer nos routes en appliquant les changements de configuration, sans perdre la connexion (réinitialisation à partir de RTA):  
(Activé sans besoin de configuration supplémentaire, voir ci-dessus.)

```
RTA#  
clear ip bgp ip_address_de_neighbor soft out
```

Désactiver la synchronisation entre BGP et votre IGP afin que BGP n'attende pas sur l'IGP avant d'injecter ses routes dans la RIB:

```
RTA#  
router bgp 100  
  no synchronization
```

Désactiver l'agrégation automatique à la classe d'adresse des routes injectée dans BGP:

```
RTA#  
router bgp 100  
  no auto-summary
```

Annoncer manuellement un réseau par BGP (de RTA dans l'AS100), l'origine sera IGP (attention la route précise correspondante doit exister):

```
RTA#  
router bgp 100  
  network numéro_du_réseau [mask masque]
```

Annoncer les réseaux provenant des routes statiques dans OSPF (de RTA):

```
RTA#  
router ospf 1  
  redistribute static subnets
```

En iBGP, l'attribut next hop est préservé. Pour qu'une route BGP apprise par iBGP figure dans la table de routage, le next hop doit être atteignable (ce qui signifie : être présent dans la table RIB de tous les routeurs iBGP).

Préférer un neighbor pour accéder aux réseaux de l'AS200 (de RTA dans l'AS100):  
(méthode utilisant des "route-map" et sa clause "Match")

```
RTA#
router bgp 100
  neighbor ip_address_de_neighbor route-map MYR in

route-map MYR permit 10
  match as-path 1
  set local-preference 120
route-map MYR permit 20
  ! Cette ligne est nécessaire pour accepter les autres routes

ip as-path access-list 1 permit _200$
```

N'autoriser l'annonce que d'une liste de réseaux (160.1.0.0/16 de RTA dans l'AS100):  
(méthode utilisant des "route-map" et sa clause "Match")

```
RTA#
router bgp 100
  neighbor ip_address_de_neighbor route-map MYR out

route-map MYR permit 10
  match ip address myNetwork
route-map MYR deny 20

ip access-list standard myNetwork
  permit 160.1.0.0 0.0.255.255
  deny any
```

N'autoriser l'annonce que d'une liste de réseaux (160.1.0.0/16 de RTA dans l'AS100):  
(méthode utilisant des "distribute-list")

```
RTA#
router bgp 100
  neighbor ip_address_de_neighbor distribute-list 1 out

access-list 1 permit 160.1.0.0 0.0.255.255
access-list 1 deny any
```

N'autoriser l'annonce que des réseaux d'un AS donné (le nôtre) (de RTA dans l'AS100):  
(méthode utilisant des "filter-list")

```
RTA#  
router bgp 100  
  neighbor ip_address_de_neighbor filter-list 1 out  
  
ip as-path access-list 1 permit ^$
```

Le dernier argument est une expression régulière:

Le "." correspond à un seul caractère.

Le "^" correspond au début de la chaîne.

Le "\$" correspond à la fin de la chaîne.

Le "\_" correspond au début ou à la fin de la chaîne, à ",", à "{", à "}" ou à un espace.

Le "\*" correspond à 0 ou plus de caractère (ou expression) le précédant.

Le "+" correspond à 1 ou plus de caractère (ou expression) le précédant.

La chaîne "[acb]" correspond soit "a", "b" ou "c".

Par exemple:

<b>a+</b>	correspondra à au moins un caractère "a".
<b>^\$</b>	correspondra à une origine de l'AS locale.
<b>^100_.*</b>	correspondra à une transmission provenant de l'AS 100.
<b>_100\$</b>	correspondra à une origine de l'AS 100.

Modification d'attributs comme l'AS\_PATH, la community et la LOCAL\_PREF:  
(méthode utilisant des "route-map" et sa clause "set")

```
RTA#  
router bgp 100  
  neighbor ip_address_de_neighbor route-map THINROUTE out  
  
route-map THINROUTE  
  set as-path prepend 100 100 100  
  set community no-export  
  set local-preference 80
```

(Etant donné qu'il n'y a pas de clause "Match", toutes les routes exportées seront modifiées)

Pour exporter les community d'une route BGP vers son voisin:

```
RTA#  
router bgp 100  
  neighbor ip_address_de_neighbor send-community
```

Pour consulter l'état des liens BGP (soit RTA):

```
RTA#  
show ip bgp neighbors  
show ip bgp summary
```

Pour contrôler les routes reçues et envoyées:

Pour les routes réellement reçues:

(Attention: le soft-reconfiguration doit avoir été activé pour ce neighbor!!!)

```
show ip bgp neighbors x.x.x.x received-routes
```

Pour les routes réellement envoyées:

```
show ip bgp neighbors x.x.x.x advertised-routes
```

Commandes debug pour voir les routes échangées ainsi que l'ajout ou le retrait de la table de routage:

```
RTA#  
debug ip routing  
debug ip bgp update
```

Pour voir les messages debug à partir d'un terminal connecté en telnet:

```
RTA#  
terminal monitor
```

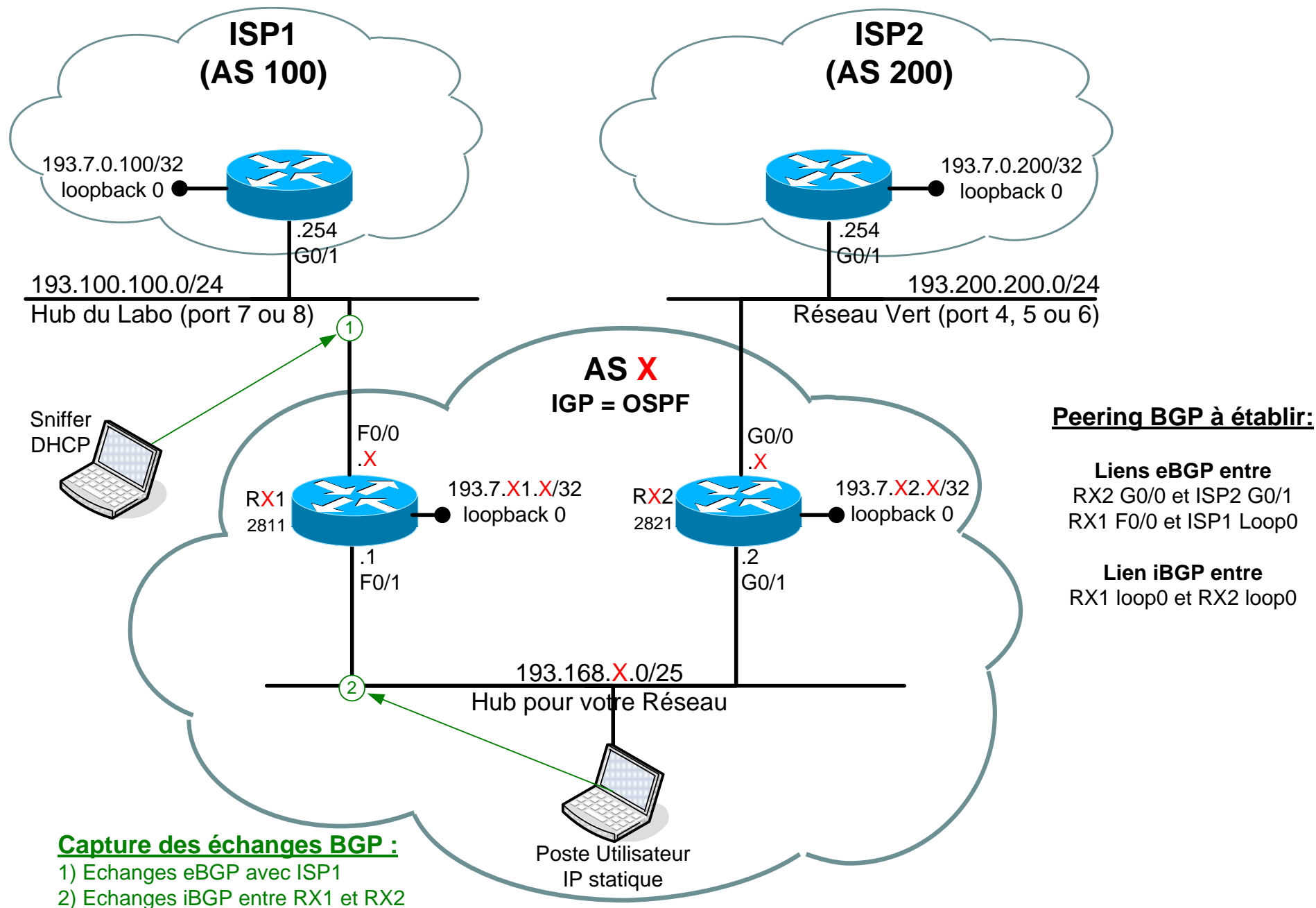
Pour désactiver toutes les commandes debug (éviter de gaspiller des ressources):

```
RTA#  
undebug all
```

Pour activer HSRP (Hot Standby Routing Protocol):

```
RTA#  
interface ???Ethernet0/1  
  standby ip adresse_IP_virtuelle  
  standby priority valeur  
  ! La valeur par défaut est de 100  
  standby preempt
```





# Manipulations

---

## Préparation

Branchez vos deux routeurs comme décrit sur le schéma ci-dessus.

Branchez aussi les deux stations comme illustré sur le schéma. La station « sniffer » est capable d'aller sur Internet à tout moment (documentation Cisco ou autre). Par contre la station « poste utilisateur » ne sera capable d'aller sur Internet qu'à l'issue d'une configuration BGP multihoming correcte pour votre réseau (durant la question 3).

Partout où figure la lettre « X » dans ce document, elle devra être remplacée par votre numéro de groupe durant toute la réalisation.

## Configuration de base des routeurs

- a) Effacez la configuration actuelle du routeur et redémarrez avec les commandes :  
`erase nvram:`, puis `reload`
- b) Abandonnez le « wizard » de configuration (répondre « no » à la question posée)
- c) Modifiez puis importez les configurations suivantes dans chacun des deux routeurs  
RX1 - 2811    cisco2811-base.cfg  
RX2 - 2821    cisco2821-base.cfg

Dans ces fichiers, il faut remplacer la chaîne « !!!X!!! » par le numéro de votre groupe. Vous pourrez ensuite coller le contenu de vos configurations modifiées à la console de chacun des deux routeurs (<configure terminal> puis cut&paste). Le mot de passe d'accès ainsi que le mot de passe « enable » sont préconfigurés à la valeur « cisco ». Merci de ne pas changer cela.

Pour différencier les deux routeurs sans chercher trop longtemps l'étiquette où est noté le modèle, vous pouvez vous rappeler que le routeur 2821 (2RU) est plus haut que le 2811 (1RU). « RU » veut dire « Rack Unit » qui a une hauteur standardisée pour les racks informatiques, qui vaut environ 4.5cm.

Contrôlez la connectivité sur toutes les interfaces à l'aide de pings.

RX1 (193.168.X.1) à RX2 (193.168.X.2) via votre petit hub

RX1 vers ISP1 (193.100.100.254)

RX2 vers ISP2 (193.200.200.254)

Contrôlez que l'OSPF préconfiguré pour vous soit établi et fonctionnel entre les deux routeurs. Il n'y a pas de raison de changer la configuration OSPF actuelle, sauf peut-être pour y redistribuer des routes nécessaires à BGP.

`show ip ospf neighbor`

`show ip route ospf`

Note pour la rédaction du rapport de laboratoire :

Pour illustrer votre rapport de laboratoire, et quand cela vous est demandé, vous fournirez toujours les commandes de configuration ajoutées sur chaque routeur ainsi qu'une capture « Sniffer » et/ou un résultat de « debug » routeur.

- a) Les **commandes** doivent être représentées dans leur contexte et **en un bloc**
- b) Les **captures** devront bien être présentées et **pertinentes** (attention à filtrer vos captures intelligemment pour éviter la pollution de vos traces pas vos voisins).
- c) Le nombre ainsi que le type de « **debug** » routeur seront soigneusement sélectionnés et les points importants seront **mis en évidence** dans le rapport.
- d) Dans le contexte de la question, **choisissez qui** de la capture ou du « debug » va le mieux **illustrer votre explication** à la rédaction du rapport.

Lisez toujours l'intégralité de la question avant de faire les manipulations demandées. Ceci vous évitera de devoir recommencer parce qu'il vous manque une capture ou un debug..

Si vous avez manqué une capture ou un debug il est très souvent possible de supprimer votre configuration en ajoutant « **no** » devant chaque commande (Attention il y a des exceptions à cette règle – faites donc des sauvegardes régulières de votre configuration).

## 1. Liens iBGP et eBGP

### 1.1) Etablir le lien iBGP entre ROUTER RX1 et le ROUTER RX2

Utilisez la Loopback0 de RX1 et de RX2 pour établir ce lien.

Note: pour s'assurer que ce lien s'établisse correctement, vous pouvez valider que ces deux loopback peuvent se pinguer l'une et l'autre. Ce ping n'est possible qu'en mode Enable.

```
ping ip_distante source loopback0
```

Contrôlez que ce lien iBGP soit établi à l'aide de la commande

```
show ip bgp summary
```

ou pour plus de détails

```
show ip bgp neighbor
```

Pour obtenir plus de détails sur ce que font vos routeurs pour cet exercice vous activerez :

- a) Les « debug » Cisco suivants sur le routeur RX2
- b) Des captures sur le poste de travail adéquat, soit celui des deux qui va voir passer le trafic pour cette session iBGP

Informations détaillées sur l'état des sessions TCP établies par le routeur

```
debug ip tcp transactions
```

Informations détaillées sur la machine d'état pour l'établissement du « peering » BGP

```
debug ip bgp event
```

```
debug ip bgp
```

Rapport : démontrer que votre lien iBGP est établi entre vos deux routeurs.

### 1.2) Etablir le lien eBGP entre le ROUTER RX2 et le ISP2

Il s'agit d'un lien eBGP tout à fait classique établi entre des routeurs directement connectés.

Contrôlez que ce lien eBGP soit établi à l'aide des mêmes commandes que ci-dessus. Dès que ce lien est actif vous devez commencer à recevoir des routes BGP en provenance des routeurs en amont. Pour que celles-ci peuplent votre table de routage il faut respecter les règles concernant la synchronisation (à désactiver).

Pour consulter votre table des routes BGP vous pouvez simplement utiliser la commande suivante. Il est possible d'obtenir plus de détails pour une route en ajoutant celle-ci à la suite.

```
show ip bgp
show ip bgp 193.5.1.0 255.255.255.0
```

### 1.3) Etablir le lien eBGP entre le ROUTER RX1 et le ISP1

Pour cette partie vous devrez établir ce lien eBGP entre votre interface Ethernet et l'interface Loopback0 du router ISP1. Attention il s'agit d'une configuration eBGP multi hop.

Pour s'assurer que ce lien s'établisse correctement, vous pouvez valider que votre routeur est capable de pinguer la loopback du routeur ISP1.

```
ping 193.7.0.100
```

Si ce n'est pas le cas il faudra songer à ajouter une route statique pour joindre cette adresse.

```
ip route ip_no_directly_connected 255.255.255.255 next_hop
```

Contrôlez que ce lien eBGP soit établi à l'aide des mêmes commandes que ci-dessus. Dès que ce lien est actif vous devez commencer à recevoir des routes BGP supplémentaires en provenance des routeurs en amont.

Note: Les routes BGP apprises par votre routeur seront normalement transmises en iBGP au routeur RX2. Mais il se peut que celui-ci ne les prenne pas en compte si le « NEXT\_HOP » de cette route n'est pas présent dans sa table de routage. Ceci peut être aisément solutionné en redistribuant la route statique ajoutée sur RX1 dans votre IGP (OSPF). Un exemple pourrait être :

```
router ospf X
 redistribute static subnets
```

Etapez ces contrôles dans votre rapport (capture Wireshark sur le « Sniffer DHCP » PC, debug Cisco sur RX1, show commandes sur tous les routeurs). Reportez l'état de vos tables de routage BGP + RIB sur RX1 et RX2 et faites part de vos remarques.

Pour consulter votre table de routage (RIB), vous pouvez simplement utiliser la commande suivante. Il est donc possible de savoir si BGP a inséré ses routes dans la table RIB par comparaison de cette table avec celle de BGP. Comparez:

```
show ip route
show ip route bgp
```

avec: `show ip bgp`

En fonction des routes BGP reçues dans vos routeurs à l'issue de cet exercice, vous devez pouvoir établir une carte des liaisons entre les différentes AS présentes. Etablissez ce dessin seulement en fonction de ce que vous retirez de vos tables BGP (notez que cette information peut être incomplète – mais il s'agit de la vision depuis votre AS des chemins à la lecture des AS\_PATH). Votre schéma doit comprendre le numéro d'AS et le/les subnets concernés.

## 2. Envoyez votre réseau à vos ISP

Importez votre réseau 193.168.X.0/25 ainsi que les deux DMZ (193.168.X.128/26, 193.168.X.192/26) qui se trouvent sur chaque routeur dans BGP. Vos réseaux doivent être **agregés en une seule route** et de plus être visibles avec un attribut « origine » valant « IGP ». Votre routeur BGP devra être configuré pour ne pas faire d'agrégation automatique sur la classe d'adresse.

Note: une route BGP importée avec la commande <network> prendra automatiquement une valeur « IGP » pour l'attribut ORIGINE. Attention: sans agrégation automatique (<no auto-summary>), il faudra dans votre table de routage une route parfaitement identique à celle que vous pensez envoyer à vos voisins (la route agrégée). Ceci peut être sans problème fait avec la méthode classique BGP, qui consiste à créer une route pointant sur l'interface <null0>.

```
ip route votre_segment_agregé 255.255.255.0 Null0
```

Attention: si un problème survient sur l'un des deux routeurs, votre communication ne doit pas être coupée avec votre ISP restant. Donc il sera important de générer et envoyer cette route sur chacun des deux routeurs.

Pour obtenir plus de détails sur les routes BGP échangées entre vos routeur et celle déposée dans la table de routage vous pouvez, *avant de procéder à la configuration*, activer les « debug » Cisco suivants sur RX1 et RX2 et capturer le trafic BGP sur vos deux sniffers.

Informations détaillées sur les routes BGP échangées

```
debug ip bgp updates
```

Informations détaillées sur les routes ajoutées ou retirée de la table de routage

```
debug ip routing
```

Contrôlez que votre réseau est présent dans les table BGP et les tables de routage de chacun des 5 routeurs de notre Backbone Internet.

Ces « Looking Glass Server » sont accessibles en telnet

Le mot de passe d'accès est « cisco »

Les commandes <show ip ...> sont acceptées.

AS500	193.5.1.1
AS400	193.4.1.1
AS300	193.3.1.1
AS200	193.2.1.1
AS100	193.1.1.1

A partir du moment où votre route est envoyée vers le reste du réseau, il vous sera possible de communiquer avec l'entier des routeurs de notre réseau, plus le réseau de l'école et le vrai Internet. Dès cet instant vous pourrez donc accéder à n'importe quel routeur ou Internet

depuis votre station appelée « poste utilisateur ». Attention: la communication entre les réseaux de différents groupes n'est pas possible depuis ce poste.

Pour cela, vous devez avoir spécifié une passerelle sur votre poste "utilisateur".

Note: l'accès au vrai Internet ne peut se faire que si vous avez renseigné un serveur DNS comme par exemple 10.192.48.101 et/ou 10.192.48.100.

Etapez ces contrôles dans votre rapport (capture Wireshark, debug Cisco, show commandes). Reportez l'état de vos tables de routage BGP + RIB sur RX1, RX2 ainsi que le « Looking Glass » de l'AS500. Faites part de vos remarques.

### 3. Configuration du « Multihoming » sans trafic de transit

Configurez vos routeurs de telle manière qu'ils reçoivent les routes des deux ISP mais qu'ils ne retransmettent pas celles reçues d'un ISP vers l'autre. Nous ne voulons pas de trafic de transit dans notre AS avec une configuration de type « Multihoming ».

Note: la méthode la plus simple pour filtrer les routes venant d'autre AS que la vôtre peut se baser sur l'attribut AS\_PATH. Nous pouvons, avec un filtre basé sur une expression régulière très simple, autoriser seulement nos routes à être envoyées à chaque ISP. Dans votre AS, vos routes contiennent un attribut AS\_PATH qui est vide (expression régulière « ^\$ » à utiliser dans votre liste d'accès d'AS\_PATH). Ce filtre devra être appliqué (<filter-list>) sur chaque ISP, donc sur les voisins eBGP de vos deux routeurs.

Contrôlez que cette configuration soit appliquée et valide. Pour ce faire contrôlez que vous ne propagez que vos routes en direction de vos voisins eBGP avec la commande :

```
show ip bgp neighbor ip_du_voisin advertised-routes
```

De la même manière vous pouvez aussi contrôler qu'aucun des deux ISP ne reçoit d'autres routes que celles que vous avez décidé de propager. La commande à entrer sur le voisin eBGP serait :

```
show ip bgp neighbor ip_du_voisin received-routes
```

N'oubliez pas que tout changement de configuration BGP pour le filtrage ou la modification d'attributs de routes nécessite un redémarrage de la session avec le voisin en question (<clear ip bgp ip\_du\_voisin >).

Attention: assurez-vous que le routeur de l'AS 500 (193.5.1.1) reçoive toujours vos routes après ce changement.

Etapez ces contrôles dans votre rapport (capture Wireshark, debug Cisco, show commandes) de manière à montrer l'état avant et après le changement. Reportez donc l'état des tables de routage BGP ainsi que les préfixes propagés ou reçus sur tous les routeurs suivants : RX1, RX2, ISP1, ISP2 et AS500. Faites ensuite part de vos remarques.

**--- FIN DE LA PREMIÈRE PARTIE ---**  
**La suite du laboratoire est pour la deuxième semaine**



## 4. Ajustement Avancé de votre routage BGP

### 4.1) Activez la fonction de reconfiguration douce

Vous ne voulez pas avoir à ré-établir complètement le lien avec votre voisin chaque fois que vous changez votre configuration BGP. Un « reset » de cette session va couper complètement la communication avec votre voisin, toutes les routes seront perdues et devront être réappries. Ceci n'est pas acceptable dans un environnement de production. Activez ce qu'il faut pour ne plus avoir à le faire et profitez d'un réapprentissage de vos routes en douceurs (« soft reconfiguration » en anglais).

Vous pourrez documenter et valider si cette fonction marche bien dans les questions suivantes. Etayez ce contrôle dans votre rapport (capture Wireshark si possible, debug Cisco, show commandes) de manière à comparer un « reset » brutal versus un « reset » avec reconfiguration en douceur.

### 4.2) Nouvelle DMZ à injecter dans votre AS

Ajoutez une nouvelle DMZ indépendante sur chaque routeur de votre AS. Utilisez l'interface « loopback 2 » pour cela. Faites en sorte que ces deux nouveaux réseaux fassent partie des « updates » qui seront envoyés à tous vos voisins eBGP et iBGP.

```
RX1  193.168.100+X.X/24  
RX2  193.168.200+X.X/24
```

Note: Inspirez-vous de ce qui a déjà été fait à la question 2. Ici il ne sera pas nécessaire d'opérer d'agrégation pour ce réseau. Seulement le routeur qui aura la DMZ sera chargé d'injecter son réseau dans BGP.

Contrôlez que ces nouvelles DMZ sont présentes dans les tables BGP et les tables de routage de chacun des 5 routeurs de notre Backbone Internet.

Etayez ces contrôles dans votre rapport (capture Wireshark si possible, debug Cisco, show commandes). Reportez l'état de vos tables de routage BGP + RIB et faites part de vos remarques.



#### 4.3a) Restriction d'exportation de routes pour ISP2

Vous voulez que votre réseau 193.168.200+X.0/24 soit envoyé à ISP2, mais que celui-ci ne soit pas autorisé à exporter cette route hors de son AS (soit AS200).

Note: Si vous décidez de modifier l'attribut « community », assurez-vous toujours que vous le transmettez à votre voisin eBPG (<send-community>). Le seul moyen de modifier un attribut pour une route spécifique est l'application d'un « route-map » sur le voisin en question. Les étapes de cette tâche seront:

- i. création d'une <access-list> pour ne sélectionner que le réseau 193.168.200+X.0/24
- ii. création d'un <route-map permit> en tête de liste de traitement
- iii. utilisez l'<access-list> créé pour sélectionner les routes à modifier (match ip add)
- iv. indiquez l'attribut que vous désirez changer avec sa valeur (<set community ...>)
- v. finalement appliquez ce <route-map> sur les routes que vous envoyez à ISP2

Note: Par défaut en fin de traitement un <route-map> bloque toutes les routes qui n'ont pas trouvé une correspondance. N'oubliez donc pas d'ajouter un <route-map permit> en queue de liste de traitement pour autoriser vos autres routes à être transmises. Un <route-map> sans clause <match> va sélectionner toutes les routes restantes et s'il n'y a pas de clause <set> elles seront transmises sans changement.

Contrôlez que votre réseau est toujours présent dans les tables BGP et les tables de routage de chacun des 5 routeurs de notre Backbone Internet. De plus, contrôlez aussi que les routeurs de l'AS 200 n'ont pas exporté ce réseau hors de l'AS (la route en question doit comporter la bonne « community » dans l'AS200).

Etapez ces contrôles dans votre rapport (capture Wireshark si possible, debug Cisco, show commandes). Reportez l'état des tables de routage BGP avant et après qui vous permettent de prouver ceci.

#### 4.3b) Indiquez votre ISP de préférence pour un réseau

Vous voulez que tous les utilisateurs se trouvant dans les autres AS (AS200 comprise) préfèrent joindre votre réseau 193.168.100+X.0/24 au travers de l'ISP1. L'ISP2 devra être utilisé seulement en cas de problème avec l'ISP1.

Note: Le premier attribut qui circule d'AS en AS pris en compte pour le choix de la meilleure route est la longueur de l'AS\_PATH. Une AS peut intégrer plusieurs fois son numéro d'AS dans un AS\_PATH. Cette technique s'appelle l'AS-PATH « prepending ». En ajoutant le bon nombre de fois votre numéro d'AS avec la route 193.168.100+X.0/24 en direction de ISP2, vous obtiendrez ce résultat.

Le seul moyen de modifier un attribut pour une route spécifique est l'application d'un « route-map » sur le voisin en question. Les étapes de cette tâche seront:

- i. création d'une <access-list> pour ne sélectionner que le réseau 193.168.100+X.0/24
- ii. création d'un <route-map permit> en tête de liste de traitement
- iii. utilisez l'<access-list> créé pour sélectionner les routes à modifier (match ip add)
- iv. indiquez l'attribut que vous désirez changer avec sa valeur (set as-path prepend)
- v. finalement appliquez ce <route-map> sur les routes que vous envoyez à ISP2

Note: Par défaut en fin de traitement un <route-map> bloque toutes les routes qui n'ont pas trouvé une correspondance. N'oubliez donc pas d'ajouter un <route-map permit> en queue de liste de traitement pour autoriser vos autres routes à être transmises. Un <route-map> sans clause <match> va sélectionner toutes les routes restantes et s'il n'y a pas de clause <set> elles seront transmises sans changement.

L'objectif étant que votre AS\_PATH sur ISP2 soit plus long que celui via ISP1 sur ce même routeur. La meilleure route pour 193.168.100+X.0/24 sur ISP2 sera donc celle via ISP1 et non celle via votre AS directement connectée.

Contrôlez que votre réseau est toujours présent dans les tables BGP et les tables de routage de chacun des 5 routeurs de notre Backbone Internet. De plus, contrôlez aussi que tous ces routeurs préfèrent la route au travers de l'ISP1 (ISP2 doit voir une deuxième route moins bonne).

Etapez ces contrôles dans votre rapport (capture Wireshark si possible, debug Cisco, show commandes). Reportez l'état des tables de routage BGP qui vous permettent de prouver ceci.

## 5. Redondance Interne pour le Poste Utilisateur

### 5.1) Passerelle redondante

Configurez vos deux routeurs de telle manière que, si l'un d'eux dysfonctionne, votre station (Poste Utilisateur) puisse continuer à accéder à Internet. Utilisez l'IP 193.168.X.126 pour l'adresse de votre passerelle redondante. Si les deux routeurs sont présents le routeur RX2 devra être la passerelle active de votre station.

Une passerelle redondante peut être configurée avec le protocole Cisco HSRP (réf. slide 293 du cours). HSRP doit être configuré sur les interfaces internes des deux routeurs. La première tâche consiste à définir l'adresse IP virtuelle de la manière suivante:

```
interface xxx_Ethernet0/1
standby ip adresse_ip_virtuelle
```

La deuxième tâche consiste à définir lequel des deux routeurs sera le routeur actif avec cette adresse IP virtuelle. Par défaut chaque routeur HSRP a une priorité de 100, le routeur qui aura la plus grande priorité (max 255) deviendra le routeur HSRP actif. Pour forcer le retour immédiat sur le routeur actif de l'adresse virtuelle, il faut activer la préemption. La configuration sur le routeur actif par défaut peut ressembler à celle-ci:

```
standby priority valeur
standby preempt
```

Pour obtenir plus de détails sur ce qui se passe au niveau de HSRP vous pouvez activer des « debug » ou la commande « show » suivante:

```
show standby [brief]
debug standby
debug standby events
```

Contrôlez que votre station (Poste Utilisateur) est capable d'accéder au réseau de l'école et/ou Internet en utilisant 193.168.X.126 comme passerelle par défaut. Si le routeur RX2 est éteint, après quelques secondes, votre communication avec Internet doit toujours être possible. **Attention à sauver votre configuration avant d'éteindre votre routeur.**

Etapez ces contrôles dans votre rapport (capture Wireshark si possible, debug Cisco, show commandes). Un ping continu sur un DNS de l'école permet de constater très simplement si cela fonctionne.

## 5.2) Indiquez votre routeur de préférence pour certains réseaux

Configurez votre routeur RX1 pour que votre station (Poste Utilisateur) accède aux réseaux de l'AS500 de préférence via lui-même. RX2 devrait être utilisé seulement si RX1 dysfonctionne.

Note: l'attribut LOCAL\_PREF permet de donner sa préférence pour une route entre des voisins iBGP (soit dans votre AS). Plus haute sera la préférence, plus cette route aura de chance de devenir la meilleure. Il est intéressant de rappeler que la valeur par défaut est de 100, donc une valeur plus grande pour les routes de l'AS500 serait souhaitée.

Le seul moyen de modifier un attribut pour une route spécifique est l'application d'un « route-map » sur le voisin en question. Les étapes de cette tâche seront:

- i. création d'une <as-path access-list> pour ne sélectionner que les réseaux qui viennent de l'AS500 (expression régulière « \_500\$ »)
- ii. création d'un <route-map permit> en tête de liste de traitement
- iii. utilisez l'<as-path access-list> créé pour sélectionner les routes à modifier (match as-path)
- iv. indiquez l'attribut que vous désirez changer avec sa valeur (set local-preference)
- v. finalement appliquez ce <route-map> sur les routes que vous recevez d'ISP1

Note: Par défaut en fin de traitement un <route-map> bloque toutes les routes qui n'ont pas trouvé une correspondance. N'oubliez donc pas d'ajouter un <route-map permit> en queue de liste de traitement pour autoriser vos autres routes à être transmises. Un <route-map> sans clause <match> va sélectionner toutes les routes restantes et s'il n'y a pas de clause <set> elles seront transmises sans changement.

Contrôlez le chemin qu'emprunte votre station (Poste Utilisateur) pour accéder aux réseaux de l'AS500. Assurez-vous qu'après votre changement le trafic passe bien par les routeurs et AS suivants:

RX2(ASX) → RX1(ASX) → 193.100.100.254(AS100)  
→ 193.6.6.4(AS400) → 193.6.6.5(AS500)

Etapez ces contrôles dans votre rapport (capture Wireshark si possible, debug Cisco, show commandes). Un « traceroute 193.5.1.1 » avant et après le changement permet de constater simplement si cela fonctionne.

## **Règles de Notation pour le laboratoire**

1/3 de la note	Points accordés à chaque question pour la partie fonctionnelle
1/3 de la note	Pertinence des résultats présentés
1/3 de la note	Contenu rédactionnel et qualité du rapport