Module M3102 – TP6

MPLS : LDP et L3-VPN

Ce qu'on veut faire dans ce TP : Permettre à l'ISP d'établir un VPN de couche 3 entre les sites distants de chaque client (3 clients ici, donc 3 VPNs).

Pourquoi : Car chaque client veut être parfaitement isolé des autres possibles clients de l'ISP : ne voir aucun trafic, ni de données ni de contrôle (comme updates de routage) d'autre client, ainsi qu'avoir la possibilité d'utiliser n'importe quelles adresses, indépendamment des autres clients, pourvu que celles-ci soit cohérentes au sein du réseau privé du client.

Comment : Par une configuration de VPNs de niveau 3, à travers le réseau de l'ISP. Utilisation de BGP dans sa version Multi-Protocol (MP-BGP) et MPLS.

Chaque routeur CE va donc être connecté au niveau de la couche 3 à l'ISP : le next hop vu dans la table de routage d'un CE est l'adresse d'un PE (pas l'adresse de CE de site distant comme si on était connecté par la couche 2 à l'ISP, qu'on verrait comme un switch).

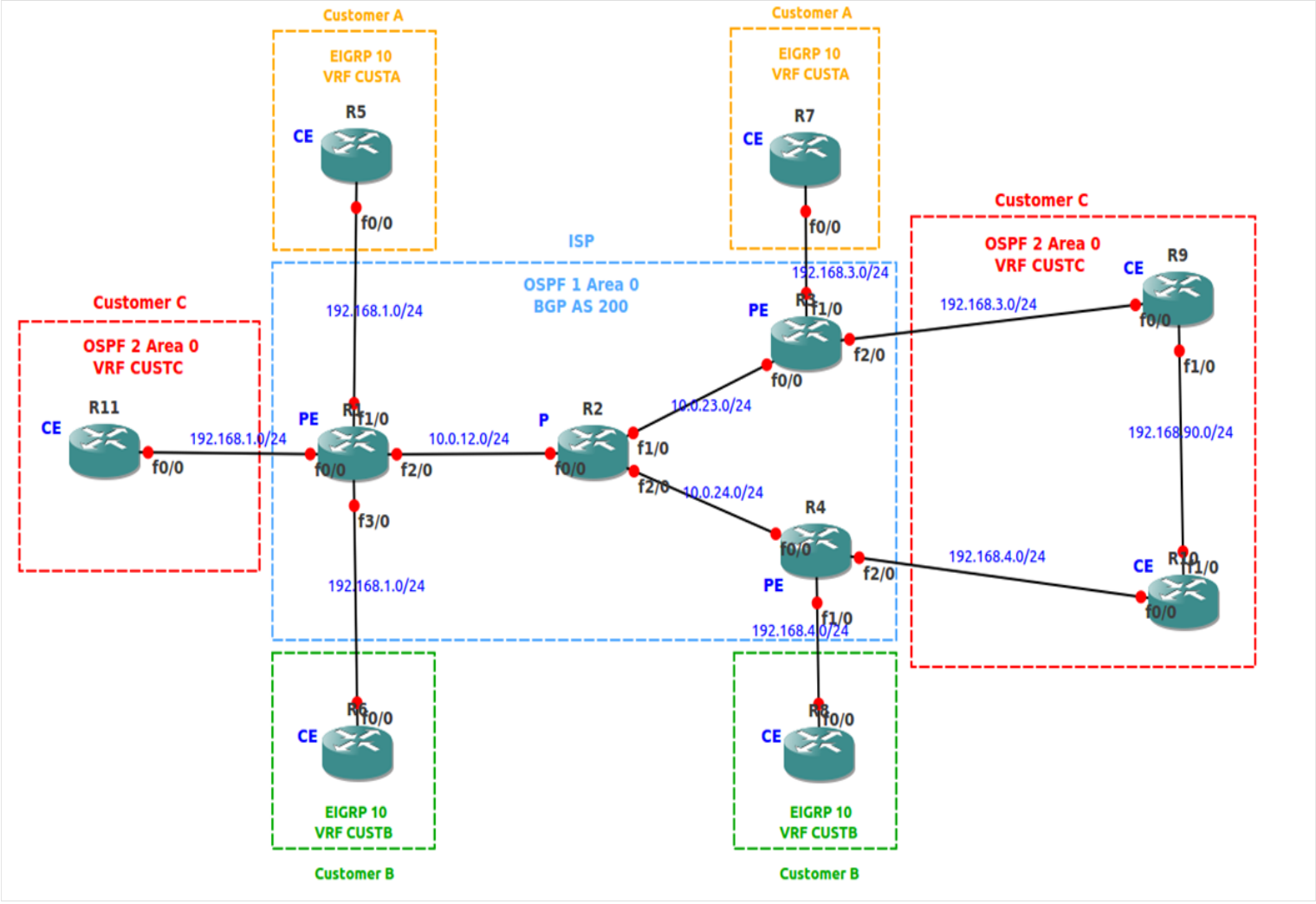
Consignes générales :

- Vous vous loggez sous votre compte perso, machine physique en Ubuntu.
- 1 compte-rendu par étudiant·e. Vous récupérez le pdf et l'odt du sujet depuis http://www.i3s.unice.fr/~sassatelli/M3102/
- Récupérez aussi le répertoire de topologie GNS3 *TP6_MPLS_l3VPN_initial.zip*.
- Joindre au rapport le fichier de config final du routeur (copié-collé de la config finale). Avant de commencer, lire les 2 pages qui suivent.

Etapes

Pour mettre en place ces 3 VPNs, vous allez devoir configurer l'ensemble des routeurs entièrement. Les étapes vont être les suivantes :

1. Attribution des adresses IP aux interfaces des CE, de P et des PE non reliées à CE
2. Configuration des processus de routage aux CE et à l'intérieur de l'ISP
3. Activation de MPLS pour établissement des LSP à l'intérieur de l'ISP
4. Création des VRFs à chaque PE
5. Associer un processus de routage à chaque VRF sur chaque PE
6. Activation de BGP dans sa version Multi-Protocol (MP-BGP) pour l'interconnexion des VPN
7. Redistribution des IGP par VRF dans MP-BGP
8. Redistribution de BGP dans IGP



Description de la topologie

La topologie d'étude sur la figure précédente.

L'ensemble des réseaux ISP et clients vous est représenté sur la figure précédente.

- Client A : IGP est EIGRP, VRF CUSTA
- Client B : IGP est EIGRP, VRF CUSTB
- Client C : IGP est OSPF, VRF CUSTC
- ISP : IGP est OSPF, ASN 200, cœur géré par MPLS

Par simplicité, on considère que tous les réseaux ont un masque de 24 bits.

Les réseaux PE-CE sont en 198.168.Y.0/24 où Y est le numéro du PE.

L'adresse IP de chaque interface physique de chaque routeur a pour dernier octet le numéro du routeur (indiqué sur figure).

En plus de ces interfaces physiques, chaque routeur a une interface de loopback d'adresse X.X.X.X /32 où X est le numéro du routeur.

I. Attribution des adresses IP aux interfaces des CE, de P et des PE non reliées à CE

1. Configurer toutes les interfaces des CE avec la bonne adresse IP, et les activer :

   ```
   ip address [ADDR] [MASK]
   no shutdown
   ```

2. Configurer de même les interfaces PE-P.
3. Sur chaque routeur, créer une interface de loopback :

   ```
   interface loopback 0
   ip address [X.X.X.X] 255.255.255.255
   no shutdown
   ```

Attention : adresse en /32 très important sinon mauvais tag mpls.

II. Configuration des processus de routage aux CE et à l'intérieur de l'ISP

1. Configurer le processus de routage OSPF 1 sur R1, R2, R3 et R4, qui ne gère que les réseaux intérieurs de l'ISP, avec les loopbacks :

   Sur R1 :

   ```
   router ospf 1
   network 1.1.1.0 0.0.0.255 area 0
   network 10.0.12.0 0.0.0.255 area 0
   ```

   Faire de même sur R2, R3 et R4.

4. Configurer le bon processus de routage, tels qu'indiqués sur la figure, sur tous les CE :

   Exemple sur R6 :

   ```
   router eigrp 10
   network 0.0.0.0 255.255.255.255
   no auto-summary
   ```

   Exemple sur R11 :

   ```
   router ospf 1
   network 0.0.0.0 255.255.255 area 0
   ```

III. Activation de MPLS pour établissement des LSP à l'intérieur de l'ISP

1. A chaque routeur de l'ISP, activer MPLS sur les interfaces non reliées à des CE. Par exemple sur Fa2/0 de R1 :

   ```
   int fastethernet 2/0
   mpls ip
   ```

2. Une fois ceci effectué, faire `show mpls forwarding-table` sur R1, R2, R3 et R4.

Indiquer la signification de chaque colonne (en reformulant sa définition). Indiquer ce que vous constatez concernant les possibles LSPs établis.

3. Faire les questions de **X.1**

IV. Création des VRFs à chaque PE

1. Sur chaque routeur PE, il faut d'abord créer les VRFs correspondant à chaque client relié à ce PE. Rappelez ci-dessous les significations et rôle de RD et RT.

2. En choisissant tous les RT et RD à 200:N, où N est le numéro du VPN, créez les VRFs sur chaque PE. Exemple sur R1 :

```
ip vrf CUSTA
rd 200:1
route-target export 200:1
route-target import 200:1
```

3. Associer ensuite chaque interface de PE à la bonne VRF. Une fois qu'une interface est associée à une VRF, il faut lui attribuer son adresse IP (si vous l'avez fait avant, il faut le refaire). Exemple pour Fa 1/0 sur R1 :

```
interface fastethernet 1/0
ip vrf forwarding CUSTA
ip address 192.168.1.1 255.255.255.0
no shutdown
```

4. Une fois les VRFs de R1, R3 et R4 configurées, vérifier sur chacun qu'il n'y a pas d'erreur par :

```
sh ip vrf interfaces
```

V. Associer un processus de routage à chaque VRF sur chaque PE

1. Sur chaque PE, il va falloir associer un processus de routage spécifique à chaque VRF, processus qui va communiquer avec le client de cette VRF.

   Exemple pour client A sur R1 :

```
router eigrp 1
no auto-summary
address-family ipv4 vrf CUSTA
   no auto-summary
   network 192.168.1.0 0.0.0.255
   network 1.1.1.0 0.0.0.255
```

```
   autonomous-system 10
```

Attention, chaque processus d'un même protocole de routage doit avoir un numéro différent.

Exemple pour client C sur R1 :

```
router ospf 2 vrf CUSTC
   network 192.168.1.0 0.0.0.255 area 0
   network 1.1.1.0 0.0.0.255 area 0
```

2. Une fois ceci réalisé sur tous les routeurs PE, vérifiez les configurations par un show run.

VI. Activation de BGP dans sa version Multi-Protocol (MP-BGP) pour l'interconnexion des VPN

1. Activation de BGP avec spécification des voisins, exemple sur R1 :

```
router bgp 200
   neighbor 3.3.3.3 remote-as 200
   neighbor 3.3.3.3 update-source Loopback0
   neighbor 4.4.4.4 remote-as 200
   neighbor 4.4.4.4 update-source Loopback0
   no bgp default ipv4-unicast
   address-family vpnv4
      neighbor 3.3.3.3 activate
      neighbor 3.3.3.3 send-community extended
      neighbor 4.4.4.4 activate
      neighbor 4.4.4.4 send-community extended
   exit-address-family
```

2. Vérifiez sur chaque routeur que la configuration intermédiaire BGP est bien la bonne. Indiquez la commande utilisée.

VII. Redistribution par MP-BGP des routes annoncées par les IGP des VRF

1. Effectuer cette redistribution des IGP clients dans tous les PE. Exemple sur R1 pour client A et C :

```
router bgp 200
   address-family ipv4 vrf CUSTA
```

```
    redistribute eigrp 10
    no synchronization
  exit-address-family
  address-family ipv4 vrf CUSTC
    redistribute ospf [NUMPROCESS]
    no synchronization
  exit-address-family
```

2. Pour vérifier que R3 a reçu l'annonce de routes reliées à CE R5 (dont loopback), indiquer et commenter le résultat de

   `sh ip bgp vpnv4 all`

VIII. Redistribution de BGP dans IGP

1. Dans chaque (processus de routage associé à) VRF, il faut redistribuer vers les routeurs des clients (CE) les routes apprises pour ce VPN par BGP depuis le cœur de l'ISP.

   Exemple pour client A sur R1 :

```
router eigrp 1
 address-family ipv4 vrf CUSTA
  redistribute bgp 200
  default-metric 10000 100 255 1 1500
```

   Exemple pour client C sur R1 :

```
router ospf 2 vrf CUSTC
 redistribute bgp 200 metric 200 subnets
```

2. Une fois que ceci a été fait sur tous les PE, vérifiez, et les indiquer dans le rapport, que toutes les routes prévues ont été apprises dans chaque VRF par :

   `show ip route vrf [NOMVRF]`

3. De même sur les CE, vérifiez, et les indiquer, que les routes désirées, et pas d'autres, ont été apprises :

   `show ip route`

IX. Tests par ping et captures

1. Vérifier que R1 peut pinger R3 à travers VPN A :

   ```
   ping vrf CUSTA 192.168.3.3 source 192.168.1.1
   ```

   Si cela ne fonctionne pas, debuggez (vérification des tables de routage, MPLS, si besoin captures).

2. Faîtes de même un ping de R5 vers R7 :

   ```
   ping 192.168.3.7
   ```

3. Une fois que cela fonctionne, lancer une capture entre R5 et R1, une entre R1 et R2, une entre R2 et R3 et une entre R3 et R7. Refaîtes le ping et analyser les 4 captures : décrire tout ce qui est représentatif des VPNs. Le corréler avec le résultat de la commande

   ```
   sh mpls forwarding-table vrf CUSTA
   ```

   effectuée sur R1.

4. Fait X.2.

X. Analyse des étapes clé

1. Analyse de LDP (Label Distribution Protocol) déclenché lors de l'activation de MPLS

1. Sur R1, R2, R3 et R4, désactiver MPLS, en faisant pour chaque interface concernée :

   ```
   no mpls ip
   ```

2. Lancer une capture wireshark sur fastethernet 2/0 de R1, reliée à R2.
3. Ré-activer MPLS partout en refaisant aux mêmes endroits qu'à la question 1 :

   ```
   mpls ip
   ```

4. Au bout de 5 secondes ou plus, arrêtez la capture et l'ouvrir. Trouvez le paquet LDP envoyé par R2 vers R1, et s'appelant « Address Message Label Mapping ».
5. A partir de ce paquet (partie Address Message), remplissez le tableau suivant :

Address 1	
Address 2	
Address 3	
Address 4	

6. A partir des parties « Label Mapping Message » du paquet, remplissez le tableau suivant (toutes les cases) :

FEC prefix	Generic label
1.1.1.1/32	
2.2.2.2/32	3
3.3.3.3/32	

Vous devez constater que le label 3 revient souvent. Cherchez sur le Web s'il signifie quelque chose de particulier. Si oui, quoi et pourquoi est-il utilisé ici ?

7. Sur R1, affichez la table mpls et la table de routage générale :

   `show mpls fowarding-table`

   `show ip route`

   Commentez-les en rapport avec ce que vous avez constaté à la question précédente : qu'est-ce qui a été retenu, pour remplir la table MPLS, du message LDP reçu et que vous venez d'analyser ? Et pourquoi ?

2. Analyse de MP-BGP (Multi-Protocol BGP)

A présent, après la question IX.3, la configuration du réseau doit normalement être finale.

1. Sur R1, regarder la table MPLS et la recopier ci-dessous. Décrire en 1 phrase les 2 parties identifiables.

2. Quelles différences avec `sh mpls forwarding-table vrf CUSTA` ?

3. Lancer une capture wireshark sur Fastethernet 2/0 de R1.
4. Sur R1, faire `clear ip bgp *`, et regarder rapidement immédiatement après la table mpls.
5. Après 20 secondes (une fois que la table mpls est revenue dans l'état initial), arrêter la capture et l'ouvrir pour analyse dans Wireshark.
6. Examiner un paquet BGP de type « UPDATE message » :
   1. Pour chaque partie BGP du paquet, dérouler complètement MP_REACH_NLRI → Network layer reachability information. Indiquer la valeur et expliquer la signification de chacun des 4 champs (Prefix length, Label Stack, Route Distinguisher et IPv4prefix).
   2. Que voyez-vous de plus dans EXTENDED_COMMUNITIES → Carried Extended Communities ?
   3. Dans R1, taper `show ip bgp vpnv4 all`, et expliquer ce que vous obtenez.
   4. Dans R1, taper `show ip bgp vpnv4 all labels`, et expliquer ce que vous obtenez.

Sources

R. Molenaar, *GNS3vault - Free Cisco labs for CCNA, CCNP and CCIE students*, online

The CCIE R&S: http://aitaseller.wordpress.com/2012/09/10/mpls-layer-3-vpns/