Table des matières

Part I
Mise en place d'un réseau d'entreprise : Conception

Part II
Mise en place d'un réseau d'entreprise : Réalisation

Liste des figures

Liste des tables

Part I
Mise en place d'un réseau d'entreprise : Conception

I.1 - Introduction

Dans ce chapitre, on va s'intéresser à la conception d'un réseau d'entreprise étendu. On va présenter ce dernier d'une manière architecturale, avant de détailler les différentes parties qui le composent. Ensuite, on va passer à l'étude des protocoles sous-jacents, les détails techniques les concernant ainsi que leurs sécurisation. A la fin, on va présenter le processus de planification de l'adressage qui va être respecté durant toutes les étapes du travail.

I.2 - Design et choix de l'architecture

Le réseau de l'entreprise est un réseau privé étendu (Wide Area Network), décomposé principalement en cinq réseaux locaux (LAN) comme suit :

- Deux Sites (Site1 et Site2)
- Deux succursale (Branch1 et Branch2)
- Un Compus.

I.2.1 - Présentation des Sites

Chacun des deux Sites est présenté avec une architecture composée de trois couches :

- Couche d'accès au réseau (Access Layer) : contient principalement des serveurs, permettant ainsi l'exploitation de leurs services respectifs.
- Couche de distribution (Distribution Layer) : composée de commutateurs de couche 2 (Switchs) et de commutateurs de couche 3 (Multilayer Switchs). Cette couche permet d'assurer la connectivité entre les serveurs de la couche précédente.
- Couche coeur (Core Layer) : composée des Routers, cette dernière a pour but d'assurer la connectivité du Site avec les autres réseau locaux (LANs) appartenant au même réseaux étendu de l'entreprise (WAN).

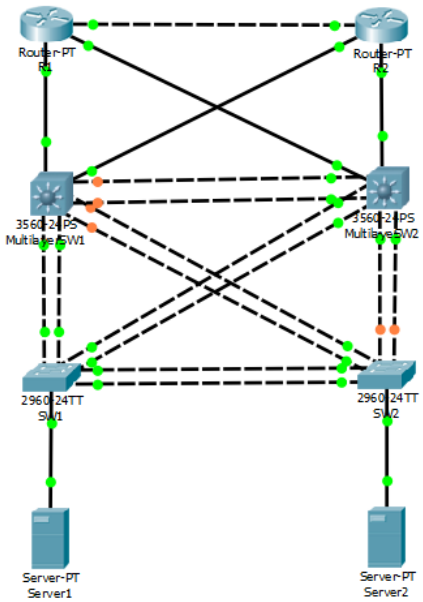

Figure I.1 – Architecture d'un Site

I.2.2 - Présentation des succursales (Branch Offices)

Chacune des deux succursales est présentée avec une architecture simple, composée de deux couches :

- Couche d'accès au réseau (Access Layer) : contient un commutateur de couche 2 (Switch) permettant aux utilisateurs de se connecter au réseau local de la succursale.
- Couche distribution-coeur (Collapsed-Core Layer) : contient un router jouant le rôle d'une passerelle (Gateway) et permettant la connectivité des utilisateurs internes avec le reste du réseau étendu.

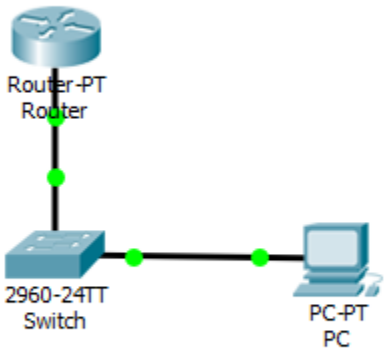

Figure I.2 – Architecture d'une succursale

I.2.3 - Présentation du Compus.

Le Compus est architecturalement décomposé en 3 couches :

- Couche d'accès au réseau (Access Layer) : présenté par six commutateurs de couche 2 (Switchs), ces derniers représentent les différents départements du Compus.
- Couche de distribution (Distribution Layer) : présenté par 2 commutateurs de couche 3 (Multilayer Switchs), ces derniers permettent la connectivité, et la gestion du trafic issu des différents départements du Compus.
- Couche cœur (Core Layer) : présenté par un router, permettant au utilisateurs internes du Compus de se connecter avec le reste du réseau étendu.

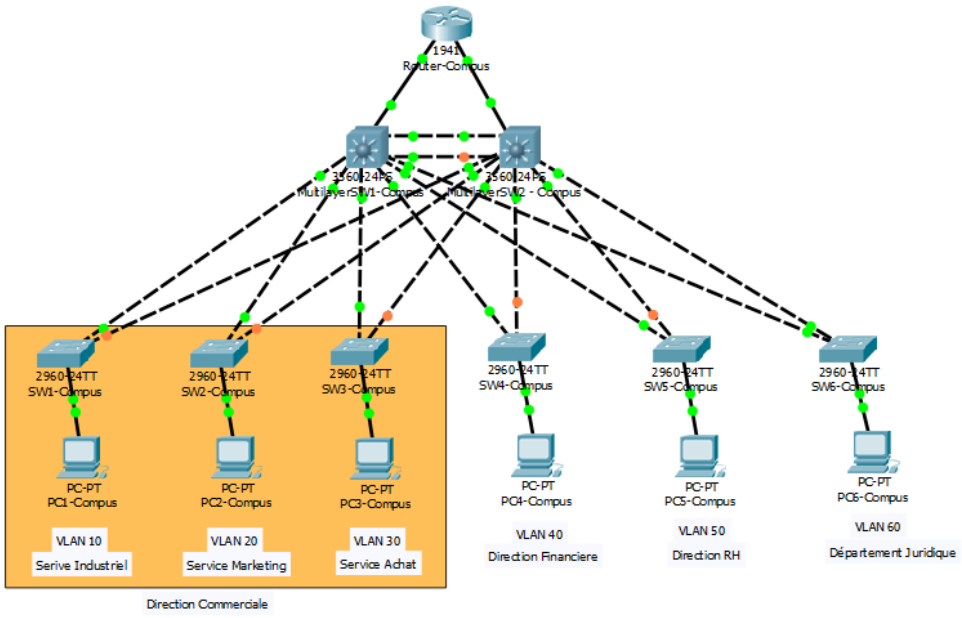

Figure I.3 – Architecture du Compus

I.2.4 - Interconnexion de l'architecture

L'architecture WAN est le résultat de l'interconnexion des différents Routers cœur des deux Sites, des deux succursale et du Compus. Les liaisons entre ces Routers sont effectuées en utilisant sept câbles série (WAN Serial) comme le montre la figure suivante.

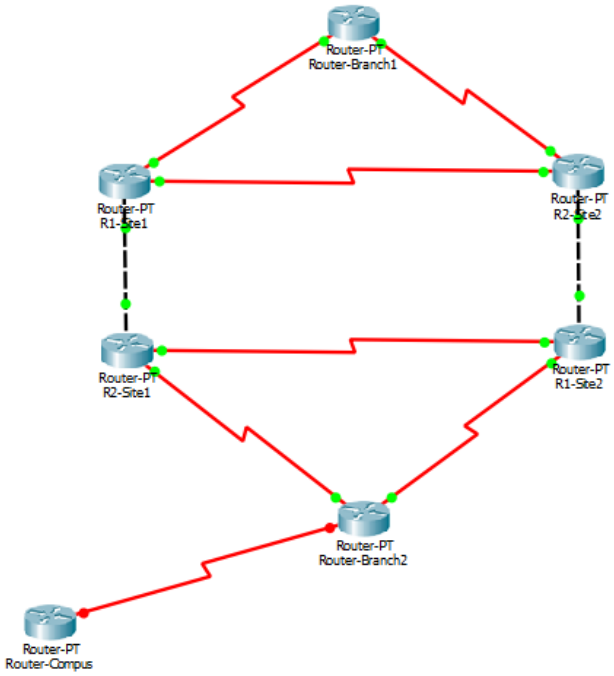

Figure I.4 – Interconnexion WAN

A la fin, on peut présenté l'architecture globale du réseau d'entreprise comme suit.

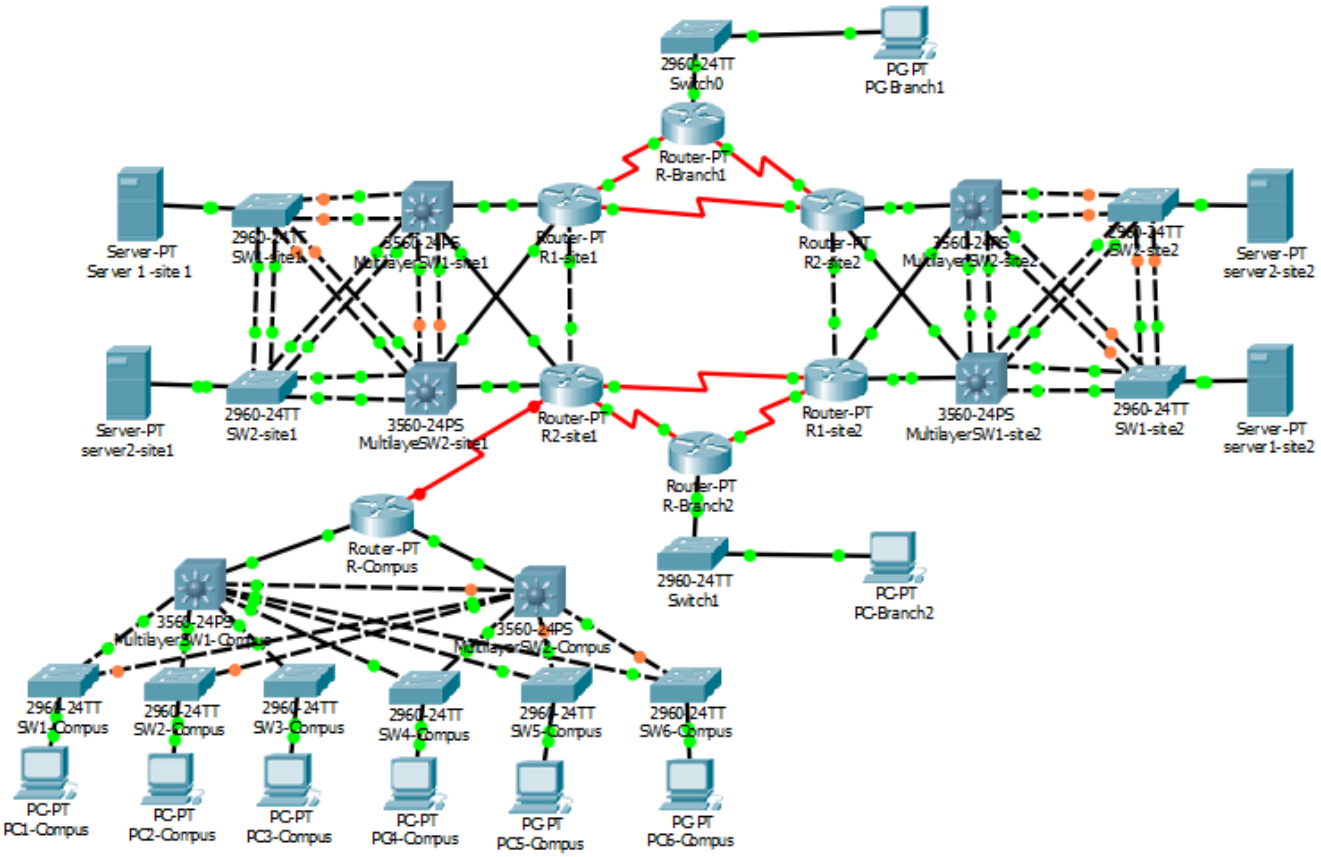

Figure I.5 – Architecture globale du réseau de l'entreprise

I.3 - Protocoles à mettre en place

I.3.1 - Protocoles exploités par les Sites

I.3.1.1 - Manipulation des VLANs

Les serveurs Server1 et Server2 d'un même Site appartiennent à deux VLANs différents; VLAN 10 et VLAN 20 respectivement.
L'intérêt des VLANs est :

- Optimisation la bande passante et amélioration de la gestion du réseau
- Séparation des flux des différents services fournis par les deux serveurs et amélioration de la sécurité.

La création des VLAN se fait dans chacun des quatre commutateurs de chaque Site.

I.3.1.2 - STP (PVST)

Pour assurer une fiabilité et une disponibilité au niveau des deux couches d'accès et de distribution, les liens entre les différents commutateurs sont multipliés (dupliqués).
L'inconvénient de cette procédure est qu'elle implique des bouclages de couche 2, provoquant ainsi des tempêtes de diffusion et une instabilité des tables MAC.

Comme solution, on utilise le protocole STP (Per Vlan Spanning-Tree), ce dernier construit des arborescences pour chaque VLAN, où les feuilles de ces arborescences sont des commutateurs; autrement dit, il supprime (logiquement) tout les liens redondants entre n'importe quels deux commutateurs.
Le concept Portfast est configuré dans les ports en mode Access, leurs permettant ainsi de s'attribuer leurs états rapidement d'un coté, et d'empêcher toutes trames malveillantes d'infecter le processus STP de l'autre.

I.3.1.3 – Etherchannel

Pour des raisons de performance, de disponibilité et de fiabilité, les liaisons entre les commutateurs sont dupliquées.
Vu que le protocole STP déjà configuré bloque les liens redondants, et pour pouvoir bénéficier de ces derniers, l'utilisation du protocole Etherchannel est recommandée.
Dans chaque Site, on créé six liens Etherchannel, qui sont organisés comme le montre la figure suivante.

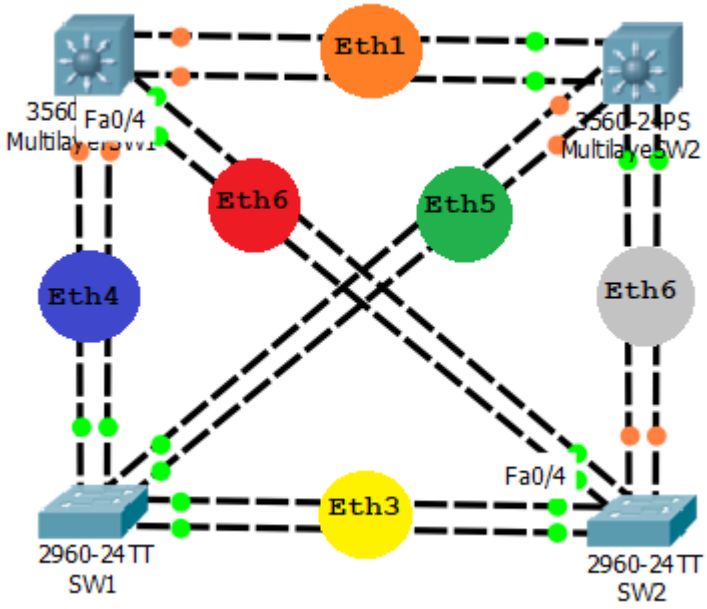

Figure I.6 – Application du protocole Etherchannel sur les liens redondants

I.3.1.4 - Routage Inter-VLAN

Pour permettre une connectivité inter-serveurs, le routage inter-VLANs est nécessaire. Ce dernier est effectué au niveau des Multilayer Switchs qui jouent les rôles de passerelles pour leurs VLANs respectifs.
Pour le Site1, le premier Multilayer Switch joue le rôle de passerelle pour le VLAN 10. Le second Multilayer Switch joue le rôle de passerelle pour le VLAN 20.
Pour le Site2, le premier Multilayer Switch joue le rôle de passerelle pour le VLAN 30. Le second Multilayer Switch joue le rôle de passerelle pour le VLAN 40.

I.3.1.5 - EIGRP

Pour assurer le routage entre les périphériques de la couche distribution et de la couche coeur, on utilise un protocole de routage dynamique qui est l'EIGRP (Enhanced Interior Gateway Routing Protocol). Pour cela, il faut que tout les réseaux en question appartiennent au même systèmes autonome qu'on le précise par la valeur 1.
Le protocole EIGRP est un protocole multi-metric, on prend les valeurs par défaut pour chaque facteur de sa metric..

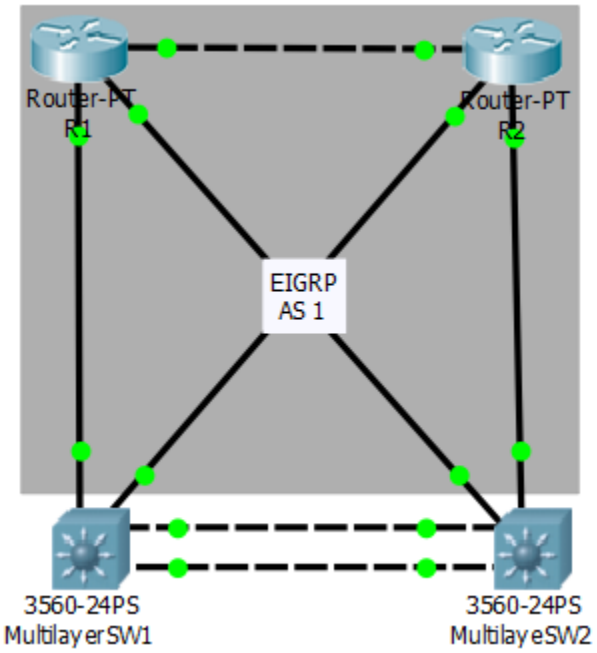

Figure I.7 – Routage Intra-Site avec EIGRP

I.3.2 - Protocoles exploités par le Compus

I.3.2.1 - Manipulation des VLANs

Au total, le Compus possède six VLANs. L'intérêt des VLANs est de séparer les trafics des différents départements organisés éventuellement dans les différents étages du Compus. La création des VLAN se fait seulement dans les Multilayer Switch.

I.3.2.2 - VTP

Pour que le reste des Switchs aient les informations nécessaires concernant les VLANs dans le Compus, on exploite le protocole VTP (VLAN Trunking Protocol), ce dernier permet de minimiser les charges administratives et éviter les erreurs liées à la configuration des VLANs.
En premier, on configure les deux Multilayer Switchs comme des serveurs VTP en précisant un domaine nommé Compus et un mot de passe lié à ce domaine : Compus.
Ensuite, on configure tout les autres Switchs de couche 2 en mode VTP client en les affectant au même domaine que le serveurs, et en leurs précisant le même mot de passe.
Une fois terminé, les serveurs VTP pourrons informer les clients VTP de tout ajouts, modifications ou suppressions concernant les VLANs du Compus.

I.3.2.3 - STP (PVST)

Pour assurer une fiabilité et une disponibilité au niveau des deux couches d'accès et de distribution, chaque Switch couche 2 est lié avec les deux Multilayer Switchs.
Ces doubles liaisons impliquent des bouclage de couche 2, provoquant ainsi une instabilité des tables MAC et des tempêtes de diffusion.
Comme solution, on utilise le protocole STP (Per VLAN Spanning-Tree), ce dernier construit des arborescences pour chaque VLAN, où les feuille de ces arborescence sont des commutateurs; autrement dis, il supprime (logiquement) tout les liens redondant entre n'importe quels deux commutateurs.

I.3.2.4 - Routage Inter-VLANs

Pour permettre une connectivité entre les différents département du Compus, le routage inter-VLANs est nécessaire. Ce dernier est effectué au niveau des Multilayer Switchs qui jouent les rôles de passerelles.
Le premier Multilayer Switch est la passerelle principale de tout les VLANs. Le second Multilayer Switch est une passerelle dupliquée qui prendra le relais en cas d'une défaillance de la passerelle initiale, et ceci dans le cadre du protocole HSRP expliqué dans le point suivant.

I.3.2.5 - HSRP

Pour des rasions de disponibilité , de fiabilité et de continuité de service de la passerelle par défaut des différents VLANs, on utilise le protocole HSRP (Hot Standby Router Protocol). Ce dernier consiste à configuré plusieurs périphériques (dans notre cas de Multilayer Switchs), qui vont partager la même fonctionnalité.
De plus leurs adresses réelles, les deux Multilayer Switchs partagent les mêmes adresses de passerelles des six VLAN, appelées adresses virtuelles. Ces dernières servent à identifier les groupes contenant les deux périphériques.
Donc, pour six VLAN , on créée six adresses virtuelles, donc six groupes HSRP.
On partage les rôles des deux Multilayer switch comme suit :

- Le premier Multilayer Switch, on lui affecte une priorité d'une valeur de 200. Le Multilayer Switch est dit actif
- Le second Multilayer Switch, on lui affecte une priorité d'une valeur de 100. Le Multilayer Switch est dit standby

Ainsi, en cas de problème survenu a la principale passerelle qui est le Multilayer Switch, la seconde passerelle (le Multilayer Switch 2) prendra le relais.

I.3.2.6 – Routage dans le Compus

Pour assurer une connectivité entre le Compus et le reste du réseau étendu, on a configuré une route par défaut 0.0.0.0/0 au niveau de chaque Multilayer Switch. Ces route par défaut menent vers le router du Compus.
Au niveau du Router, on a configuré deux route statique résumée. La première vers le réseau 10.0.0.0/8 via le premier Multilayer Switch, et la seconde vers le réseau 10.0.0.0/8 via le second Multilayer Switch. Ces routes ont les distancess administratives 253 et 254 respectivement.

I.3.2.7 - DHCP

Pour alléger la charge administrative, éviter les erreurs de configuration et pour une meilleur gestion de l'adressage dans le Compus, on opte pour le protocole DHCP (Dynamic Host Configuration Protocol), ce dernier est un protocole de distribution automatique d'adresses.
Les deux Multilayer Switchs sont configurés comme des serveur DHCP pour affecter les informations d'adressage aux périphériques appartenant six VLANs.

I.3.2.8 - Sécurisation du Compus

L'architecture du Compus mise en place est caractérisée par quelques points de défaillance résumés dans ce qui suit :

- Possibilité d'une connexion au réseau du Compus par des personnes tiers, impliquant ainsi un problème d'accès non autorisé.
- Possibilité d'attaque Rogue DHCP ou DHCP Spoofing impliquant ainsi un problème de saturation de service
- Possibilité de trafic inter-VLANs non autorisé, pouvant impliquer ainsi un problème de confidentialité.

I.3.2.8.1 - Port Security

Le protocole Port Security permet d'éviter les problèmes issus des accès non autorisés. Avec son approche réactive, une configuration Port Security permet d'éliminer les connectivités des périphériques qui n'appartiennent pas à une "liste" de périphériques légitimes configurés au préalable.
Pour cela, on configure le active Port Security sur tout les ports en mode Access au niveau des six Switchs du Compus. Permettant ainsi à ces premiers de s'éteindre (car configurés en mode Shutdown) dans le cas d'un branchement d'un périphérique non légitime.

I.3.2.8.2 - DHCP Snooping

L'attaque la plus fréquente dans une architecture DHCP, est celle du DHCP Spoofing. Cette dernière consiste à mettre en place des périphériques malicieux demandant en permanence des adresses IP aux serveurs DHCP installés. Après certaines demandes, les serveurs DHCP se trouvant dans l'incapacité de fournir de nouvelle adresses IP, et c'est là que le résultat de l'attaque aie lieu. Autrement

dis, un périphérique légitime demandant une adresse IP ne pourra pas en avoir une, et restera donc isolé du réseau du Compus.
Une autre attaque connu sous le nom de Rogue DHCP peut avoir lieu. Cette dernière est basée sur l'existance d'un périphérique attaquant à l'état Man In The Middle (homme du milieu) qui va en premier lieu intercepter les requêtes DHCP des clients. En second lieu, fournir des adresses IP erronées à ces mêmes clients DHCP.
DHCP Snooping est une technique implémentée dans le Compus afin d'éviter les conséquences issues du DHCP Spoofing et du Rogue DHCP. En effet ce premier consiste à configuré des ports sur les différents commutateurs du Compus (Switchs et Multilayer Switchs) en les prenant comme des ports de confiance (trusted); autrement dis, des ports dont leurs requêtes DHCP seront bien servis, ou leurs réponse DHCP seront autorisée à être utilisé. Toutes requêtes DHCP issue d'autre port sera immediatement ignorée.

I.3.2.8.3 - Dynamic ARP Inspection

Dynamic ARP Inspection (DAI) est un concept de sécurité qui valide les paquets ARP dans le réseau. DAI permet à l'administrateur réseau d'intercepter, valider ou bannir les paquets ARP avec une combinaison Adresse MAC-Adresse IP non valide. Cette technique protege le réseau du Compus de certaines attaques de l'homme du milieu (Man In The Middle).

I.3.2.8.4 - IP Source guard

IP Source Guard procures un filtrage des addresse IP source au niveau de la couche 2 des port pour empecher tout peropherique malicieux de proclamé une identité d'un prepherique legitime qui n'est pas la sienne. La technique crée implicitement une liste de controle d'access basé sur les ports.

I.3.2.8.5 - ACL

Pour empcher d'eventuel attaque interne d'une part, et limiter la consommation inutile de la bande passante d'une autre part. La configuration d'une liste de controle d'access (Access Control List) est donc necessaire.
On configure donc une ACL etendu ayant le role résumé dans les points suivant :

- Autoriser le traffic intra-direction commerciale. c'est a dire que tout traffic reliant les trois services Industriel, Marketing et Achat sera autorisé.
- Autorisé les traffic intra-VLAN. c'est a dire que tout traffic au sein de la meme direction, du meme service ou du meme département sera autorisé
- Autoriser le trafic 10.0.0.0/8 vers 172.16.0.0/16 et vers 192.168.0.0/16 et vice versa. Cela permet aux VLANs d'eter connectés avec le reste du réseau étendu.
- Interdire tout autre trafic

Remarque : Après avoir configuré l'ACL, certains services (tels que HSRP et DHCP) pourront être implicitement interdit, il est nécessaire d'ajouter des commandes pour les autoriser en fonction des protocoles de transport et des numéros de ports utilisés par leurs messages respectifs.

I.3.3 - Protocoles exploité par l'ensemble de l'architecture

Afin d'assurer la connectivité entre les différentes infrastructures du réseau (Sites, succursales et Compus), il est nécessaire de mettre en place un protocole de routage entre les liaisons WAN qui relient les Routers coeur de chaque LAN.

I.3.3.1 - OSPF Multi-Area

Le protocole Open Shortest Path First Multi-Area est le protocole choisit pour assurer le routage WAN. C'est un protocole à états de liens et permettant d'organiser l'ensemble des Routers sur des surfaces nommée Area pour des raisons d'économie des infrastructures du réseau.

- Les deux succursales Branch1 et Branch2 forment deux Areas séparées qui sont Area1 et Area2 respectivement .
- Le Compus forme l'Area 3.
- L'Area 0, quant à elle, est les liaisons reliant les quatre Routers issus des 2 Sites.

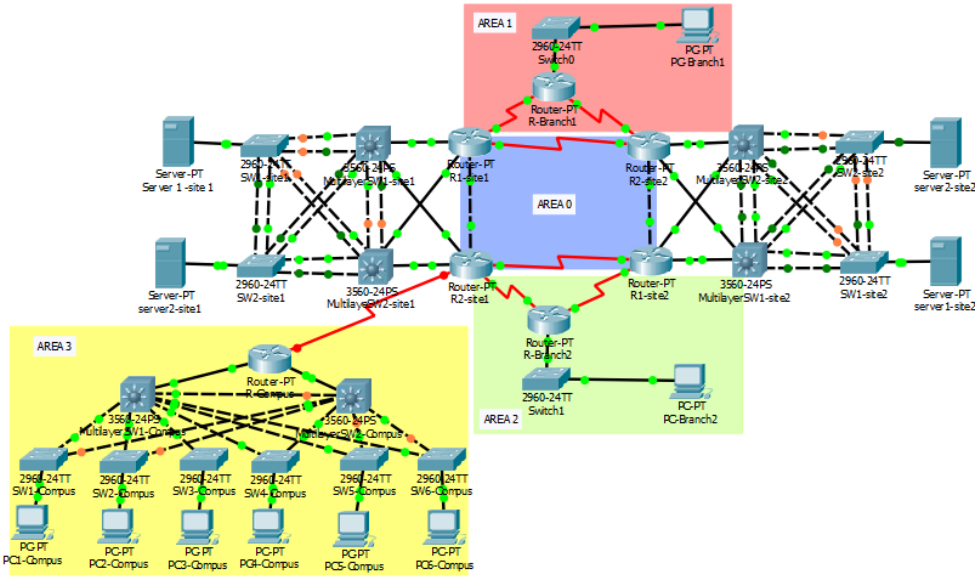

Figure I.8 – Organisation du routage OSPF Inter-AREAs

I.3.3.2 - Redistribution des routes

Vu l'utilisation de deux protocoles de routage dynamique différents (EIGRP et OSPF), il est nécessaire que ces deux derniers puissent s'échanger des informations de routage entre eux via leurs messages de mis à jour respectifs.
Le concept de redistribution de routes est utilisé; en effet, cela consiste à permettre à un Router ayant plusieurs interfaces configurées avec des protocoles de routage différents de faire échanger les informations de routage mutuellement entre ces derniers.
Concernant la redistribution des route OSPF dans le protocole de routage EIGRP, il est nécessaire de spécifié les metrics que ce dernier prendra en compte. Puisque EIGRP est un protocole multi-metrics, on choisit les valeurs 1500, 100, 255, 1, 1500 pour désigner la bande passante, charge du lien, latence, la fiabilité et la MTU respectivement.

I.3.3.3 – NTP

NTP (Network Time Protocol) est un protocole qui permet de synchroniser, via un réseau informatique, l'horloge locale des périphériques réseau sur une référence d'heure. Cette dernière ne sera

autre que l'horloge locale du second Router du premier site ; qui est considéré comme serveur NTP. Tout les autres périphériques de couche 3 sont considérés comme clients NTP.

I.4 - Choix du plan d'adressage

Le schéma d'adressage est planifié comme suit :

Le premier Site (Site1) bénéficie des sous réseaux de l'adresse privée 172.16.1.0/24

Ce Site possède deux VLANs (VLAN 10 et VLAN 20) contenant les deux serveurs séparément et ayant les adresses 172.16.1.0/25 et 172.16.1.128/26 respectivement.

Le Site1 possède aussi cinq sous réseaux reflétant les liaisons reliant les périphériques des couches coeur et distribution. Les sous réseaux sont partagés comme suit.

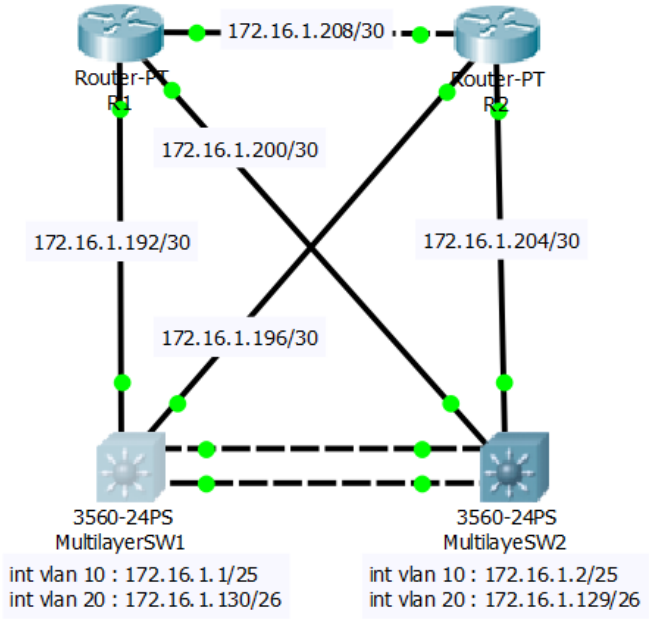

Figure I.9 – Adressage Site 1

Le second Site (Site2) bénéficie des sous réseaux de l'adresse privée 172.16.2.0/24

Ce Site possède deux VLANs (VLAN 30 et VLAN 40) contenant les deux serveurs séparément et ayant les adresses 172.16.2.0/25 et 172.16.2.128/26 respectivement.

Le Site2 possède aussi cinq sous réseaux reflétant les liaisons reliant les périphériques des couche coeur et distribution. Les sous réseaux sont partagés comme suit.

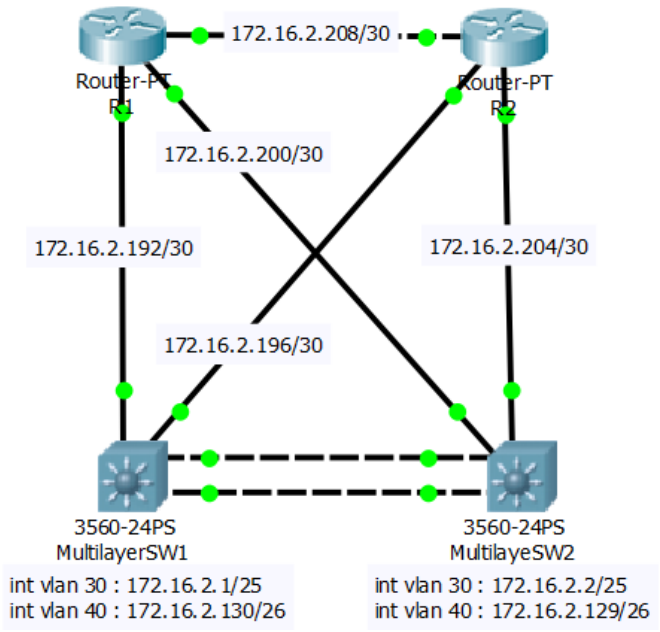

Figure I.10 – Adressage Site 2

Les succursales et les liaisons WAN (séries) partagent les sous réseaux du réseaux 192.168.0.0/16 où la première succursale (Branch1) et la seconde succursale (Branch2) exploitent les réseaux 192.168.8.0/24 et 192.168.7.0/24 respectivement.
Concernant les liaisons WAN, leurs sous-réseaux respectifs sont indiqués dans la figure suivante.

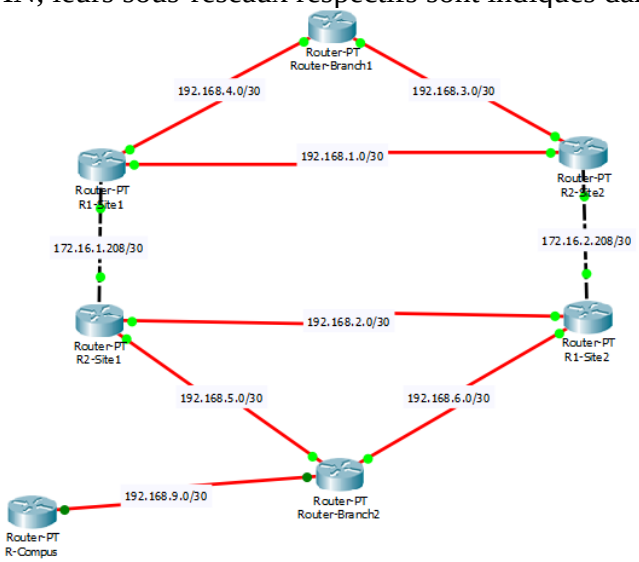

Figure I.11 – Adressage des liaisons WAN

Concernant le Compus, il bénéficie des sous réseaux de l'adresse privée 10.0.0.0/16. Possédant six VLANs, ces derniers sont présenté comme suit .

VLAN ID	VLAN Address
10	10.0.10.0/24
20	10.0.20.0/24
30	10.0.30.0/24

40	10.0.40.0/24
50	10.0.50.0/24
60	10.0.60.0/24

Tab I.1 – Adressage des VLANs au niveaua du Compus

Les liaisons entre le premier Multilayer Switch et le Router du Compus aura l'adresse réseau 10.0.70.0/30.
Les liaisons entre le second Multilayer Switch et le Router du Compus aura l'adresse réseau 10.0.80.0/30.

Finalement, on peut résumer le plan d'adressage de toutes la platforme comme suit.

Name	Interface	IP address	Default Gateway
Server1-site1	Fa0	172.16.1.126/25	172.16.1.1/25
Server2-site1	Fa0	172.16.1.190/26	172.16.1.129/26
Server1-site2	Fa0	172.16.2.126/25	172.16.2.1/25
Server2-site2	Fa0	172.16.2.190/26	172.16.2.129/26
MultiSW1-site1	Vlan 10	172.16.1.1/25	
	Vlan 20	172.16.1.130/26	
	F0/7	172.16.1.197/30	
	F0/6	172.16.1.193/30	
MultiSW2-site1	Vlan 10	172.16.1.2/25	
	Vlan 20	172.16.1.129/26	
	F0/7	172.16.1.205/30	
	F0/6	172.16.1.201/30	
MultiSW1-site2	Vlan 30	172.16.2.1/25	
	Vlan 40	172.16.2.130/26	
	Fa0/1	172.16.2.197/30	
	Fa0/2	172.16.2.193/30	
MultiSW2-site2	Vlan 30	172.16.2.2/25	
	Vlan 40	172.16.2.129/26	
	Fa0/7	172.16.2.205/30	
	Fa0/6	172.16.2.201/30	
R1-site1	Fa0/1	172.16.1.202/30	
	Fa0/0	172.16.1.194/30	
	Fa1/0	172.16.1.209/30	
	S0/0	192.168.1.1/30	

	S0/1	192.168.4.1/30	
R2-site1	Fa0/1	172.16.1.206/30	
	Fa0/0	172.16.1.198/30	
	Fa1/0	172.16.1.210/30	
	S0/0	192.168.2.2/30	
	S0/1	192.168.5.2/30	
	S0/2	192.168.9.2/30	
R1-site2	Fa0/1	172.16.2.202/30	
	Fa0/0	172.16.2.194/30	
	Fa1/0	172.16.2.209/30	
	S0/0	192.168.2.1/30	
	S0/1	192.168.6.1/30	
R2-site2	Fa0/1	172.16.2.206/30	
	Fa0/0	172.16.2.198/30	
	Fa1/0	172.16.2.210/30	
	S0/0	192.168.1.2/30	
	S0/1	192.168.3.2	
R-Branch1	S0/0	192.168.4.2/30	
	S0/1	192.168.3.1/30	
	Fa0/0	192.168.8.254/24	
R-Branch2	S0/1	192.168.5.1/30	
	S0/0	192.168.6.2/30	
	Fa0/0	192.168.7.254/24	
PC-Branch1	Fa0	192.168.8.1/24	192.168.8.254
PC-Branch2	Fa0	192.168.7.1/24	192.168.7.254

Tab I.2 – Adressage des Sites et des Succursales

Name	Interface	IP address	Default Gateway
MultilayerSW1-Compus	Int vlan 10	10.0.10.252/24 virtual @ : 10.0.10.254/24	
	Int vlan 20	10.0.20.252/24 virtual @ : 10.0.20.254/24	
	Int vlan 30	10.0.30.252/24 virtual @ : 10.0.30.254/24	
	Int vlan 40	10.0.40.252/24 virtual @ : 10.0.40.254/24	

	Int vlan 50	10.0.50.252/24 virtual @ : 10.0.50.254/24	
	Int vlan 60	10.0.60.252/24 virtual @ : 10.0.60.254/24	
	Eth2/0	10.0.70.1/30	
MultilayerSW2-Compus	Int vlan 10	10.0.10.253/24 virtual @ : 10.0.10.254/24	
	Int vlan 20	10.0.20.253/24 virtual @ : 10.0.20.254/24	
	Int vlan 30	10.0.30.253/24 virtual @ : 10.0.30.254/24	
	Int vlan 40	10.0.40.253/24 virtual @ : 10.0.40.254/24	
	Int vlan 50	10.0.50.253/24 virtual @ : 10.0.50.254/24	
	Int vlan 60	10.0.60.253/24 virtual @ : 10.0.60.254/24	
	Eth2/0	10.0.80.1/30	
R-Compus	Fa0/0	10.0.70.2/30	
	Fa0/1	10.0.80.2/30	
	S0/0	192.168.9.1/30	
PC1-Compus	Fa0	Learned via DHCP Servers	10.0.10.254/24 (Learned via DHCP Servers)
PC2-Compus	Fa0	Learned via DHCP Servers	10.0.20.254/24 (Learned via DHCP Servers)
PC3-Compus	Fa0	Learned via DHCP Servers	10.0.30.254/24 (Learned via DHCP Servers)
PC4-Compus	Fa0	Learned via DHCP Servers	10.0.40.254/24 (Learned via DHCP Servers)
PC5-Compus	Fa0	Learned via DHCP Servers	10.0.50.254/24 (Learned via DHCP Servers)
PC6-Compus	Fa0	Learned via DHCP Servers	10.0.60.254/24 (Learned via DHCP Servers)

Tab I.3 – Adressage du Compus

I.5 - Conclusion

Dans ce chapitre, on a présenté le réseau d'entreprise et l'architecture de ses differentes parties. Ensuite on a énuméré les différents protocoles utilisés au sein de l'architecture. Enfin, on a planifié un adressage pour l'ensemble de la plateforme.

Part II
Mise en place d'un réseau d'entreprise : Réalisation

II.1 – Introduction

Ce chapitre concerne les détails de configuration des différentes technologies citées dans le chapitre précédent. En premier, on va présenté l'environnement de simulation et d'émulation. On présentera ensuite les différents lignes de commandes permettant la configurations des protocoles conçus. Le chapitre est clôturé par une partie de test et de validation.

II.2 – Environnement de travail

En premier, et pour l'application des concepts présentés dans le chapitre précedent d'une part, et étant donnée que le materiel disponible est pratiquement des peripheriques Cisco d'une auter part, on utilise le simulateur réseau Packet Tracer.

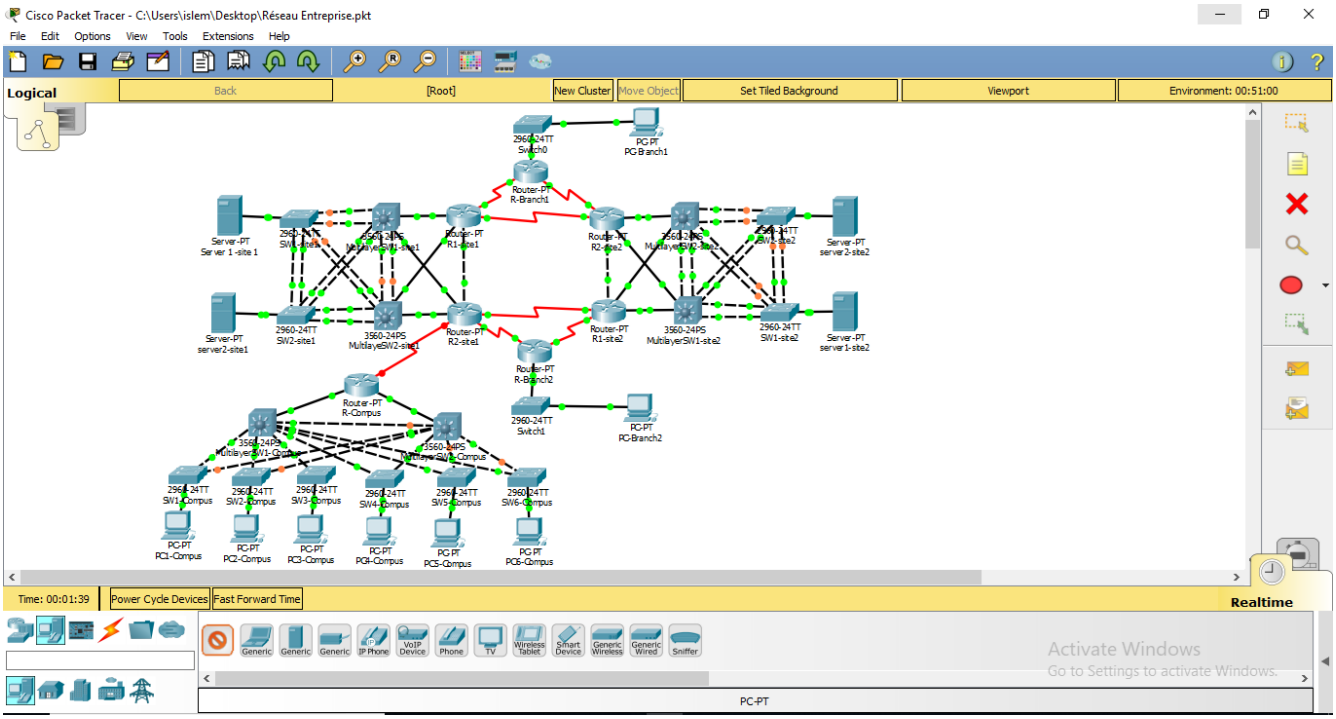

Figure II.1 – Simulation du réseau sur Packet Tracer

En second, et pour s'approcher du monde réel, on passe à l'émulateur GNS3, en utilisant des images Cisco IOS.
Enfin, et vu que certains protocoles exigent du vrai matériel, et pour pouvoir les exploiter, on a utilisé des licences Cisco IOU en utilsant GNS3 VM via VMware Workstation.

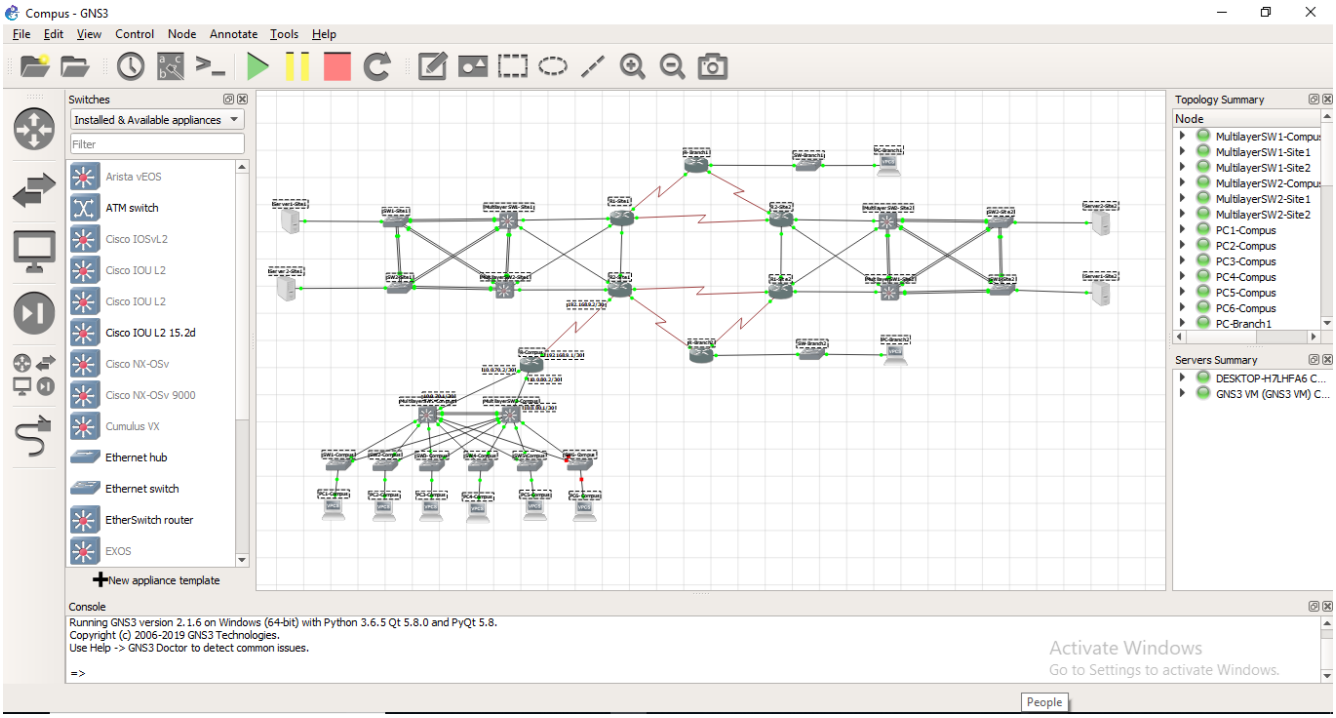

Figure II.2 – Émulation du réseau sur GNS3

II.3 – Implémentation

II.3.1 - Configuration implementée au niveau des Sites

II.3.1.1 - Configuration des VLANs

La création des VLANs se fait sur tout les commutateurs du site comme suit.

MultilayerSW1-Site1(config)#vlan 10
MultilayerSW1-Site2(config)#vlan 20

II.3.1.2 - Configuration Etherchannel

Suivant la figure **Figure II.6**, ci-dessous une instance de configuration du protocole Etherchannel.

MultilayerSW1-Site1(config)#interface range f0/0-1
MultilayerSW1-Site1(config-if-range)#sw mode trunk
MultilayerSW1-Site1(config-if-range)#sw trunk allowed vlan all
MultilayerSW1-Site1(config-if-range)#channel-group 1 mode on
MultilayerSW1-Site1(config)#interface port-channel 2
MultilayerSW1-Site1(config-if)#sw mode trunk
MultilayerSW1-Site1(config-if)#sw trunk allowed vlan all
MultilayerSW1-Site1(config-if)#no sh

II.3.1.3 - Configuration STP (PVST)

MultilayerSW1-Site1(config)#spanning-tree mode pvst
MultilayerSW1-Site1(config)#spanning-tree vlan 10 root primary

MultilayerSW1-Site1(config)#spanning-tree vlan 20 root primary
MultilayerSW2-Site1(config)#spanning-tree mode pvst
MultilayerSW2-Site1(config)#spanning-tree vlan 10 root secondary
MultilayerSW2-Site1(config)#spanning-tree vlan 10 root secondary
SW1-Site1(config)#spanning-tree mode pvst

On configure aussi les ports liés aux serveurs en Portfast et BPDU guard.

SW1-Site1(config)#int f0/8
SW1-Site1(config-if)#spanning-tree portfast
SW1-Site1(config-if)#spanning-tree bpduguard enable

II.3.1.4 - Configuration Routage Inter-VLAN

Apres avoir configurer les adressages des interfaces VLANs dans chaque Multilayer Switch, on active le routage comme suit.

MultilayerSW1-Site1(config)#ip routing

II.3.1.5 - Configuration EIGRP

Sur les deux Routers et les deux Multilayer Switchs, on configurer le protocole de routage EIGRP comme suit.

MultilayerSW1-Site1(config)#router eigrp 1
MultilayerSW1-Site1(config-router)#network 172.16.1.192 0.0.0.3
MultilayerSW1-Site1(config-router)#network 172.16.1.196 0.0.0.3
MultilayerSW1-Site1(config-router)#no auto-summary

Où les réseaux introduit avec la commande *network* sont les réseaux directement connectés au périphérique en question.

II.3.2 - Configuraiton implémentée au niveau du Compus

II.3.2.1 - Configuration des VLANs

Les VLANs sont créés seulement au niveau des Multilayer Switchs.

MultilayerSW1-Compus(config)#vlan 10
MultilayerSW1-Compus(config)#vlan 20
MultilayerSW1-Compus(config)#vlan 30
MultilayerSW1-Compus(config)#vlan 40
MultilayerSW1-Compus(config)#vlan 50
MultilayerSW1-Compus(config)#vlan 60

II.3.2.2 - Configuration VTP

Les deux Multilayer Switchs ont la meme configuration de VTP Server.

MultilayerSW1-Compus(config)#vtp mode server

MultilayerSW1-Compus(config)#vtp domain Compus
MultilayerSW1-Compus(config)#vtp password Compus

Tout les autres Switchs sont configurés en VTP Client.

SW1-Compus(config)#vtp mode client
SW1-Compus(config)#vtp domain Compus
SW1-Compus(config)#vtp password Compus

II.3.2.3 - Configuration STP (PVST)

MultilayerSW1-Compus(config)#spanning-tree mode pvst
MultilayerSW1-Compus(config)#spanning-tree vlan 10 root primary
MultilayerSW1-Compus(config)#spanning-tree vlan 20 root primary
MultilayerSW1-Compus(config)#spanning-tree vlan 30 root primary
MultilayerSW1-Compus(config)#spanning-tree vlan 40 root primary
MultilayerSW1-Compus(config)#spanning-tree vlan 50 root primary
MultilayerSW1-Compus(config)#spanning-tree vlan 60 root primary

MultilayerSW2-Compus(config)#spanning-tree mode pvst
MultilayerSW2-Compus(config)#spanning-tree vlan 10 root secondary
MultilayerSW2-Compus(config)#spanning-tree vlan 20 root secondary
MultilayerSW2-Compus(config)#spanning-tree vlan 30 root secondary
MultilayerSW2-Compus(config)#spanning-tree vlan 40 root secondary
MultilayerSW2-Compus(config)#spanning-tree vlan 50 root secondary
MultilayerSW2-Compus(config)#spanning-tree vlan 60 root secondary

On configure aussi les ports liés aux serveurs en Portfast et BPDU guard.

SW1-Compus(config)#spanning-tree mode pvst
SW1-Compus(config)#int f0/3
SW1-Compus(config-if)#sw mode access
SW1-Compus(config-if)#sw access vlan 10
SW1-Compus(config-if)#spanning-tree portfast
SW1-Compus(config-if)#spanning-tree bpduguard enable

II.3.2.4 - Configuration Routage Inter-VLAN

Après avoir configurer les adressages des interfaces VLANs dans chaque Multilayer Switch, on active le routage comme suit.

MultilayerSW1-Compus(config)#ip routing

II.3.2.5 - Configuration HSRP

MultilayerSW1-Compus(config)#int vlan 10
MultilayerSW1-Compus(config-if)#ip add 10.0.10.252 255.255.255.0
MultilayerSW1-Compus(config-if)#standby version 2
MultilayerSW1-Compus(config-if)#standby 10 ip 10.0.10.254
MultilayerSW1-Compus(config-if)#standby 10 preempt

MultilayerSW2-Compus(config)#int vlan 10
MultilayerSW2-Compus(config-if)#ip add 10.0.10.253 255.255.255.0
MultilayerSW2-Compus(config-if)#standby version 2
MultilayerSW2-Compus(config-if)#standby 10 ip 10.0.10.254
MultilayerSW2-Compus(config-if)#standby 10 preempt

II.3.2.6 - Configuration du routage dans le Compus

On configure des routes par défaut au niveau des Multilayer Switchs comme suit.

MultilayerSW1-Compus(config)#ip route 0.0.0.0 0.0.0.0 eth2/0
MultilayerSW2-Compus(config)#ip route 0.0.0.0 0.0.0.0 eth2/0

On configure des routes résumées des addresse des VLANs au nievau du Router comme suit.

Router-Compus(config)# ip route 10.0.0.0 255.0.0.0 f0/0 253
Router-Compus(config)# ip route 10.0.0.0 255.0.0.0 f0/1 254

II.3.2.7 - Configuration DHCP

Au niveau des deux Multilayer Switchs, on configure les serveurs DHCP comme suit.

MultilayerSW1-Compus(config)#ip dhcp pool vlan10
MultilayerSW1-Compus(dhcp-config)#network 10.0.10.0 255.255.255.0
MultilayerSW1-Compus(dhcp-config)#default-router 10.0.10.254
MultilayerSW1-Compus(config)#ip dhcp pool vlan20
MultilayerSW1-Compus(dhcp-config)#network 10.0.20.0 255.255.255.0
MultilayerSW1-Compus(dhcp-config)#default-router 10.0.20.254
MultilayerSW1-Compus(config)#ip dhcp pool vlan30
MultilayerSW1-Compus(dhcp-config)#network 10.0.30.0 255.255.255.0
MultilayerSW1-Compus(dhcp-config)#default-router 10.0.30.254

MultilayerSW1-Compus(config)#ip dhcp pool vlan40
MultilayerSW1-Compus(dhcp-config)#network 10.0.40.0 255.255.255.0
MultilayerSW1-Compus(dhcp-config)#default-router 10.0.40.254
MultilayerSW1-Compus(config)#ip dhcp pool vlan50
MultilayerSW1-Compus(dhcp-config)#network 10.0.50.0 255.255.255.0
MultilayerSW1-Compus(dhcp-config)#default-router 10.0.50.254
MultilayerSW1-Compus(config)#ip dhcp pool vlan60

MultilayerSW1-Compus(dhcp-config)#network 10.0.60.0 255.255.255.0
MultilayerSW1-Compus(dhcp-config)#default-router 10.0.60.254

II.3.2.8 - Sécurisation du Compus

II.3.2.9 - Configuration Port Security

La configuration est faite sur tout les ports configurés en mode access, au niveau de tout les Switchs du Compus.

SW1-Compus(config)#int eth0/3
SW1-Compus(config-if)#sw port-security
SW1-Compus(config-if)#sw port-security mac-add sticky
SW1-Compus(config-if)#sw port-security violation shutdown

II.3.2.10 - Configuration DHCP Snooping

La première étape consiste à activer le protocole DHCP snooping sur tout les commutateurs.

MultilayerSW1-Compus(config)#ip dhcp snooping

La seconde étape consisté àd éfinir toutes les interfaces, pouvant recevoir une requête ou une réponse DHCP, en mode trust.

MultilayerSW1-Compus(config)#int eth0/2
MultilayerSW1-Compus(config-if)#ip dhcp snooping trust

II.3.2.11 - Configuration Dynamic ARP Inspection

La première étape consiste à activer le protocole IP ARP Inspection sur tout les commutateurs.

MultilayerSW1-Compus(config)#ip arp inspection vlan 10-60

La seconde étape consisté à définir toutes les interfaces fonctionnelles en mode trust.

MultilayerSW1-Compus(config)#int eth0/2
MultilayerSW1-Compus(config-if)#ip arp inspection trust

II.3.2.12 - Configuration IP Source guard

Cela consiste à activer le protocole IP Source guard sur toutes les interfaces fonctionnelles.

MultilayerSW1-Compus(config)#int eth0/2
MultilayerSW1-Compus(config-if)#ip source verify

II.3.2.13 - Configuration ACL

On configure une ACL étendue au niveau de chaque Multilayer Switch. Cette première a pour but de gérer le trafic Inter-VLANs d'une part, et d'assurer la connectivité du Compus avec le reste du réseau étendu d'une autre.

```
MultilayerSW1-Compus(config)#ip access-list extended 100
MultilayerSW1-Compus(config-ext-nacl)#10 permit udp any any eq 1985
MultilayerSW1-Compus(config-ext-nacl)#20 permit udp any any eq bootps
MultilayerSW1-Compus(config-ext-nacl)#30 permit udp any any eq bootpc
MultilayerSW1-Compus(config-ext-nacl)#40 permit ip 10.0.10.0 0.0.0.255 10.0.20.0 0.0.0.255
MultilayerSW1-Compus(config-ext-nacl)#50 permit ip 10.0.10.0 0.0.0.255 10.0.30.0 0.0.0.255
MultilayerSW1-Compus(config-ext-nacl)#60 permit ip 10.0.20.0 0.0.0.255 10.0.10.0 0.0.0.255
MultilayerSW1-Compus(config-ext-nacl)#70 permit ip 10.0.20.0 0.0.0.255 10.0.30.0 0.0.0.255
MultilayerSW1-Compus(config-ext-nacl)#80 permit ip 10.0.30.0 0.0.0.255 10.0.20.0 0.0.0.255
MultilayerSW1-Compus(config-ext-nacl)#90 permit ip 10.0.30.0 0.0.0.255 10.0.10.0 0.0.0.255
MultilayerSW1-Compus(config-ext-nacl)#100 permit ip 10.0.0.0 0.255.255.255 172.16.0.0 0.0.255.255
MultilayerSW1-Compus(config-ext-nacl)#110 permit ip 10.0.0.0 0.255.255.255 192.168.0.0 0.0.255.255
MultilayerSW1-Compus(config-ext-nacl)#120 permit ip 172.16.0.0 0.0.255.255 10.0.0.0 0.255.255.255
MultilayerSW1-Compus(config-ext-nacl)#130 permit ip 192.168.0.0 0.0.255.255 10.0.0.0 0.255.255.255
MultilayerSW1-Compus(config-ext-nacl)#140 deny ip any any
```

II.3.3 - Configuration implementé au niveau des liaison WAN

II.3.3.1 - Configuration OSPF Multi-Area

Sur les septs Routers WAN, on configurer le protocole de routage OSPF comme suit.

```
Router2-Site1(config)#router ospf 1
Router2-Site1(config-router)#network 172.16.1.208 0.0.0.3 area 0
Router2-Site1(config-router)#network 192.168.2.0 0.0.0.3 area 0
Router2-Site1(config-router)#network 192.168.5.0 0.0.0.3 area 2
Router2-Site1(config-router)#network 192.168.9.0 0.0.0.3 area 3
```

Où les réseaux introduits avec la commande *network* sont les réseaux directement connectés au périphérique en question selon les Areas précisées dans la figure **Figure I.8**.

II.3.3.2 - Configuration Redistribution des routes

Dans chaque Router fonctionnant à la fois avec OSPF et EIGRP, on active le redistribution des routes comme suit.

```
Router1-Site1(config)#router ospf 1
Router1-Site1(config-router)#redistribute connected subnets
Router1-Site1(config-router)#redistribute eigrp 1 subnets
```

Router1-Site1(config)#router eigrp 1
Router1-Site1(config-router)#redistribute connected
Router1-Site1(config-router)#redistribute ospf 1 metric 1500 100 255 1 1500

II.3.3.3 – NTP

En premier, on configure l'horloge locale du serveur NTP comme suit.

Router2-Site1#clock set 10:55:00 4 april 2019
Router2-Site1(config)#ntp master

En second, on configure tout les clients NTP comme suit.

Router1-Site1(config)#ntp server 192.168.2.2

II.4 – Vérifications, tests et validation

Une étape importante après avoir configurer le réseau est la vérification de la configuration. Les différentes commandes *show* permettent la vérification de l'adressage et des protocoles implémentés. Une autre étape complémentaire consiste à tester la connectivité entre les différents équipements. Enfin, la mise hors tension des différents ressources (liens entre périphériques par exemple) et tester les scénarios potentiels permettent de valider la fiabilité des connexions alternatives.

II.5 - Conclusion

Ce dernier chapitre à été dédié à la réalisation d'un réseau d'entreprise. En premier, on a simulé le réseau sur Packet Tracer. Pour des résultats plus réels, on a utilisé GNS3. Le problème était que certains périphériques sont limités vis à vis les protocoles supportés. La solution été d'utiliser des licences IOU via GNS VM.
Le chapitre présente aussi les différentes lignes de commandes relatives aux configurations, et il est clôturé par l'invocation de la dernière étape du travail qui est la vérification et la validation du réseau.