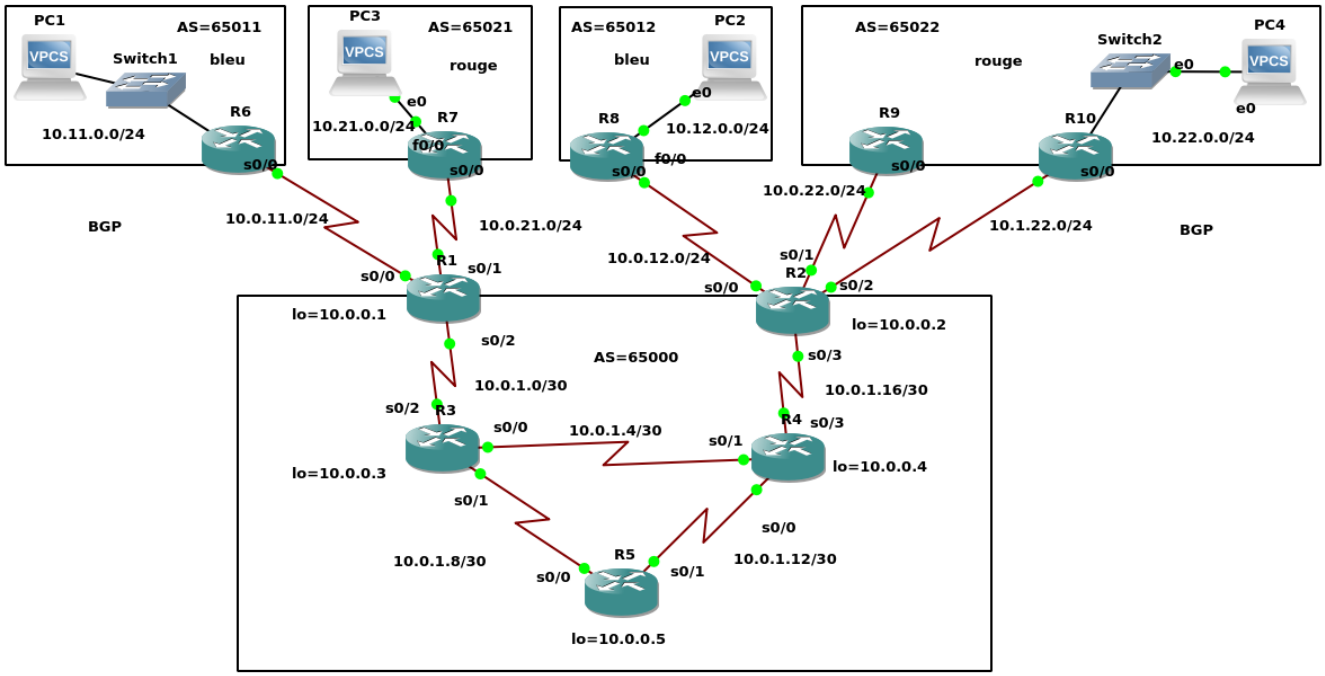
TP – MPLS – VPN et MP-BGP

Objectifs

Mettre en place les réseaux privés de 2 entreprises situées sur 2 sites différents. Pour cela, il faut cloisonner l'adressage IP de chaque client pour empêcher l'accès d'un PC d'une entreprise vers l'autre. Le principe VRF sera mis en place pour séparer les réseaux des 2 entreprises puis le système de tunnel MPLS/VPN sera mis en place pour garantir le lien entre les différents sites d'une même entreprise.
Connectez-vous avec les droits root pour permettre l'utilisation de wireshark.

1ère Réalisation – Activation OSPF/MPLS entre R1-R2-R3-R4-R5



https://www.cisco.com/c/en/us/support/docs/multiprotocol-label-switching-mpls/mpls/13733-mpls-vpn-basic.html

La configuration IP est indiquée sur le schéma ci-dessus.

Dans un premier temps vous ne réalisez qu'une configuration IP/OSPF/MPLS.

Vérification
Vérifiez à l'aide la commande ping que chaque liaison permet un échange IP avec chaque voisin direct.
Ensuite, vérifiez les liste de vos routeurs OSPF voisins : show ip ospf neighbors
Finalement, vérifiez que votre liste de préfixes est complète dans la table de routage : show ip route

2ème Réalisation – Adressage et cloisonnement avec VRF

Ajoutez le cloisonnement entre les 2 entreprises ROUGE et BLEU avec VRF, ainsi que l'adressage IP associé.

Vérification
Vérifiez à l'aide la commande ping que chaque liaison permet un échange IP avec chaque voisin direct.
Vérifiez également que les tables de routage depuis R1 sont différentes :
show ip route
show ip route vrf bleu
show ip route vrf rouge

3ème Réalisation – BGP et MP-BGP

Activez BGP sur les routeurs R6-R7-R8-R9-R10
et MP-BGP sur les routeurs R1 et R2 avec vpnv4 et vrf pour relier les 2 sites de chaque couleur

Vérification
Vérifiez que les tables de routage sont bien séparées entre R6 et R7
Vérifiez que le protocole BGP est complet : show bgp all summary
Vérifiez que les tables de routage sont complètes entre R1 et R2 sur les 3 domaines (opérateur, bleu, rouge)

4ème Réalisation – Tunnels avec ingénierie de trafic

Vérifiez les chemins entre PC1-PC2, PC2-PC1, PC3-PC4, PC4-PC3 et PC1-PC3 et relevez les chemins.

PC1-PC2 :
PC2-PC1 :

PC3-PC4 :
PC4-PC3 :

PC1-PC3 :
PC3-PC1 :

Activez 1 tunnel explicite de R1 vers R2 passant par R5.
Vérifiez à nouveau les chemins entre PC1-PC2, PC3-PC4 et PC1-PC3 et relevez les chemins.

PC1-PC2 :
PC2-PC1 :

PC3-PC4 :
PC4-PC3 :

PC1-PC3 :
PC3-PC1 :

Activez un deuxième tunnel explicite de R1 vers R2 sans passer par R5 pour répartir la charge entre les 2 chemins.
Vérifiez à nouveau les chemins entre PC1-PC2, PC3-PC4 et PC1-PC3 et relevez les chemins.

PC1-PC2 :
PC2-PC1 :

PC3-PC4 :
PC4-PC3 :

PC1-PC3 :
PC3-PC1 :

Interceptez le trafic sur R5 avec Wireshark et indiquez le type des paquets ICMP passants et le nombre d'en-tête MPLS devant IP.

Même question avec une interception sur l'interface s0/0 de R3.