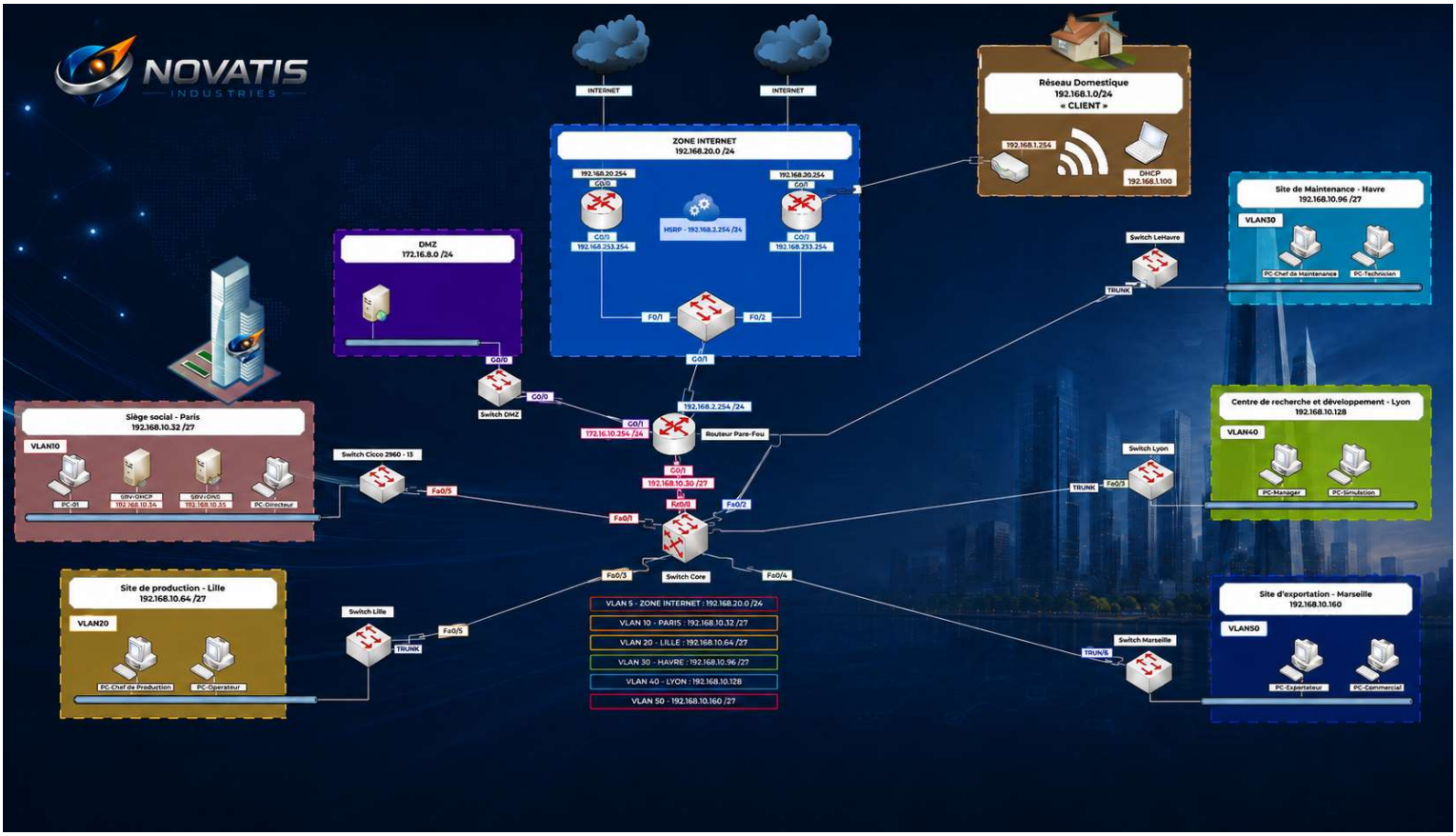
PROJET PERSONNEL – MISE EN PLACE D'UNE INFRASTRUCTURE RESEAU MULTI-SITES SECURISEE ET INTERCONNECTEE

BRETON Théo

Projet N°13 : PROJET NOVATIS INDUSTRIES

DHCP • OSPF • NAT• ISS • HSRP • SwitchCoeur L3/L2



Contexte :

Dans le cadre de son développement et de la modernisation de son infrastructure réseau et système, NOVATIS Industries souhaite mettre en place une architecture cohérente, sécurisée et évolutive, capable de répondre aux besoins de l'ensemble de ses collaborateurs répartis sur ses différents sites.

Segmentation réseau

La société dispose de cinq sites. L'adresse réseau définie par NOVATIS Industries est 192.168.10.0 avec un masque par défaut en 255.255.255.0. Il vous est demandé de modifier ce masque afin de segmenter ce réseau en cinq sous-réseaux distincts, chacun correspondant à un site géographique de l'entreprise, tout en optimisant l'utilisation de l'espace d'adressage disponible.

DMZ – Serveur

NOVATIS Industries souhaite disposer d'un site web vitrine présentant son activité, ses cinq sites et ses métiers. Plutôt que de recourir à un hébergement externe, la direction a fait le choix d'un site auto-hébergé sur l'infrastructure de l'entreprise, afin de conserver la maîtrise complète des données, de la disponibilité et des évolutions du service.

Serveur DHCP

Pour automatiser l'attribution des adresses IP sur l'ensemble des sites, un serveur DHCP sera mis en place. Des plages d'adresses distinctes seront définies pour chaque site afin d'assurer une segmentation claire du réseau et de faciliter l'identification des équipements selon leur localisation géographique.

Protocole de routage OSPF

Le routage dynamique entre les différents sites sera assuré par le protocole OSPF (Open Shortest Path First). Ce protocole de routage à état de liens permettra aux routeurs du réseau de partager automatiquement les informations de topologie, de calculer les meilleurs chemins et de s'adapter rapidement en cas de panne ou de modification de l'infrastructure.

Access Lists

Mettre en place les politique de sécurité nécessaire pour la société novatis.

Protocole HSRP

NOVATIS Industries souhaite qu'en cas de panne d'un routeur assurant l'accès réseau d'un site vers le reste de l'infrastructure, les utilisateurs ne perçoivent aucune coupure de service. Un mécanisme de redondance de passerelle doit donc être mis en place entre au moins deux routeurs partageant un même segment, avec un basculement automatique et transparent, ainsi qu'une reprise de service maîtrisée une fois l'équipement principal rétabli.

Partie théorique :

Tout d'abord quels sont les éléments que nous a communiqué l'entreprise et quel est le besoin ?

@Réseau	192.168.10.0
Masque par défaut	255.255.255.0
Nombre de site	5 sites distant

Quel masque faut-il utilisé pour segmenter le réseau ?

2^3>5 = 8 sous réseaux possible

Masque choisis : 255.255.255.1110 0000

PAS DE 32

5 sous réseaux pour les 5 sites distants :

1er sous réseau : 192.168.10.0 – 255.255.255.224 - /27
Passerelle : 192.168.10.30
@Diffusion : 192.168.10.31
Plage disponible : 192.168.10.1 – 192.168.10.30

2ème sous réseau : 192.168.10.32 – 255.255.255.224 - /27
Passerelle : 192.168.10.62
@Diffusion : 192.168.10.63
Plage disponible : 192.168.10.33 – 192.168.10.61

3ème sous réseau : 192.168.10.64 – 255.255.255.224 - /27
Passerelle : 192.168.10.94
@Diffusion : 192.168.10.95
Plage disponible : 192.168.10.65 – 192.168.10.93

4ème sous réseau : 192.168.10.96 – 255.255.255.224 - /27
Passerelle : 192.168.10.126
@Diffusion : 192.168.10.127
Plage disponible : 192.168.10.97 – 192.168.10.125

5ème sous réseau : 192.168.10.128 – 255.255.255.224 – /27
Passerelle : 192.168.10.158
@Diffusion : 192.168.10.159
Plage disponible : 192.168.10.129 – 192.168.10.157

6ème sous réseau : 192.168.10.160 – 255.255.255.224 - /27
Passerelle : 192.168.10.190
@Diffusion : 192.168.10.191
Plage disponible : 192.168.10.161 – 192.168.10.189

7ème sous réseau : 192.168.10.192 – 255.255.255.224 /27
Passerelle : 192.168.10.222
@Diffusion : 192.168.10.223
Plage disponible : 192.168.10.193 – 192.168.10.221

8ème sous réseau : 192.168.10.224 – 255.255.255.224 /27
Passerelle : 192.168.10.254
@Diffusion : 192.168.10.255
Plage disponible : 192.168.10.225 – 192.168.10.253

Partie Pratique :

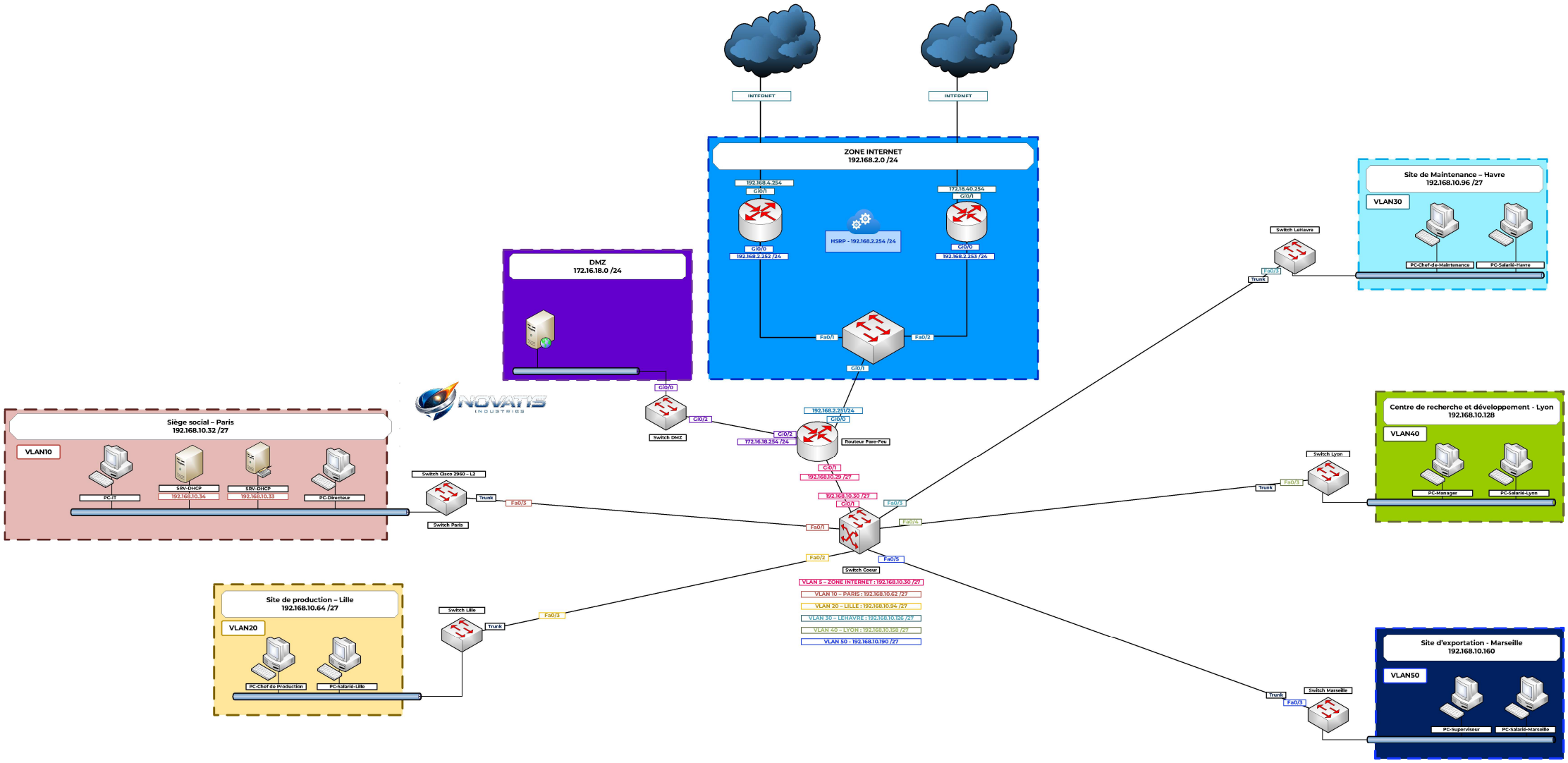
PARTIE 1 – MISE EN PLACE DE L'ENVIRONEMENT

Etape 1 : Maquettage sur Visio et mise en tableau sur Excel

Tableau des sous-réseaux pour la société NOVATIS – Partie Site Entreprise :

SR	Adresse Réseau	Passerelle	Adresse Diffusion
SR_1 - ZONE_INTERNET	192.168.10.0	192.168.10.30	192.168.10.31
SR_2 - PARIS	192.168.10.32	192.168.10.62	192.168.10.63
SR_3 - LILLE	192.168.10.64	192.168.10.94	192.168.10.95
SR_4 - LEHAVRE	192.168.10.96	192.168.10.126	192.168.10.127
SR_5 - LYON	192.168.10.128	192.168.10.158	192.168.10.159
SR_6 - MARSEILLE	192.168.10.160	192.168.10.190	192.168.10.191
Prochain_SR	192.168.10.192	192.168.10.222	192.168.10.223

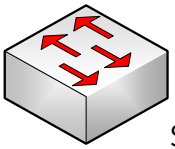
Schéma Réseau de l'infrastructure de NOVATIS :



PARTIE 2 – ADMINISTRATION RESEAU – COUCHE_2_LIAISON

- ☞ **Paramétrage IP des Interfaces**
- ☞ **Paramétrage des VLANs pour chaque site**

<u>Etape 1 :</u> Administration des différentes vlans et interfaces sur les Switch de niveau 2 :



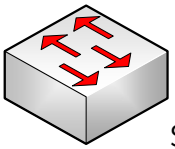
Switch N°1 – Paris :

Configuration du VLAN 10 - Paris

```
Switch(config)#vlan 10
Switch(config-vlan)#name Paris
Switch(config-vlan)#exit
Switch(config)#
Switch(config)#interface range fa0/1-2
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan 10
Switch(config-if-range)#no sh
Switch(config-if-range)#exit
Switch(config)#
Switch(config)#interface fa0/4
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 10
Switch(config-if)#no sh
Switch(config-if)#exit
Switch(config)#
```

Configuration du mode trunk pour l'étiquetage des paquets

```
Switch(config)#interface fa0/3
Switch(config-if)#switchport mode trunk
Switch(config-if)#exit
Switch(config)#
```



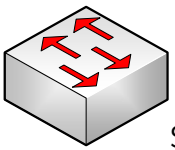
Switch N°2 – Lille :

Configuration du VLAN 20 – Lille

```
Switch(config)#vlan 20
Switch(config-vlan)#name Lille
Switch(config-vlan)#exit
Switch(config)#interface range fa0/1-4
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#interface range fa0/1-4
Switch(config-if-range)#switchport access vlan 10
Switch(config-if-range)#no sh
Switch(config-if-range)#exit
```

Configuration du mode trunk pour l'étiquetage des paquets

```
Switch(config)#interface fa0/3
Switch(config-if)#switchport mode trunk
Switch(config-if)#no sh
Switch(config-if)#exit
```



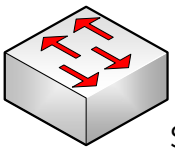
Switch N°3 – Le Havre :

Configuration du VLAN 30 – LeHavre

```
Switch(config)#vlan 30
Switch(config-vlan)#name LEHAVRE
Switch(config-vlan)#exit
Switch(config)#
Switch(config)#interface range fa0/1-2
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan 30
Switch(config-if-range)#no sh
Switch(config-if-range)#exit
Switch(config)#
```

Configuration du mode trunk pour l'étiquetage des paquets

```
Switch(config)#interface fa0/3
Switch(config-if)#switchport mode trunk
Switch(config-if)#no sh
Switch(config-if)#exit
```



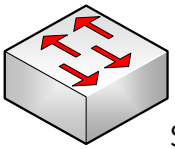
Switch N°4 – Lyon :

Configuration du VLAN 40 – Lyon

```
Switch(config)#vlan 40
Switch(config-vlan)#name Lyon
Switch(config-vlan)#exit
Switch(config)#
Switch(config-if)#int gi0/1
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 40
Switch(config-if)#exit


Switch(config)#
Switch(config)#int gi0/0
Switch(config-if)#switchport trunk encap dot1q
Switch(config-if)#switchport mode trunk
Switch(config-if)#no sh
Switch(config-if)#exit
```

Configuration du mode trunk pour l'étiquetage des paquets

```
Switch(config)#int gi0/0
Switch(config-if)#switchport trunk encap dot1q
Switch(config-if)#switchport mode trunk
Switch(config-if)#no sh
Switch(config-if)#exit
Switch(config)#
```



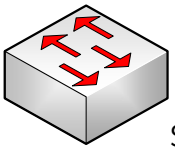
Switch N°5 – Marseille :

Configuration du VLAN 50 – Marseille

```
Switch(config)#vlan 50
Switch(config-vlan)#name Marseille
Switch(config-vlan)#exit
Switch(config)#
Switch(config)#int gi0/1
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 50
Switch(config-if)#no sh
Switch(config-if)#exit
```

Configuration du mode trunk pour l'étiquetage des paquets

```
Switch(config)#int gi0/0
Switch(config-if)#switchport trunk encap dot1q
Switch(config-if)#switchport mode trunk
Switch(config-if)#no sh
Switch(config-if)#exit
Switch(config)#
```



Switch N°6 – ZONE_INTERNET :

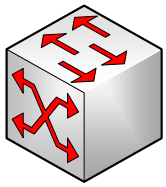
Configuration du VLAN 60 – ZONE_INTERNET

```
Switch(config)#interface gi0/1
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 60
Switch(config-if)#no sh
Switch(config-if)#exit

Switch(config)#interface gi0/2
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 60
Switch(config-if)#no sh
Switch(config-if)#exit
```

Configuration du mode trunk pour l'étiquetage des paquets

```
Switch(config)#interface gi0/0
Switch(config-if)#switchport trunk encap dot1q
Switch(config-if)#swichport mode trunk
Switch(config-if)#switchport mode trunk
Switch(config-if)#no sh
Switch(config-if)#exit
```

Etape 2 : Administration des différentes vlans et interfaces sur le Switch Cœur.



SwitchCoeur :

Configuration des VLANs

```
SwitchCoeur(config)#vlan 5
SwitchCoeur(config-vlan)#name ZONEINTERNET
SwitchCoeur(config)#vlan 10
SwitchCoeur(config-vlan)#name PARIS
SwitchCoeur(config-vlan)#EXIT
SwitchCoeur(config)#
SwitchCoeur(config-vlan)#exit
SwitchCoeur(config)#vlan 20
SwitchCoeur(config-vlan)#name LILLE
SwitchCoeur(config-vlan)#exit
SwitchCoeur(config)#
SwitchCoeur(config)#vlan 30
SwitchCoeur(config-vlan)#name HAVRE
SwitchCoeur(config-vlan)#exit
SwitchCoeur(config)#
SwitchCoeur(config)#vlan 40
SwitchCoeur(config-vlan)#name LYON
SwitchCoeur(config-vlan)#exit
SwitchCoeur(config)#
SwitchCoeur(config)#vlan 50
SwitchCoeur(config-vlan)#name MARSEILLE
SwitchCoeur(config-vlan)#exit
```

Configuration IP des interfaces de chaque VLANs :

```
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#interface vlan 5
Switch(config-if)#ip address 192.168.10.30 255.255.255.224
Switch(config-if)#no sh
Switch(config-if)#exit
Switch(config)#

Switch(config)#interface vlan 10
Switch(config-if)#ip address 192.168.10.62 255.255.255.224
Switch(config-if)#no sh
Switch(config-if)#exit
Switch(config)#

Switch(config)#interface vlan 20
Switch(config-if)#ip address 192.168.10.94 255.255.255.224
Switch(config-if)#no sh
Switch(config-if)#exit

Switch(config)#interface vlan 30
Switch(config-if)#ip address 192.168.10.126 255.255.255.224
Switch(config-if)#no sh
Switch(config-if)#exit

Switch(config)#interface vlan 40
Switch(config-if)#ip address 192.168.10.158 255.255.255.224
Switch(config-if)#no sh
Switch(config-if)#exit

Switch(config)#interface vlan 50
Switch(config-if)#ip address 192.168.10.190 255.255.255.224
Switch(config-if)#no sh
Switch(config-if)#exit
```

Configuration du mode trunk sur chaque port :

```
SwitchCoeur(config)#interface range fa0/1-5
SwitchCoeur(config-if-range)#switchport trunk encap dot1q
SwitchCoeur(config-if-range)#switchport mode trunk
SwitchCoeur(config-if-range)#no sh
SwitchCoeur(config-if-range)#exit
```

PARTIE 3 – ADMINISTRATION RESEAU – COUCHE_3_RESEAU

- ☞ **Paramétrage du Routage dynamique avec le protocole OSPF**
- ☞ **Paramétrage du protocole OSPF avec la zone internet**

Eléments à mettre en place une fois la maquette fonctionnelle

- ☞ **Paramétrage du protocole de redondance HSRPv2**
- ☞ **Paramétrage du NAT dynamique**
- ☞ **Paramétrage des ACL demandé par l'employeur de NOVATIS**

Etape 1 : Configuration des interfaces physique de la zone internet :

Routeur 1 – ZONE_INTERNET :

```
Router(config)#interface GigabitEthernet0/0
Router(config-if)#ip address 192.168.2.253 255.255.255.0
Router(config-if)#no shutdown
```

Routeur 2 – ZONE_INTERNET :

```
Router(config)#interface GigabitEthernet0/0
Router(config-if)#ip address 192.168.2.252 255.255.255.0
Router(config-if)# no shutdown
```

Routeur-PareFeu :

```
Router(config)#interface gi0/1
Router(config-if)#ip address 192.168.10.29 255.255.255.224
Router(config-if)#no sh
Router(config-if)#exit

Router(config)#interface gi0/0
Router(config-if)#ip address 192.168.2.251 255.255.255.0
Router(config-if)#no sh
Router(config-if)#exit

Router(config)#interface gi0/2
Router(config-if)#ip address 172.16.18.254 255.255.255.0
Router(config-if)#no sh
Router(config-if)#exit
```

SwitchCoeur – Port router :

Pour utiliser le sous-réseau 192.168.10.0/27, j'ai passé un port en mode access affecté au VLAN 5 pour créer un segment réseau pour accéder à la ZONE_INTERNET.

```
SwitchCoeur(config)#interface gi0/1
SwitchCoeur(config-if)#switchport mode access
SwitchCoeur(config-if)#switchport access vlan 5
SwitchCoeur(config-if)#no sh
SwitchCoeur(config-if)#exit
```

<u>Etape 2 :</u> Configuration du routage dynamique avec le protocole OSPF :

Quels réseaux connait déja le Routeur-Parefeu ?

```
Router#sh ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
* - candidate default, U - per-user static route, o - ODR
P - periodic downloaded static route

Gateway of last resort is not set

172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks
C 172.16.18.0/24 is directly connected, GigabitEthernet0/2
L 172.16.18.254/32 is directly connected, GigabitEthernet0/2
192.168.2.0/24 is variably subnetted, 2 subnets, 2 masks
C 192.168.2.0/24 is directly connected, GigabitEthernet0/0
L 192.168.2.251/32 is directly connected, GigabitEthernet0/0
192.168.10.0/24 is variably subnetted, 2 subnets, 2 masks
C 192.168.10.0/27 is directly connected, GigabitEthernet0/1
L 192.168.10.29/32 is directly connected, GigabitEthernet0/1
```

Il connait les réseaux suivants :

- **172.16.18.0/24**
- **192.168.2.0/24**
- **192.168.10.0/24**

Quels réseaux connait déja le SwitchCoeur ?

```
SwitchCoeur(config)#do sh ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
* - candidate default, U - per-user static route, o - ODR
P - periodic downloaded static route

Gateway of last resort is not set

192.168.10.0/27 is subnetted, 6 subnets
C 192.168.10.0 is directly connected, Vlan5
C 192.168.10.32 is directly connected, Vlan10
C 192.168.10.64 is directly connected, Vlan20
C 192.168.10.96 is directly connected, Vlan30
C 192.168.10.128 is directly connected, Vlan40
C 192.168.10.160 is directly connected, Vlan50
```

Il connait les réseaux suivants :

- **192.168.10.0/27**
- **192.168.10.32/27**
- **192.168.10.64/27**
- **192.168.10.96/27**
- **192.168.10.128/27**
- **192.168.10.160/27**

Conclusion :

Le Switch Cœur ne connait que les VLANs auquel il est directement connecté et le Routeur-Pare-Feu ne connait que les réseaux voisins auquel il est connecté.

Pour le Routeur il doit pouvoir connaitre l'ensemble des VLANs pour pouvoir appliquer des futurs ACL correctement.
Pour le Switch Cœur, il doit pouvoir connaitre la DMZ et la ZONE_INTERNET.

Pour l'OSPF on ne déclare que les réseaux qui sont directement connecté à l'équipement.

Configuration OSPF sur le Switch Cœur :

Réseau Inconnus :

- **172.16.18.0/24**
- **192.168.2.0**

```
SwitchCoeur#conf t
Enter configuration commands, one per line. End with CNTL/Z.
SwitchCoeur(config)#router ospf 1
SwitchCoeur(config-router)#network 192.168.10.0 0.0.0.31 area 0
SwitchCoeur(config-router)#network 192.168.10.32 0.0.0.31 area 0
SwitchCoeur(config-router)#network 192.168.10.64 0.0.0.31 area 0
SwitchCoeur(config-router)#network 192.168.10.96 0.0.0.31 area 0
SwitchCoeur(config-router)#network 192.168.10.128 0.0.0.31 area 0
SwitchCoeur(config-router)#network 192.168.10.160 0.0.0.31 area 0
SwitchCoeur(config-router)#exit
SwitchCoeur(config)#
```

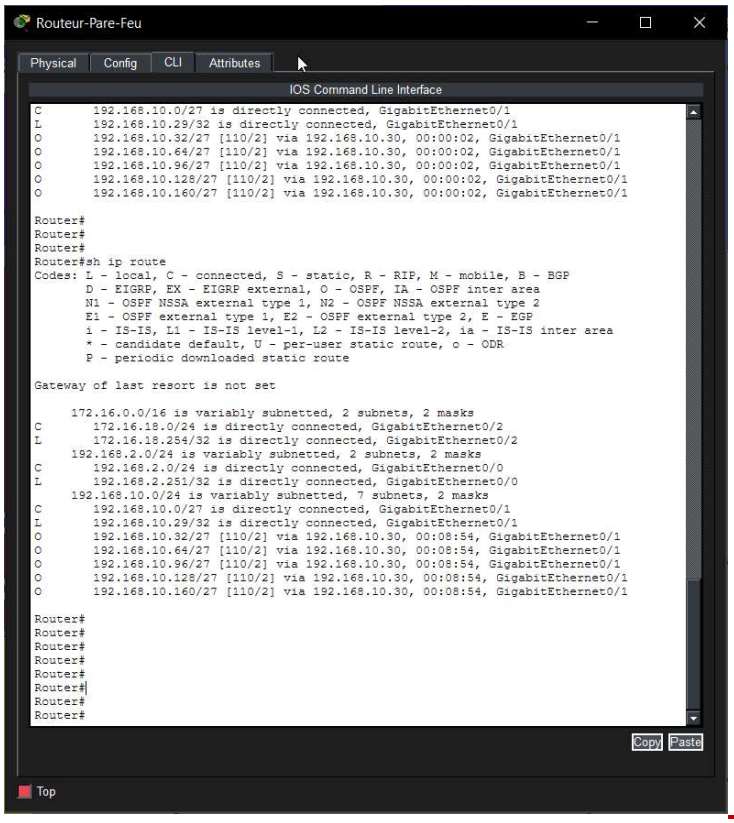
Configuration OSPF sur le Routeur Pare Feu :

Réseau Inconnus :

- **L'ensemble des VLANs**

```
RouteurPareFeu(config)#router ospf 1
RouteurPareFeu(config-router)#network 172.16.18.0 0.0.0.255 area 0
RouteurPareFeu(config-router)#network 192.168.2.0 0.0.0.255 area 0
RouteurPareFeu(config-router)#network 192.168.10.0 0.0.0.31 area 0
```

Bilan de communication :



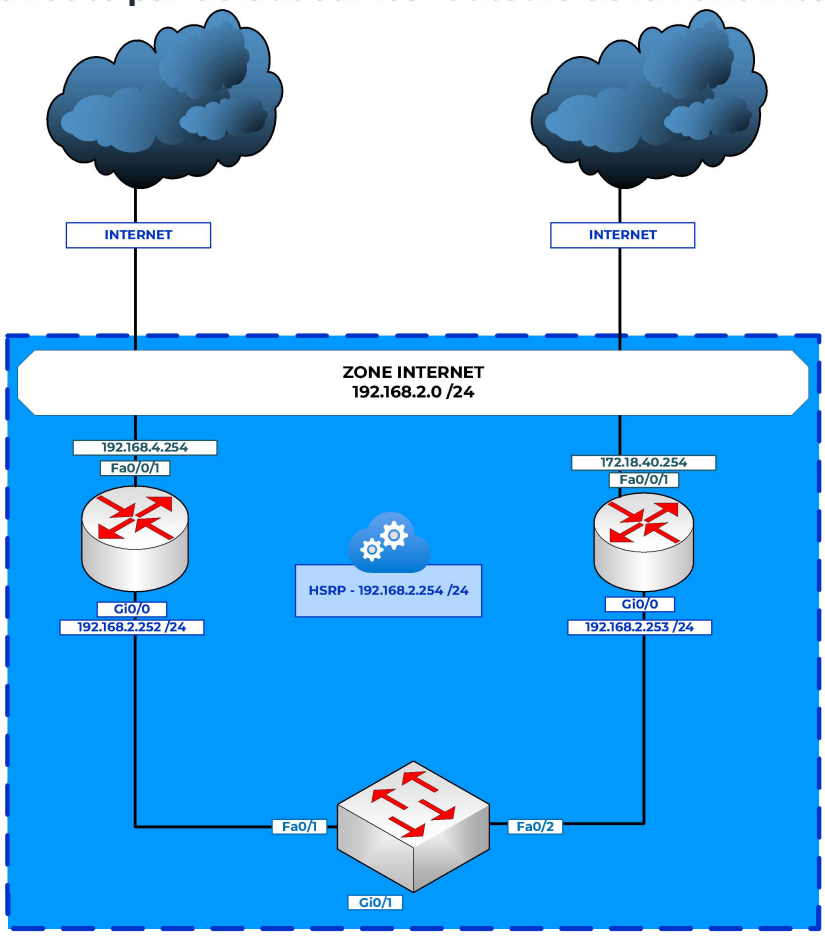
Le routeur-Pare-Feu arrive à bien à voir les suivants :

- **192.168.10.0/27**
- **192.168.10.32/27**
- **192.168.10.64/27**
- **192.168.10.96/27**
- **192.168.10.128/27**
- **192.168.10.160/27**

Le SwitchCoeur arrive bien à voir les réseaux suivants :

- **172.16.18.0/24**
- **192.168.2.0**

Etape 3 : Configurer la route par défaut sur les routeurs de la zone internet




```
Router(config)#ip route 0.0.0.0 0.0.0.0 192.168.2.251
```

Etape 4 : Configuration HSRP v2, Zone Internet NOVATIS

Rappel des adresses dans la zone internet

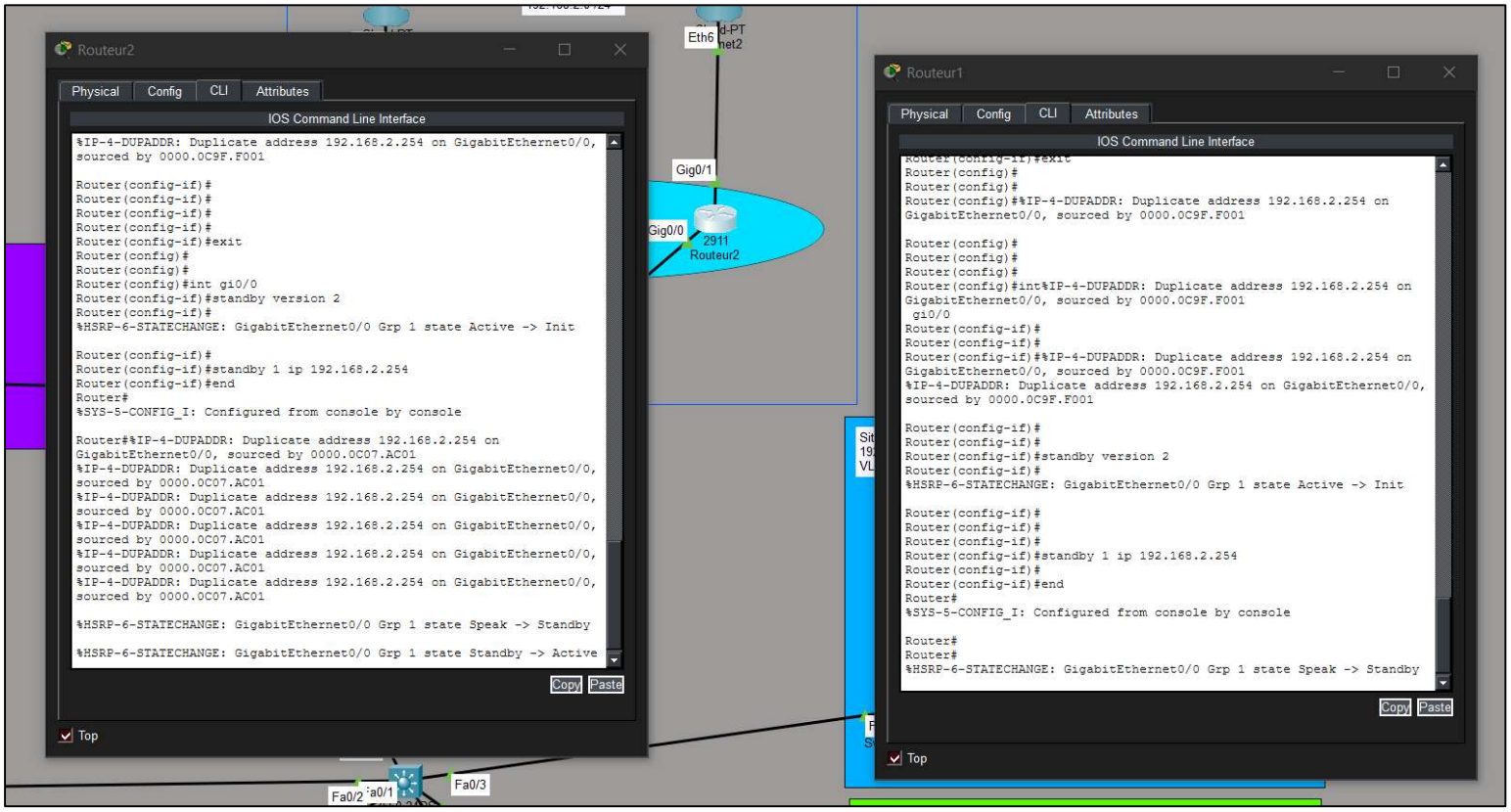
@IP	Nom
192.168.2.251	Passerelle Routeur Pare Feu
192.168.2.252	Passerelle Routeur 1
192.168.2.253	Passerelle Routeur 2
192.168.2.254	VIP HSRP

Sur le routeur 1 :

```
Router(config)#interface gi0/0
Router(config-if)# standby version 2
Router(config-if)#standby 1 ip 192.168.2.254
Router(config-if)#no sh
Router(config-if)#exit
```

Sur le routeur 2 :

```
Router(config)#interface gi0/0
Router(config-if)#standby version 2
Router(config-if)#standby 1 ip 192.168.2.254
Router(config-if)#no sh
Router(config-if)#exit
```

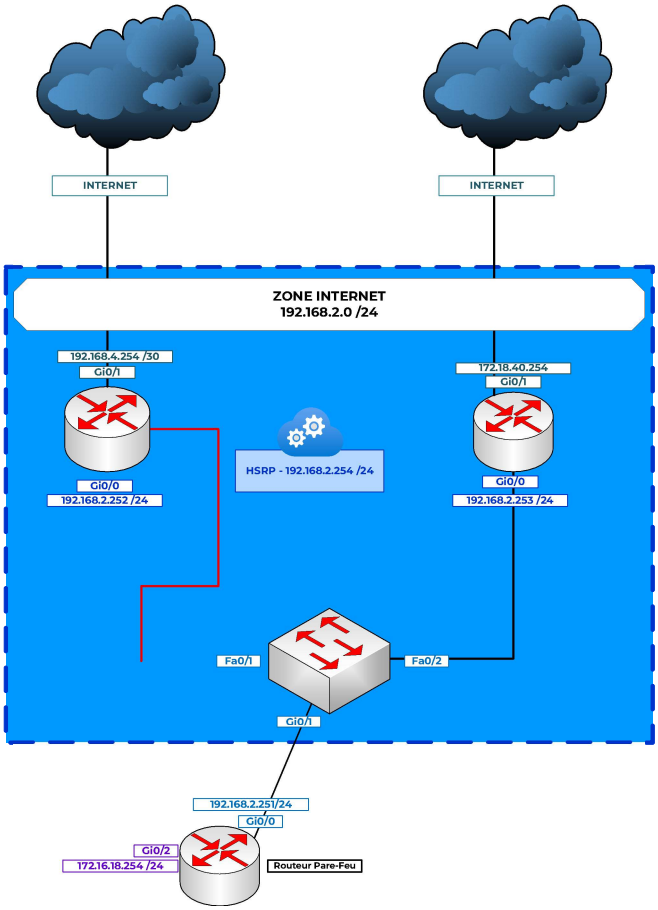


Sur le routeur Pare-Feu :

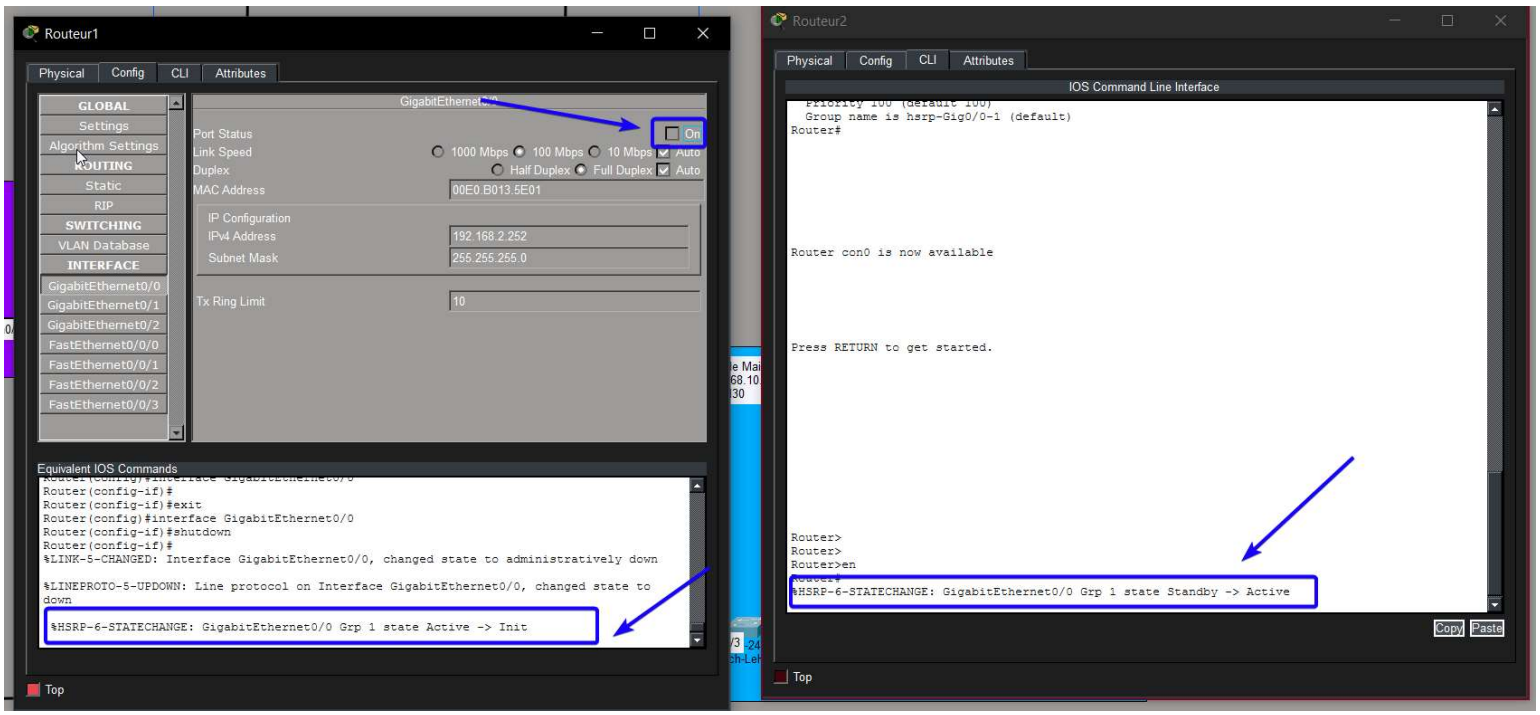
Comme les deux interfaces font partie du même groupe il faut ajouter une route par défaut pour dire au pare feu d'envoyer sur la VIP ce qui va envoyer les paquets sur les deux interfaces.

```
Router(config)#ip route 0.0.0.0 0.0.0.0 192.168.2.254
```

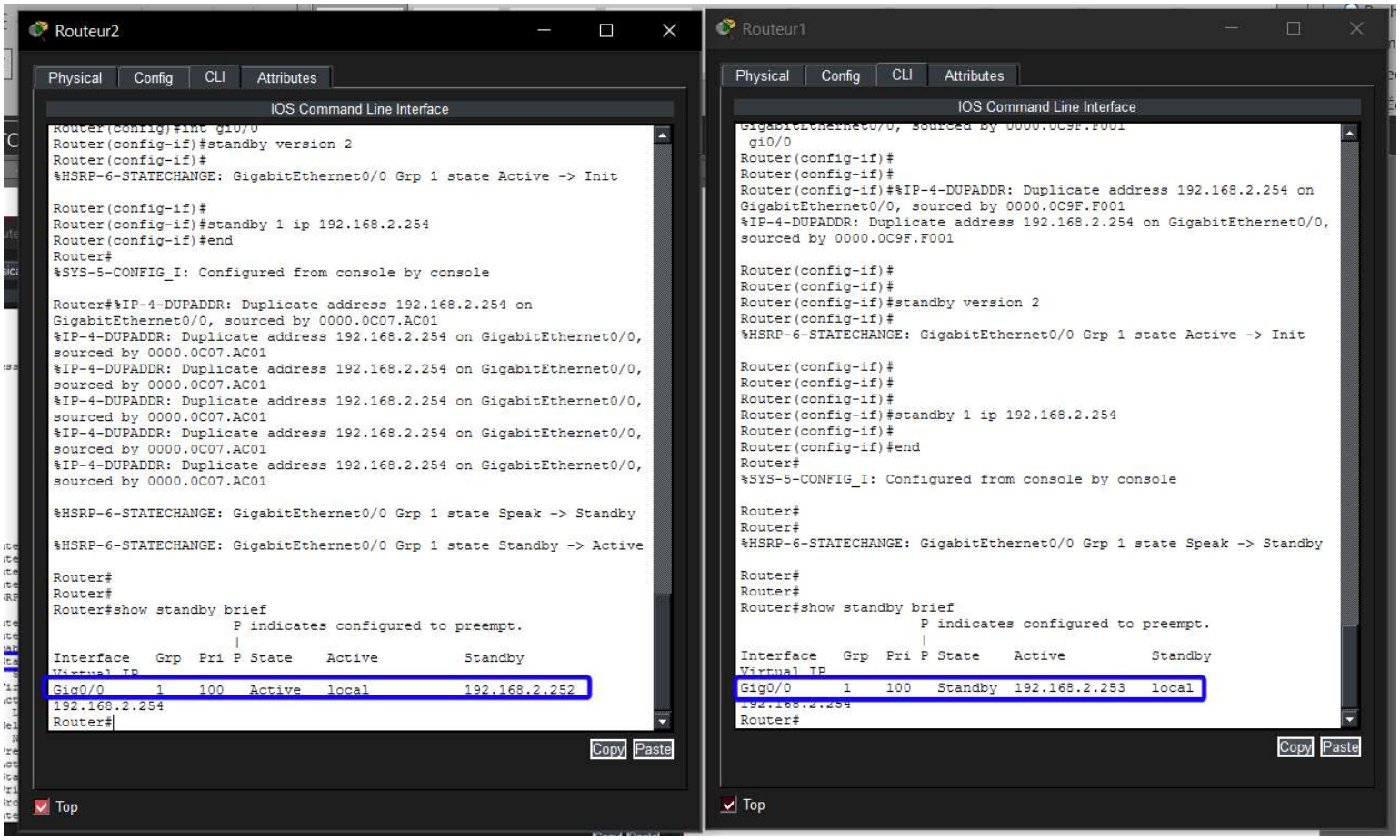
Test de fonctionnement - Rupture de liens



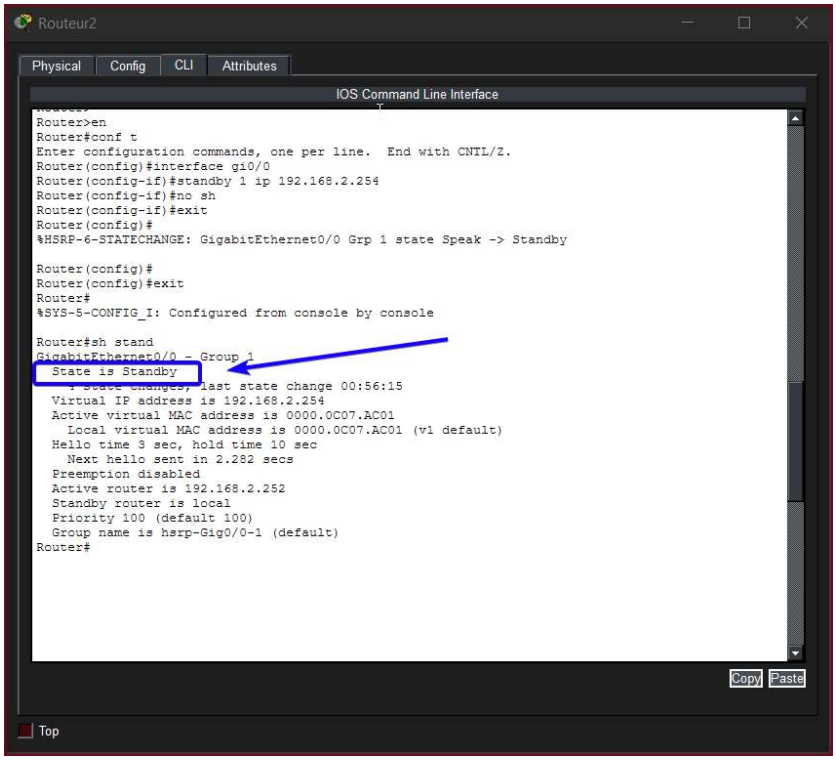
Dés que j'ai coupés le lien dans le Routeur 1 et le Routeur Pare Feu, le logs m'indique qui avertis l'interface voisine de prendre le relay et sur le Routeur 2, le logs confirme que c'est maintenant la Gi0/0 du Routeur 2 qui assure la transmission du flux vers Internet.



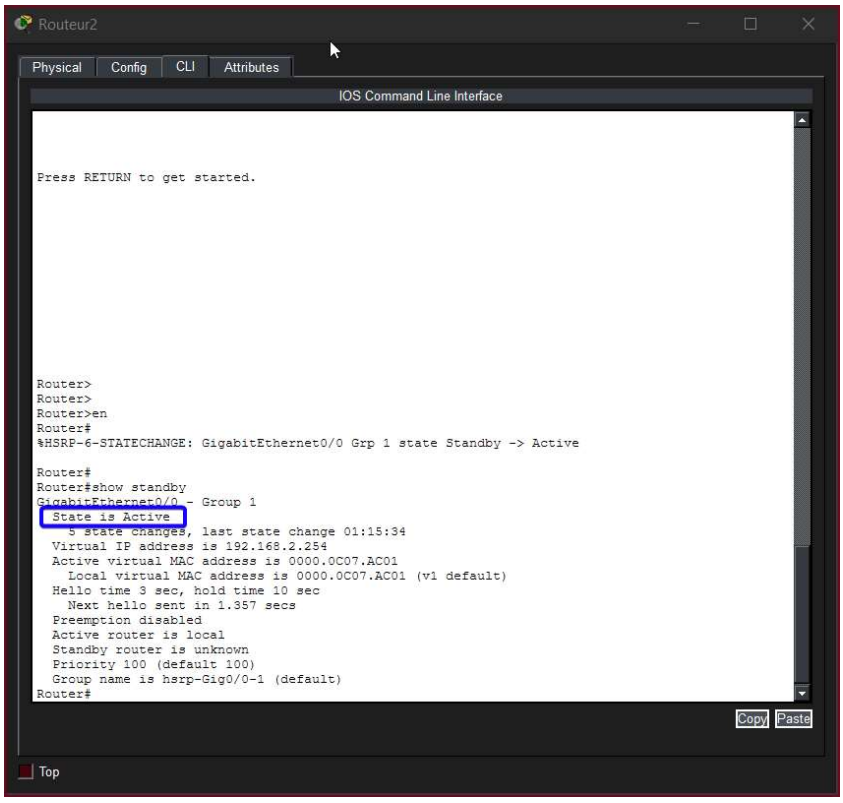
Le protocole HSRP pointe bien sur l'interface voisine de l'autre routeur dans les deux cas :



Tout à l'heure elle indiquait quel été juste présente dans le groupe.



Maintenant comme le lien et rompus elle a le statut active :



<u>Etape 5 :</u> Configuration du NAT dynamique sur les Routeur 1 et 2

Routeur 1 :

Création du pool de translation de d'adresse :

```
Router(config)#ip nat pool NOVATIS-POOL1 192.168.4.1 192.168.4.100 netmask
255.255.255.0
```

Création d'ACL avec des « permit » autorisant le traffic à passer le routeur pour les sous réseau de NOVATIS

```
Router(config)#access-list 10 permit 192.168.10.0 0.0.0.31
Router(config)#access-list 10 permit 192.168.10.32 0.0.0.31
Router(config)#access-list 10 permit 192.168.10.64 0.0.0.31
Router(config)#access-list 10 permit 192.168.10.96 0.0.0.31
Router(config)#access-list 10 permit 192.168.10.128 0.0.0.31
Router(config)#access-list 10 permit 192.168.10.160 0.0.0.31
```

Affectation de la liste 10 d'ACL venant avec les SR Interne inscrit. D'où le inside.

```
Router(config)#ip nat inside source list 10 pool NOVATIS-POOL1
```

Pour effectuer correctement la translation d'adresse on designe les interfaces interne (inside) et externe (ouside) pour le NAT s'applique

```
Router(config)#interface gi0/0
Router(config-if)# ip nat inside
Router(config-if)#exit
Router(config)#
Router(config)#interface gi0/0
Router(config-if)# ip nat outside
Router(config-if)#exit
```

Routeur 2 :

Création du pool de translation de d'adresse :

```
Router(config)#ip nat pool NOVATIS-POOL2 172.18.40.1 172.18.40.100 netmask
255.255.255.0
```

Création d'ACL avec des « permit » autorisant le traffic à passer le routeur pour les sous réseau de NOVATIS

```
Router(config)#access-list 10 permit 192.168.10.0 0.0.0.31
Router(config)#access-list 10 permit 192.168.10.32 0.0.0.31
Router(config)#access-list 10 permit 192.168.10.64 0.0.0.31
Router(config)#access-list 10 permit 192.168.10.64 0.0.0.31
Router(config)#access-list 10 permit 192.168.10.128 0.0.0.31
Router(config)#access-list 10 permit 192.168.10.160 0.0.0.31
Router(config)#
```

Affectation de la liste 10 d'ACL venant avec les SR Interne inscrit. D'où le inside.

```
Router(config)#ip nat inside source list 10 pool NOVATIS-POOL2
```

Pour effectuer correctement la translation d'adresse on designe les interfaces interne (inside) et externe (ouside) pour le NAT s'applique

```
Router(config)#interface gi0/0
Router(config-if)# ip nat inside
Router(config-if)#exit
Router(config)#
Router(config)#interface gi0/1
Router(config-if)#ip nat outside
Router(config-if)#exit
```

<u>Etape 5 :</u> Pour protéger la DMZ et le réseau local de l'entreprise, établir les ACLs nécéssaire sur le routeur pare-feu.

Travail 1 : Tous les sites doivent pouvoir sortir vers Internet, sauf le site de maintenance du Havre (192.168.10.96 /27).

- **Que doit faire l'ACL ? L'ACL doit bloquer le sous réseau 192.168.10.96/27 d'accéder à la zone Internet.**
- **Sur quel routeur faut-il la créer ? Routeur Pare Feu**
- **Sur quelle interface doit-on l'activer ? Interface la plus de la destination : Gi0/0**
- **Dans quel sens ? En out pour bloquer le traffic sortant du sous réseau vers internet.**
- **Type d'ACL : Standard – Entendue Pourquoi ? C'est une ACL Standard car on cherche à bloquer une seule source qui est celle du service maintenance.**

```
RouteurPareFeu(config)#access-list 10 deny 192.168.10.96 0.0.0.31
RouteurPareFeu(config)#access-list 10 permit any

----------------------------------------
deny all (par défaut)

RouteurPareFeu(config)#
RouteurPareFeu(config)#int gi0/0
RouteurPareFeu(config-if)#ip access-group 10 out
RouteurPareFeu(config-if)#exit
```

Travail 2 : Le serveur Web de la DMZ (172.16.18.0 /24) doit être consultable seulement en HTTP par tous les postes internes. Aucun autre service de ce serveur ne doit leur être accessible.

- **Que doit faire l'ACL ? Elle doit empêcher le serveur de délivré autre chose que le protocole HTTP aux sous réseaux.**
- **Sur quel routeur faut-il la créer ? Routeur – Pare feu**
- **Sur quelle interface doit-on l'activer ? Interface la plus de la source (le serveur) Gi0/2**
- **Dans quel sens ? En in on filtre le traffic interne du réseau 172.16.18.0**
- **Type d'ACL : Standard – Entendue Pourquoi ? C'est une ACL Etendue on filtre à la source les protocoles que dois renvoyer le serveur au client.**
-

```
RouteurPareFeu(config)#access-list 110 permit tcp host 172.16.18.1 eq 80
192.168.10.32 0.0.0.31
RouteurPareFeu(config)#access-list 110 permit tcp host 172.16.18.1 eq 80
192.168.10.64 0.0.0.31
RouteurPareFeu(config)#access-list 110 permit tcp host 172.16.18.1 eq 80
192.168.10.96 0.0.0.31
RouteurPareFeu(config)#access-list 110 permit tcp host 172.16.18.1 eq 80
192.168.10.128 0.0.0.31
RouteurPareFeu(config)#access-list 110 permit tcp host 172.16.18.1 eq 80
192.168.10.160 0.0.0.31

----------------------------------------
deny all (par défaut)
```

```
RouteurPareFeu(config)#
RouteurPareFeu(config)#int gi 0/2
RouteurPareFeu(config-if)#ip access-group 110 in
RouteurPareFeu(config-if)#exit
```

Travail 3 : Le serveur Web de la DMZ doit être joignable depuis Internet, mais uniquement en HTTP et HTTPS.

- **Que doit faire l'ACL ? Elle doit rendre accessible le serveur web de la DMZ seulement en HTTP / HTTPS**
- **Sur quel routeur faut-il la créer ? Routeur Pare-feu**
- **Sur quelle interface doit-on l'activer ? Interface la plus de la source (le client) : Gi0/0**
- **Dans quel sens ? Comme c'est du traffic entrant qui vient d'internet c'est in.**
- **Type d'ACL : Standard – Entendue Pourquoi ? Une ACL entendue est nécéssaire pour filtrer les paquets que renvoie le serveur aux clients d'internet.**

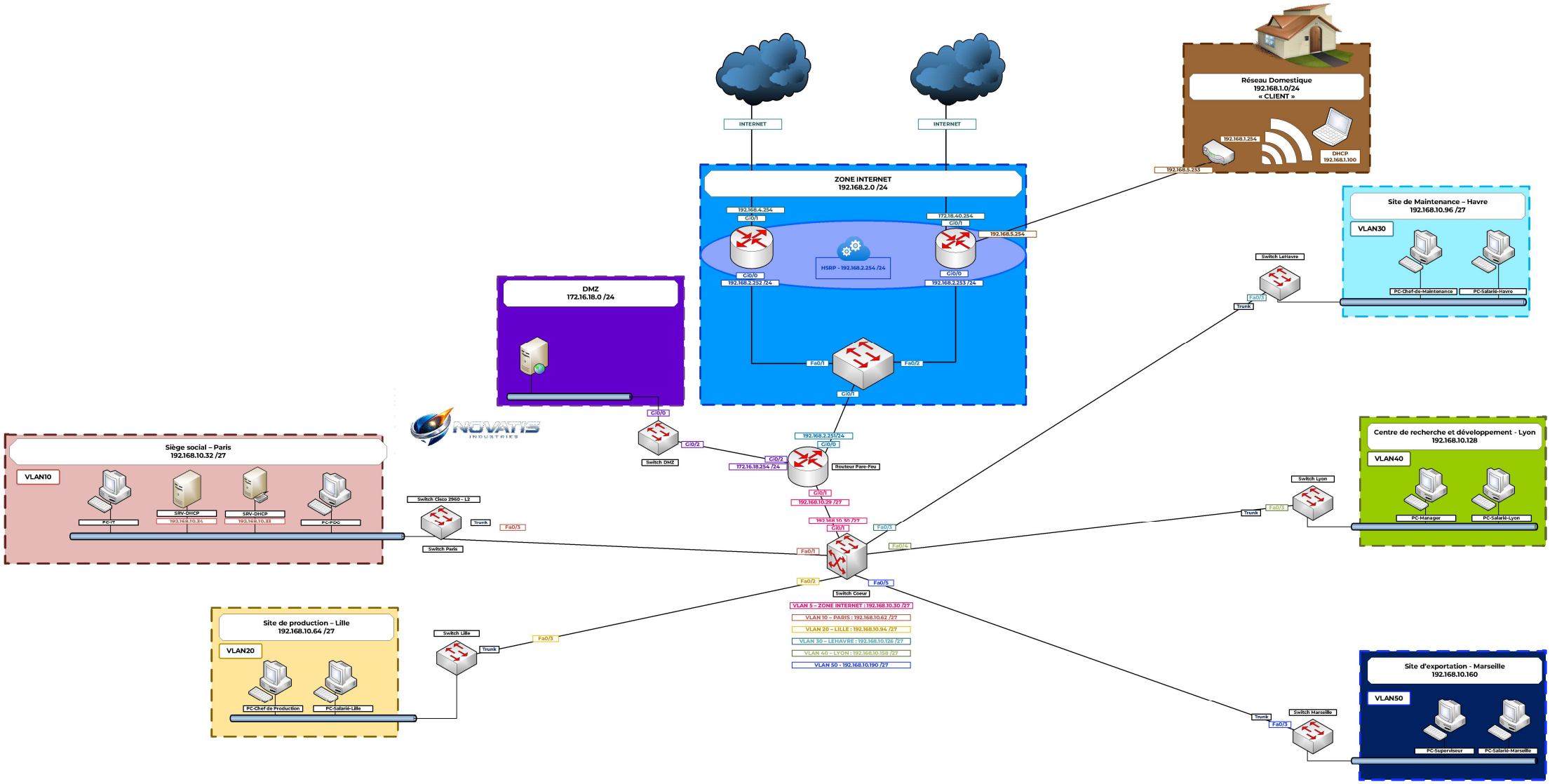
```
RouteurPareFeu#conf t
RouteurPareFeu(config)#access-list 110 permit tcp 192.168.5.0 0.0.0.255 host
172.16.18.1 eq 80
RouteurPareFeu(config)#access-list 110 permit tcp 192.168.5.0 0.0.0.255 host
172.16.18.1 eq 443
RouteurPareFeu(config)#exit

----------------------------------------
deny all (par défaut)

RouteurPareFeu # conf t
RouteurPareFeu (config)# int gi 0/0
RouteurPareFeu (config-if)# ip access-group 120 in
```

Pour que le retour du serveur se fasse il faut ajouter les lignes suivantes à l'ACL qui correspond au traffic retour entrant du SRV-WEB vers le RouteurParFeu qui indique que le réseau 192.168.5.0/24 accède en HTTP/HTTPS au site. Le réseau 192.168.1.0 à effectuer une translation d'adresse pour aller vers le Internet donc par concéquent le paquets prend l'adresse de segment WAN.

Schéma Réseau :

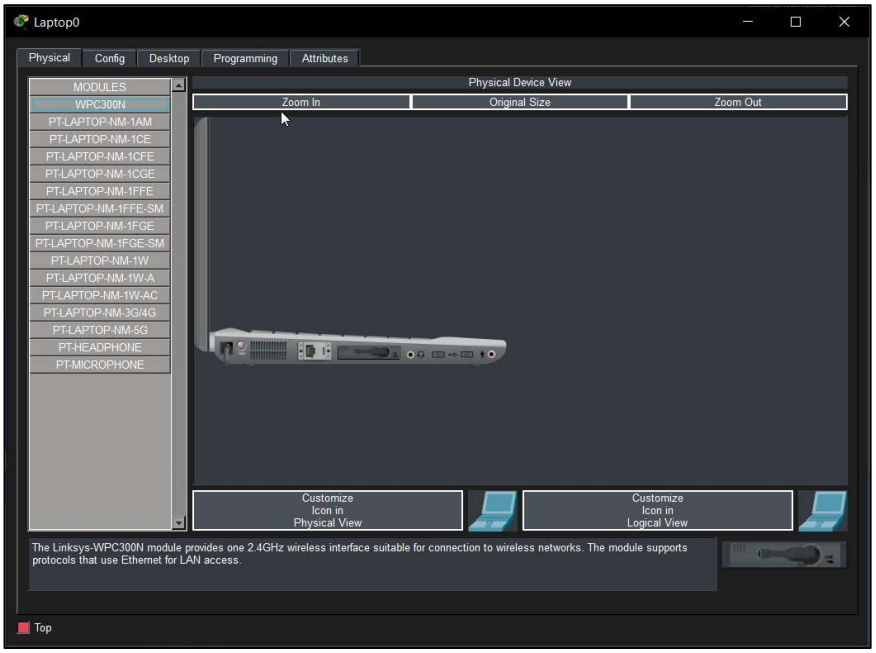
Ajout du réseau Domestique pour tester l'ACL d'Internet :

- **Un réseau domestique en 192.168.1.0/24**
- **Un segment réseau pour le WAN (Internet) en 192.168.5.0/24**

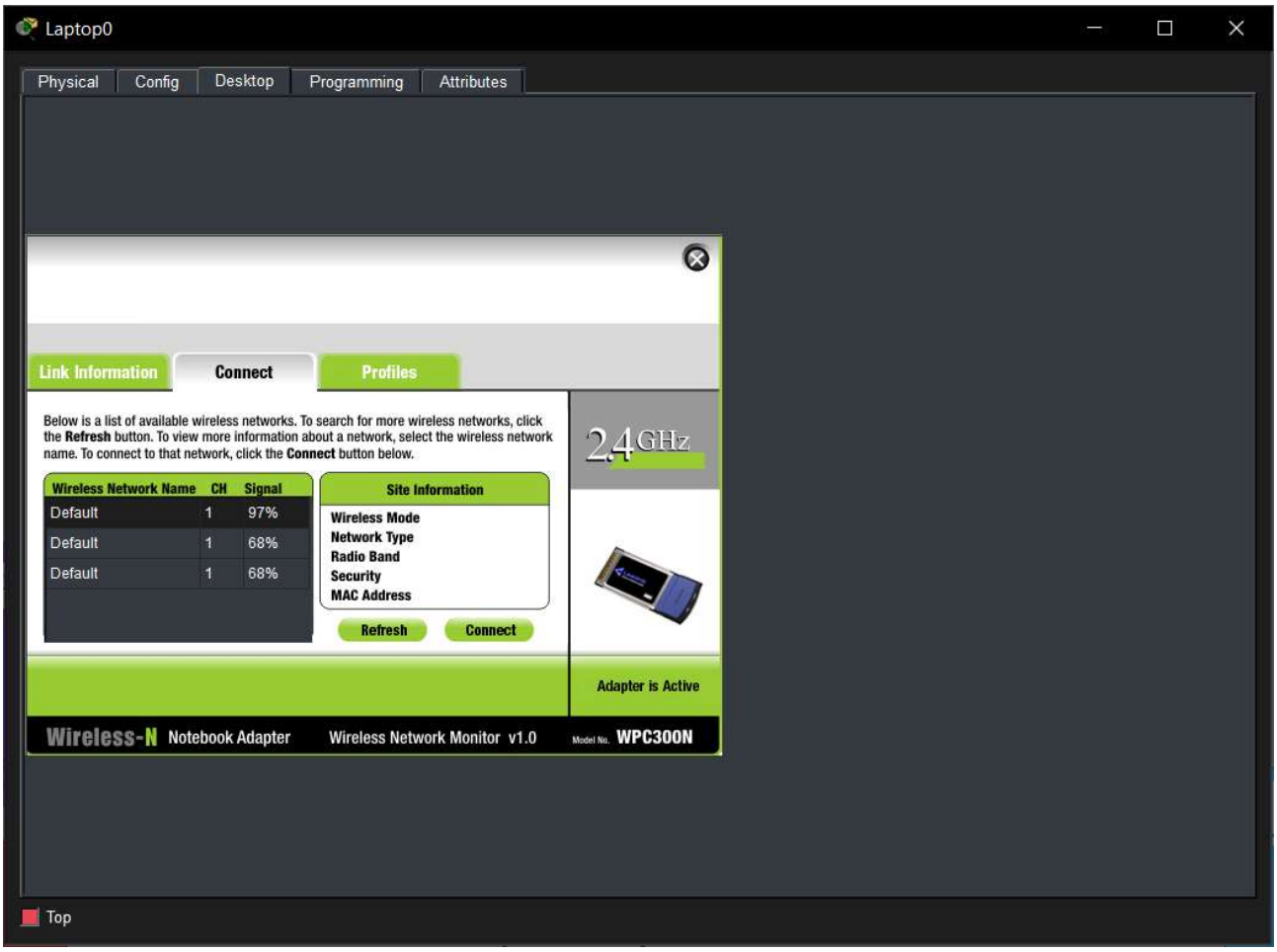


Paramétrage de la Boxe du FAI pour le Client à son domicile :

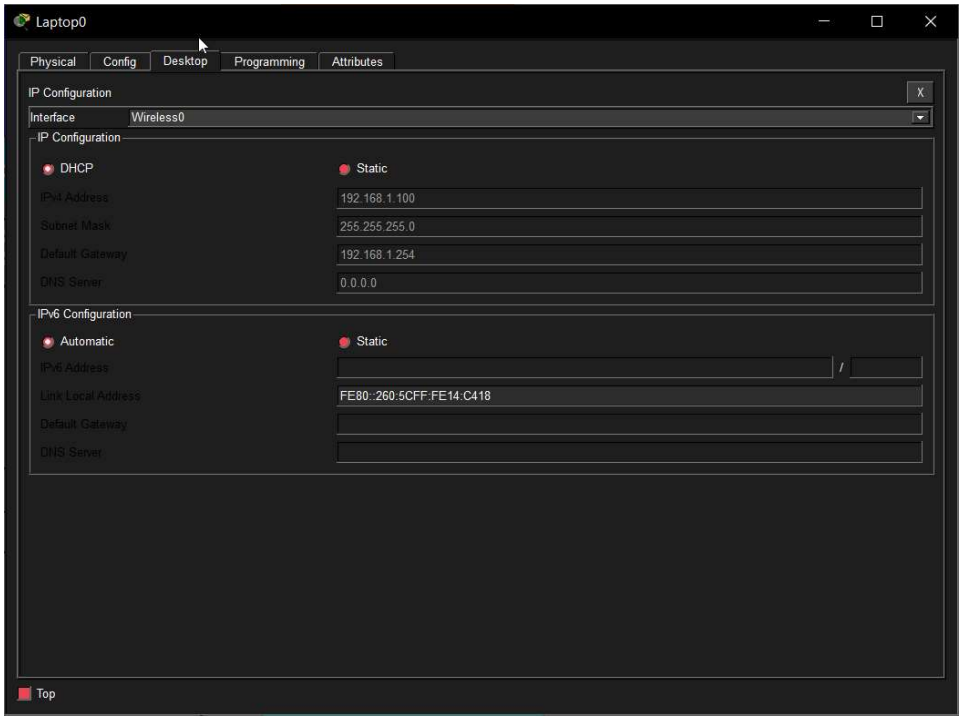
❶ Ajout d'une carte Wi-Fi sur le PC Portable du client :



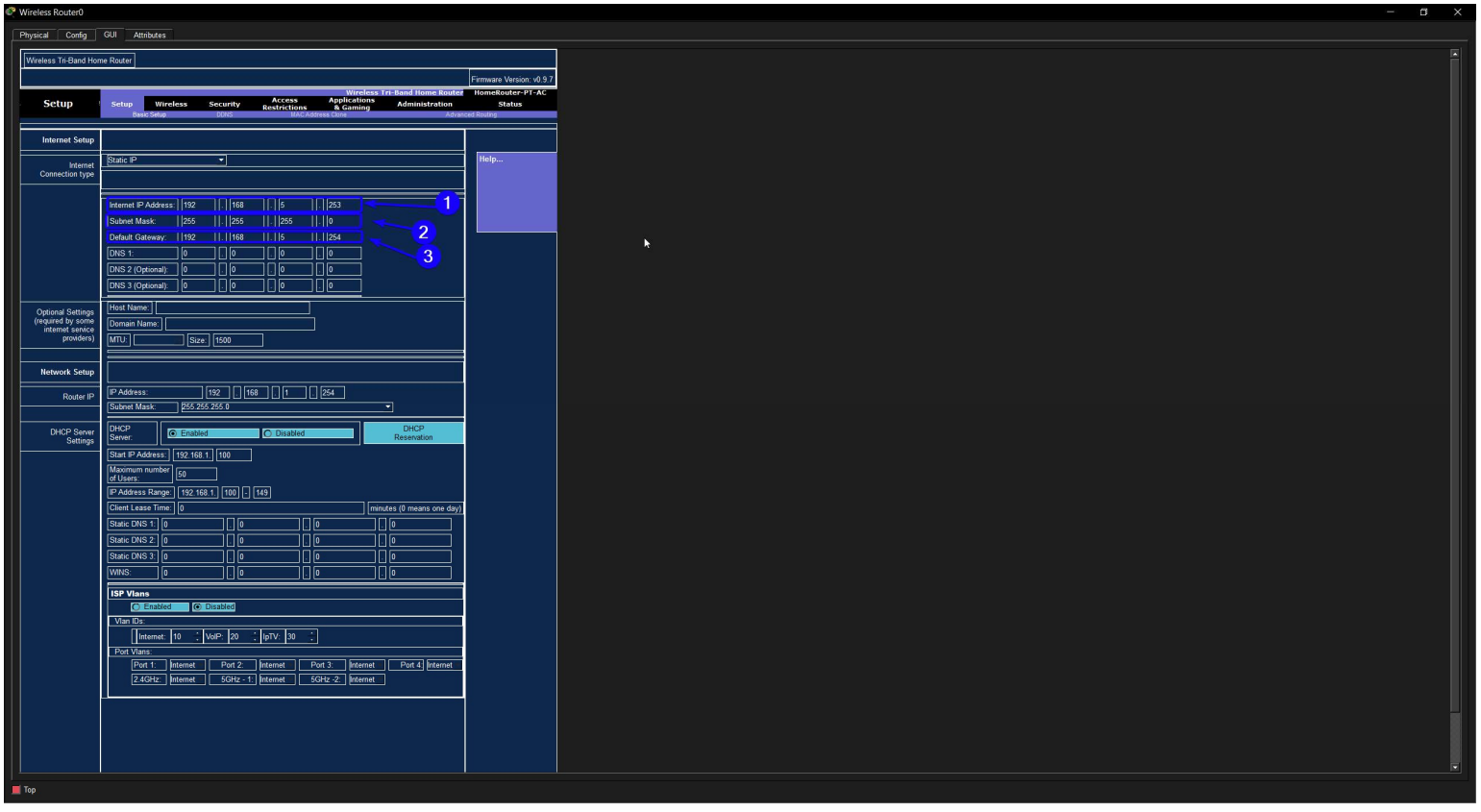
❷ Activation du Wifi :



❸ Le PC reçoit sont sa config IP grâce au DHCP de la Boxe.



❹ Adressage Statique sur l'interface Internet.



Routage à mis en place pour cela fonctionne en aller/retour :

Routage statique sur le RouteurParefeu :

Le RouteurPareFeu doit connaitre le segement WAN 192.168.5.0/24

```
RouteurPareFeu#conf t
RouteurPareFeu(config)#ip route 192.168.5.0 255.255.255.0 192.168.5.253
```

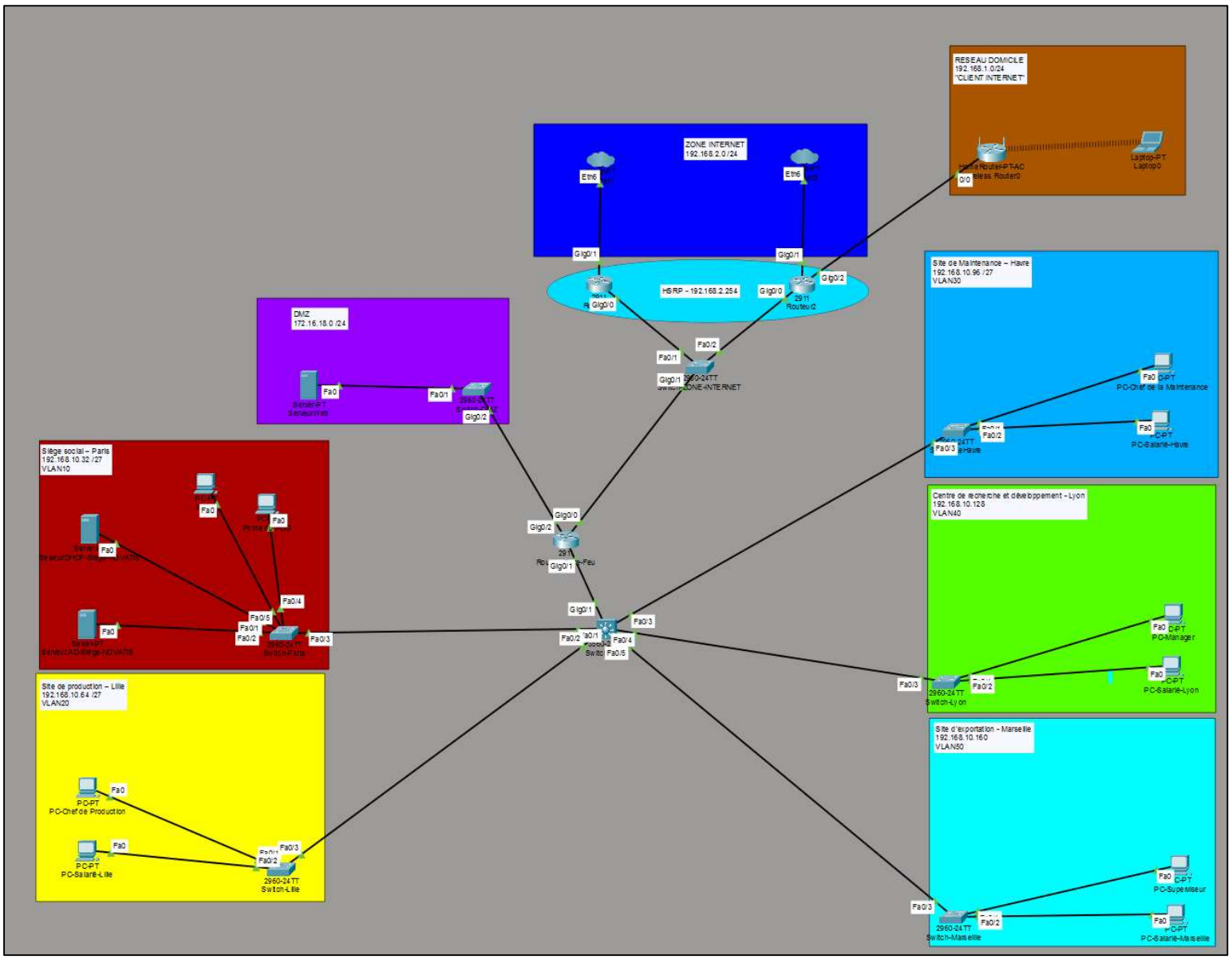
Routage statique sur le Routeur1 :

Le Routeur doit connaitre le réseau 192.168.1.0/24

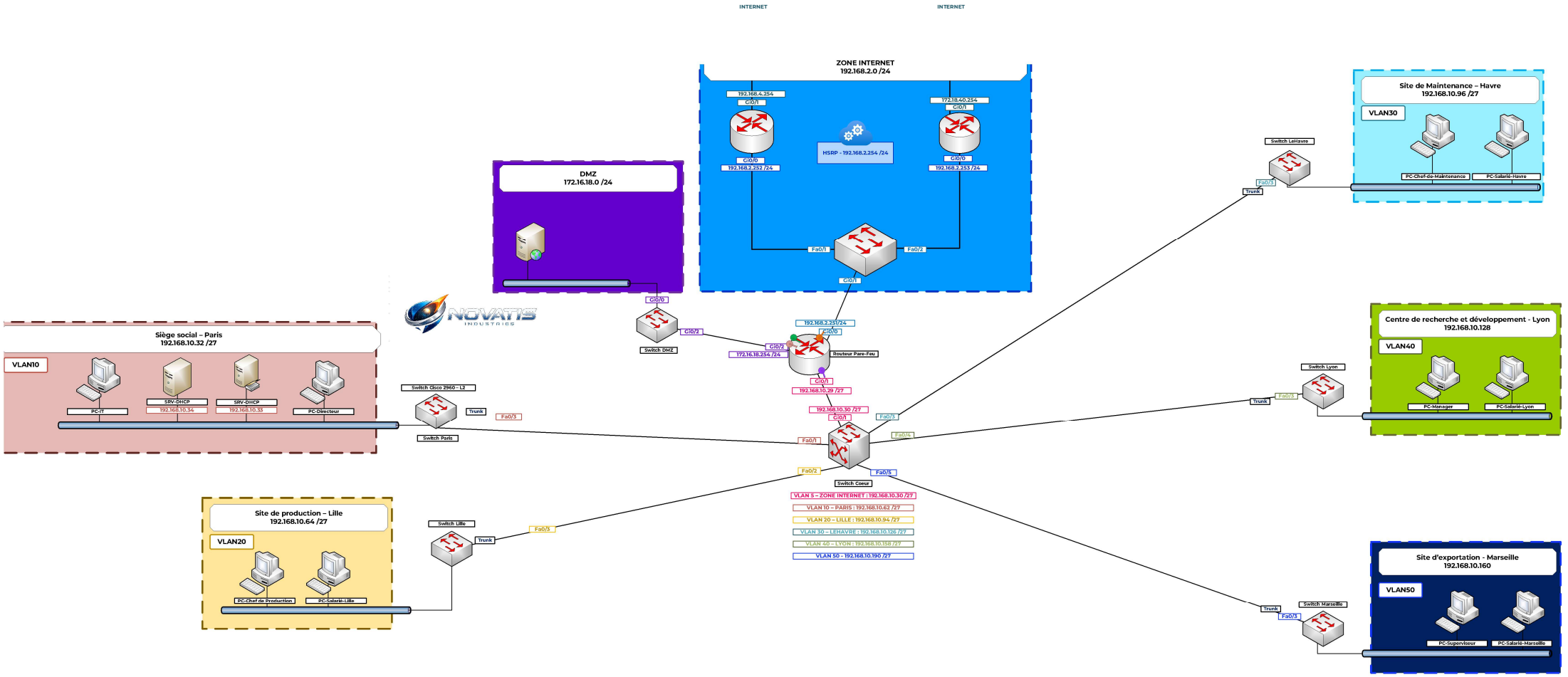
```
RouteurPareFeu#conf t
RouteurPareFeu(config)# ip route 192.168.1.0 255.255.255.0 192.168.5.253
```

En suite mise en place l'ACL du Travail n°3

Résultat sur Packet Tracer :



Comme les ACLs se configure qu'en ligne de commande pour avoir un visuel et les paquets entrants et sortants j'ai mit des pastilles et des flèches de couleurs correspondant à chaque ACL affecté à telle interface.



Travail 4 : Seul le PC-IT du siège de Paris doit pouvoir ouvrir une session d'administration avec le protocole SSH à distance sur le routeur pare-feu lui-même. Toute autre machine, interne comme externe, est refusée.

- **Que doit faire l'ACL ?** L'ACL doit bloquer tous les autres hôtes de NOVATIS sauf le PC IT de l'entreprise.
- **Sur quel routeur faut-il la créer ?** Routeur Pare-Feu
- **Sur quelle interface doit-on l'activer ?** line vty 0 4
- **Dans quel sens ?** En in car c'est du traffic entrant emis par l'IT depuis le siège de NOVATIS.
- **Type d'ACL : Standard – Entendue Pourquoi ?** J'ai choisi de faire une ACL Etendue pour etre au plus proche de source qui émet le traffic pour établir une session SSH.

Mise en place du SSH pour l'IT sur le Routeur Pare Feu

```
Router>en
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
RouteurPareFeu (config)#line vty 0 4
RouteurPareFeu (config-line)#transport input ssh
RouteurPareFeu (config-line)#login local
RouteurPareFeu (config-line)#password cisco
RouteurPareFeu (config-line)#ip domain name novatis.key
RouteurPareFeu(config)#crypto key generate rsa general-keys modulus 2048
The name for the keys will be: RouteurPareFeu.novatis.key

% The key modulus size is 2048 bits
% Generating 2048 bit RSA keys, keys will be non-exportable...[OK]
*Mar 2 5:0:38.64: %SSH-5-ENABLED: SSH 1.99 has been enabled
RouteurPareFeu(config)#username admin password cisco
RouteurPareFeu(config)#
```

Mise en place de l'ACL :

```
RouteurPareFeu(config)#ip access-list standard ADMIN_VTY
RouteurPareFeu(config-std-nacl)#permit host 192.168.10.36
RouteurPareFeu(config-std-nacl)#exit
RouteurPareFeu(config)#
```

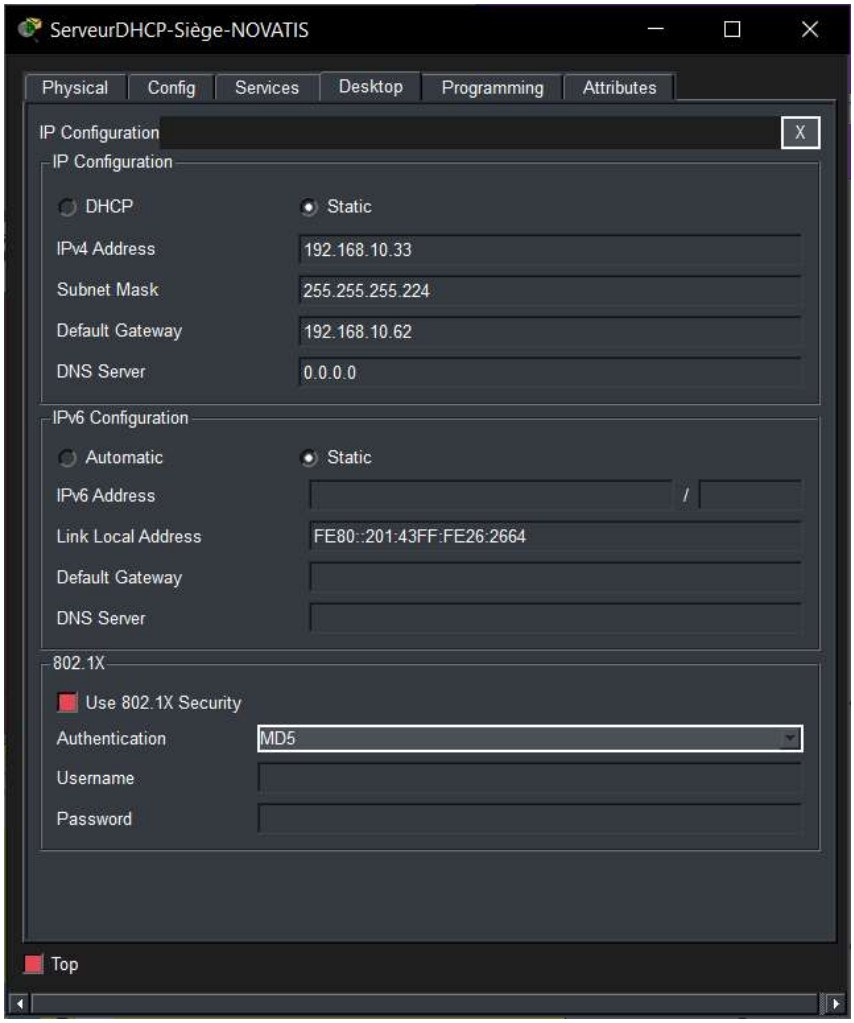
Application de l'ACL sur le line vty :

```
RouteurPareFeu(config)#line vty 0 4
RouteurPareFeu(config-line)#access-class ADMIN_VTY in
RouteurPareFeu(config-line)#password cisco
RouteurPareFeu(config-line)#login local
```

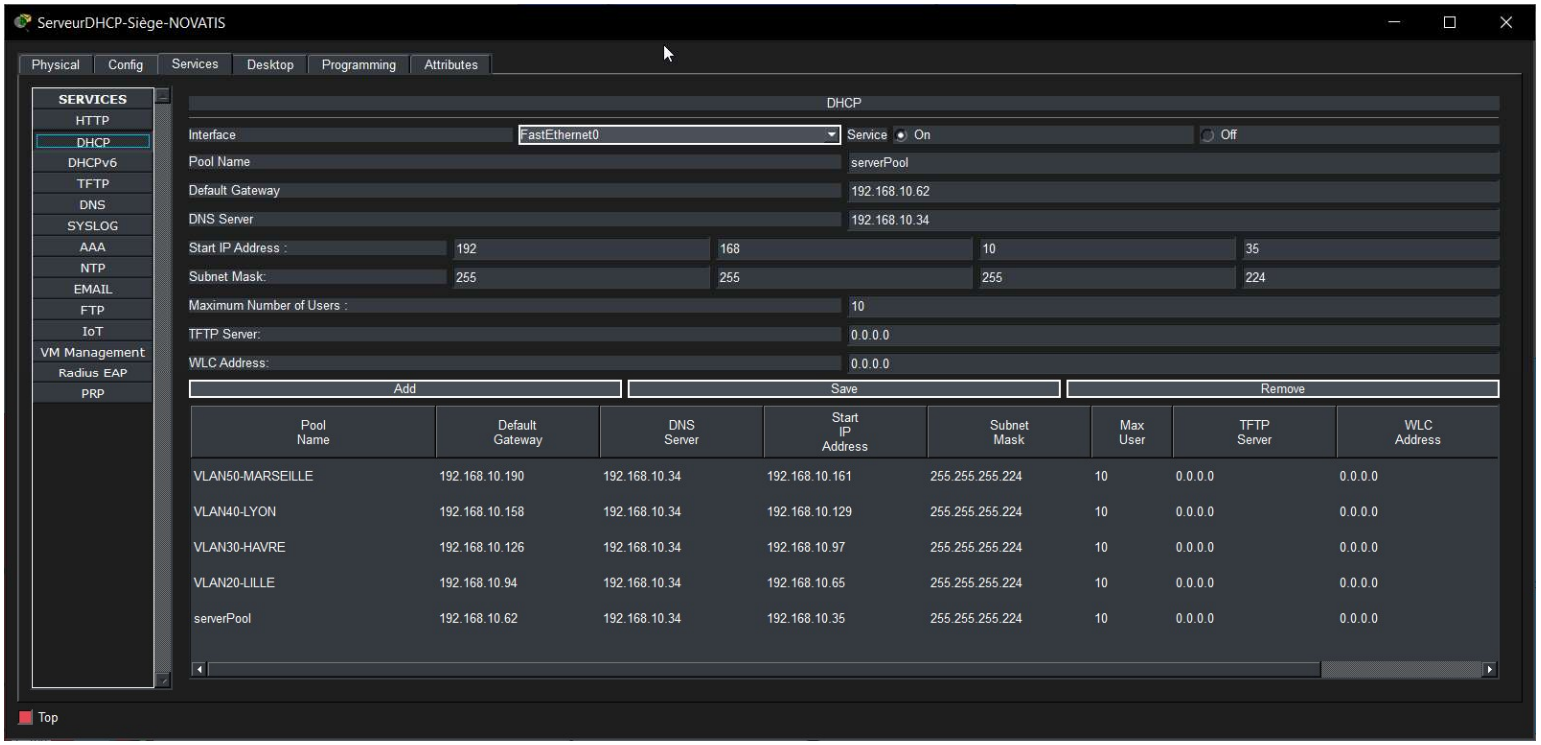
PARTIE 4 – ADMINISTRATION SYSTEME

- ☞ **Mettre en place le rôle DHCP avec les différents pools d'adresse correspondant au sous réseau prédéfinis.**
- ☞ **Configurer les carte réseau des Serveurs_AD et DHCP**

Etape 1 : Configuration Carte Réseau – SRV-AD



Etape 2 : Configuration des pools DHCP sur le serveur :



Configuration des « ip helper-address » sur les interfaces de chaque Vlan.

```
SwitchCoeur(config)#interface vlan 20
SwitchCoeur(config-if)#ip helper-address 192.168.10.33
SwitchCoeur(config-if)#exit
SwitchCoeur(config)#
SwitchCoeur(config)#interface vlan 30
SwitchCoeur(config-if)#ip helper-address 192.168.10.33
SwitchCoeur(config-if)#exit
SwitchCoeur(config)#
SwitchCoeur(config)#interface vlan 40
SwitchCoeur(config-if)#ip helper-address 192.168.10.33
SwitchCoeur(config-if)#exit
SwitchCoeur(config)#
SwitchCoeur(config)#interface vlan 50
SwitchCoeur(config-if)#ip helper-address 192.168.10.33
SwitchCoeur(config-if)#exit
```

Vérification de la présence de mes « ip helper address »

```
Switch#show run | include helper
 ip helper-address 192.168.10.33
 ip helper-address 192.168.10.33
 ip helper-address 192.168.10.33
 ip helper-address 192.168.10.33
```

Résultat : Quand un poste client des VLANs 20, 30, 40 et 50 va demander une adresse ip, le paquet sera directement envoyé au serveur DHCP de NOVATIS.

Etape 3 : Configuration des cartes réseaux des serveurs AD, et DHCP en statique :