Rapport de Projet Vergis Corp.





Table des matières

[Maquette 3](#_Toc476788845)

[Matériel 5](#_Toc476788846)

[Spécifications techniques 6](#_Toc476788847)

[Découpage du réseau 6](#_Toc476788848)

[Topologie du réseau 7](#_Toc476788849)

[HSRP (Hot Standby Router Protocol) 10](#_Toc476788850)

[DHCP (Dynamic Host Configuration Protocol) 11](#_Toc476788851)

[ACL (Access Control List) : 12](#_Toc476788852)

[VTP (Vlan Trunking Protocol) 12](#_Toc476788853)

[Affectation VLAN 13](#_Toc476788854)

[Serveur HTTP 13](#_Toc476788855)

[Serveur Mail 13](#_Toc476788856)

[Serveur DNS 13](#_Toc476788857)

[SSH 14](#_Toc476788858)

[Mode privilégié 14](#_Toc476788859)

[Wifi 14](#_Toc476788860)

[Les Ondes Wifi 15](#_Toc476788861)

[Bilans 16](#_Toc476788862)

[Julien Mazzia 16](#_Toc476788863)

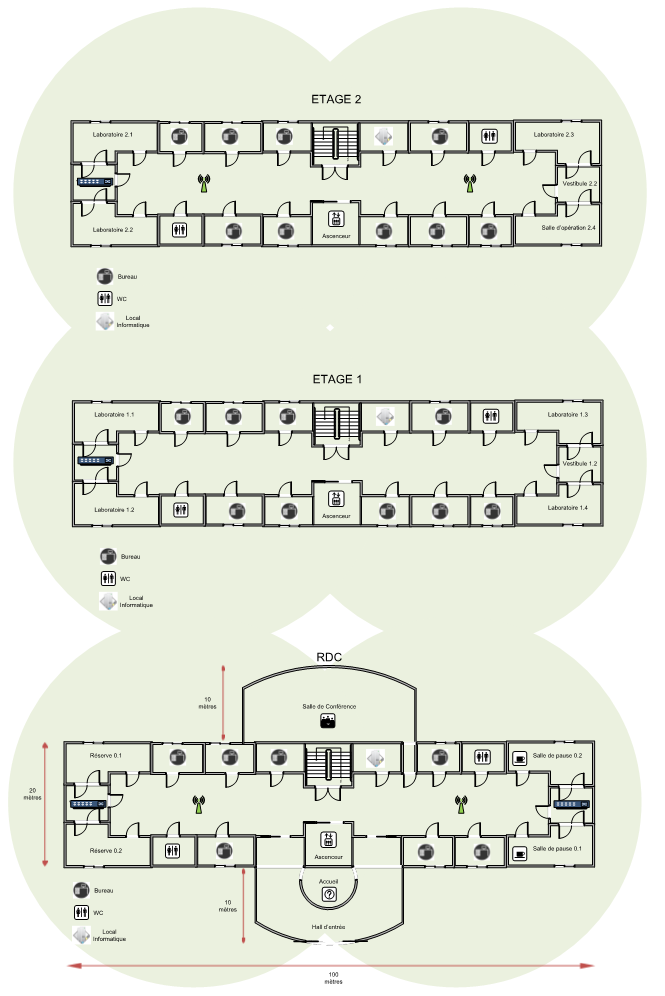
[Romain Verhaeghe 16](#_Toc476788864)

[Dylan Cattelan 16](#_Toc476788865)

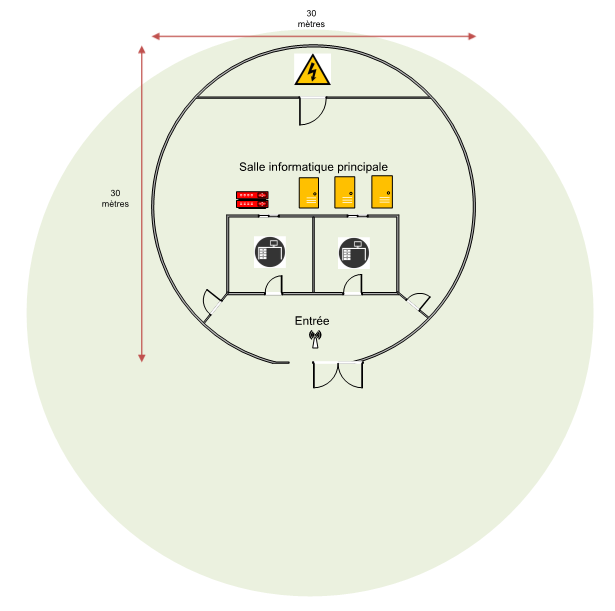
[Bilan de groupe 16](#_Toc476788866)

**Annexes…………………...………………………………………………….………..Dossier en annexe**

# **Maquette**

Dans chacun des trois bâtiments constituants le campus de Vergis Corp, nous avons intégré aux éléments déjà présents 4 bornes Wifi Cisco Aironet 2700i, respectivement au rez-de-chaussée et au 2e étage, afin que celles-ci puissent couvrir la totalité de chaque bâtiment.

De plus, nous avons mis un Switch Catalyst 3750 par étage dans un local technique, ainsi qu’un deuxième Switch dit « de secours » au rez-de-chaussée de chaque bâtiment.

  
  
  
  
Concernant le local informatique, nous y avons entreposé les différents serveurs ainsi que les routeurs ASR 1001-X, qui sont au nombre de deux, un principal et un autre de secours (protocole HSRP mis en place)

Egalement, une borne Wifi est installée dans ce local.

La totalité du campus est disponible dans un fichier annexe appelé « Plan Campus Vergis Corp ».

Une maquette technique est également disponible en annexe sous le nom de « Projet Vergis Corp.pkt ».

# **Matériel**

En annexe de ce document se trouve « Devis matériel société Vergis Corporation », ce document étant la liste et le devis du matériel sélectionné par nos soins. Ci-contre une explication détaillée de chaque matériel sélectionné. Nous avons pris l’initiative de choisir tous nos équipements certifiés Cisco car nous connaissons la réputation et la fiabilité de cette entreprise, mais également la personnalisation et la facilité de configuration de leur matériel.

* Switch : Catalyst 31750 – 48 ports - http://amzn.eu/5TIKv4T – 12390€ (885€ x14 )

A la vue du nombre de machines connectées par étage, nous avons choisis des switches de 48 ports afin de pouvoir prendre en compte une éventuelle évolution de l’entreprise. Le Catalyst 31750 de CISCO est un switch relativement récent et avec la technologie « Cisco EnergyWise » qui permet de réguler la consommation électrique du switch.

* Routeurs : ASR 1001-x – 6 ports, 2.5 > 20 Gbps BW - <http://amzn.eu/0NM6uvB> - 24094€ (12047€ x2)

Anticipant l’évolutivité de l’entreprise, notre choix s’est porté sur ces routeurs car ils s’adaptent à la bande passante entrante et protègent les données en intégrant un pare-feu performant (Cisco IOS Firewall). De plus, il propose certaines applications de contrôle afin de vérifier et sécuriser en profondeur les données entrantes et sortantes, mais également un système de virtualisation de LAN privés, une interconnexion entre différents Data Center, le tout en restant d’une taille plus que convenable (1 Rack unit). Nous en avons pris deux au cas où d’une panne sur le premier, le deuxième pourra ensuite prendre la relève afin de permettre une fiabilité de la connexion dans tout le campus.

* Bornes Wifi : Cisco Aironet 2700i – 1.3Bgps, 50 connexions - <http://amzn.eu/fxbeK2z> - 10270€ (790€ x13)

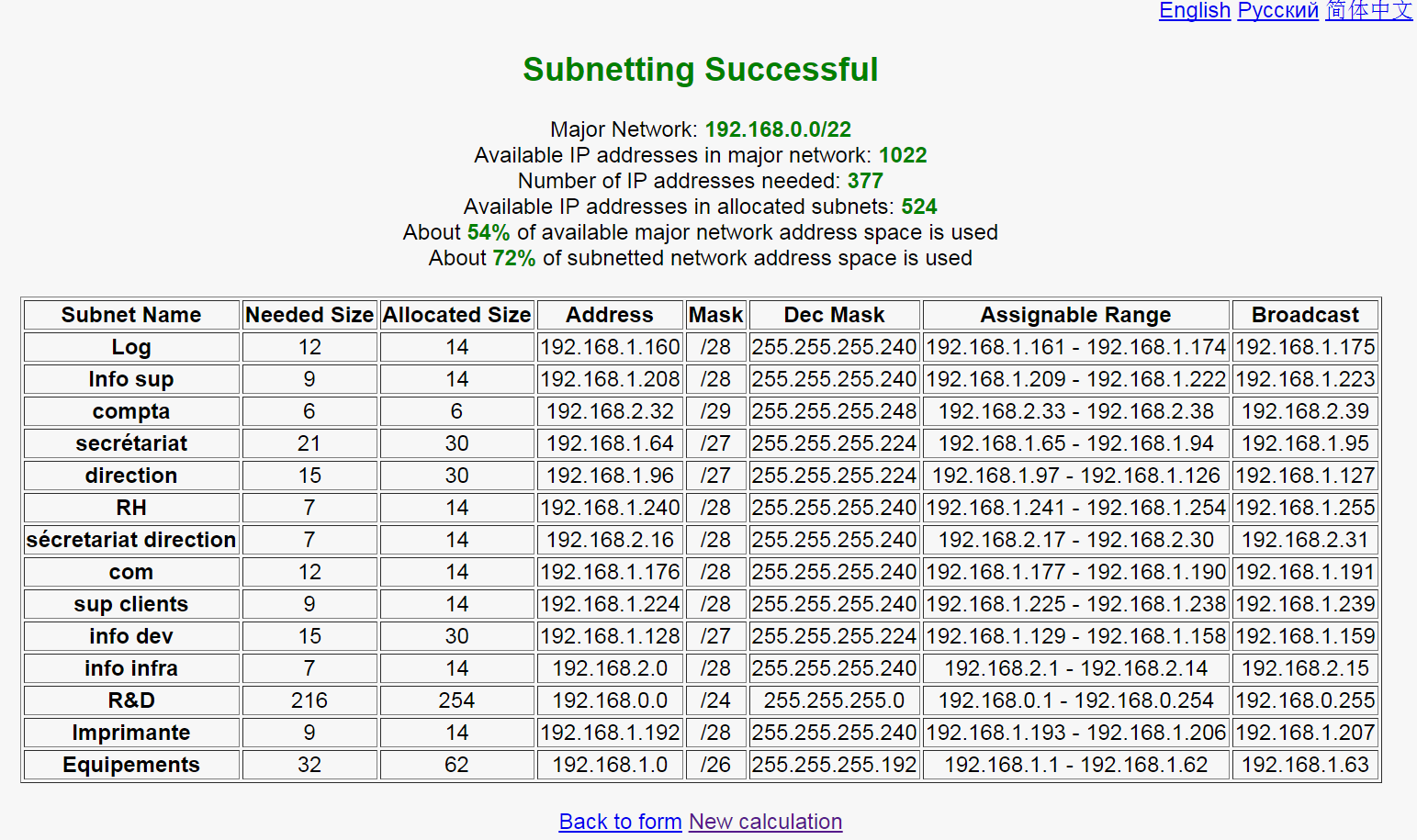
La fiabilité Cisco reste également présente dans notre choix de borne Wifi avec l’Aironet 2700i. Nous nous sommes portés sur ces bornes Wifi car elles proposent une bande passante personnelle allant jusqu’à 1.3Gbps fréquencé à 2.4 Ghz, 802.11ac, le tout supportant jusqu’à 50 connexions simultanées et en Roaming Wifi (possibilité de se déplacer sur le campus sans être déconnecté.). De plus, la technologie CleanAir embarquée permet de réduire les soucis de performance liés aux interférences.

# **Spécifications techniques**

## Découpage du réseau

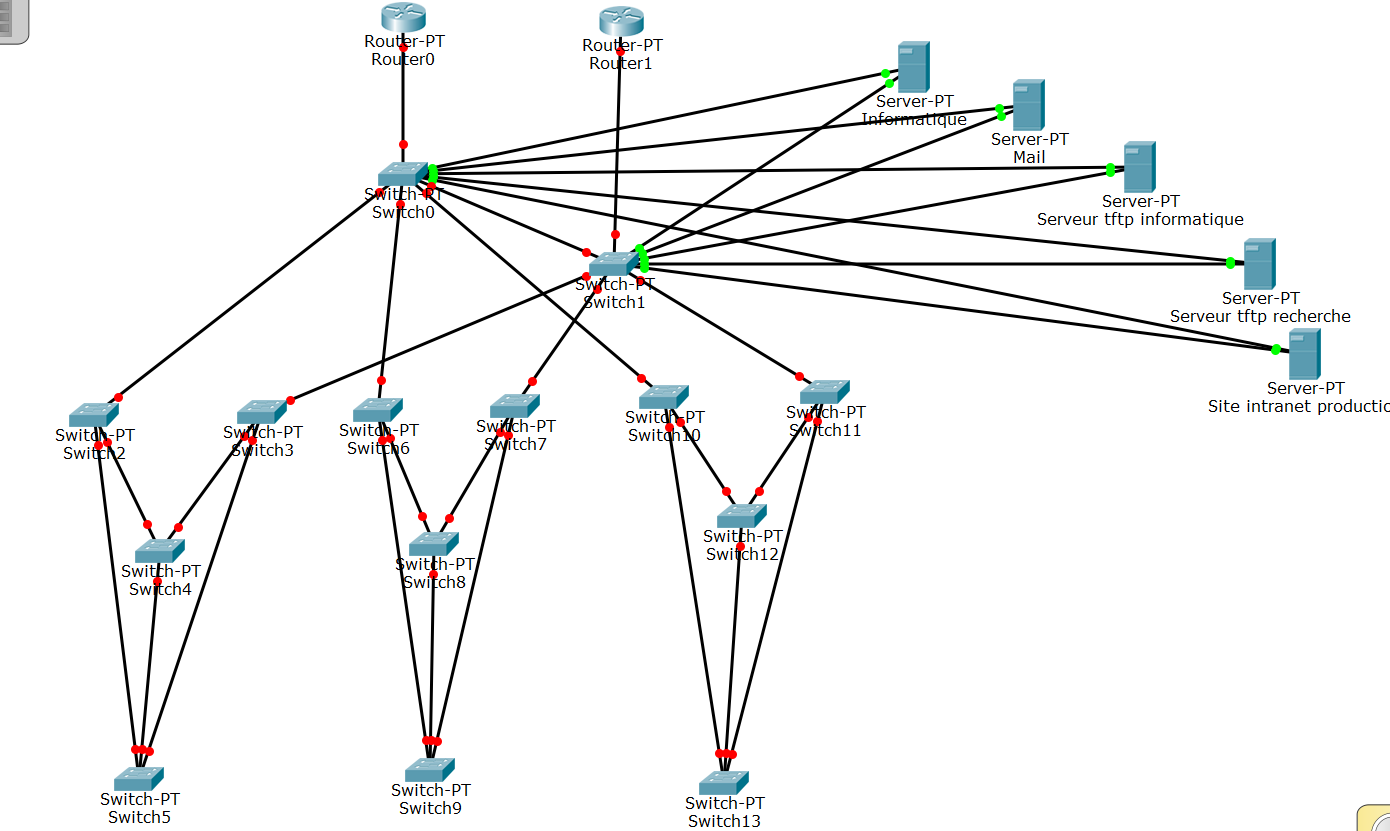
Pour notre réseau, nous avons choisi de découper chaque service en un sous réseau. Nous avons pris l’adresse 192.168.0.0 avec pour masque de sous-réseau 255.255.252.255 ce qui nous donne 524 adresses allouables. Pour chaque service, 50% d’adresses utilisables ont été rajouté pour chaque service, ainsi on a 216 adresses pour le service R&D au lieu des 144 demandés pour prévoir l’évolution du réseau.

On obtient le découpage suivant :

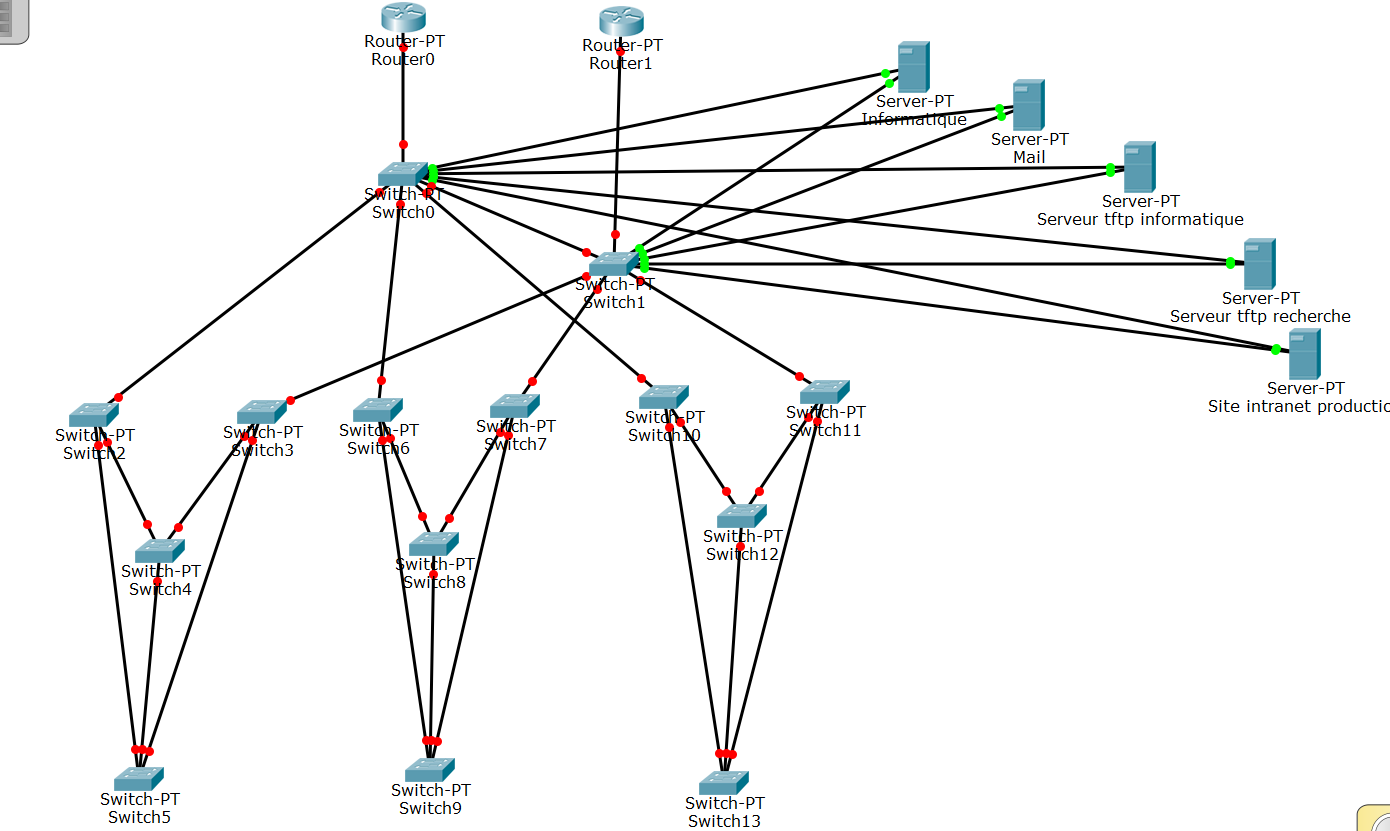


## Topologie du réseau

La topologie du réseau choisie est un mixte entre une topologie hiérarchique et maillée. La topologie hiérarchique permet de découper le réseau en plusieurs entités (salle informatique, étages des bâtiments, …). La topologie maillée permet d’assurer une redondance dans le réseau en interconnectant les différents équipements pour garder un chemin disponible vers le routeur.

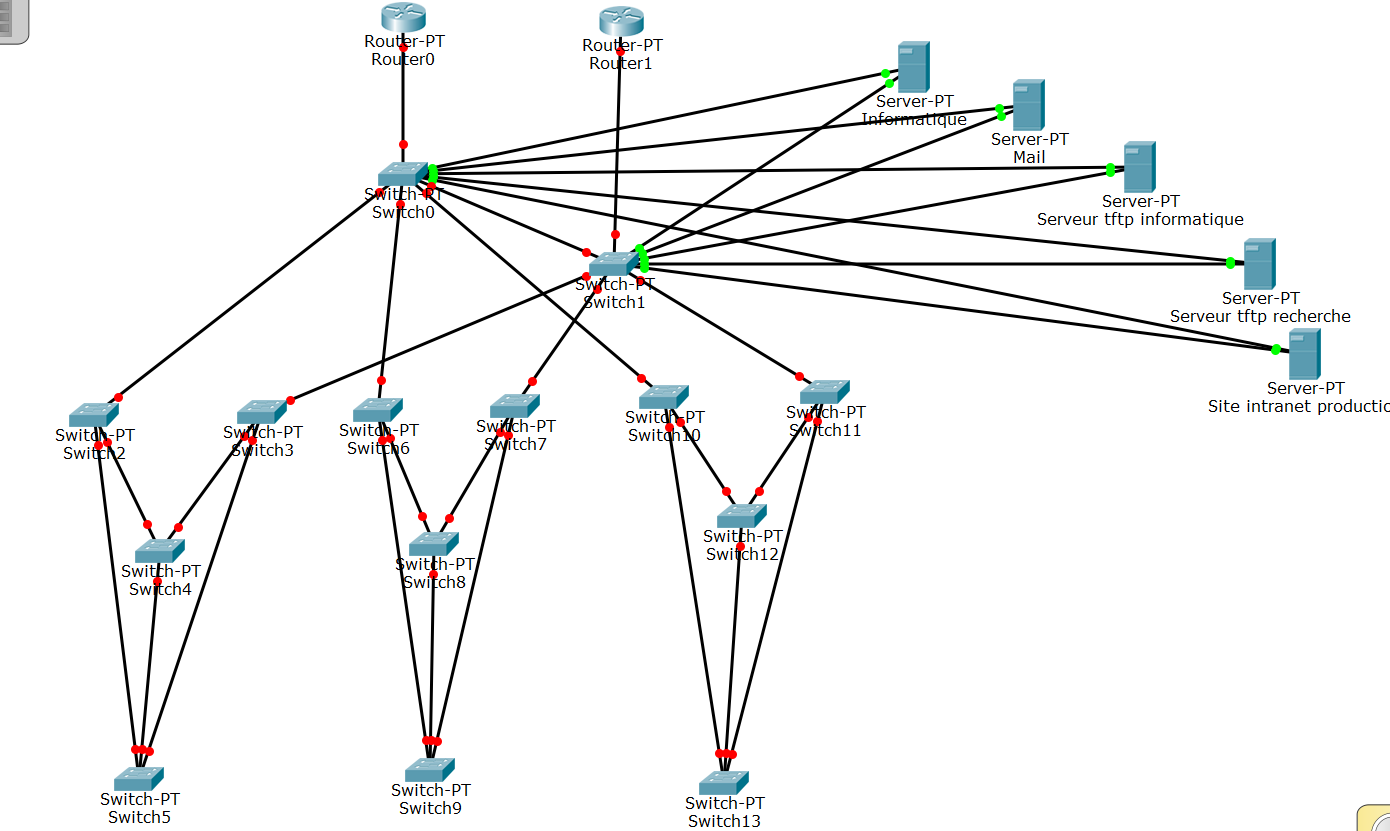


Si l’un des deux routeurs, l’autre prend le relais avec HSRP (voir plus bas) :



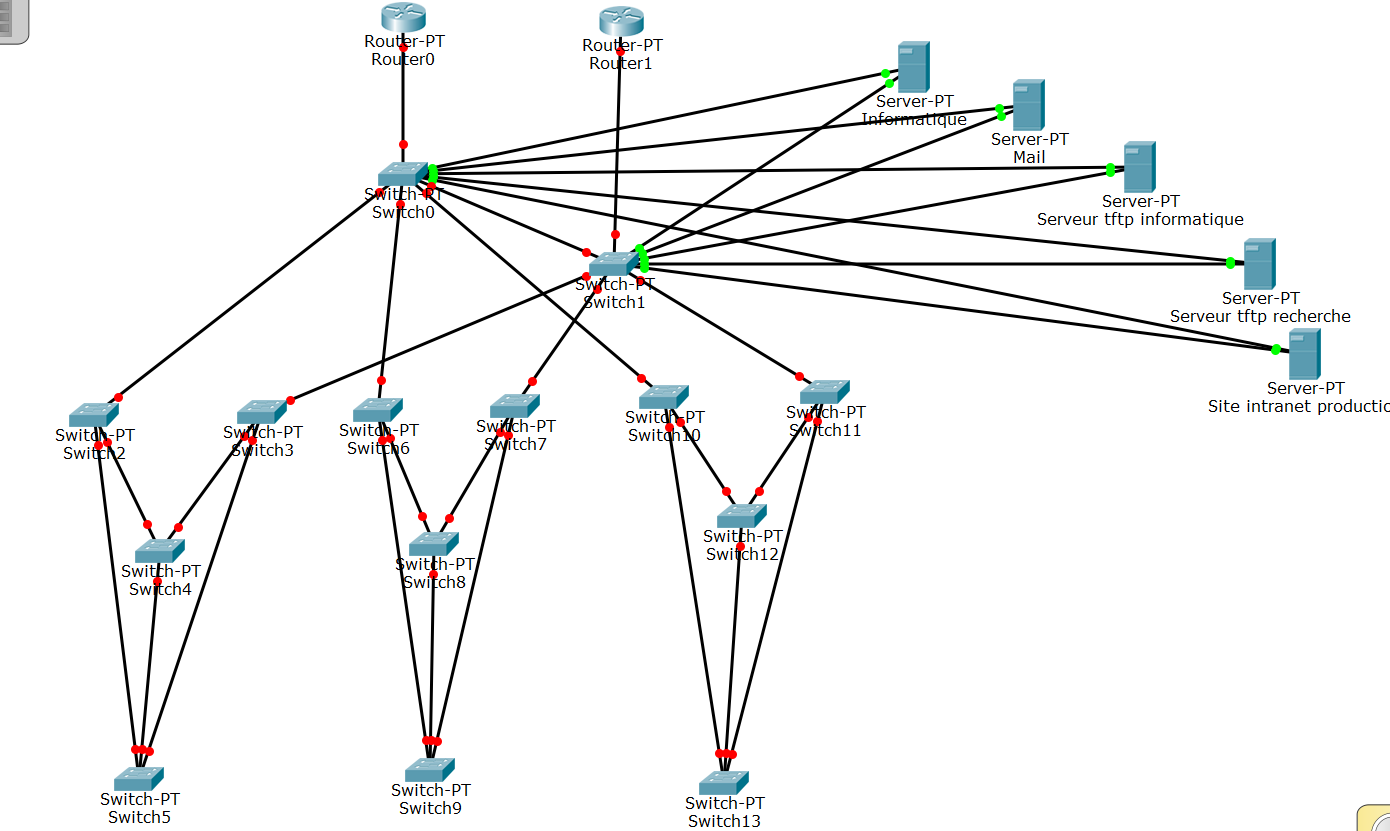
Ici, router1 prend le relais.

Si un des deux switches de la salle informatique tombe en panne, le réseau marche :



Switch1 prend le relais. Les rez-de-chaussée des bâtiments ont toujours une connexion vers les routeurs.

Enfin si un des routeurs du rez-de-chaussée tombe en panne, l’autre prend le relais :



Le switch3 prend le relais si le switch2 tombe en panne et assure la connexion aux switches des étages (switch 4 et 5)

**Configuration et mise en place des protocoles :**

## HSRP (Hot Standby Router Protocol)

Le protocole HSRP est un protocole propriétaire Cisco (donc propre aux équipements Cisco) qui peut être mis en place sur un routeur ou un commutateur de couche 3.

Il permet de prévenir d’une panne d’une connexion via un routeur.

Le principe est le suivant : Pour un réseau avec deux ou plusieurs routeurs connectés directement à Internet, nous allons créer un groupe de routeur qui contiendra une adresse IP virtuelle qui servira au protocole HSRP. Cette adresse IP sera la même pour les routeurs avec une interface dans le même groupe et servira de passerelle par défaut. Ainsi si l’un des routeurs tombe en panne, l’autre pourra prendre le relais sans que l’on ait à changer l’IP de la passerelle par défaut.

Dans ce système, on aura un routeur actif possédant la priorité la plus haute, qui recevra les paquets, et les autres en standby. Ils ne feront qu’écouter les messages du routeur actif.

Pour communiquer entre eux, les routeurs utilisent des paquets Hello (envoyé par défaut toutes les 3 secondes).

Le réseau peut ainsi continuer à avoir une passerelle par défaut malgré la panne d’un routeur.

La configuration de HSRP est en général comme suit :

*Interface type d’interface numéro d’interface*

*IP adresse IP masque de sous-réseau (on définit ici l’adresse physique du routeur)*

*Standby numéro ip IP HSRP*

*Standby numéro priority numéro de priorité (100 de base)*

*Standby numéro preempt*

Dans notre cas, HSRP est très utile au niveau de la connexion Internet. On va donc créer configurer le HSRP pour chaque sous-interface correspondant au nombre de VLAN (ainsi la VLAN 3 a comme sous interface fa0/0.3) en utilisant 3 addresses de son sous-réseau :

- 1 pour l’addresse physique du 1er routeur

- 1 autre pour le 2éme routeur

- 1 pour l’addresse ip du HSRP

La différence de configuration est le rajout d’une encapsulation dot1q pour désencapsuler les paquets et les analyser pour connaître la VLAN de celui-ci.

Le choix de commencer les sous-interfaces à fa0/0.2 était voulu pour laisser le VLAN 1 comme VLAN par défaut.

## DHCP (Dynamic Host Configuration Protocol)

DHCP permet d’allouer dynamiquement une adresse IP à un poste en lui précisant différentes informations comme la passerelle par défaut ou encore un DNS propre à son réseau.

Ce protocole permet d’allouer une adresse seulement aux postes connectés, il prend en compte les paramètres et les répercute sur le réseau et enfin il permet une centralisation des paramètres.

Un DHCP peut être configuré sur un serveur dans notre cas à nous, la mise en place d’un serveur DHCP devait être sur un routeur à cause des sous-interfaces.

La configuration du DHCP a dû être faites dans chaque sous-interface. Ainsi quand le routeur reçoit un paquet DHCP, il observe dans quel VLAN se trouve le poste et lui renvoi l’adresse IP correspondant à son réseau.

La configuration standard de DHCP était :

*Ip dhcp pool nom de la VLAN*

*Network IP de réseau masque de sous-réseau*

*Default-router IP de la passerelle par défaut*

## ACL (Access Control List) :

Les ACL sont des listes qui répertorient les paquets pouvant entrer ou sortir d’un réseau. Elle est placée sur l’interface d’un équipement (souvent un routeur).

Il existe les acces-list standard qui permettent de filtrer les paquets par leur IP et les access-list étendues qui elles rajoutent le masque de sous réseau, le protocole utilisé ou encore l’adresse de destination.

Pour notre réseau nous avons utilisé principalement des access-list étendues car nous devons regarder les adresses de destinations ou encore les protocoles (comme DHCP ou TFTP) utilisés sur le réseau.

Au total nous avons mis un pare-feu entre internet et les routeurs regardant l’adresse de destination. Elle doit correspondre avec l’adresse du réseau, ce qui veut dire qu’elle s’adresse bien à un poste du réseau.

Il y a un pare feu par vlan qui bloque l’accès aux autres VLAN car ils ne doivent pas communiquer entre eux, sauf pour les 3 services informatiques. A chaque fois l’accès aux imprimantes a été autorisé car tous les services doivent y avoir accès. Le serveur DHCP à été autorisé grâce à la ligne : access-list 102 permit udp host 0.0.0.0 eq bootpc host 255.255.255.255 eq bootps.

Au niveau des serveurs TFTP, une access-list permet à chaque serveur de n’accepter les requêtes venant des services informatiques pour les serveur TFTP informatique et des services recherches et développement pour le serveur TFTP recherche.

## VTP (Vlan Trunking Protocol)

Le protocole VTP permet d'administrer les VLAN de son réseau de manière simple.

Pour le mettre en place on élit d'abord un switch qui sera le "switch serveur". On définit ensuite les différentes VLANS sur switch. Les autres switches doivent être configurés en tant que switch client. La liaison entre les switches doit être une liaison de type Trunk. Cela permet de faire passer des trames peu importe leur appartenance à un VLAN.

Les switches clients vont recevoir une "VLAN Database" qui n'est autre qu'une copie que la VLAN database du switch serveur. Dès lors que l'on modifie, ajoute ou supprime une VLAN sur le switch serveur les switches clients seront automatiquement mis à jour.

## Affectation VLAN

Pour que les postes utilisateurs soient affectés à des VLANS il est impératif de définir à quel VLAN ils appartiennent sur l'interface à laquelle ils sont connectés. Par exemple, un PC administratif est relié à l'interface fa0/1 d'un switch. On va entrer dans le mode config de cette interface (enable -> configure terminal -> interface fa0/1) et on attribue le VLAN voulu à ce port.

## Serveur HTTP

Un serveur HTTP permet de stocker des sites web et de les envoyer à des clients. Pour configurer un serveur HTTP sur Packet Tracer il suffit d'activer le service HTTP dans l'onglet "Services". On couple à ce service un service DNS qui permet de faire de la résolution de nom. Cela permettra aux clients de se connecter sur le site local en tapant l'adresse "www.vergis.fr" plutôt que d'avoir à taper directement l'adresse IP du serveur.

## Serveur Mail

Pour configurer le service mail il faut lui aussi l'activer dans l'onglet "Service", on choisit ensuite un nom de domaine (ici vergis.fr). On crée ensuite une liste d'utilisateurs ainsi que leurs mots de passe associés.

Sur les postes clients de ces utilisateurs il faudra renseigner l'adresse IP du serveur en tant qu’adresse de serveur mail entrant et sortant. Ils devront ensuite se connecter à l'aide des identifiants créés précédemment, et créer une adresse mail qui respecte le nom de domaine choisi.

## Serveur DNS

Comme précédemment il faudra activer le service puis ajouter un nouvel enregistrement. Cet enregistrement doit contenir le nom à traduire et son adresse associée.

Il faut ensuite spécifier l'adresse du serveur DNS dans les différents pool DHCP de notre réseau. Pour ce faire, on ajoute la ligne dns-server IPSERVEUR dans chacune des pools DHCP de notre réseau.

## SSH

Le SSH permet à des utilisateurs distants de se connecter sur le terminal d’une machine afin d’y effectuer des manipulations. A la différence du Telnet, le SSH passe par une connexion sécurisée et utilise le port 22. Afin de réaliser ceci, il faut attribuer un compte utilisateur/mdp, un hostname, attribuer un nom de domaine, générer une clé de chiffrement et ensuite activer le SSH pour chaque équipement.

## Mode privilégié

Chaque switch ou routeur possède un mode dit « privilégié » disponible à l’aide de la commande « enable ». Afin de protéger le campus, nous avons mis un mot de passe hashé sur ce mode. De ce fait, les équipements sensibles restent inaccessibles.

## Wifi

Le campus étant équipé de plusieurs bornes Wifi, nous les avons sécurisés à l’aide d’une sécurité WPA2 encryptée en AES, chaque borne Wifi ayant son propre SSID et sa propre clef de sécurité.

Les différentes commandes de configuration sont disponibles en annexe dans le dossier « Commandes configuration ».

# **Les Ondes Wifi**

Depuis la création de cette technologie, les études et les recherches se succèdent afin de savoir l’impact des ondes Wifi sur le corps humain. Certaines affirmant que ces ondes provoquent des migraines, de la fatigue voire même une augmentation de risque de cancer, d’autres stipulant qu’elles n’impactent en rien notre corps et qu’il n’y a aucun risque encouru. Qu’en est-il réellement ?

Une onde Wifi est une onde radio qui, effectivement, émet des radiations. Ce mot qui déchaine les passions et qui effraie ceux et celles n’osant pas s’aventurer plus loin. Des radiations sont émises par plus ou moins tout objet qui émet des ondes, comme par exemple le téléphone, la télévision, mais aussi la lumière du soleil ou encore le son qui sort des enceintes. Mais qu’elles sont les différences entre les « bonnes » radiations et les « mauvaises » radiation ? La longueur d’onde. Effectivement, il y a deux grandes familles de radiations, qui sont les radiations ionisantes (celles qui sont mauvaises pour le corps, provoquant des mutations cellulaires et augmentant les risques de cancer (Rayons X, rayons Gamma ...)), et celles dites non-ionisantes, qui sont inoffensives pour le corps humain, celles qui n’ont pas assez d’énergie pour ioniser les atomes, comme celles du Wifi, des Talkie-Walkie ou encore des micro-ondes.

De plus, et afin de rassurer les plus sceptiques, la « Loi en carré inverse » démontre qu’en fonction de la distance nous séparant avec une source d’énergie (en l’occurrence, une borne wifi), la quantité d’énergie reçue est inversement proportionnelle au carré de la distance de l’origine. En d’autres termes, assumant que les ondes Wifi soient mauvaises pour le corps, et en prenant en compte qu’une borne Wifi propage 1W d’énergie (là où un micro-ondes envoie 700W d’énergie), et même si nous étions directement devant la borne Wifi, il n’y aurait pas du tout de risque ni d’impact sur notre corps.

L’unique soucis étant la pensée d’un chacun associant « Ondes » et « Radiations » avec « Nucléaire » et « Apocalypse », ou autre catastrophe que nous avons l’habitude de voir un peu partout à la télévision et sur l’ordinateur.

En conclusion, il faut prendre en compte les différents types de radiation en cause, et comprendre l’impact de chacun d’entre eux, et ensuite associer l’onde avec le type de radiation. Suite à cela uniquement nous saurons si une certaine onde est néfaste pour le corps humain. Bien évidemment, les recherches scientifiques sont encore en cours afin de démontrer plus précisément cette situation et de pouvoir la propager pour que les personnes ne s’inquiètent plus.

# **Bilans**

## Julien Mazzia

« Ce projet paraissait simple aux premiers abords, lorsqu’on rendre dans la partie technique tout devient beaucoup plus intéressant. Rapidement on est submergé par beaucoup de tâches et on ne sait plus où donner de la tête. Je pense que ce projet m’a énormément apporté de connaissances au niveau du réseau et, malgré quelques légers écarts, nous avons réussis à proposer une maquette fonctionnelle et à la hauteur de nos attentes. »

## Romain Verhaeghe

« Le projet Vergis Corp était plus imposant que ce que je pensais, mais cela ne nous a pas empêché d’arriver jusqu’à la fin de celui-ci sans de trop grands écarts. La partie Packet Tracer semblait insurmontable, mais après beaucoup d’acharnement et de recherches, nous sommes arrivés à nos fins. Je suis globalement satisfait de ce projet et de ce groupe. »

## Dylan Cattelan

« Ayant de grandes difficultés en réseau, j’appréhendais énormément ce projet. Cependant, et en grande partie grâce à mon groupe, j’ai pu aborder ce projet d’un point de vue différent et j’ai pu m’adapter, mais également réaliser le travail demandé non-sans-mal. D’un point de vue personnel, j’ai encore énormément de progrès à faire, d’un point de vue de groupe, celui-ci était très performant et très satisfaisant. »

## Bilan de groupe

« Le groupe a su s’adapter et ancrer un rythme de travail propre à lui-même durant ce projet. Le fait de diviser le travail en trois et de devoir synchroniser relativement souvent ce dernier a instauré une certaine discipline dans ce groupe. De plus, la masse de travail a pu être rapidement cernée et de ce fait nous avons pu réagir en conséquence. Globalement, ce projet est une réussite et ce groupe fut une bonne expérience. »