Laboratoire de téléinformatique

BGP Introduction

Auteurs : Kenza Majbar, Alexandre Délez

Professeur : Fabien Bruchez

Version : 1.1 11/03/2009

Groupe No : _____

Elèves : _____

_____

heig-vd
Haute Ecole d'Ingénierie et de Gestion du Canton de Vaud

Table des matières

Introduction

Le but de ce travail est de bien assoir ses connaissances sur les manipulations avancées avec des routeurs, ceci avec un exercice de peering BGP simple.

Le laboratoire va permettre à l'étudiant de parfaire sa pratique de la configuration et du debug de routeurs Cisco ainsi que la capture « chirurgicale » avec un sniffer. Tout cela en se familiarisant avec les bases de BGP en illustration de la théorie. Les aspects abordés sont :

- Câblage de l'infrastructure et contrôle de fonctionnement
- Gestion des routeurs en Telnet et console
- Capture Sniffer avec filtres précis sur la communication à épier
- Activation du mode « debug » pour certaine fonctions du routeur
- Mise en service d'un lien eBGP et réceptions des routes
- Emission d'une route BGP depuis son AS vers son partenaire
- Contrôle de fonctionnement puis capture des échanges de messages BGP entre les différents « peers », ceci illustré avec une trace et un debug pour chaque opération

Matériel

Chaque poste de travail est composé des éléments suivants :

- 2 clients Windows XP (PCX1 et PCX2) avec:
  - Un analyseur réseau Ethereal/Wireshark (au minimum la version 0.10.x)
  - Un serveur TFTP (Pumpkin ou TFTP32)
  - 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 (près de 300'000 préfixes au 1er janvier 2009) 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.

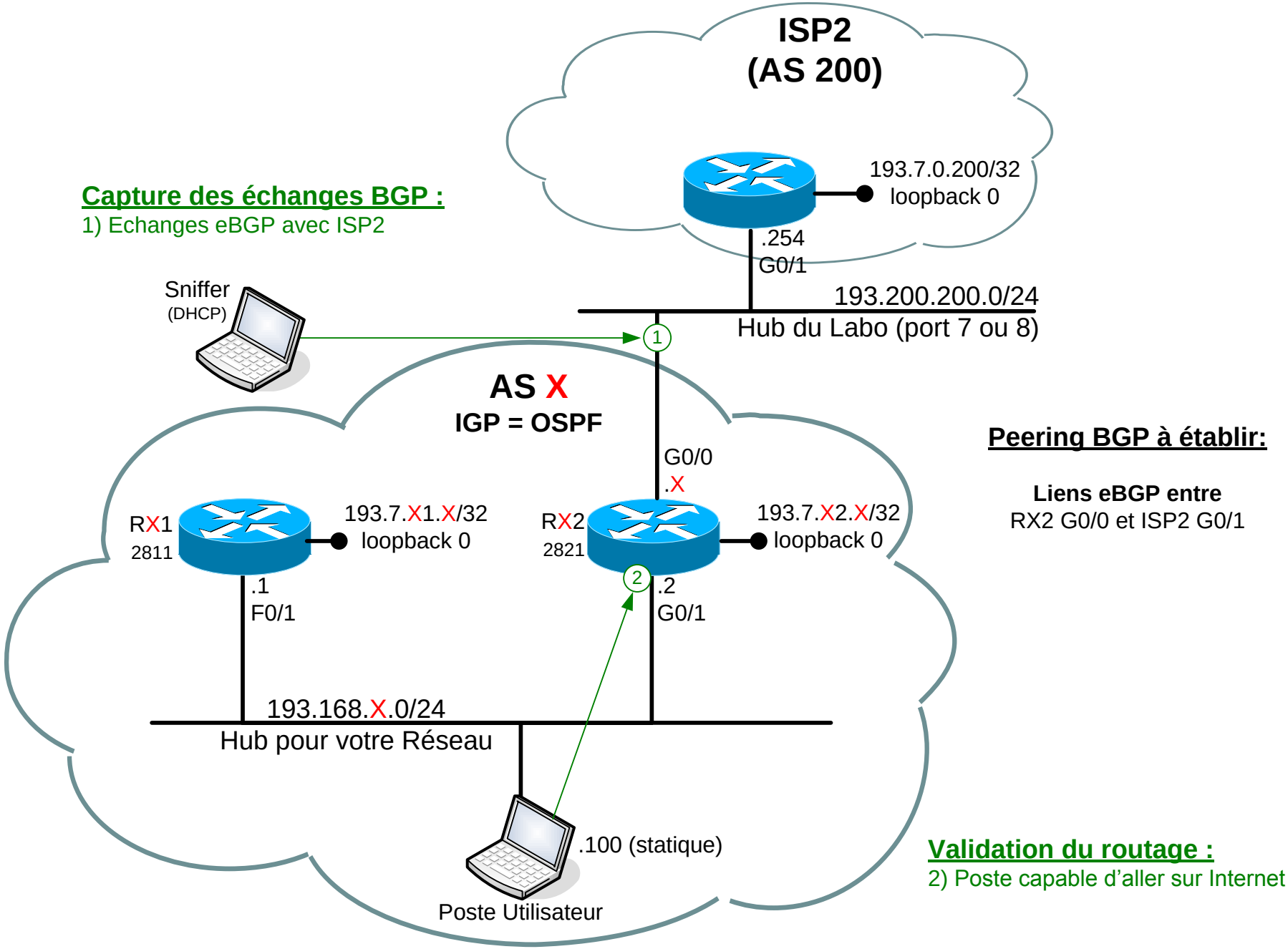
Dans BGP, le fait d'établir un « peering » ne suffit pas pour échanger nos informations de routage. Il faut annoncer les réseaux que l'on veut transmettre à l'extérieur en prenant garde, dans le cas du « Multihoming », de ne pas laisser nos liens servir comme réseau de transit.

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 Gatway 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 (family).



Capture des échanges BGP :

1) Echanges eBGP avec ISP2

Peering BGP à établir:

Liens eBGP entre
RX2 G0/0 et ISP2 G0/1

Validation du routage :

2) Poste capable d'aller sur Internet

Manipulations

Préparation

Les fichiers nécessaires à ce laboratoire se trouvent sur :

"\\Eint20\Profs\FBZ\Cours ADN\Lab Intro"

Branchez vos deux routeurs comme décrit sur le schéma ci-dessus. Pensez-aussi à les allumer avant de démarrer votre laboratoire.

Branchez aussi les deux stations comme illustré sur le schéma. La station « sniffer » en DHCP est capable d'aller sur Internet à tout moment (documentation Cisco ou autre). Par contre la station « poste utilisateur » avec un **IP statique** ne sera capable d'aller sur Internet qu'à l'issue d'une configuration BGP correcte pour votre réseau (durant la question 4).

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

1. Configuration de base des routeurs

Objectifs : Monter l'infrastructure et opérer les contrôles de fonctionnement
Connexion de la console (9600-8-N-1, no flow control)
Remise à zéro de la configuration du routeur (**<erase nvram:>**)
Charger le modèle initial de configuration
Etat des interfaces (**<show interface>**)
Connectivité (**<ping>**, **<show arp>**)
Contrôle Routage (OSPF)

a) Connectez les deux consoles sur le poste appelé « sniffer » sur le schéma

Assurez-vous que les deux consoles HyperTerminal sont configurées comme suit :

Port :	COM1 respectivement COM2
Baud rate :	9600
Data bits :	8
Parity :	None
Stop bit :	1
Flow control :	None

b) Effacez la configuration actuelle du routeur et redémarrez avec les commandes :
`router>` **`enable`**
`router#` **`erase nvram:`** puis `router#` **`reload`**

c) Abandonnez le « wizard » de configuration (répondre **<no>** à la question posée)

d) 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 (entrez en mode configuration avec **<configure terminal>** puis copier/coller). Validez qu'aucune commande ne soit rejetée par le routeur.

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 une hauteur standardisée pour les racks informatiques, qui vaut environ 4.5cm.

A tout moment il vous est possible de sauvegarder la configuration de vos routeurs. Cette opération devra être au minimum réalisée à la fin de chaque journée de laboratoire, ceci de manière à pouvoir poursuive la semaine suivante le travail en cours. Pour ce faire procédez comme suit :

- Configurez le routeur pour ne pas s'arrêter après chaque page d'affichage avec la commande **<terminal length 0>** (le défaut est 24).
- Depuis HyperTerminal activez la sauvegarde dans un fichier de tout le contenu de votre console (menu transfer → capture text).
- Au Shell privilégié (symbole #) entrer la commande suivant pour afficher la configuration : **<show running>**
- Stoppez l'enregistrement et placez cette configuration en lieu sûr. Elle pourra être rechargée très simplement avec la fonction « Transfer → Receive File… » d'HyperTerminal.

e) Contrôlez l'état de toutes vos interfaces

Pour contrôler l'état de vos interfaces les commandes suivantes sont utiles:

```
RX2# show ip interface brief
RX2# show interface <interface-name>
RX2# show ip interface <interface-name>
```

Examples:

```
RX2# show ip interface brief
Interface                  IP-Address      OK? Method Status  Protocol
GigabitEthernet0/0         193.200.200.X   YES NVRAM  up      up
GigabitEthernet0/1         193.168.x.2     YES NVRAM  up      up
Loopback0                  193.7.X2.X      YES NVRAM  up      up
```

Un « status » différent de **<up>** indique très souvent que l'interface n'est pas active

Un « protocol » différent de **<up>** indique la plupart du temps que l'interface n'est pas connectée correctement (en tout cas pour Ethernet).

f) Contrôlez la connectivité sur toutes les interfaces à l'aide de la commande **<ping>**.

Pour contrôler la connectivité les commandes suivantes sont utiles:

```
RX2# ping <ip-address>
RX2# show arp (utile si un firewall est actif)
```

Examples:

```
RX2# ping 193.68.X.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 193.68.X.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
```

Pour votre topologie il est utile de contrôler la connectivité entre :

RX2 (193.68.X.2) et RX1 (193.68.X.1) via votre petit hub

RX2 (193.68.X.2) et votre poste « utilisateur »

RX2 vers ISP2 (193.200.200.254)

RX2 vers votre port « sniffer »

g) Contrôlez que le routage OSPF est fonctionnel.

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. Les commandes utiles sont les suivantes:

```
RX2# show ip ospf neighbor
RX2# show ip route ospf
RX2# show ip ospf interface
```

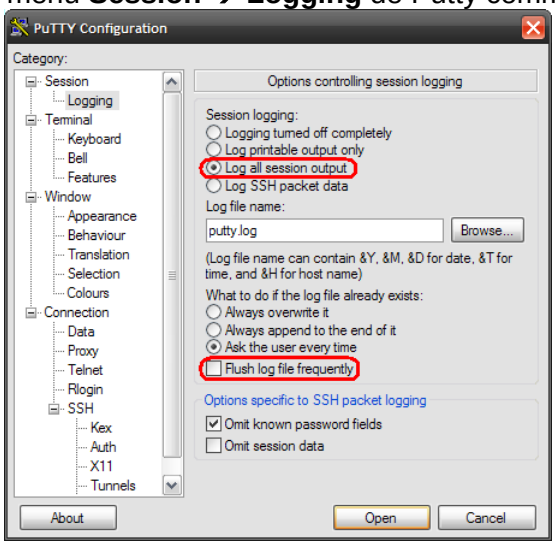
2. Connexion en Telnet ou SSH :

Dans ce laboratoire, il faudra se connecter aux routeurs avec une connexion rapide. Pour ce faire, l'utilitaire "Putty" sera utilisé pour se connecter aux routeurs via le protocole telnet. Il est disponible sur tous les postes du laboratoire ou téléchargeable sur le site http://www.putty.nl/ (Pour le télécharger directement: http://www.putty.nl/latest/x86/putty.exe).

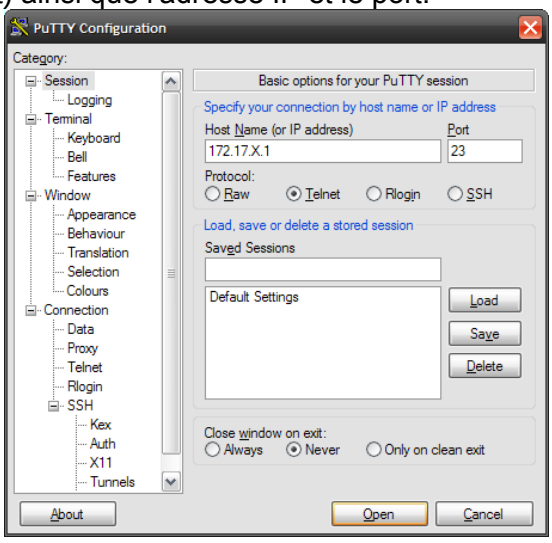
a) Capture du contenu d'une session Putty

Pour vos manipulations dans ce laboratoire il est aisé de démarrer deux sessions telnet depuis le poste « utilisateur », une sur chaque routeur. Il sera ainsi possible d'activer l'affichage de messages sur la session telnet on non plus sur la console qui une vitesse relativement limitée. Afin de documenter correctement votre rapport il est possible de capturer dans un fichier texte l'ensemble des événements et des messages affichés dans la session putty. La console peut toujours être utilisée pour entrer les commandes de configuration.

Vous pouvez activer l'enregistrer de tous les messages qui seront affichés dans un fichier en modifiant le menu **Session → Logging** de Putty comme suit:



Ensuite vous pouvez vous connecter aux routeurs, il suffit de préciser le protocole (en l'occurrence telnet) ainsi que l'adresse IP et le port:



b) Génération et capture des messages

Un routeur Cisco dispose de 8 niveaux de sévérité de messages (severity).

```
<0-7>          Logging severity level
emergencies    System is unusable                (severity=0)
alerts         Immediate action needed           (severity=1)
critical       Critical conditions               (severity=2)
errors         Error conditions                  (severity=3)
warnings       Warning conditions                (severity=4)
notifications  Normal but significant conditions (severity=5)
informational  Informational messages            (severity=6)
debugging      Debugging messages                (severity=7)
```

Il est aussi capable d'afficher ces messages sur plusieurs environnements notamment :

Console : la console du routeur à 9600

Monitor : une session VTY vers laquelle on a redirigé les messages avec la commande **<terminal monitor>**

Buffer : Un espace mémoire circulaire à l'intérieur du routeur que l'on peut afficher avec la commande **<show logging>**

Host : un serveur capable de récupérer des messages formatés selon le protocole « Syslog »

Il est très important de diminuer le niveau d'affichage des messages à la console pour ne pas charger celle-ci qui est limitée à 9600bps. Trop de messages à la console peuvent bloquer le routeur et le faire redémarrer. La configuration ci-dessous va :

- Afficher uniquement les messages de niveau critique et supérieur à la console
- Afficher tous les messages (y-compris debug) dans les sessions de monitoring
- Et rediriger tous les messages dans un log interne au routeur de 400KB

```
RX2(config)# logging console critical
RX2(config)# logging monitor debugging
RX2(config)# logging buffered 409600 debugging
```

Pour activer le mode de monitoring et ainsi rediriger tous les messages à partir d'un terminal connecté en telnet il faut entrer la commande suivante:

```
RX2# terminal monitor
```

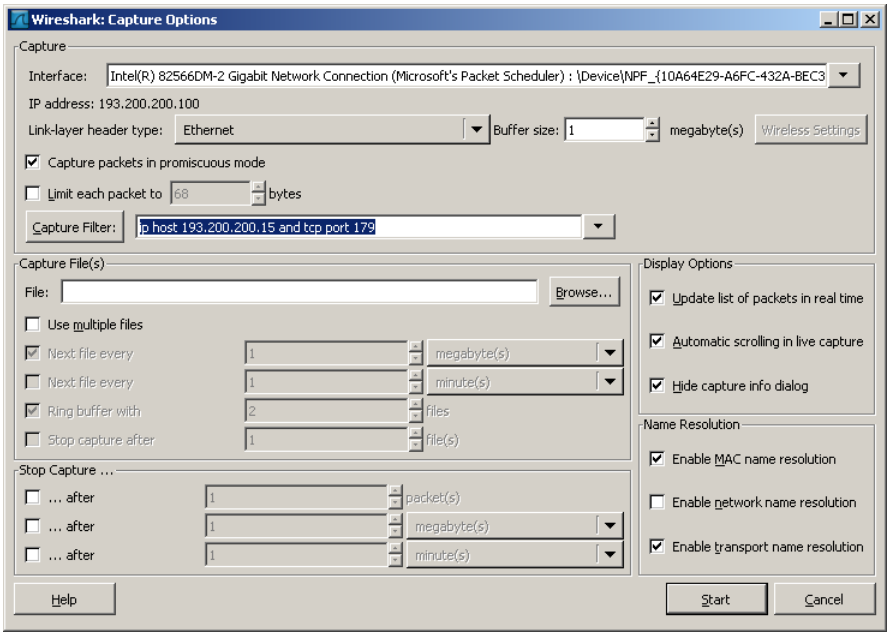
c) Note pour la rédaction des rapports de laboratoire

Pour illustrer vos rapports de laboratoire, et quand cela vous est demandé, vous fournirez toujours une capture « Sniffer », un résultat de « debug » routeur et une copie des commandes de configuration ajoutées sur chaque équipement.

i. Les commandes doivent être représentées dans leur contexte et en un bloc
ii. Les captures devront bien être présentées et pertinentes (attention à filtrer vos captures intelligemment pour éviter la pollution de vos traces par vos voisins).
iii. Le nombre ainsi que le type de « debug » routeur seront savamment sélectionnés et les points importants seront mis en évidence dans le rapport.

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).

Exemples :
Capture du traffic BGP (tcp/179) envoyé depuis le routeur ayant l'adresse 193.200.200.15.



Les commandes « debug » vous permettent de voir des messages supplémentaires concernant la fonction activée. Elles s'activent avec la commande suivante:

```
RX2# debug <fonction-à-debugger>
```

Un debug ne doit généralement par être continuellement activé en exploitation. Toutes les debugs actifs peuvent être désactivées avec la commande suivante:

```
RX2# undebug all
```

3. Lien eBGP

Le but est d'établir un lien eBGP entre le routeur RX2 et ISP2. Il s'agit d'un lien eBGP tout à fait classique entre des routeurs directement connectés.

a) Mise en service du lien eBGP

Pour établir ce lien un exemple de configuration serait:

- Activation d'un routeur BGP pour votre numéro d'AS (mettre votre numéro de groupe)
- Désactivation de la synchronisation entre BGP et votre IGP afin que BGP n'attende pas sur l'IGP pour considérer les routes reçues
- Activation de l'affichage d'un message en cas de changement d'état du lien avec un voisin BGP
- Configuration du lien eBGP avec l'adresse IP de votre voisin ISP2 (193.200.200.254) dans l'AS 200 (un numéro d'AS différent indique un peering eBGP).
- Désactivation de la communication avec votre voisin (**<shutdown>**). Elle pourra être activée (même ligne précédée de **<no>**) et désactivée à la demande, ceci surtout quand vous serez prêt avec la capture de vos debug et traces.
- La « soft-reconfiguration » permet la reconfiguration du lien BGP sans réinitialisation complète et sans perte de connexion.

```
R2X(config)#
      router bgp <your_AS_number=X>
       no synchronization
       bgp log-neighbor-changes
       neighbor <ip_address_of_ISP2> remote-as <ISP2_AS_number>
       neighbor <ip_address_of_ISP2> shutdown
       neighbor <ip_address_of_ISP2> soft-reconfiguration inbound
```

b) Activation du lien et commandes « show »

Une fois toutes ces commandes entrées correctement vous pouvez activer le lien avec :

```
R2X(config-router)# no neighbor <ip_address_of_ISP2> shutdown
```

Contrôlez que ce lien eBGP soit établi à l'aide des quelques commandes 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 populent votre table de routage il faut respecter les règles concernant la synchronisation (désactivé dans notre cas). A titre de référence capturez le résultat de chacune de ces commandes et pointez les éléments qui vous semblent importants.

Affichage rapide de l'état de votre table BGP et de vos liens BGP.

```
R2X# show ip bgp summary
```

Affichage de l'état détaillé de tous les liens BGP (BGP state=Established, indique que le lien est bien établi, par contre l'état « Active » indique que le routeur tente activement de l'établir).

```
R2X# show ip bgp neighbors
```

Consulter la liste des routes BGP reçues

```
R2X# show ip bgp
```

Il est possible d'obtenir plus de détails pour une route en ajoutant celle-ci à la suite.
```
R2X# show ip bgp 193.5.1.0 255.255.255.0
```

Afficher le contenu complet de la RIB (table de routage du routeur)
```
R2X# show ip route
```

Contrôlez quelle route BGP sera mise dans la RIB (table de routage du routeur)
```
R2X# show ip route bgp
```

Contrôler les routes reçues au travers du lien avec un voisin BGP (attention la soft-reconfiguration doit avoir été activé pour que vous puissiez utiliser cette commande)
```
R2X# show ip bgp neighbors 193.200.200.254 received-routes
```

Contrôler quelles routes vous envoyez vers un voisin BGP
```
R2X# show ip bgp neighbors 193.200.200.254 advertised-routes
```

c) Activation de « debug » et analyse des messages reçus

Maintenant que vous êtes familier avec les commandes « show » nous allons travailler avec les commandes de « debug ». A titre de référence capturez les messages envoyés lord du ré-établissement complet de votre lien BGP avec ISP2, pointez les messages qui vous rappellent la théorie. Trouvez ci-dessous les commandes de « debug » à activer avant de réinitialiser votre lien BGP. Une trace sniffer de la communication entre RX2 et ISP2 sera aussi nécessaire à la bonne compréhension des échanges BGP.

Activer les messages détaillés relatif à l'établissement du lien BGP (repérer dans ces messages les changements d'état - <BGP: 193.200.200.254 OPEN …>)
```
RX2# debug ip bgp
```

Activer les messages détaillés relatif aux échanges de routes BGP (repérer les attributs dans les updates - <BGP(0): 193.200.200.254 rcv UPDATE …>)
```
RX2# debug ip bgp update
```

Activer les messages détaillés relatif à l'ajout ou la suppression d'une route dans la table de routage (messages de la RIB - <RT: add/del …>)
```
RX2# debug ip routing
```

Pour que les changements apportés à BGP soient pris en compte ou pour redémarrer des liens actifs, nous devons réinitialiser ces liens. La commande suivante réinitialise complètement tous les liens
```
RX2# clear ip bgp *
```

Celle-ci réinitialise seulement le lien avec ISP2
```
R2X# clear ip bgp 193.200.200.254
```

4. Envoyez votre réseau à vos ISP2

a) Configuration de l'importation de route dans BGP et capture de l'activité

Importez votre réseau 193.168.X.0/24 qui se trouve sur l'interface GigabitEthernet0/1 de votre routeur RX2 dans BGP. Votre réseau doit être visibles avec un attribut « ORIGINE » valant « IGP ». Pour ce faire la route doit être importée dans BGP avec la commande `<network>`.

```
R2X(config)#
      router bgp <your_AS_number=X>
       network 193.168.X.0 mask 255.255.255.0
```

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

```
      no debug ip bgp
      debug ip bgp updates
      debug ip routing
```

b) Contrôle de l'émission de la route et des tables de routage Internet

Utilisez la commande « show » appropriée pour voir si votre route est bien transmise à votre voisin IPS2 (`<show ip bgp neighbors 193.200.200.254 advertised-routes>`).

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

Ces « Route Server » sont accessibles en telnet
Le mot de passe d'accès est « cisco »
Les commandes <show ip bgp … & show ip route …> 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

c) Contrôle de fonctionnement

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.

Note : pour que cela fonctionne bien, vous devez avoir spécifié une passerelle sur votre « poste utilisateur » (si possible RX2) et un serveur de DNS (comme 10.192.48.100 et/ou 10.192.48.101).

Rappel : pour que les changements apportés à BGP soient pris en compte sur les liens actifs, nous devons normalement réinitialiser les liens. Il est possible de redémarrer un lien sans le couper complètement et juste calculer le delta dans les « UPDATE ».

Recalcule des « UPDATE » à envoyer à un voisin précis
```
R2X# clear ip bgp 193.200.200.254 soft out
```

Re-contrôle des « UPDATE » en provenance d'un voisin précis. Attention la reconfiguration entrante doit être activée au préalable. Le routeur va ainsi tenir à double la liste de ce qu'il a reçu de ce voisin en plus de la liste des meilleures routes BGP qu'il conserve toujours après traitement.
```
R2X# clear ip bgp 193.200.200.254 soft in
```

Règles de Notation pour le laboratoire

Aucun rapport n'est nécessaire pour ce laboratoire. Il constitue pour vous une base d'apprentissage importante pour les laboratoires suivants. Si ce laboratoire est compris et pratiqué comme demandé il vous permettra de gagner du temps pour les prochains !