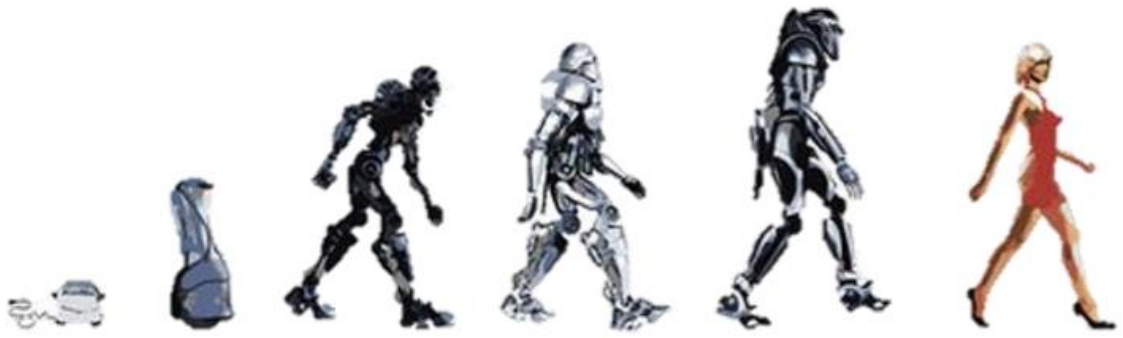
CAMPUS
D'ENSEIGNEMENT SUPÉRIEUR
ET DE FORMATION PROFESSIONNELLE

Louis MARJOLET
Anatole COUASNON
Charles AGOSTINI
Vicente VAZ

Rapport de Spécification

Projet Vergis

EXIA A2 Groupe 2



Louis MARJOLET
Anatole COUASNON
Charles AGOSTINI
Vicente VAZ

Table des matières

Louis MARJOLET
Anatole COUASNON
Charles AGOSTINI
Vicente VAZ

1. TOPOLOGIE

Nous avons opté pour une topologie en 3 couches. (Core, Disctribution, Access)

Cette topologie assure une évolutivité et une maintenabilité constante. De plus, il est plus aisé d'introduire de la redondance dans un réseau adoptant cette topologie.

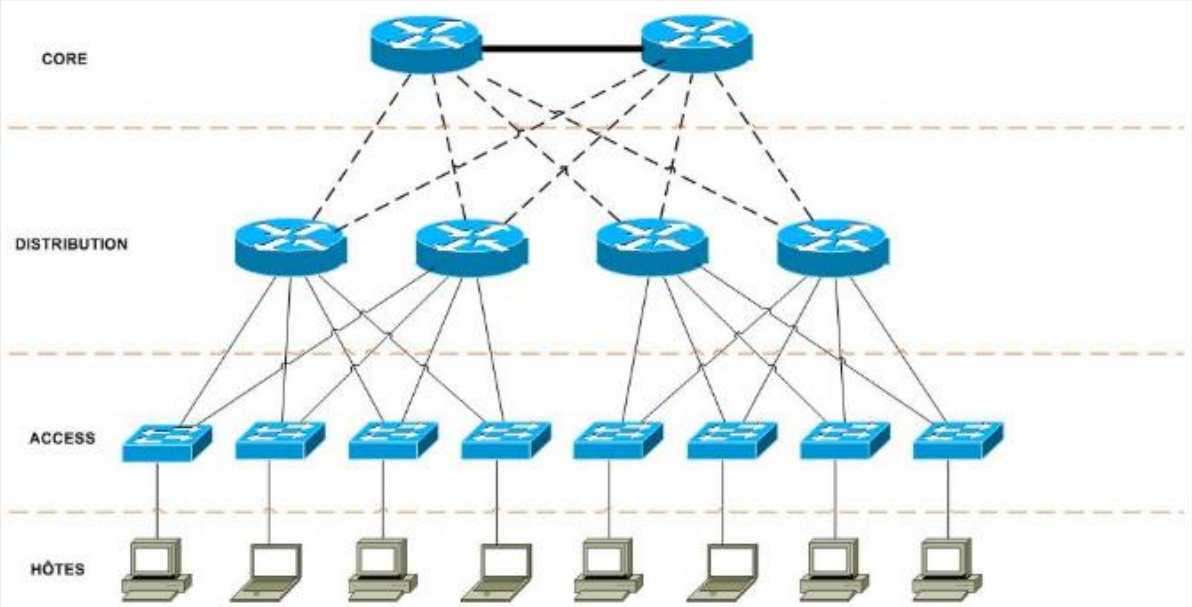
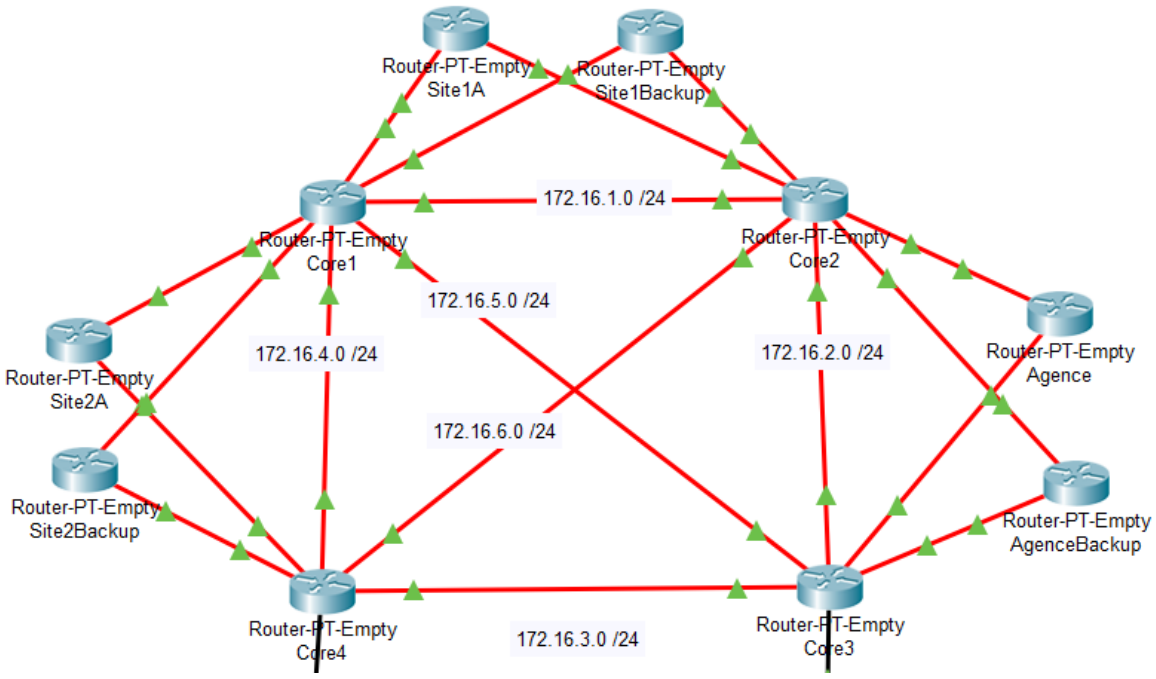


Schéma réseau de la topologie. La redondance est apportée par les liens multiples, en plus du doublage des routeurs/switchs si besoin.

Louis MARJOLET
Anatole COUASNON
Charles AGOSTINI
Vicente VAZ

1. Core

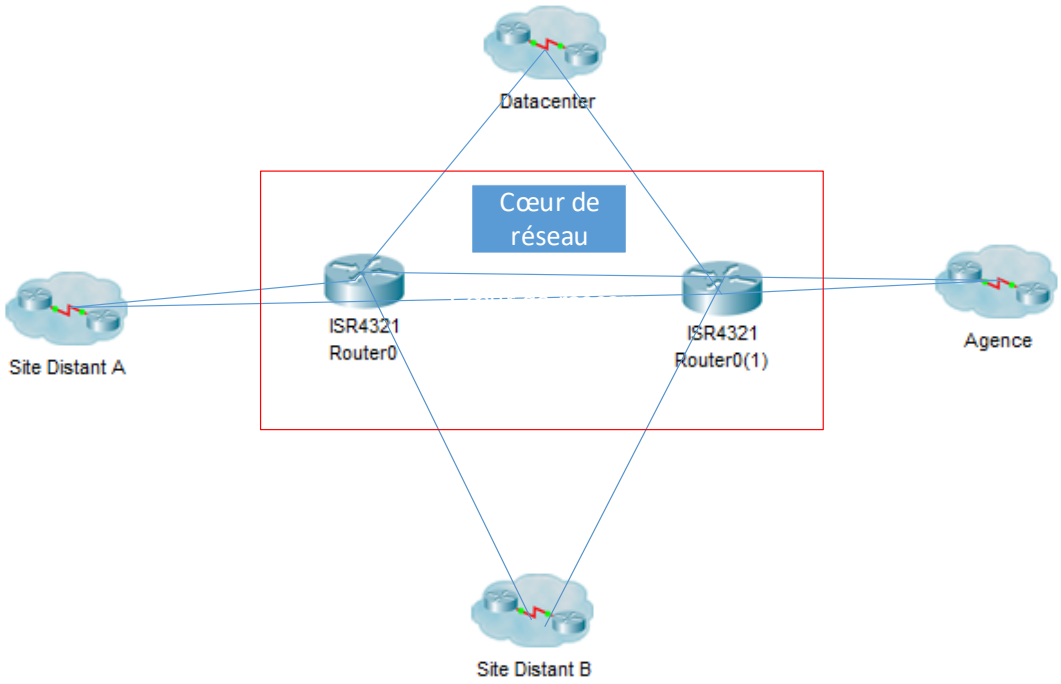
La première topologie adoptée comprenait un cœur composé de routeurs assurant la redondance.



Malheureusement, nous avons eu des problèmes de compatibilités entre l'OSPF et l'HSRP. En effet, quand les paquets arrivaient sur le routeur de backup, nous n'arrivions pas à les rediriger vers le routeur principal, occasionnant la mort du paquet.

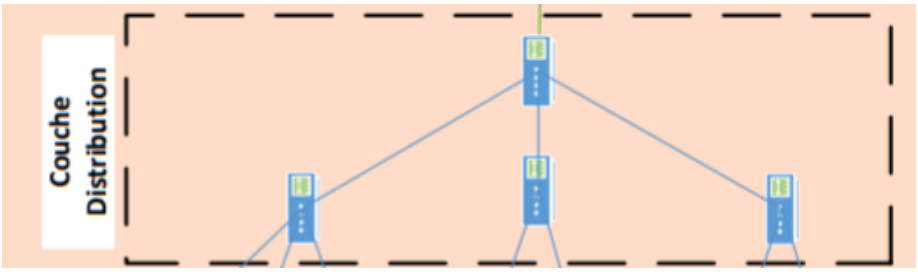
Manquant de temps pour trouver le problème engendrant cette erreur, nous avons fait le choix de simplifier drastiquement la topologie afin d'avoir un cœur plus simple, ceci dans l'espoir de faire communiquer les différents sites, au péril de la redondance :

Louis MARJOLET
Anatole COUASNON
Charles AGOSTINI
Vicente VAZ



2. Distribution

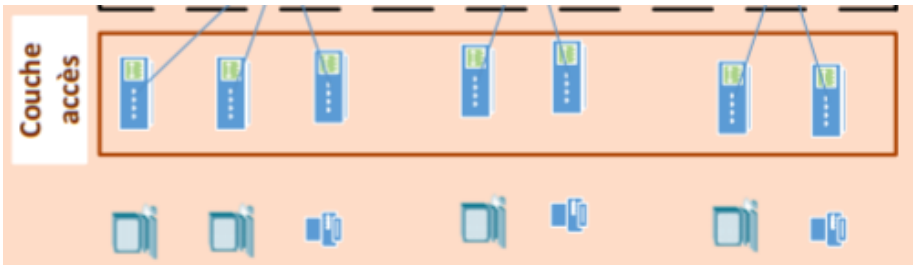
La couche de distribution sert à filtrer, router autoriser ou non les paquets … il s'agit de la liaison entre le cœur et la couche d'accès.



Notre couche de distribution utilise essentiellement des commutateurs de niveau 3.

3. Access

La couche d'accès est la couche sur laquelle les différents appareils du réseau sont reliés. Elle est composée de commutateurs et est suivie des pcs / imprimantes ….



2. ADRESSAGE

Pour l'adressage de nos réseaux nous avons choisis d'utiliser les plages d'adresses suivantes :

- **Site principal et agence** : 192.168.0.0/23
- **Site Secondaire** : 192.168.2.0/23
- **Datacenter** : 192.268.4.0/24

Ces plages d'adresses nous offrent assez d'adresses dans l'optique d'un agrandissement du réseau et d'une séparation optimale des différents VLANS.

1. Adressage du Site Principal

Major Network: **192.168.0.0/23**
Available IP addresses in major network: **510**
Number of IP addresses needed: **285**
Available IP addresses in allocated subnets: **428**
About **89%** of available major network address space is used
About **67%** of subnetted network address space is used

Subnet Name	Needed Size	Allocated Size	Address	Mask	Dec Mask	Assignable Range	Broadcast
Vlan 4 R&D	144	254	192.168.0.0	/24	255.255.255.0	192.168.0.1 - 192.168.0.254	192.168.0.255
Vlan 14 Admin	60	62	192.168.1.0	/26	255.255.255.192	192.168.1.1 - 192.168.1.62	192.168.1.63
Vlan 9 Secret Normal	14	14	192.168.1.64	/28	255.255.255.240	192.168.1.65 - 192.168.1.78	192.168.1.79
Vlan 12 Dir	10	14	192.168.1.80	/28	255.255.255.240	192.168.1.81 - 192.168.1.94	192.168.1.95
Vlan 2 Dev	10	14	192.168.1.96	/28	255.255.255.240	192.168.1.97 - 192.168.1.110	192.168.1.111
Vlan 5 Commu	8	14	192.168.1.112	/28	255.255.255.240	192.168.1.113 - 192.168.1.126	192.168.1.127
Vlan 6 Logistique	8	14	192.168.1.128	/28	255.255.255.240	192.168.1.129 - 192.168.1.142	192.168.1.143
Vlan 16 Info sup	6	6	192.168.1.144	/29	255.255.255.248	192.168.1.145 - 192.168.1.150	192.168.1.151
Vlan 7 Support client	6	6	192.168.1.152	/29	255.255.255.248	192.168.1.153 - 192.168.1.158	192.168.1.159
Vlan 10 Compta	4	6	192.168.1.160	/29	255.255.255.248	192.168.1.161 - 192.168.1.166	192.168.1.167
Vlan 11 RH	4	6	192.168.1.168	/29	255.255.255.248	192.168.1.169 - 192.168.1.174	192.168.1.175
Vlan 3 Infra	4	6	192.168.1.176	/29	255.255.255.248	192.168.1.177 - 192.168.1.182	192.168.1.183
Vlan 8 Secret Dir	4	6	192.168.1.184	/29	255.255.255.248	192.168.1.185 - 192.168.1.190	192.168.1.191
Vlan 15 Imprimante	3	6	192.168.1.192	/29	255.255.255.248	192.168.1.193 - 192.168.1.198	192.168.1.199

2. Adressage du site Secondaire

Subnetting Successful

Major Network: **192.168.2.0/23**
Available IP addresses in major network: **510**
Number of IP addresses needed: **306**
Available IP addresses in allocated subnets: **466**
About **97%** of available major network address space is used
About **66%** of subnetted network address space is used

Subnet Name	Needed Size	Allocated Size	Address	Mask	Dec Mask	Assignable Range	Broadcast
R&D : 4	144	254	192.168.2.0	/24	255.255.255.0	192.168.2.1 - 192.168.2.254	192.168.2.255
Administration : 14	60	62	192.168.3.0	/26	255.255.255.192	192.168.3.1 - 192.168.3.62	192.168.3.63
Suport Clients : 7	16	30	192.168.3.64	/27	255.255.255.224	192.168.3.65 - 192.168.3.94	192.168.3.95
Sécrétariat : 9	14	14	192.168.3.96	/28	255.255.255.240	192.168.3.97 - 192.168.3.110	192.168.3.111
Direction : 12	10	14	192.168.3.112	/28	255.255.255.240	192.168.3.113 - 192.168.3.126	192.168.3.127
Informatique Développeurs : 2	10	14	192.168.3.128	/28	255.255.255.240	192.168.3.129 - 192.168.3.142	192.168.3.143
Imprimantes : 15	9	14	192.168.3.144	/28	255.255.255.240	192.168.3.145 - 192.168.3.158	192.168.3.159
Communication : 5	8	14	192.168.3.160	/28	255.255.255.240	192.168.3.161 - 192.168.3.174	192.168.3.175
Logistique : 6	8	14	192.168.3.176	/28	255.255.255.240	192.168.3.177 - 192.168.3.190	192.168.3.191
Informatique Support : 16	6	6	192.168.3.192	/29	255.255.255.248	192.168.3.193 - 192.168.3.198	192.168.3.199
Commerciaux : 13	5	6	192.168.3.200	/29	255.255.255.248	192.168.3.201 - 192.168.3.206	192.168.3.207
Comptabilité : 10	4	6	192.168.3.208	/29	255.255.255.248	192.168.3.209 - 192.168.3.214	192.168.3.215
Informatique Infrastructure : 3	4	6	192.168.3.216	/29	255.255.255.248	192.168.3.217 - 192.168.3.222	192.168.3.223
Ressources humaines : 11	4	6	192.168.3.224	/29	255.255.255.248	192.168.3.225 - 192.168.3.230	192.168.3.231
Sécrétariat Direction : 8	4	6	192.168.3.232	/29	255.255.255.248	192.168.3.233 - 192.168.3.238	192.168.3.239

Louis MARJOLET
Anatole COUASNON
Charles AGOSTINI
Vicente VAZ

3. PROTOCOLE DE ROUTAGE DYNAMIQUE

Le cahier des charges exigeait une redondance quasi-parfaite du réseau, il a donc fallu sélectionner un protocole de routage dynamique afin d'éviter les boucles, et afin d'avoir une distribution rapide des paquets.

1. OSPF

Le premier choix porte sur OSPF, sa portée étant infinie il n'y aura aucun problème si le réseau est amené à grandir énormément. Sa convergence est rapide, il s'agit d'un protocole évènementiel qui se met à jour lorsque c'est nécessaire et non pas sur un intervalle de temps. OSPF utilise une notion d'aires qui nous est familière et utilise l'algorithme de DIJKSTRA qui est très performant dans le domaine du réseau. Enfin, c'est le protocole qui a été vu en cours, la mise en place de celui est donc facilitée.

2. EIGRP

Eigrp était aussi une bonne alternative, car le choix des chemins est "plus intelligent", il prend en compte plus d'éléments afin faire son choix de route à enprunter. Sa convergence est également plus rapide, il est cependant limité en nombre de saut (bien que sa limite soit difficile à atteindre). L'entreprise étant amené à beaucoup se développer, OSPF permettait de garantir une flexibilité plus grande.

3. RIPV2

Le protocole RIPV2 n'a pas été retenu car ses caractéristiques ne correspondent pas à nos besoins.

4. Choix

Les caractéristiques qu'offre OSPF sont tout à fait satisfaisantes, c'est donc le choix qui a été retenu.

4. REDONDANCE

Dans le cas d'une panne d'un appareil tel qu'un routeur ou un switch occupant des fonctions importantes dans la structure du réseau, il est important d'assurer la redondance afin que la panne ne se fasse pas ressentir. Pour cela il est nécessaire d'utiliser un protocole de redondance.

Plusieurs protocoles existent, nous nous sommes posé la question duquel correspond le plus à nos besoins. Ci-dessous les 3 protocoles sur lesquels nous nous sommes penchés.

- HSRP (Hot Standby Routing Protocol)
- VRRP (Virtual Router Redundcy Protocol)
- GLBP (Gateway Loas Balancing Protocol)

1. HSRP

Il s'agit d'un protocole de redondance propriétaire cisco qui gère la redondance des routeurs, il fonctionne avec un système de priorité qui détermine quel routeur sera utilisé. Son implémentation a été vue en cours.

2. VRRP

Fourni une continuité de service principalement pour les passerelles par défaut, ce protocole n'est pas propriétaire cisco.

3. GLBP

Il s'agit également d'un protocole propriétaire cisco permettant de faire de la redondance et de la répartition de charges sur différents routeurs. Cela répartie donc la charge entre les routeurs au lieux d'en avoir un « de secours »

4. Choix

Le protocole GLBP semble être intéressant car sa répartition des charges sur les routeurs permet une meilleure optimisation du réseau. Cependant pour des raisons de temps et de complexité de mise en place nous avons préféré nous tourner vers **HSRP** qui convient tout à fait à nos besoins et dont nous avons déjà mis en place sur d'autres projets.

5. SECURITÉ

5. Accès SSH

Afin d'administrer les switchs a distance, nous avons choisi d'utiliser le mode d'accès SSH, avec des clés d'acces RSA en 2048 bits. C'est la sécurité maximale des clés RSA. La génération des clés en 2048 est un peu plus lente mais cela offre une meilleure sécurité, dans le cas du domaine de l'entreprise VERGIS CORPORATION portant sur diverses technologies militaires, cela semblait nécéssaire.
L'accès en TELNET n'a pas été retenu car il s'agit d'une technologie possédants plusieurs failles de sécurité connues du public averti.

Nous avons aussi sécurisé tous notre matériel avec des mots de passes.

6. Listes de Contrôle d'Accès

Pour contrôler les accès nous avons aussi défini des listes d'accès afin de réduire les accès selon les autorisations définies.
L'accès internet est ainsi interdit pour les VLANS ne devant pas y accéder, la DMZ ne possède pas non plus cet accès. L'intranet est interne au site et n'est pas accessible depuis l'extérieur.

Nous avons aussi créé une DMZ, sécurisé par un pare-feu.

Enfin, nous avons sécurisé l'accès à internet à l'aide d'un pare feu.