Les VPN MPLS/BGP

Objectifs

Mettre en place des VPN MPLS/BGP, en comprendre les mécanismes et en observer les échanges et encapsulation.

1 Présentation générale

Le but de cette séance est de construire les VPN permettant d'acheminer le trafic entre les sites des différents clients de l'opérateur du réseau de la figure 1.

La configuration partielle du réseau vous est fournies sous forme de scripts à lancer. L'utilisation de ces scripts est décrite en annexe à la fin de ce document.

1.1 Le réseau de notre expérimentation

Voici une description du réseau qui vous est fourni.

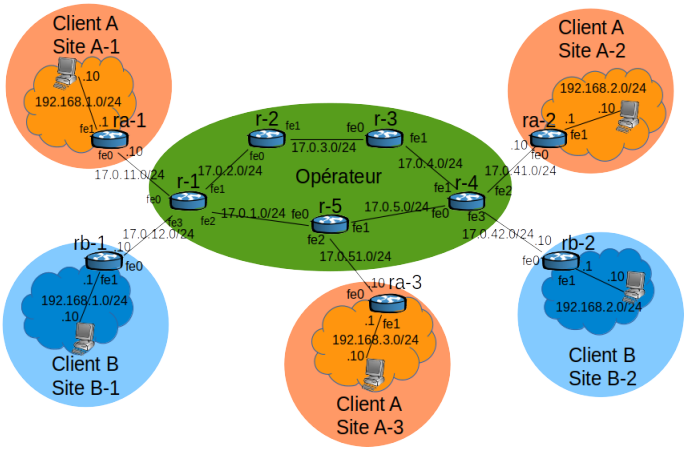

FIGURE 1 – Le réseau de cet exercice

Pour ne pas surcharger davantage le dessin, les octets de poids faible ne sont pas toujours précisés. Ils ont les valeurs suivantes :

— pour les routeurs de l'opérateur (`r-1` à `r-5`), c'est le numéro du routeur (1 à 5) ;
— pour les routeurs des clients (`ra-1`, `rb-2`, ...) c'est 10 pour l'interface "extérieure" (ou publique) et 1 pour l'interface interne ;
— pour chaque machine interne des clients (une seule par réseau) c'est 10.

Tout l'adressage du réseau est mis en place dans les fichiers qui vous sont fournis.

Chacun des routeurs de l'opérateur dispose également d'une interface virtuelle `d0` dont l'adresse est `10.0.0.n` où `n` est sont numéro. C'est cette adresse qui sera utilisée comme identifiant lorsque nécessaire.

Le routage interne à l'opérateur est mis en place. C'est ici le protocole OSPF qui est utilisé.

Les fonctionnalités MPLS sont également activées sur les routeurs de l'opérateur, mais aucune configuration n'est fournie.

Sur les machines des clients, le routage par défaut est configuré, ainsi que sur leurs routeurs d'accès Internet.

Pour des raisons techniques, tous les démons nécessaires dans cette séance (`ospfd`, `bgpd`, ...) sont déjà démarrés dans le réseau qui vous est fourni. Vous n'avez plus qu'à les configurer en y accédant grâce à la commande `telnet`, par exemple :

```
r-1 # telnet 127.0.0.1 ripd
```

1.2 Objectifs de la séance

L'objectif est ici de construire des VPN, mis en place par l'opérateur grâce à MPLS et BGP. Afin de simplifier les explications, nous distinguerons deux types de routeurs de l'opérateur : les routeurs d'accès seront les routeurs qui desservent directement un ou plusieurs clients et les autres seront les routeurs de cœur.

Nous allons devoir réaliser les opérations suivantes :

— Nous allons créer des "*Attachment Circuits*", c'est-à-dire des liens entre les routeurs d'accès de l'opérateur et ceux de ces clients.
— Nous allons ensuite créer, sur chaque routeur d'accès de l'opérateur, une VRF pour chacun des clients que dessert ce routeur.
— Nous devrons ensuite activer MPLS sur tous les routeurs de l'opérateur.
— Afin de mettre en place les labels MPLS dans le réseau de l'opérateur, nous allons y déployer le protocole LDP.
— Les routeurs d'accès de l'oparateur devront être configurés pour utiliser BGP.
— Il nous faudra ensuite, sur chaque routeur d'accès, configurer dans BGP la getion de chacune des VRF préalablement créées.
— Nous supposerons ici que le protocole de routage utilisé par les clients est RIP que nous devrons donc configurer sur les routeurs d'accès de l'opérateur.
— Il ne nous restera alors plus qu'à configurer RIP chez les clients.

Chacune de ces opérations va faire l'objet d'une des sections suivantes.

2 Mise en place du routage interne

Il est nécessaire, dans un premier temps, de mettre en place le routage interne dans le réseau de l'opérateur. Nous utiliserons pour cela le protocole OSPF, configuré avec une seule zone.

Le routage est déjà configuré dans le réseau fourni. Il sera donc uniquement nécessaire d'attendre quelques secondes après le démarrage pour s'assurer que les routes sont correctes.

▷ **Exercice 1 : Configuration de** OSPF

Vérifier le bon fonctionnement du routage ; on s'assurera en particulier que les routeurs des clients peuvent communiquer au travers de leurs adresses publiques.

Donner les routes d'un routeur d'accès et d'un routeur de cœur. Sur le(s)quel(s) trouve-t-on des routes pour les réseaux internes des clients ? Pourquoi ?

■

3 Mise en place des *Attachment Circuits*

L'objectif ici est de mettre en place un *Attachment Circuit* (ou AC) entre chaque routeur d'un client et son routeur de desserte chez l'opérateur.

Imaginons que l'opérateur fournisse le service d'accès Internet à son client au travers d'une interface Ethernet (sur un équipement de l'opérateur situé chez le client). Il pourra alors lui offrir le service de VP au travers de la même interface mais *via* un VLAN Ethernet spécifique. C'est ce que nous allons mettre en place ici, et c'est ce VLAN Ethernet qui constitue l'AC que nous utiliserons par la suite.

▷ **Exercice 2 : Mise en place des** AC

Mettre en place un AC *entre chaque routeur de chaque client et son routeur de desserte. On utilisera pour cela un* VLAN *Ethernet.*

En vérifier le bon fonctionnement.

Un lien existe déjà entre le routeur du client et celui de l'opérateur, pourquoi faut-il en activer un second ? ■

On notera que les adresses IP utilisées pour ces liaisons point à point sont sans intérêt et n'ont en particulier pas besoin d'être routables.

4 Mise en place des VRF

▷ **Exercice 3 : Création des** VRF**s**

Qu'est-ce qu'une VRF *? Quel est son utilité dans les réseaux que nous sommes en train de mettre en place ?*

Sur chaque routeur d'accès de l'opérateur, créer une VRF *pour chacun des clients desservis.*

On y ajoutera l'interface précédemment créée : celle au travers de laquelle le service sera rendu au client. ■

5 Activation de MPLS

C'est le protocole MPLS qui va être utilisé pour mettre en place les réseaux privés virtuels. Il est donc nécessaire de l'activer sur l'ensemble des routeurs de l'opérateur.

Sur le réseau qui vous est founi ici, cette activation a déjà été réalisée.

▷ **Exercice 4 : Rôle de** MPLS

Quel est ici le rôle de MPLS *? Pourquoi en avons-nous besoin ? Un autre protocole (lequel ?) pourrait-il le remplacer ?* ■

6 Configuration de LDP

Il est maintenant nécessaire de configurer le protocole LDP sur l'ensemble des routeurs de l'opérateur. Il nous permettra de mettre en place des LSP MPLS fondés sur le routage mis en place pe OSPF.

On utilisera comme identifiant les adresses en `10.0.0.n/32` attribuées aux routeurs.

▷ **Exercice 5 : Configuration de** LDP
Après avoir lancer un outil d'observation du réseau (tel que `tcpdump` *ou* `wireshark`*), configurer le protocole* LDP *sur chacun des routeurs de l'opérateur.* ■

Il est ensuite utile de vérifier que tout se passe comme prévu !

▷ **Exercice 6 : Observation des échanges**
Vérifier, grâce à l'outil d'observation préalablement lancé, que les échanges entre deux routeurs sont corrects. ■

Si les échanges se passent correctement, on peu également observer l'état de chaque instance de LDP.

▷ **Exercice 7 : Vérification des voisinages**
Observer les relations de voisinages construites par les routeurs de l'opérateur. ■

Il est alors possible d'observer que les tables MPLS sont correctement sontruite et que le trafic dans le réseau est effectivement acheminé au travers de MPLS.

▷ **Exercice 8 : Vérification de la mise en place des** LSP
Utiliser la commande `ip -f mpls route show` *pour observer les tables* MPLS *sur les routeurs de l'opérateur.*
Grâce à une commande `ping`*, générer du trafic entre deux routeurs (par exemple* `r-2` *et* `r-5`*) et observer son encapsulation sur un lien intermédiaire (par exemple entre* `r-1` *et* `r-2`*).* ■

7 Configuration de BGP

Il est maintenant possible de mettre en place le deuxième outil de base de nos VPN. C'est en effet le protocole BGP qui va être utilisé pour échanger les informations entre les routeurs d'accès permettant la cohérence des VPN.
Nous allons dans un premier temps nous contenter d'activer BGP, mettre en place les relations de voisinage et les activer pour les VPNs.

▷ **Exercice 9 : Mise en place de** BGP
Configurer BGP *sur les routeurs d'accès de l'opérateurs pour utiliser la famille d'adresse* `ipv4 vpn` *et établir les relations entre eux.* ■

Il est alors possible de vérifier que les relations ont bien été mises en place.

▷ **Exercice 10 : Observation des échanges**
Grâce à l'outil d'observation réseau lancé préalablement, vérifier que les échanges BGP *se déroulent correctement entre routeurs.* ■

L'état des routeurs permettra alprs de valider la mise en place des sesions BGP.

▷ **Exercice 11 : Observation des relations entre routeurs**
Utiliser les commandes BGP *pour vérifier l'état des sessions* BGP*.* ■

8 Prise en compte des VRF dans BGP

Maintenant que les relations BGP entre routeurs sont établies, nous allons pouvoir intégrer dans BGP la prise en compte des VRF préalablement créées.

▷ **Exercice 12 : Encore du BGP ?!**
Pourquoi faut-il une configuration supplémentaire de BGP ? En quoi celle que l'on vient de faire est-elle insuffisante ? ■

Il est pour cela nécessaire de configurer chacune des VRF préalablement créées. Pour chacun de ces réseaux, c'est bien la famille d'adresse `ipv4 unicast` qui est utilisée. Comme elle n'est plus la famille par défaut, il sera nécessaire de le préciser explicitement.

Pour ce qui est des *Route Distinguisher*, on utilisera par exemple un format de type 1, c'est-à-dire sous la forme `a.b.c.d:nn` où `a.b.c.d` est une adresse IP (typiquement une adresse publique du site d'un client) et `nn` est un nombre sur 2 octets permettant de garantir l'unicité (par exemple lorsque plusieurs VPN sont fournis au même client sur le même site, ce qui n'est pas le ca ici, on pourra donc prendre systématiquement la valeur 1).

En ce qui concerne les *Route Target*, nous utiliserons le format `as:n` où `as` est le numéro d'AS et `n` un identifiant permettant de garantir l'unicité (par exemple le numéro du client).

▷ **Exercice 13 : Intégration des VRF dans BGP**
Mettre en place la configuration de BGP sur les 3 routeurs d'accès de l'opérateur et ce pour les 2 clients concernés. ■

9 Activation de RIP chez l'opérateur

Notre objectif est en particulier d'échanger des informations de routage entre les différents sites de chaque client, et ce au travers du VPN.

Il est donc nécessaire que les routeurs d'accès de l'opérateur soient capables de dialoguer avec ceux de ses clients. Nous allons supposer ici que le seul protocole offert par l'opérateur soit RIP.

Nous allons donc devoir l'activer dans les VRF associées aux clients et lui préciser de redistribuer les routes apprises par BGP.

▷ **Exercice 14 : Activation de RIP chez l'opérateur**
Sur chaque routeur d'accès de l'opérateur, et pour chaque client desservi, configurer le routage RIP dans la VRF correspondante. ■

10 Configuration de RIP chez les clients

La dernière étape est ici la configuration du routage dans le réseau de chaque client. Bien entendu, ce routage peut avoir été mis en place bien plus tôt, mais les réseaux auxquels nous nous intéressons ici sont tellement simples qu'ils ne nécessitaient aucune conofiguration du routage. L'inteconnexion des sites au travers du VPN change un peu la donne et nécessite la mise en place d'un outil de routage. Nous allons donc choisir ici le protcole IP.

▷ **Exercice 15 : Configuration de RIP chez les clients**
Sur chaque routeur de chaque client, configurer le routage RIP.

Pourquoi n'est-il plus question de VRF *ici ?*
Quels sont les réseaux (ou les interfaces) intégrés dans la configuration de RIP *?* ■

11 Observation du trafic

La configuration étant complète, il est maintenant possible de vérifier et d'observer le fonctionnement de nos VPN. On pourra ainsi vérifier que

— les routeurs `ra-?` et `rb-?` arrivent à communiquer entre eux *via* leurs adresses publiques (ce qui signifie que l'accès internet fourni par l'opérateur fonctionne correctement) ;
— les routeurs `ra-?` arrivent à communiquer avec toutes les machines de tous les sites du client A et de même pour B (ce qui signifie que les VPNs sont opérationnels).

▷ **Exercice 16 : Observation des échanges**
Vérifier grâce à la commande `ping` *le bon fonctionnement des services fournis par l'opérateur (on ne sera pas exhaustif !).* ■

Il est maintenant particulièrement intéressant d'observer les échanges entre les machines et leur encapsulation.

▷ **Exercice 17 : Observation des échanges**
Déterminer le chemin emprunter par des paquets allant du site `A-1` *au site* `A-2` *et du site* `B-1` *au site* `B-2`.
Utiliser un outil d'observation pour analyser l'encapsulation qui est réaliser. Comment les paquets des deux clients peuvent circuler sans ambiguïté malgré un plan d'adressage incompatible ?
■

A Utilisation de l'outil de simulation du réseau

Ce réseau utilisé dans cette séance est "simulé" à l'aide d'un outil d'isolation fourni par le noyau Linux (les *Namespaces* réseau). Une description plus complète est disponible à l'adresse suivante
`http://chaput.perso.enseeiht.fr/teaching/ressources/tp-reseaux-virtualises`

Si vous avez déjà utilisé ces outils, vous pouvez passer à la section suivante.

A.1 Installation des fichiers

La page web citée plus haut décrit les différentes façons d'obtenir les fichiers vous permettant de démarrer la séance.

Grâce à l'aide de cette page et/ou de votre enseignant·e, vous pouvez donc maintenant démarrer un *shell* dans le répertoire contenant les fichiers de la séance voulue et dans lequel vous prendrez l'identité de l'administrateur (nécessaire pour la suite des opérations) :

```
$ cd le-dossier-de-mon-tp
$ sudo su
#
```

vous pouvez alors démarrer la séance.

A.2 Démarrage et arrêt du simulateur

Le lancement du simulateur se fait de la façon suivante

```
# ./creerReseau
```

Un terminal est alors ouvert sur les machines principales du réseau.

Une liste d'options utilisables pour wireshark vous est également fournie. Vous pourrez l'utiliser pour observer le trafic sur les interfaces des différentes machines.

Pour cela, vous lancerez, par exemple, dans le même terminal

```
#  wireshark  -i /tmp/nssi/host1/v0
```

Ce qui vous permettra d'observer le trafic sur l'interface `v0` de la machine `host1`.

Notez que vous pouve bien sûr lancer la commande `tcpdump` directement dans le terminal de la machine correspondante !

Vous pourrez arrêter la simulation ainsi :

```
# ./detruireReseau
```

Attention, lorsque vous arrêtez le réseau, toutes la manipulations faites sur les machines sont définitivement perdues !

A.3 Lancement d'une commande ou d'un terminal dans une machine

Si vous avez malencontreusement fermé le terminal d'une machine, vous pouvez le relancer de la façon suivante

```
# ./creerReseau -r machine
```

où `machine` est le nom de la machine.

Vous pouvez également lancer une commande sur une machine :

```
# ./creerReseau -r machine "commande et options"
```

Les guillemets sont nécessaires, par exemple

```
# ./creerReseau -r m1 "ip link show"
```