Mini Projet : VPN BGP-MPLS

Ce projet est à réaliser en binôme et à rendre le 21/5/2023 au plus tard sur le dépôt Moodle prévu à cet effet.

Avant de commencer

Présentation générale du Projet

La figure 1 décrit l'environnement dans lequel vous travaillerez : il n'y aura pas de configurations inter-domaines à proprement parler (du moins pour la partie obligatoire du projet), c'est à dire pas à large échelle entre les différents groupes (vos binômes), mais seulement à une échelle relativement locale (intra groupe/binôme), c'est à dire que votre domaine principal (constitué de vos PE et P) interconnecte les six sous-réseaux de la figure (matérialisés par autant de CE et leur VPN respectif).

L'objectif principal de ce TP / mini-projet est d'inter-connecter les différents sous-sites, au moyen de VPN-BGP MPLS, avec un espace d'adressage privé (attention de ne pas rentrer en conflit avec les autres domaines si vous voulez atteindre la dernière question facultative) et re-utilisé pour les deux VPN. Votre domaine, son routage interne, et ses liens avec les CE sont déjà pré-configurés ; en revanche les liens CE avec leur hôte sont laissés à vos soins ainsi que toute la configuration plus avancée (MPLS, session iBGP et routage des adresses privées sur le CE – avec leur hôte ou avec des loopback locales).

Pour atteindre les configurations souhaitées vous devrez expérimenter deux pistes : en full-mesh et en hub & spoke. En option finale, vous pourrez essayer de connecter vos hubs et leurs clients à l'Internet...

La suite de l'énoncé vous guide étape par étape à cette fin. En premier lieu, vérifiez la connectivité interne entre les CE, P et PE du domaine principal puis définissez des protocoles/options de routage distincts entre les CE et leur PE pour annoncer les adresses privées que vous configurerez entre les CE et leurs hôtes (ou aussi en ajoutant des loopback privées à vos CE).

Modalités de rendu

En plus de l'ensemble des fichiers de configurations, nous vous demandons un rapport soigné et au format PDF (10 pages au maximum hors annexes de configurations). Celui-ci contiendra les explications (de vos configurations et tests ainsi que leurs interprétations) et réponses à chacune des questions de l'énoncé.

Ainsi, merci de nous fournir, avant la date limite, dans le dépôt Moodle prévu à cet effet :

- Les configurations de tous les routeurs de votre domaine sous forme d'une archive ;
- Un document PDF résumant votre compréhension du sujet, généralement et pour chaque question, la manière dont vous avez choisi de deployer la solution demandée (en justifiant vos choix), et des captures d'écran, de texte si possible, décrivant l'effet de vos (blocs de) commandes (avant/après).

On rappelle que les configurations peuvent être récupérées à l'aide de la commande `save_configs.sh` suivie d'un `scp`.

Pour comprendre l'état de connectivité de votre réseau (plan de contrôle), veillez à utiliser les looking glasses pour les aspects inter-domaines et surtout contrôler les tables de routage (notamment les virtuelles) plutôt que de vous limiter à la matrice (vue partielle et souvent avantageuse du plan de données inter-domaine, et surtout quasi hors sujet pour ce projet). Enfin, pour aussi tester le plan de données, vous effectuerez des tests avec `nping` (avec TCP) et `traceroute` (et/ou ping avec `route-record`) notamment depuis les stations de PE1 et PE6 jusqu'à PE3 et son hôte, d'abord en intra-domaine puis en inter-domaine et commenterez les résultats obtenus (à relancer plusieurs fois).

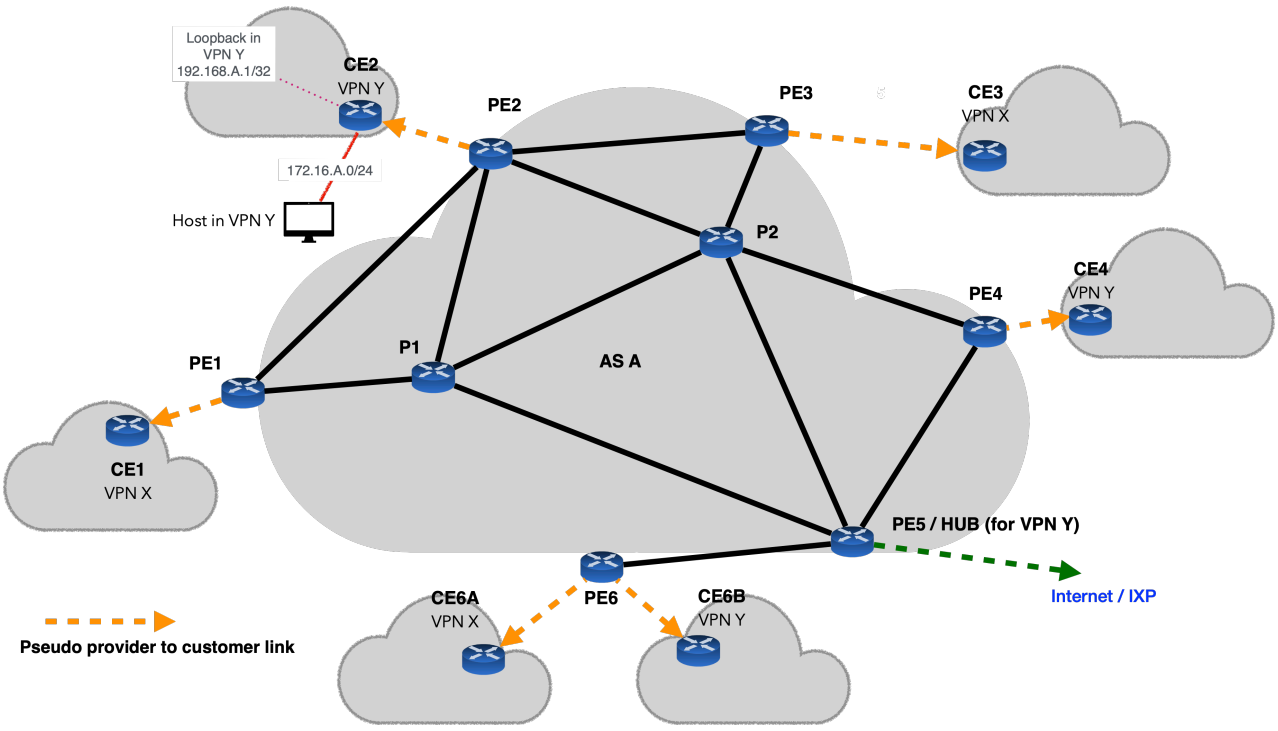

FIGURE 1 – La structure interne de votre domaine et ses voisins feuilles

Sujet : VPN IP au niveau opérateur

Finalisez le plan d'adressage de votre réseau en allouant des préfixes privées entre les CE et leurs hôtes. N'oubliez pas de définir les interactions entre les CE et leur PE : comment les PE vont apprendre les préfixes privées des CE ? Utilisez au moins trois méthodes distinctes pour le VPN X !

Question 1

Commencez par vous occuper du VPN X en full-mesh : déployez des VRF avec un RD arbitraire dans les PE concernés et activez MPLS dans l'ensemble du réseau. Définissez une RT commune entre les PE.

1. Que constatez vous ? Expliquez le rôle de BGP et de MPLS dans le fonctionnement global ;
2. Testez et expérimentez le plan de contrôle comme le plan de données (prenez soin de prendre garde à ECMP si besoin) ;
3. Montrez les effets de l'ajout d'un nouveau préfixe IP privé dans ce VPN depuis le CE de votre choix (pour cela ajoutez lui une loopback).

Question 2

Faites en de même pour le VPN Y mais en hub & spoke, avec PE5 en hub. Contrairement à la Q1, votre RT sera adaptée à chaque rôle et le hub devra relayer la signalisation iBGP.

1. Trouvez plusieurs moyens pour configurer cette solution (au moins deux). Que constatez vous dans chaque cas ?
2. Testez et expérimentez le plan de contrôle comme le plan de données.
3. Appliquez des filtres/politiques sur le hub.

Question 3

Faculctatif : Connectez votre hub à l'IXP 81 pour offrir une connexion Internet au VPN Y. Démontrez la connectivité de ses sites malgré l'utilisation d'un espace d'adressage privée.