

SAé- Réseau Multi-sites

I. Introduction

Vous êtes un intégrateur réseau et vous avez été retenu pour l'appel d'offre "Etude et fourniture de l'architecture de deux entreprises dans l'e-commerce : UC Exchange et ABC Conseil.

Suite à de nombreuses discussions avec les directeurs et leurs services informatiques, vous avez maintenant une bonne vision du travail à fournir. Vous avez déjà appris beaucoup de choses et vous êtes bientôt prêt à réaliser une maquette fonctionnelle.

Les deux entreprises sont présentes dans l'Est de la France : Strasbourg, Nancy et Metz.

Toutes les succursales ont le même gabarit :

- Le siège social comptera 4 services : service informatique, la direction, service financier et salle des serveurs (DNS, DHCP, Web/DNS secondaire, mail, AD)
- Les autres sites compteront 4 services dont une la salle des serveurs (DHCP, AD)
- Tous les sites doivent être équipés informatiquement
- L'adressage IP LAN fourni est le suivant :
 - o UC exchange : 10.242.xy.0/17
 - o ABC Conseil : 10.252.xy.0/18

Où "x" représente le numéro du site et "y" le numéro de Vlan dans le site "x"

- Chaque site est abonné à deux fournisseurs d'accès afin d'assurer la haute disponibilité entre leurs sites.
- Les plages d'adressage dynamique sont uniquement affectées aux machines. Les serveurs, les switch/routeurs doivent avoir des adresses statiques.

Pour mieux gérer le projet de manière efficace et valider les différents process, vous décomposez votre projet en trois parties :

- Administration des réseaux LANs.
- Mise en œuvre des services réseaux.
- Interconnexion des sites de chaque entreprise.

En termes d'équipements, vous aurez à votre disposition 3 PC ainsi qu'un retour et un commutateur.

- Le PC1 sera consacré à la mise en place de la maquette LAN (EVE-NG) de l'entreprise UC Exchange.
- Le PC2 sera consacré à la mise en place de la maquette du FAI sur EVE-NG.
- Le PC3 sera consacré à la mise en place de l'ensemble des services réseaux de l'entreprise UC Exchange.

II. Administration des réseaux LANs

Pour rendre le réseau opérationnel, les demandes des deux entreprises doivent être prises en compte, à savoir :

- Chaque site possède une architecture commutée hiérarchique, les routeurs seront utilisés que pour assurer la haute disponibilité.

- Pour assurer une communication permanente, des liens redondants entre les commutateurs doivent être opérationnels. Vous êtes amenés à proposer une solution qui permet d'assurer une communication tolérante aux pannes matériels.
- Le protocole de Spanning-Tree doit être opérationnel, les deux entreprises souhaitent utiliser le protocole Multi Spanning Tree (**MST**) comme solution.
- Les **VLANs** sont créés suivants les services et doivent respecter l'adresse IP globale du site
- Le routage **inter-vlans** doit être opérationnel
- La communication vers l'extérieur doit être **NATée**, le mécanisme **PAT** sera mis en œuvre.
- La haute disponibilité doit être activée, le choix s'est porté sur le protocole **VRRP**

Travail demandé :

Vous devez proposer une maquette qui prend en compte les contraintes des deux entreprises. Vous proposez un plan d'adressage de chaque site.

Rapport :

Proposez une architecture des sites, avec un plan d'adressage bien détaillé et argumenté. Intégrez les configurations (que des équipements les plus importants)

Avoir des captures d'écran pour les différents tests avec des commentaires

III. Mises en œuvre des services réseaux

Les deux entreprises souhaitent déployer leur propre service **DNS**, serveur **web Apache** et leur serveur **mail**. Elles demandent à ce que ces services soient déployés dans la salle des serveurs. Le serveur DNS primaire sera sous **Windows Server 2019**, tandis que les autres seront sous **Linux**, avec la distribution de votre choix **mais uniquement en ligne de commandes** (la présence d'un gestionnaire graphique sera vérifiée).

1) Service DNS

Chaque entreprise gère le domaine portant son nom, sans majuscule et sans espace et terminera pour un .com. Par exemple, l'entreprise UC Exchange aura comme nom de domaine **ucexchange.com**. Chaque domaine sera géré par un serveur nommé **ns** et l'adresse mail de l'administrateur sera **"admin@nom" de domaine**. Sur ce serveur uniquement le trafic DNS est autorisé. Un serveur DNS secondaire devra également être déployé sur un serveur distinct qui aura comme nom **ns2.mondomaine**. **Les échanges liés au transfert de zone devront être chiffrés avec DNSSEC pour les étudiants en FI et laissés en clair pour les FA.** Il sera possible d'accéder en SSH au second serveur, mais uniquement les machines qui ont le même masque réseau pourront s'y connecter, les autres se verront refuser l'accès avec comme retour un message TCP reset afin de partiellement tromper les logiciels de scan de port.

2) Service Web

Un service web devra être déployé sur le même serveur que le DNS secondaire. Ce serveur devra héberger deux sites web, un lié à l'intranet et donc accessible uniquement aux clients de l'entreprise, un second disponible pour les machines extérieures. Le serveur web aura pour nom : **"www.nom de domaine"**. Il conviendra également d'ajouter le trafic HTTP comme trafic autorisé. L'objectif étant de valider le concept, une page web simple vous sera demandé comme preuve du bon fonctionnement.

3) Service Mail

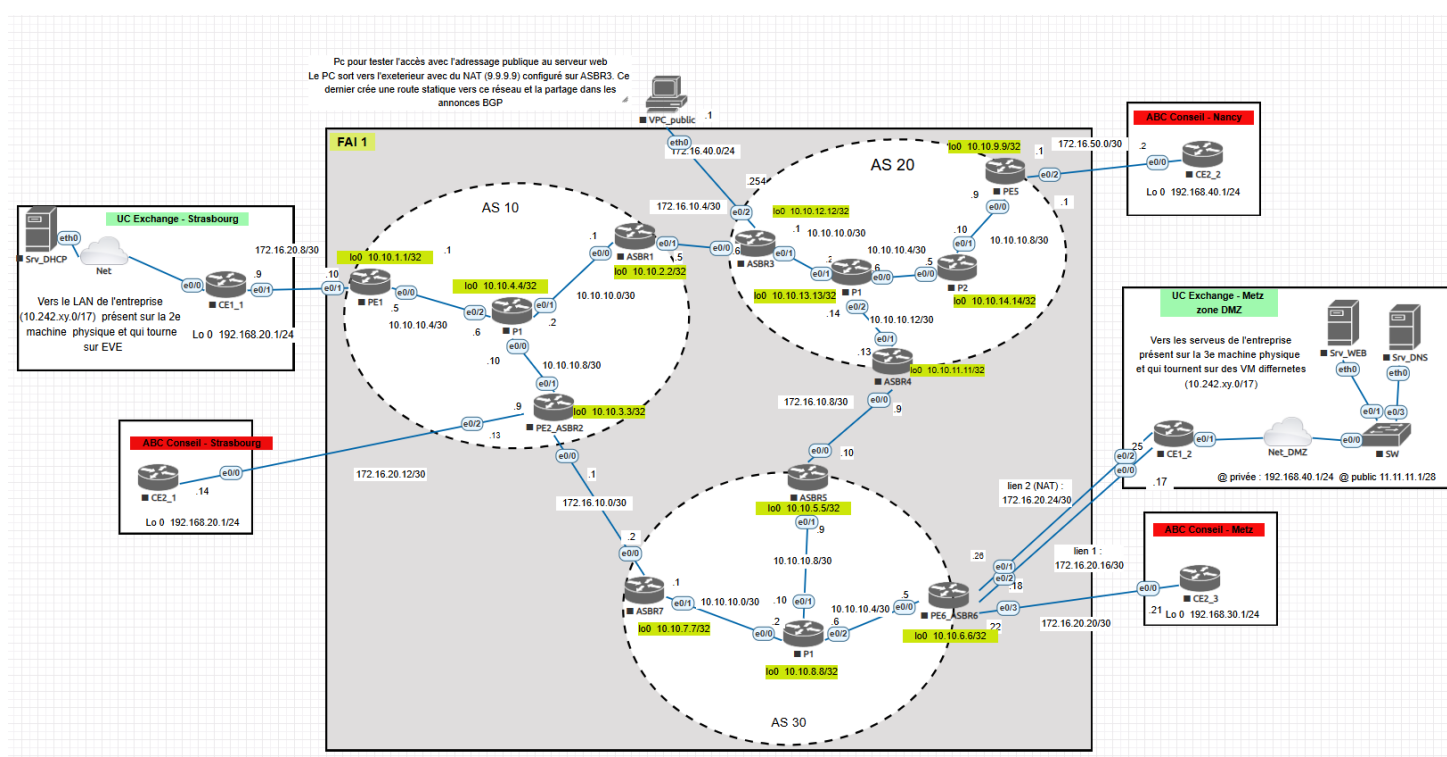
Un service mail devra être fourni en déployant sur le serveur DNS secondaire/ Web, un service **SMTP** ainsi qu'un service **IMAP**. Vous devrez créer un compte admin et un compte client afin que chacun possède une boîte mail. Vous pourrez tester votre configuration en utilisant un poste dans le réseau et en vous connectant au serveur SMTP via TELNET puis en utilisant les commandes SMTP. Il conviendra d'ajouter le trafic SMTP et IMAP comme autorisés.

4) Service Active Directory (Activité Bonus et uniquement disponible pour les FI)

Il vous a été demandé de déployer le service Active Directory sur le serveur Windows. Il vous sera demandé d'utiliser le même service DNS, afin d'utiliser le domaine déjà établi. Afin de tester le bon fonctionnement, ajouter un utilisateur dans le domaine et connectez-vous depuis un PC Windows.

IV. Interconnexion des sites de chaque entreprise

La maquette pour le réseau du FAI est la suivante :



Cette maquette représente :

- La structure du cœur réseau du **FAI**, (partie en gris) composée de trois AS.
- Le client **ABC conseil** se trouvant sur trois sites géographiques (Strasbourg, Nancy et Metz). Ce client est présent uniquement virtuellement sur votre VM EVE-NG.
- Le client **UC Exchange** présent sur vos deux autres machines (**PC1**, **PC3**) et les routeurs ainsi que les interconnexions cloud vers ce client depuis la VM EVE-NG (**PC2**).

Ces deux clients sollicitent du FAI une connectivité entre leurs différents sites respectifs grâce à l'offre **MPLS-VPN**. Votre travail sera de réaliser cette maquette en respectant le cahier de charge suivant :

1. Le FAI à configurer s'étale sur trois AS (système autonome). La composition de chaque AS ainsi que le plan d'adressage utilisé est indiqué sur le schéma ci-dessus.
2. Configurer les @IP des interfaces physiques ainsi que des loopbacks.
3. Renommer chaque équipement avec le nom désigné sur la maquette.
4. Configurer le routage **RIP** pour l'**AS 10** et **20** et **OSPF** pour l'**AS 30**
5. Assurer la connectivité totale au sein de chaque AS.
6. Pour chaque AS créer des sessions **BGP** et **MP-BGP** afin de transférer les préfixes **ipv4** et **vpn4**. Afin d'éviter de créer des sessions entre chaque paire de routeur dans l'AS, vous allez utiliser la configuration avec la méthode **Route-Reflector (RR)**. Ainsi dans chaque AS le routeur **P1** jouera le rôle de **RR** et les autres seront des clients.
7. Les sessions BGP doivent être montées en utilisant la configuration en **peer-group**.
8. Monter les sessions **BGP** et **MP-BGP** nécessaires pour assurer la communication **inter-AS**. Les routeurs concernés sont les **ASBR** (AS border router).
9. Afin de transmettre les routes **vpn4** entre les AS, il est nécessaire d'activer la commande "**no bgp default route-target filter**" au niveau des ASBR afin que ces derniers acceptent les routes **vpn4** sans pour autant configurer des **VRF** dessus.
10. Le nom des clients à utiliser pour les **VRF** est celui indiqué dans la maquette (ABC_conseil et UC_Exchange)
 - a. Le RD et RT pour le client ABC conseil est **10:1**
 - b. Le RD et RT pour le client UC Exchange est **10:2**
11. Au niveau des routeur concernés, créer les **VRF** nécessaires afin d'assurer la communication avec les CE. Le routage entre les CE et PE est assuré par :
 - a. Routage **statique** pour le client **UC Exchange**
 - b. Routage **RIP** pour le client **ABC conseil**
12. Vous faite en sorte que seul les préfixes des clients transitent dans les sessions MP-BGP. Ainsi les préfixes d'interconnexion ne sont pas autorisés à circuler d'un site à un autre.

Test de fonctionnement :

Pour vérifier que votre configuration fonctionne bien, effectuer la batterie des tests suivants qui doivent passer sans problème :

1. Les pings à l'intérieur de chaque AS vers les loopback de chaque routeur composant l'AS.
2. Le ping entre les routeurs des trois sites de l'entreprise ABC conseil.
3. Arrêter l'interface e0/0 du PE2_ASBR2 et vérifier le ping depuis le CE2_1 vers les deux autres sites. Puis remettez l'interface en état de marche puis faire le même test en arrêtant l'interface e0/0 du ASBR4. L'objectif est de vérifier que la redondance mise en place fonctionne.

Pour les parcours FI

L'entreprise **UC Exchange** demande au FAI un 2e service. En effet, en plus d'accès **MPLS-VPN** à son serveur web se trouvant sur le site de Metz, l'entreprise a besoin d'exposer se même serveur au grand public grâce à une translation **NAT**. L'adresse publique à utiliser est marquée sur la maquette. Pour simplifier la tâche, on suppose que le fournisseur fournit deux liaisons réseaux au **CE** du site **Metz** pour assurer les services demandés : un pour la connexion MPLS-VPN et l'autre pour le NAT.

1. Le **VPC_public** représente un client lambda qui accède aux différents services se trouvant sur Internet, et entre autres, les services dont votre FAI assure la connectivité. Pour cela la machine VPC_public possède l'adresse publique **9.9.9.9** grâce à une translation assurée par le routeur ASBR3.
2. Le FAI décide que tout flux du client **UC Exchange** entre ces deux sites doit forcément passer via l'AS 20. Appliquer le filtrage BGP nécessaire permettant de réaliser cela.
3. L'entreprise **ABC Conseil** décide que son siège social soit sur Strasbourg et que l'accès VPN ne soit autorisé que depuis le siège vers les autres sites et jamais entre les différents sites. Décrivez puis mettez en place la configuration à réaliser pour assurer ce besoin.

Test de fonctionnement :

Pour vérifier que votre configuration fonctionne bien, effectuer la batterie des tests suivants :

1. Le VPC_public doit pouvoir effectuer un ping vers l'adresse IP publique du serveur 11.11.11.1.
2. Arrêter l'interface e0/0 du PE2_ASBR2 et vérifier que le ping depuis le VPC_public vers 11.11.11.1 passe ainsi que le ping depuis CE2_1 vers les deux autres sites. Puis remettez l'interface en état de marche puis faire le même test en arrêtant l'interface e0/0 du ASBR4. L'objectif est de vérifier que la redondance mise en place fonctionne.
3. Un traceroute depuis un poste de **UC Exchange** depuis Strasbourg vers un poste sur Metz doit montrer le trafic passe par l'AS 20.
4. La communication entre les sites de Metz et Nancy pour le client **ABC Conseil** ne doit pas être possible.