

TD : Négociation de service avec MPLS

1. Principes de fonctionnement de l'architecture

- Dans les réseaux IP classiques, le routage n'utilise que le préfixe de destination pour trouver le prochain saut. Cela est souvent insuffisant par rapport aux besoins des opérateurs. Nous avons vu dans le TD sur BGP que ce protocole permet de définir une politique de routage arbitraire, cependant celle-ci ne concerne que le routage inter-domaine. Dans un réseau intra-domaine, l'opérateur peut vouloir faire prendre un chemin spécifique à certains types de trafics ou à certains flots de communication avec une garantie de débit. On appelle cela de l'ingénierie de trafic. Par ailleurs l'opérateur peut souhaiter mettre en place des VPNs pour ses clients. Tout cela peut être réalisé avec le *Multi Protocol Label Switching* (MPLS). L'objectif initial de MPLS était d'améliorer la commutation IP en utilisant des mécanismes de circuits virtuels similaires à ceux d'ATM ou de Frame Relay. Ces circuits virtuels sont définis dans le réseau et des labels sont utilisés dans les tables de chaque équipement pour effectuer la commutation. Les paquets reçoivent un label en entrée de réseau et sont ensuite commutés avec ce label.
- MPLS définit la notion de *Forwarding Equivalence Class* (FEC). Tous les paquets d'une FEC sont traités de la même façon : même interface de sortie, même prochain saut (*next hop*), même file d'attente (si QoS). Un label est associé à une FEC de façon locale ou globale par un protocole de signalisation. L'association peut être déclenchée par les informations de contrôle ou par les données. La granularité d'une FEC est variable :
 - FEC large : préfixe réseau 192.168.0.0/18
 - FEC fine : flux RSVP @S, @D, port S, port D
- Dans un équipement, il peut y avoir une table de commutation MPLS par interface d'entrée (portée du label = lien) ou bien une table MPLS commune (portée du label = équipement).
- Un *Label Switch* est un équipement qui commute des paquets en utilisant leurs labels. Un *Label Switching Router* (LSR) est un routeur qui peut commuter des paquets en utilisant leurs labels. Un *Label Edge Router* (LER) est un routeur qui insère des labels dans les paquets.
- Un *Label-Switched Path* (LSP) est une séquence de sauts (routeur 0...routeur n) dans laquelle un paquet transite de R0 à Rn en utilisant des mécanismes de commutation par labels. Un LSP peut être choisi dynamiquement, en fonction de mécanismes normaux de routage ou bien il peut être configuré manuellement. Un tunnel LSP est une connexion configurée entre deux routeurs, dans laquelle les paquets sont expédiés par commutation de label.
- L'architecture MPLS est définie dans la RFC 3031 qui est récupérable sur le site de l'IETF ici <http://www.ietf.org/rfc/rfc3031>. La définition et l'empilement des labels sont définis dans la RFC 3032 récupérable ici <http://www.ietf.org/rfc/rfc3032>. Le protocole de distribution des labels est défini dans la RFC 5036 récupérable ici <http://www.ietf.org/rfc/rfc5036>. Il y a en tout plus de cent cinquante RFCs qui traitent des mécanismes liés à MPLS.

2. Mise en place

1. Ce TD utilise `GNS3` et `dynamips` qui sont installés sur les machines. Configurez `GNS3` dans les préférences pour qu'il trouve `dynamips` dans `/usr/bin`. Testez son lancement.
2. Récupérez une image pour le **Cisco 7200** et configurez `GNS3` pour qu'il la trouve localement sur votre machine.
3. Dans chaque routeur configurez le `slot 0` avec un module `C7200-IO-FE2` et le `slot 1` avec un module `PA-8T`.
4. Les commandes **Cisco** données ci-dessous sont à **compléter correctement**, pour MPLS voir ici http://www.cisco.com/en/US/docs/ios/12_0st/12_0st14/feature/guide/rtr_14st.html#wp1067821

3. Réseau d'opérateur simple

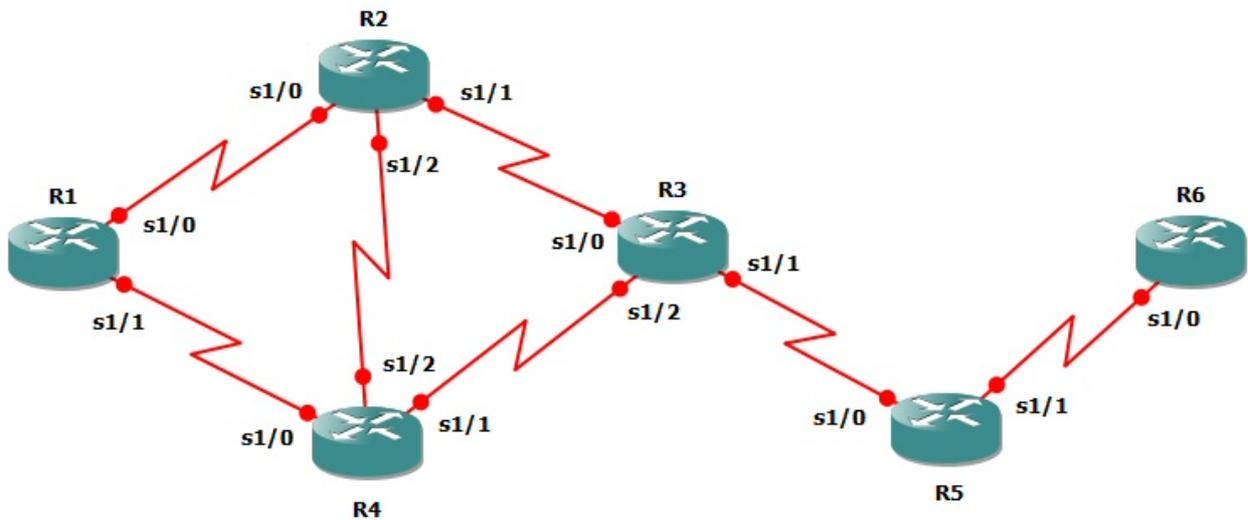


Figure 1. Topologie réseau de l'opérateur.

5. Créez la topologie de la figure 1 dans **GNS3** en connectant les routeurs par des liens série. Démarrez les routeurs.
6. Configurez bien la valeur *Idle PC* des routeurs sinon vos processeurs seront sollicités en permanence à 100%.
7. Choisissez des plages d'adresses pour chaque lien. Etablir un plan d'adressage précis (adresses des interfaces des routeurs). Créez des interfaces de **loopback** sur chaque routeur. L'adresse IP donnée à chaque interface représentera l'identifiant du routeur. Configurez les adresses IP de toutes les interfaces des routeurs avec `(config-if) ip address`. Vérifier les connexions directes.
8. Démarrez **wireshark** sur chaque lien. Choisissez l'encapsulation HDLC pour le lien série. Vous pourrez observer les paquets échangés. Quels types de paquets sont échangés ?
9. Remplissez les tables de routage à l'aide d'OSPF sur chaque routeur. Vérifiez que toutes les machines peuvent communiquer entre elles par des **ping**.
10. Sauvegarder la configuration des routeurs avec `copy running-config startup-config`. Ensuite dans **GNS3** sauvegardez votre projet complet. Pour cela, allez dans `file->save project as...` puis tapez un nom de fichier et cochez la case `save IOS startup files` afin de conserver toute votre topologie avec les configurations des routeurs.
11. Activez MPLS sur les routeurs avec `(config) ip cef` puis `(config) mpls ip` puis enfin `(config) mpls label protocol ldp`. Configurez MPLS sur les interfaces désirées avec `(config-if) mpls ip`. Visualisez les tables de label des différents routeurs avec `show mpls`.
12. Pour le préfixe P6 de l'interface de **loopback** de R6, donnez le contenu des tables de routage et de labels des différents routeurs. En déduire les paquets (avec leurs labels) qui vont transiter de R1 à R6 (et retour) si on exécute **ping** P6 depuis R1. Vérifiez ou infirmez ce comportement :
 - a. Avec des captures de trames analysées avec **wireshark**
 - b. Avec **traceroute**
13. Les labels utilisés de R3 à R5 pour le même préfixe P6 dépendent-ils de l'interface d'entrée dans R3 ? Un label peut-il être utilisé dans les deux sens sur le même lien ? Peut-il être utilisé sur plusieurs liens d'un même routeur ? Les routeurs utilisent-ils le *penultimate popping* ?
14. Etudiez et montrez l'effet de la commande `[no] mpls ip propagate-ttl`.

15. Un nouveau préfixe P7 est ajouté sur R6 (interface 101 sur R6). Décrivez tous les échanges liés aux protocoles OSPF et LDP qui ont lieu suite à cette configuration. L'affectation des labels est elle *downstream on demand* ?
16. Si le lien R1-R2 est coupé, quels sont les échanges des différents protocoles ?
17. Si le lien R3-R4 est coupé, quels sont les échanges des différents protocoles ?
18. Si le routeur R2 tombe en panne, quels sont les échanges des différents protocoles ?

4. Réseau d'opérateur avec VPNs

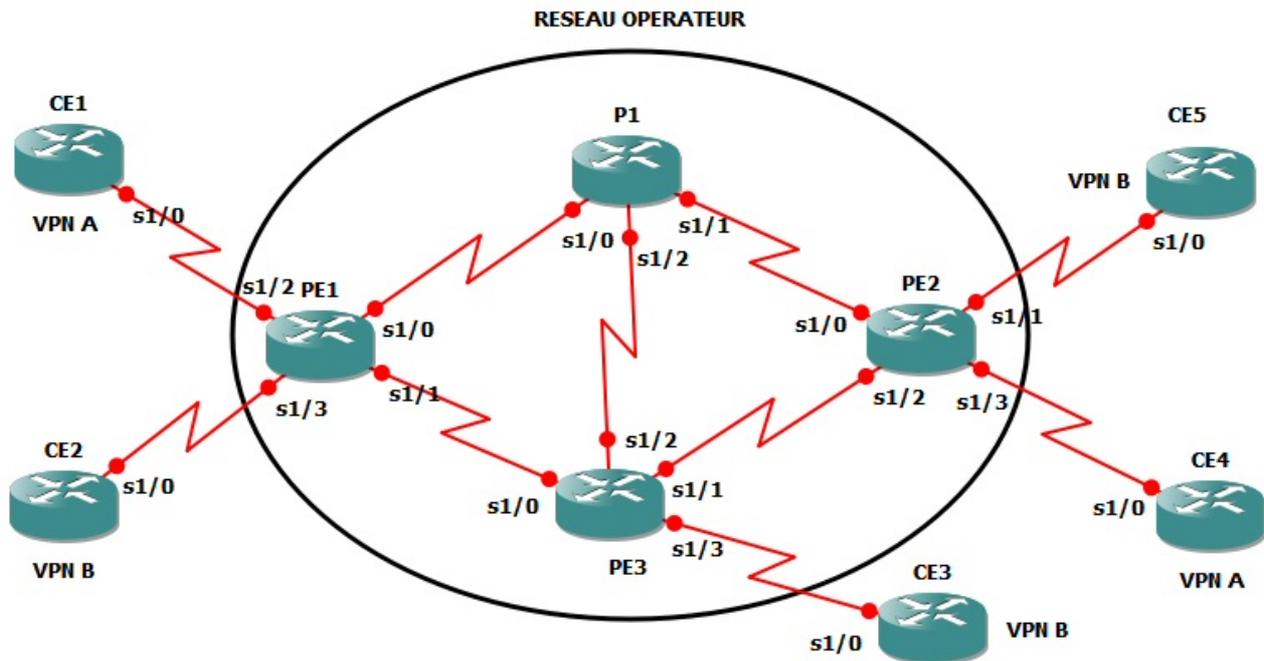


Figure 2. Topologie réseau de l'opérateur et des VPNs clients.

19. L'architecture permettant de déployer des VPNs clients sur un réseau d'opérateur en utilisant MPLS et BGP avec extensions, est définie dans la RFC 4364 qui est récupérable sur le site de l'IETF ici <http://www.ietf.org/rfc/rfc4364>. Dans cette RFC sont définis les *Customer Equipment* (CE) qui sont des routeurs simples (avec routage intra-domaine par exemple), les *Provider Equipment* (PE) qui sont des routeurs BGP/MPLS et les équipements internes du *Provider* (P) qui sont des routeurs MPLS (LSR). Un nouveau type de table nommé *Virtual Routing and Forwarding* (VRF) contient les RIB et FIB virtuelles d'un VPN donné.
20. Créez la nouvelle topologie de la figure 2 ci-dessus dans GNS3 en connectant les routeurs par des liens série. Démarrez les routeurs.
21. Configurez bien la valeur *Idle PC* des routeurs sinon vos processeurs seront sollicités en permanence à 100%.
22. Choisissez des plages d'adresses pour chaque lien. Etablir un plan d'adressage précis (adresses des interfaces des routeurs). Créez des interfaces de *loopback* sur chaque routeur. L'adresse IP donnée à chaque interface représentera l'identifiant du routeur. Configurez les adresses IP de toutes les interfaces des machines et des routeurs avec `(config-if) ip address`.
23. Configurez un routage OSPF dans le réseau de l'opérateur, un routage statique dans le VLAN A et un routage RIP dans le VLAN B.
24. Configurez MPLS dans ce réseau d'opérateur comme expliqué dans la section précédente.

25. Configurez une VRF par client sur chaque PE concerné :
 - a. Créez la VRF avec `(config) ip vrf nom-client`.
 - b. Créez un identifiant *route distinguisher* (RD) pour chaque VRF avec `(vrf) rd route-distinguisher`.
 - c. Créez une *route target* avec `(vrf) route-target both route-target-community-nb`. Le *community number* a le même format que le RD.
 - d. Associez la VRF à l'interface faisant face à un routeur CE avec `(config-if) ip vrf forwarding nom-client`, puis ensuite configurez son adresse IP avec `(config-if) ip address`.
26. Configurez l'instance VRF dans BGP sur chaque PE :
 - a. Définissez la famille d'adresse : `(router) address-family ipv4 unicast vrf nom-client`.
 - b. Redistribuez les connexions : `(router) redistribute connected|static|rip`.
 - c. Configurez le voisin CE : `(address-family) neighbor IP@ remote-as no-as`.
 - d. Activez le voisin CE : `(address-family) neighbor IP@ activate`.
27. Configurez le routage PE vers PE :
 - a. Utilisez l'adresse de *loopback* comme adresse source : `neighbor IP@ update-source Loopbackn`
 - b. Définissez les voisins PE et activez la famille d'adresses VPNv4 :
 - `(router) neighbor IP@ remote-as no-as`
 - `(router) neighbor IP@ activate`
 - `(address-family) address-family vpnv4 unicast`
 - `(address-family) neighbor IP@ remote-as no-as`
 - `(address-family) neighbor IP@ activate`
 - `(address-family) neighbor IP@ send-community extended`
(pour *route-target*)
28. Si un site client du VPN utilise RIP, redistribuez RIP dans la VRF de BGP (fait au 26.b.) et redistribuez la VRF dans RIP :
 - a. `(config) router rip`
 - b. `(router) address-family ipv4 vrf client`
 - c. `(router) redistribute BGP num-as metric m`
 - d. `(router) network prefixe`
29. Vérifiez la connectivité avec `ping` et `traceroute` dans chaque VPN puis vérifiez les tables de routage des routeurs de l'opérateur et des routeurs des VPN (et leurs VRF associées).
30. Les préfixes des VPN sont-ils visibles sur le routeur P ?
31. Listez tous les labels utilisés. Illustrez le cheminement d'un `ping` d'un VPN à travers le réseau opérateur ainsi que sa réponse associée.
32. Détaillez la signalisation échangée par les protocoles LDP, BGP, OSPF et RIP quand :
 - a. on ajoute un nouveau PE,
 - b. on ajoute un nouveau VPN sur un PE,
 - c. on ajoute un nouveau préfixe dans un site VPN existant.

5. Réseau d'opérateur avec TE et VPNs

33. Utilisez pour cette section le réseau configuré précédemment. L'objectif est de tester l'utilisation de l'ingénierie de trafic (TE) pour acheminer les données des clients (VPNs). Mettre en place les mécanismes d'ingénierie de trafic avec MPLS, et montrer comment le trafic des VPNs peut utiliser les tunnels construits par TE.
34. Définissez des tunnels TE qui n'empruntent pas les chemins les plus courts afin de vérifiez leur bon fonctionnement.
35. Commandes pour configurer l'ingénierie de trafic TE :
 - a. Activer les tunnels TE avec `(config) mpls traffic-eng tunnels`
 - b. Activer OSPF-TE avec `router ospf 10` puis avec `(router) mpls traffic-eng router-id loopback0` et avec `(router) mpls traffic-eng area 0`
 - c. Pour chaque interface où on souhaite réserver des tunnels TE :
 - `(config-if) mpls ip`
 - `(config-if) mpls traffic-eng tunnels`
 - `(config-if) ip rsvp bandwidth 512`
 - d. Déclarez tous les tunnels :
 - `(config) interface tunnel nb`
 - `(config-if) ip unnumbered Loopback0`
 - `(config-if) tunnel destination IP@`
 - `(config-if) tunnel mode mpls traffic-eng`
 - `(config-if) tunnel mpls traffic-eng bandwidth 256`
 - `(config-if) tunnel mpls traffic-eng autoroute announce`
 - `(config-if) tunnel mpls traffic-eng path-option 1 explicit name tunnel-un`
 - `(config) ip explicit-path name tunnel-un`
 - Pour chaque saut: `(explicit-path-configuration) next-address IP@`

6. Travail à rendre

A la fin des séances de ce TD, vous rendrez un rapport de TD par binôme, au format PDF, que vous enverrez par e-mail à votre chargé de TD. Ce rapport contiendra les réponses aux questions posées dans ce sujet en y incluant tous les justificatifs nécessaires :

- Extraits pertinents des `running-configuration` des routeurs ou listings des commandes IOS utilisées pour résoudre les questions
- Extraits des tables de routage intra- (`sh ip ro`) et inter- (`sh ip bgp`) domaines et des tables de commutation (`sh mpls`) pertinentes
- Extraits pertinents des captures de trames prises par `wireshark`
- Sorties des commandes `ping` et `traceroute`

7. Références

Ce TD est dérivé des sujets de J-J. Pansiot.