SAE 21

Construire un réseau informatique pour une petite structure

Alexandre Dussaux & El Mahdi Margoum 1B

L'objectif est de construire un réseau d'entreprise typique d'une PME.

<u>Cahier des charges :</u>

Nous allons rappeler le cahier des charges, notre réseau devra être composé d'un switch de niveau 3, (MLS), de 3 VLAN afin de différencier les différents groupes de travail, d'un FAI nous permettant d'obtenir un range d'adresse publique.

SOMMAIRE

I) Le départ

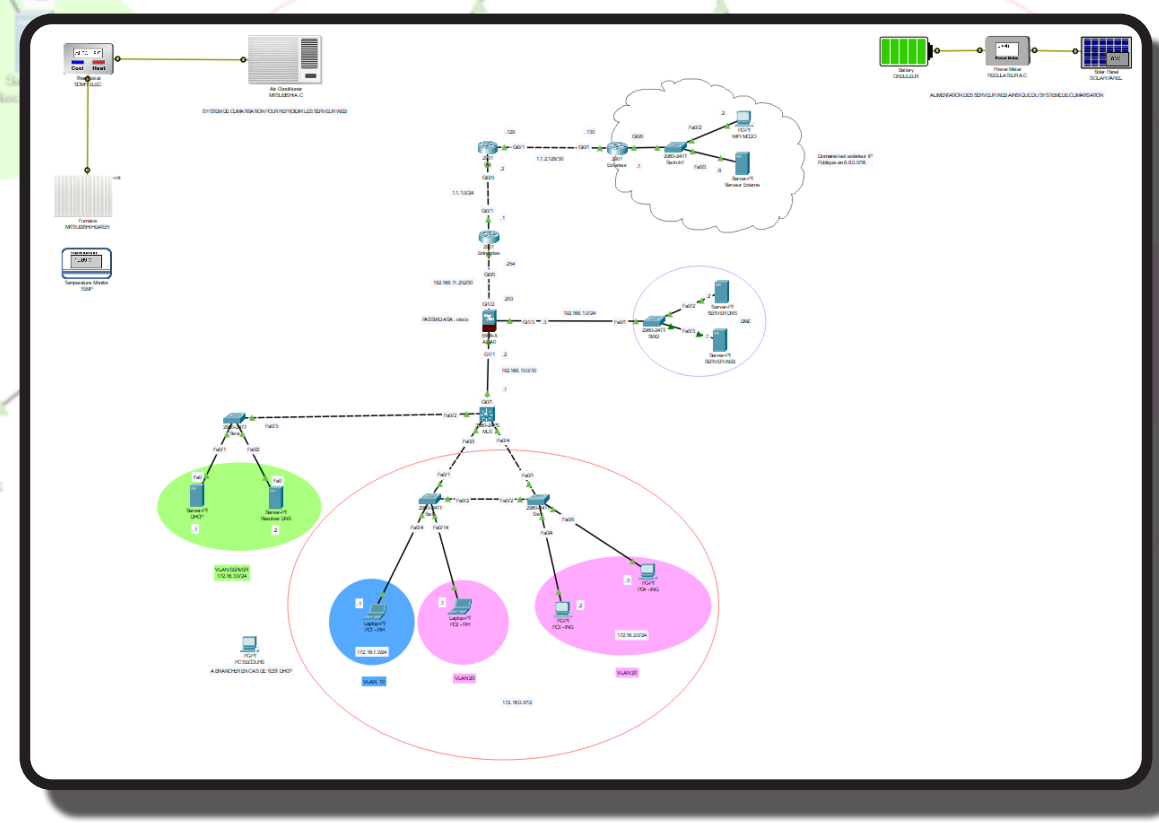
II) Ajout de l'ASA et du service DHCP

III) Ajout de la DMZ ainsi que le routeur FAI

IV) Ajout du réseau publique interconnecté FAI

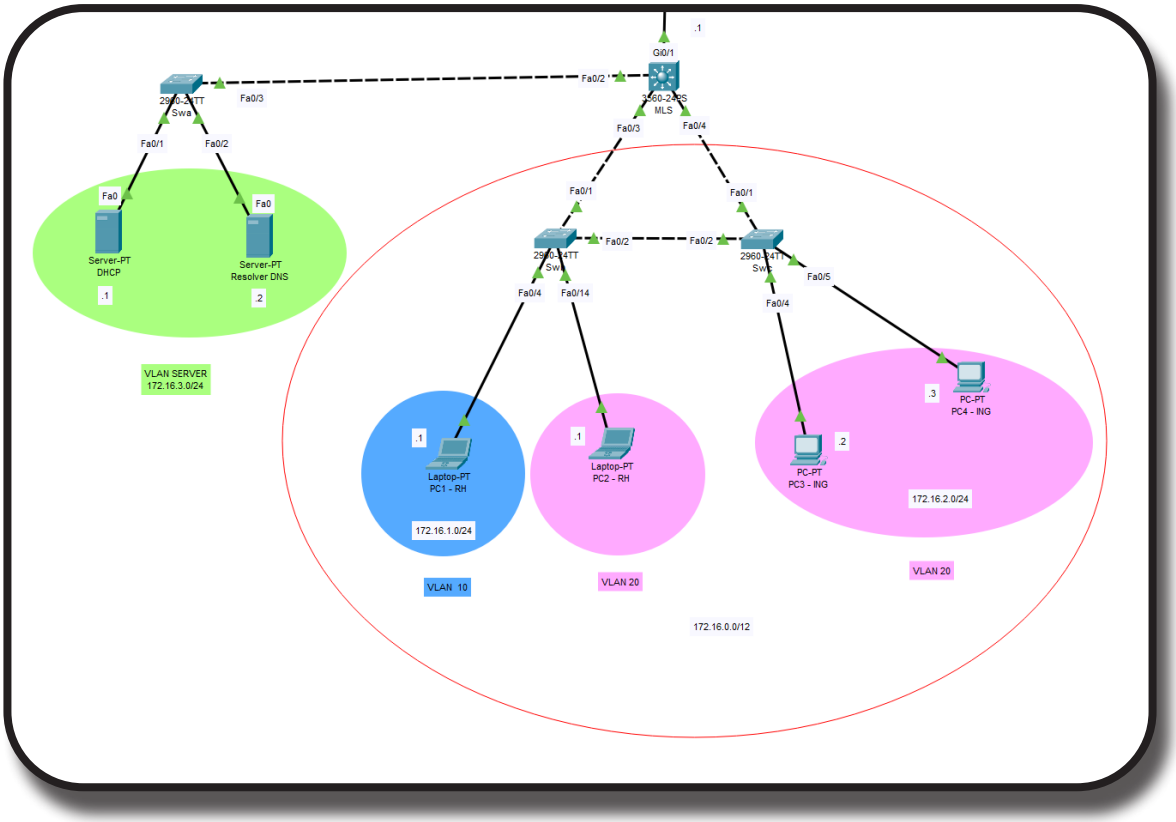
V) Conclusion

Vue d'ensemble de la topologie



I) Le départ

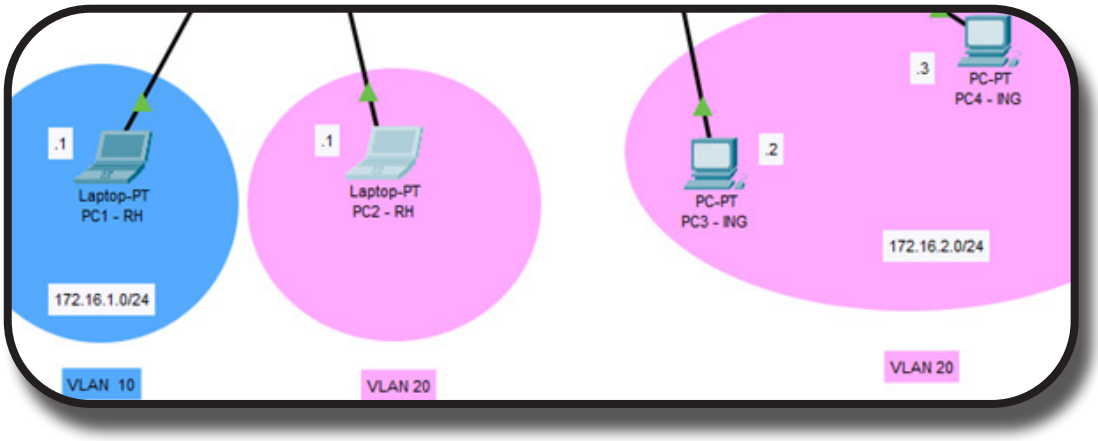
Pour commencer nous allons lancer Cisco Packet Tracer, d'après notre cahier des charges nous allons placer les 3 switchs ainsi que le MLS, le serveur DHCP ainsi que le DNS, ensuite nous allons ajouter les différents postes de travail.



Nous ajoutons ensuite alors les différentes @IP aux postes.

@IP du réseau : 172.16.0.0/12

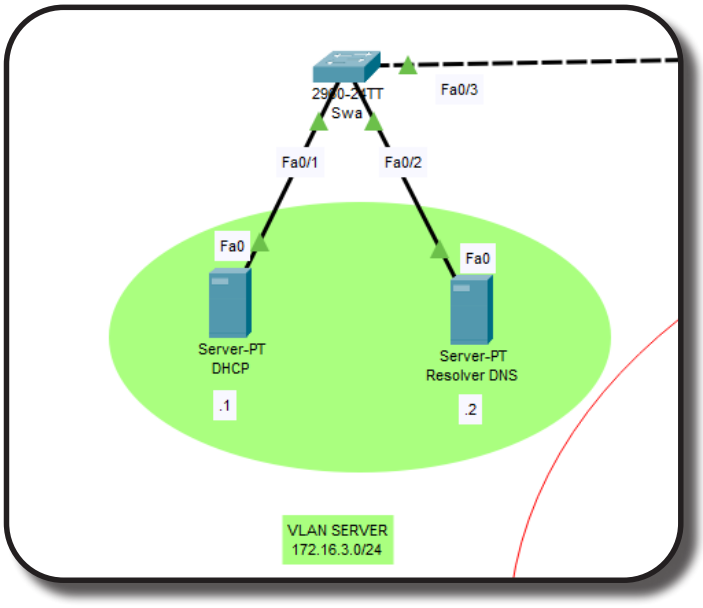
PC1 RH (VLAN10)	172.16.1.1
PC2 ING (VLAN20)	172.16.2.1
PC3 ING (VLAN20)	172.16.2.2
PC4 ING (VLAN20)	172.16.2.3



Nous faisons également la même chose pour le serveur DHCP et le DNS sur les serveurs internes (VLAN30).v

@IP du réseau : 172.16.3.0/24

SERVEUR DHCP	172.16.3.1
SERVEUR DNS	172.16.3.2



Nous allons donc passer ensuite aux VLAN, d'après le cahier des charges nous avons 3 VLAN : VLAN 10 qui représente le département RH, le VLAN 20 qui représente le département INGENIEUR, et pour finir le VLAN 30 qui représente le département SERVEUR.

Configuration de Swa :

```
-en
#conf t
conf) hostname Swa
conf) vlan 10
conf-vlan) name RH
conf-vlan) vlan 20
conf-vlan) name ING
conf-vlan) vlan 30
conf-vlan) name SERV
conf-vlan) ex
conf) int range fa0/1-24
conf-if) switchport mode access
conf-if) switchport access vlan 30
conf-if) ex
conf) int fa0/3
conf-if) switchport mode trunk
conf-if) ex
conf)
```

Configuration de Swb :

```
-en
#conf t
conf) hostname Swb
conf) vlan 10
conf-vlan) name RH
conf-vlan) vlan 20
conf-vlan) name ING
conf-vlan) vlan 30
conf-vlan) name SERV
conf-vlan) ex
conf) int range fa0/1-2
conf-if) switchport mode trunk
conf-if) ex
conf) int range fa0/3-13
conf-if) switchport mode access
conf-if) switchport access vlan 10
conf-if) ex
conf) int range fa0/14-24
conf-if) switchport mode access
conf-if) switchport access vlan 20
conf-if) ex
conf)
```

Configuration de Swc :

```
-en
#conf t
conf) hostname Swc
conf) vlan 10
conf-vlan) name RH
conf-vlan) vlan 20
conf-vlan) name ING
conf-vlan) vlan 30
conf-vlan) name SERV
conf-vlan) ex
conf) int range fa0/1-2
conf-if) switchport mode trunk
conf-if) ex
conf) int range fa0/3-24
conf-if) switchport mode access
conf-if) switchport access vlan 20
```

Nous allons donc ensuite passer à la configuration du MLS :

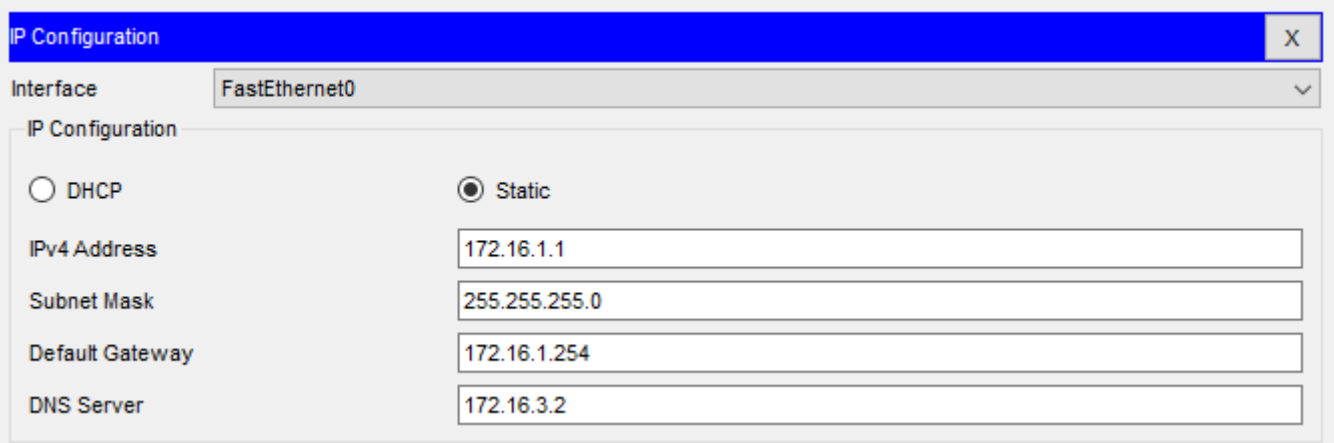
```
-en
#conf t
conf) hostname MLS
conf) vlan 10
conf-vlan) name RH
conf-vlan) vlan 20
conf-vlan) name ING
conf-vlan) vlan 30
conf-vlan) name SERV
conf-vlan) ex
conf) int vlan 10
conf-vlan) ip address 172.16.1.254 255.255.255.0      (cette @ servira comme gateway aux pc)
conf-vlan) ip helper-address 172.16.3.1                (cette @ servira pour DHCP pour plus tard)
                    - Nous faisons pareil pour le VLAN 20 et le VLAN 30 -
conf-vlan) ex
conf) int vlan 20
conf-vlan) ip address 172.16.2.254 255.255.255.0
conf-vlan) ip helper-address 172.16.3.1
conf-vlan) ex

conf-vlan) ex
conf) int vlan 30
conf-vlan) ip address 172.16.3.254 255.255.255.0
conf-vlan) ip helper-address 172.16.3.1
conf-vlan) ex
```

Nous passons ensuite aux interfaces du MLS, c'est-à-dire aux interfaces fa0/2, 3 et 4.

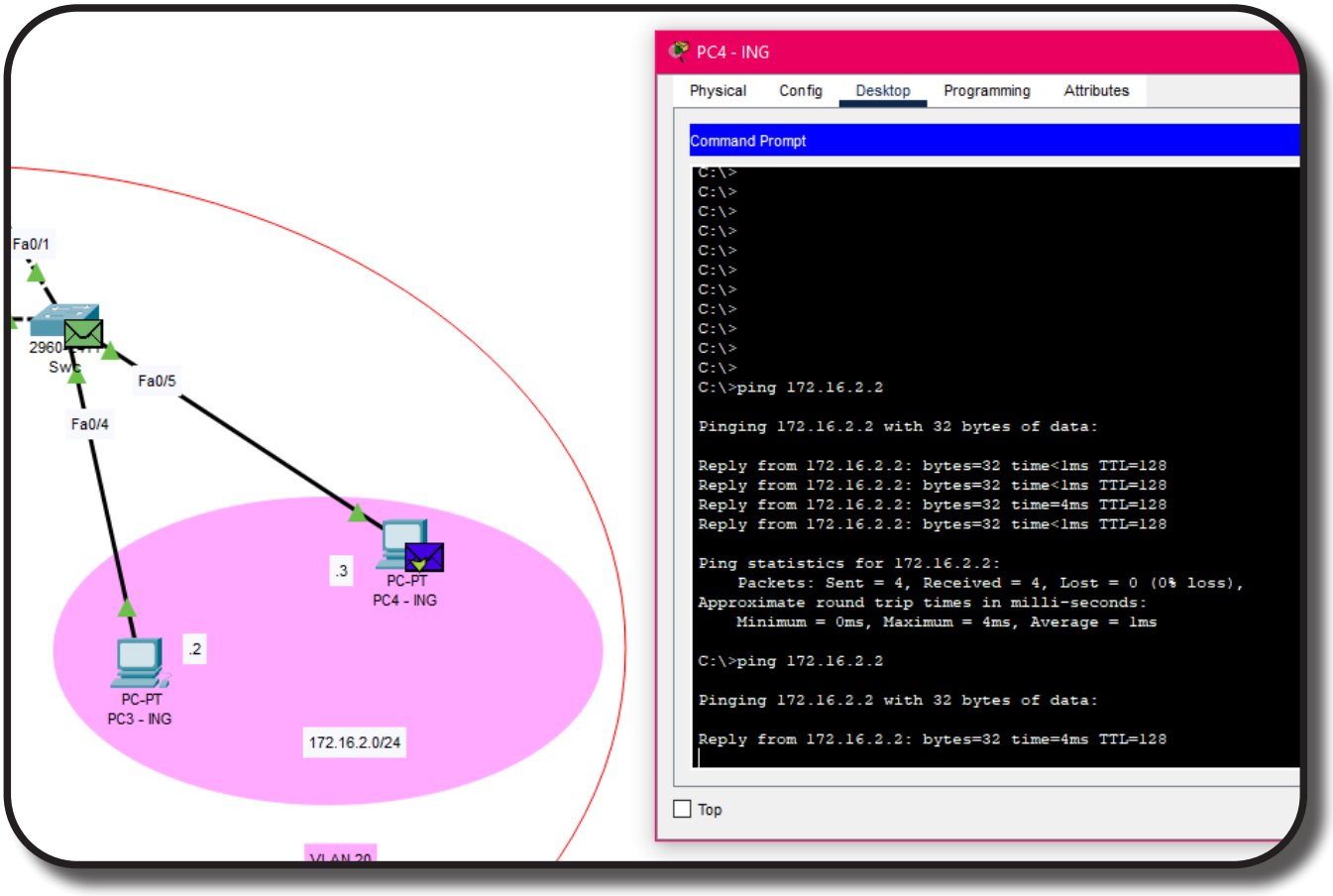
```
conf) int range fa0/2-4
conf-if) no sh
conf-if) switchport mode trunk
conf-if) switchport trunk allowed vlan 10,20,30
conf-if) switchport trunk encapsulation dot1q
conf-if) ex
                    - Nous nous avançons sur l'interface vers l'ASA -
conf) int g0/1
conf-if) no sh
conf-if) ip address 192.168.10.1 255.255.255.252
conf-if) ex
                    - Nous ajoutons la chemin STP -
conf) spanning-tree vlan 10,20,30 priority 24576
```

Après cette étape, théoriquement cela devrait fonctionner, allons vérifier.
Dans la configuration des PCs nous ajoutons dans l'@ de gateway l'@ des différentes VLANs auxquelles ils appartiennent.

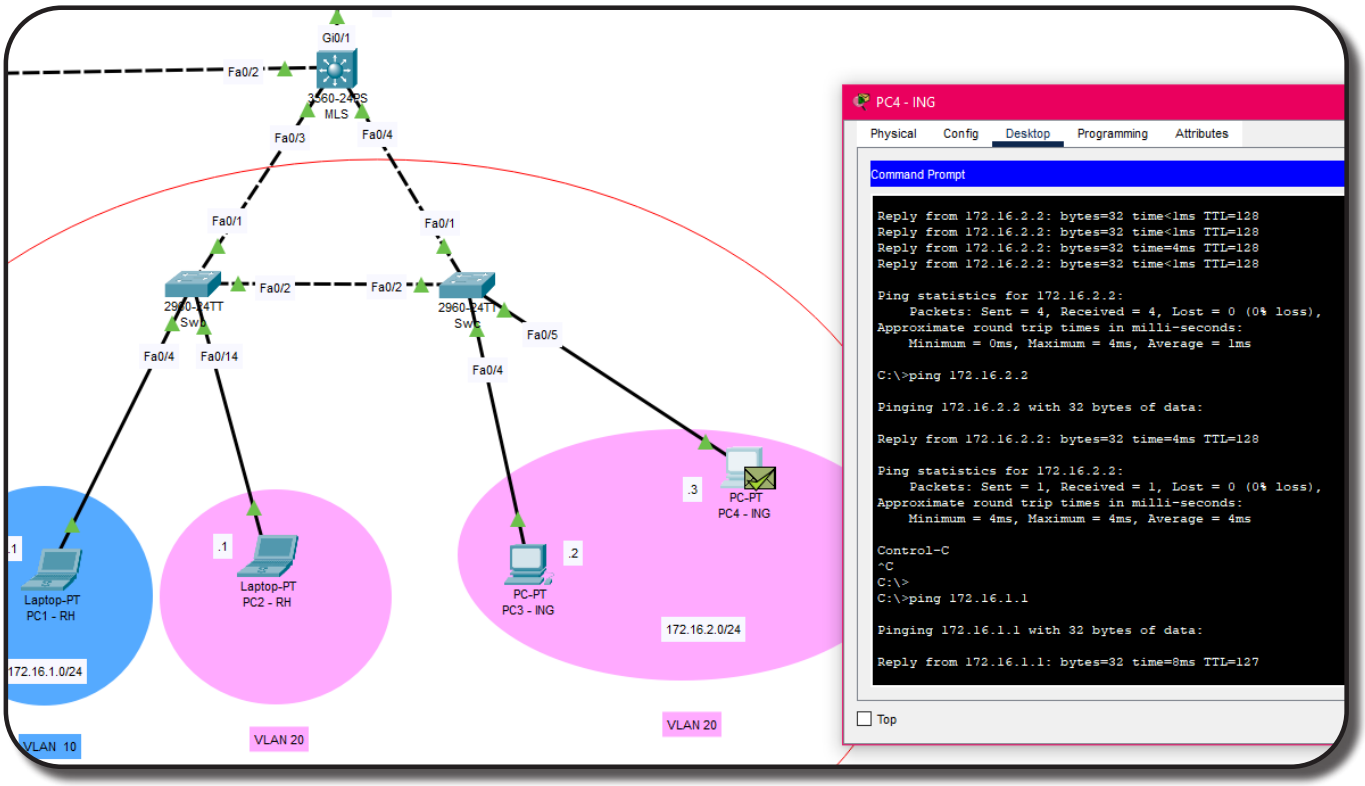


Nous ajoutons également l'@ du serveur DNS (pour plus tard).

Essayons alors ensuite de ping le PC3 au PC2...



Cela fonctionne ! nous allons donc ensuite essayer avec un ordinateur qui n'est pas sur le même VLAN, essayons avec le PC1...

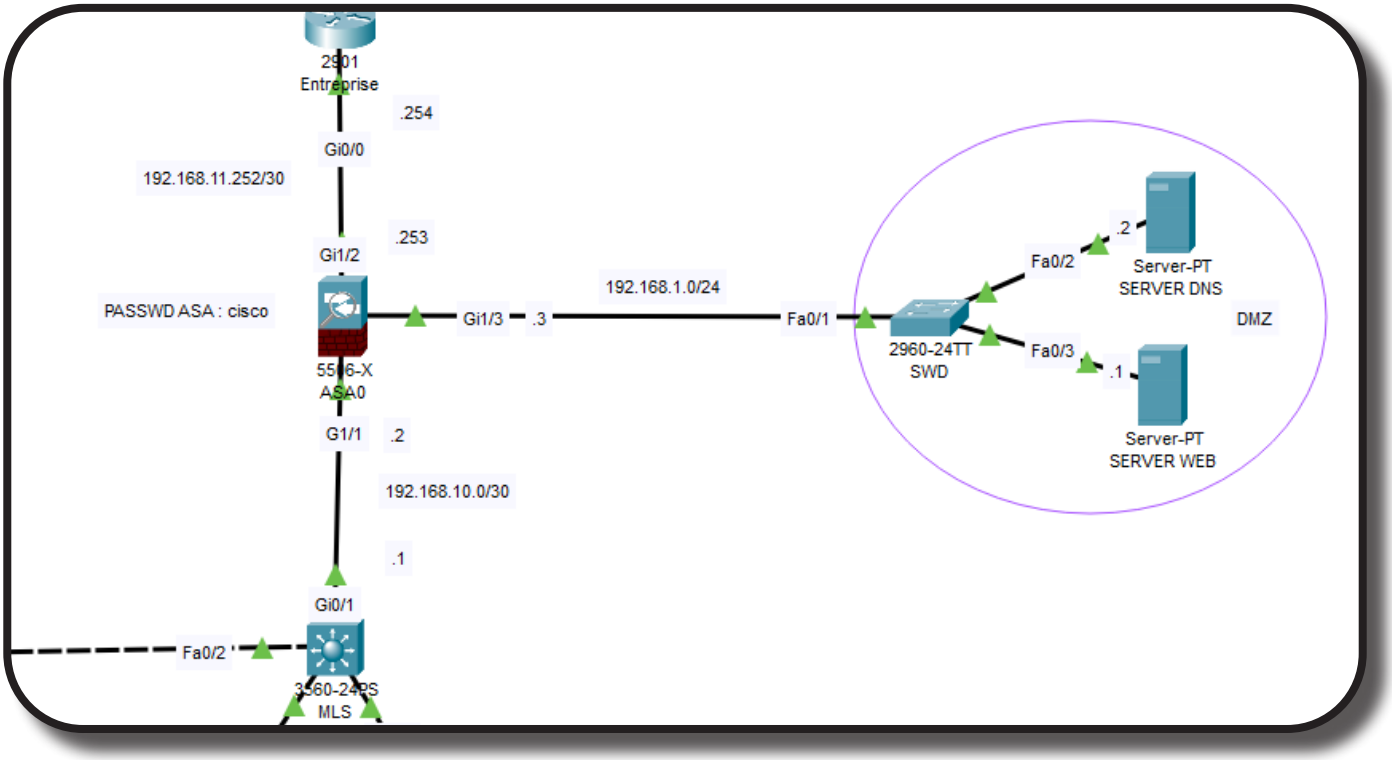


Quand nous faisons un ping notre ping passe bien par le MLS grâce à notre configuration STP mise précédement.

Nous pouvons également voir que nos configurations de trunk fonctionnent.

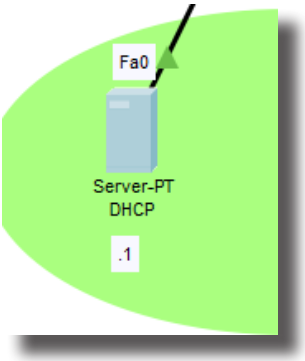
II) Ajout de l'ASA et du service DHCP

Nous allons passer à l'ajout de l'ASA dans notre topologie, nous le relions à notre DMZ et notre MLS.



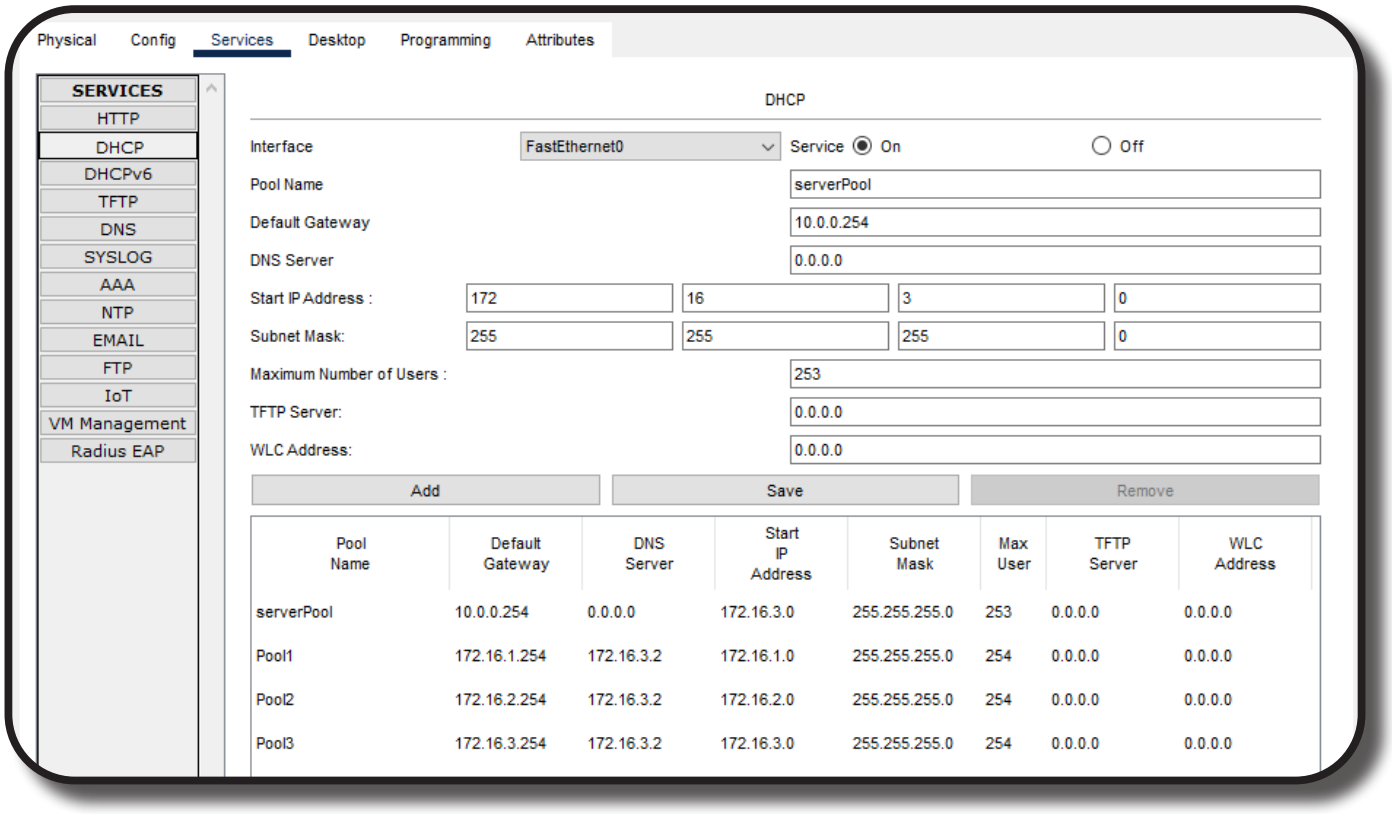
Avant de configurer l'ASA, nous allons configurer le DHCP de notre topoligie.

Dans un premier temps, nous devons activer le service DHCP dans le serveur que nous avons placé au préalable dans le VLAN Serveur.

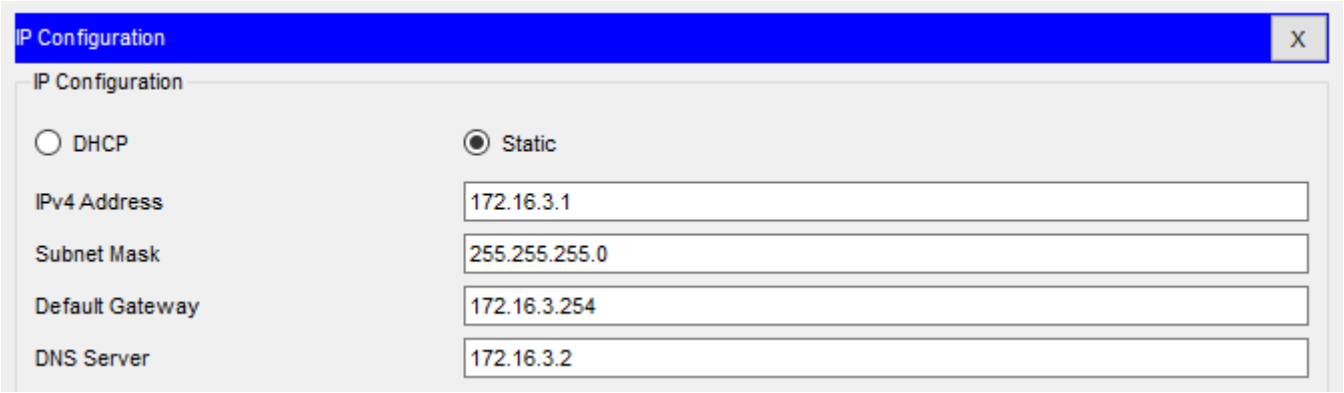


Après avoir activer le service DHCP, nous devons définir trois pools d'adresses ainsi que le servicePool.

Nous avons le Pool1 : 172.16.1.0/24
Pool2 : 172.16.2.0/24
Pool3 : 172.16.3.0/24

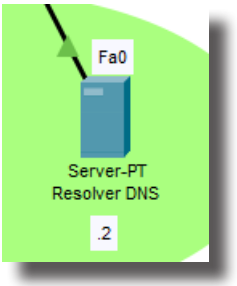


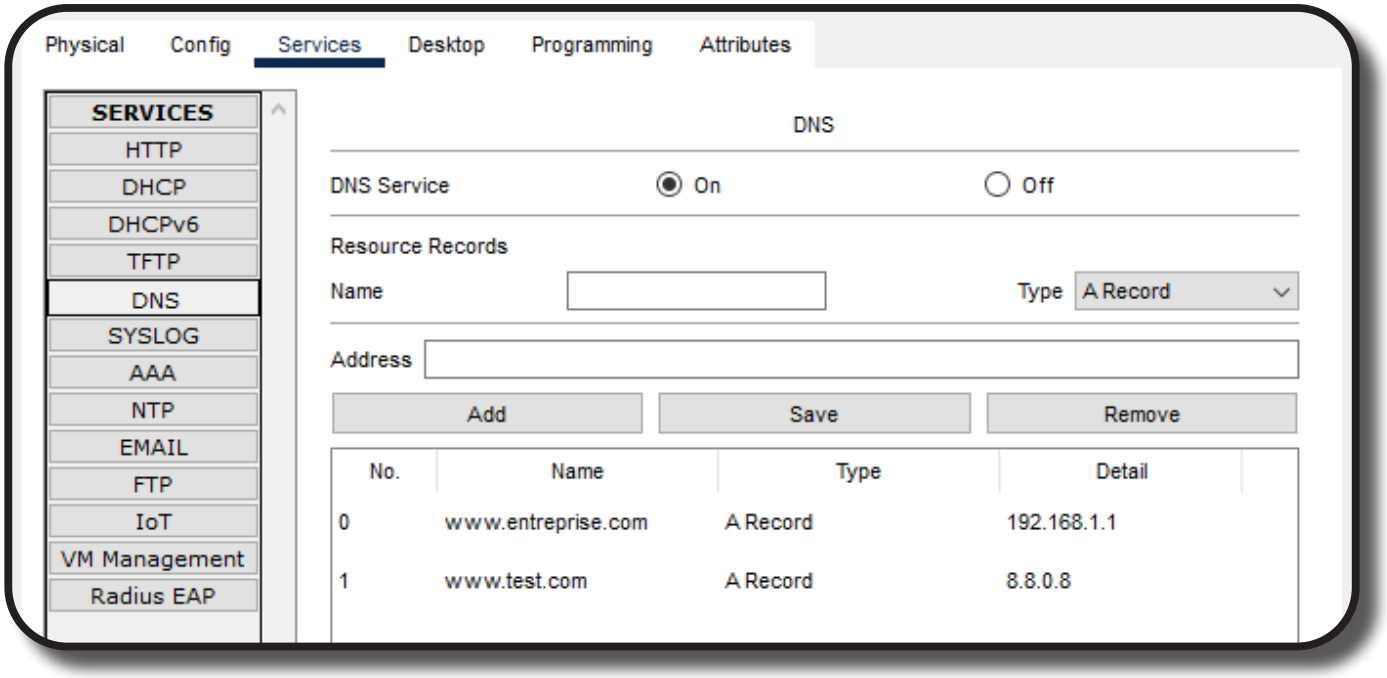
Voici les 3 pools différents

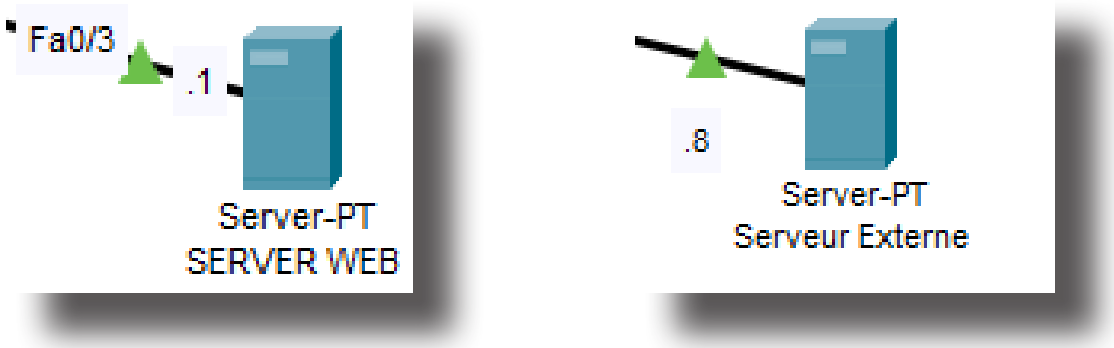


Voici ça configuration

Nous passons ensuite au service DNS, nous activons le DNS du serveur dans la VLAN Server.





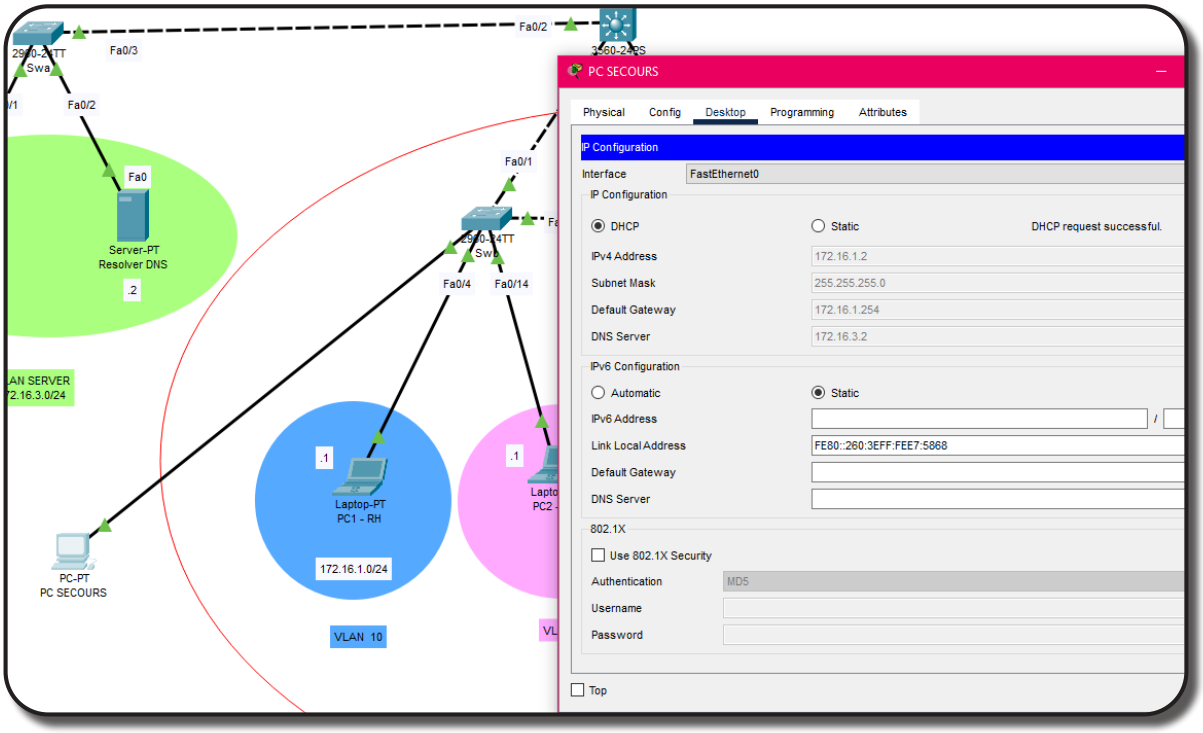


Nous rajoutons les deux enregistrements qui correspondent à :

- www.entreprise.com au server de la DNS
- www.test.com à l'IP du serveur externe

Il nous faut choisir le bon type, le bon type est le (A Record) qui correspond à la redirection d'un nom d'hote vers une adresse IP numérique.

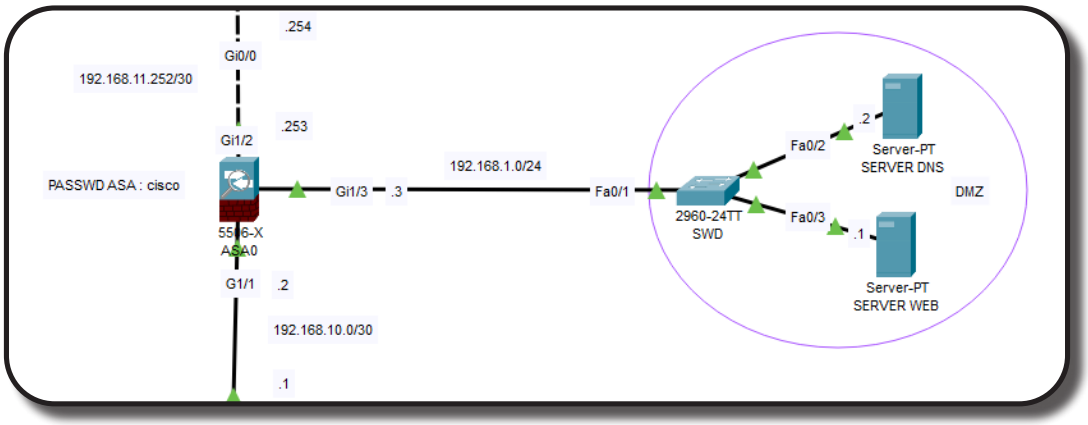
L'enregistrement NS est un enregistrement qui précise à quel serveur le nom à authorité pour le domaine, et l'enregistrement MX permet aux courriels destinés à votre domaine d'êtres redirigés vers un autre serveur.



Nous pouvons vérifier la validité du DHCP en ajoutant un PC SECOURS dans le VLAN 1, puis nous attendons que l'interface du switch soit UP, puis dans les paramètres du PC nous mettons l'@ IP en mode DHCP, puis cela fonctionne il nous donne une @IP automatiquement.
Le partage d'@ IP du DHCP est permise grâce à l'ip adresse helper que nous avons rentré tout à l'heure dans le MLS.

III) Ajout de la DMZ ainsi que le routeur FAI

Nous allons passer à l'ajout de la DMZ ainsi que du routeur FAI, la DMS sera sur l'@ 192.168.1.0/24 et elle sera reliée au firewall.



Nous allons donc ajouter les différentes @IP au DNS ainsi qu'au Server Web.

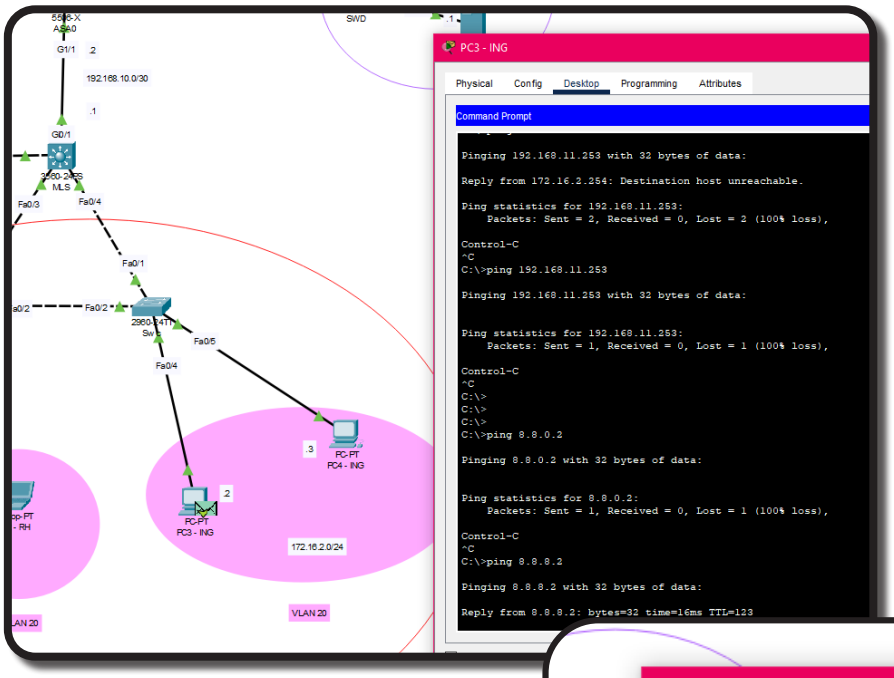
- Server Web 192.168.1.1
- DNS 192.168.1.2

Avant cela, nous allons donc ensuite passer à la configuration de l'ASA :

```
-en
#conf t
conf) hostname ASA
conf) int gi1/1
conf-if) ip add 192.168.10.2 255.255.255.252
conf-if) nameif inside
conf-if) no sh
conf-if) ex
conf) int gi1/2
conf-if) ip add 192.168.11.253 255.255.255.252
conf-if) nameif outside
conf-if) no sh
conf-if) ex
conf) int gi1/3
conf-if) ip add 192.168.1.3 255.255.255.0
conf-if) nameif dmz
conf-if) security-level 50
conf-if) no sh
conf-if) ex
conf) access-list outside_access extended permit tcp any object server_web eq www
conf) access-list outside_access extended permit tcp any object server_web eq 443
conf) access-list outside_access extended deny ip any any
conf) access-list outside_access extended permit icmp any any
- Ces ACL là permettent de recevoir les requêtes venant du port 443, les @www mais pas les @IP -
conf) object network network_dmz
conf-object) subnet 192.168.1.0 255.255.255.0
conf) object network network_inside
conf-object) subnet 192.168.10.0 255.255.255.0
conf) object network network_outside
conf-object) subnet 1.1.1.0 255.255.255.0
conf) object network server_dns
conf-object) host 192.168.1.2
conf) object network server_web
conf-object) host 192.168.1.1
conf-object) nat (dmz,outside) static 192.168.11.253
conf) access-group outside_access in interface outside
                    - Nous appliquons les ACL à l'interface outside -
```

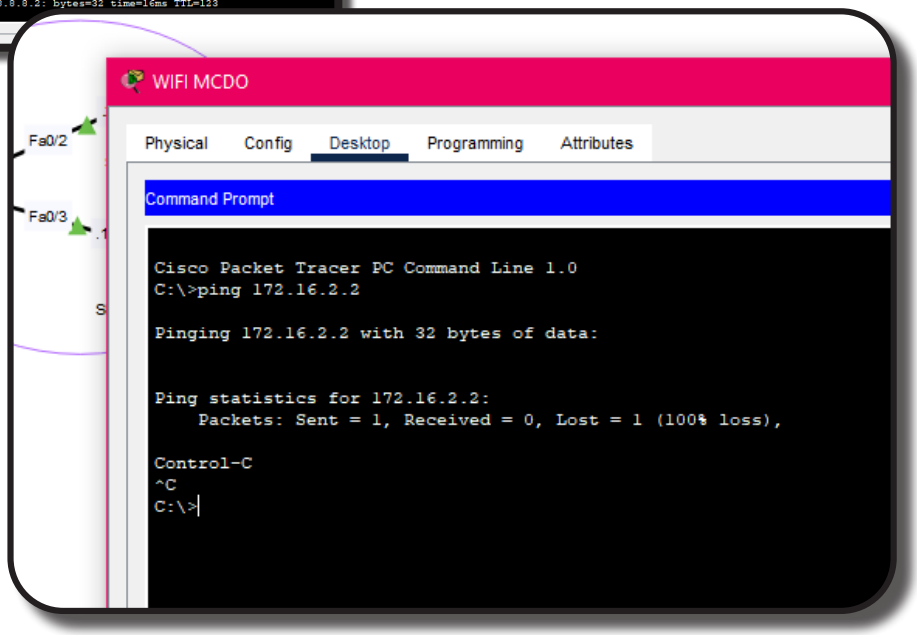
```
conf) class-map inspection_default
conf-class) match default-inspection-traffic
                                        - Pour inspecter le traffic -
conf) policy-map global_policy
conf-policy) class inspection_default
conf-policy) inspect icmp
```

Après avoir rentré ces ACL, nous pouvons ping l'extérieur et recevoir le ping sans pour autant que l'extérieur puisse ping l'intérieur du réseau.
Les pings inités depuis l'intérieur fonctione.



Ping :
INSIDE -->OUT
Fonctionne !

Ping :
OUTSIDE --> INS
Ne fonctionne pas !



Nous allons alors pouvoir passer au NAT dynamique, c'est pourquoi nous allons configurer le routeur Entreprise :

```
-en
#conf t
conf) hostname entreprise
conf) int gi0/0
conf-if) ip add 192.168.11.254 255.255.255.0
conf-if) no sh
conf-if) ex
conf) int gi0/1
conf-if)  ip add 1.1.1.1 255.255.255.0
conf-if) no sh
conf-if) ex
conf) ip nat inside source list 10 interface GigabitEthernet0/1 overload
conf) ip nat inside source static tcp 192.168.1.1 80 1.1.1.253 80
conf) ip nat inside source static tcp 192.168.1.1 443 1.1.1.253 443
conf) ip route 192.168.1.0 255.255.255.0 192.168.11.253
conf) ip route 0.0.0.0 0.0.0.0 1.1.1.2
conf) ip route 172.16.0.0 255.255.0.0 192.168.11.253
                                    - Nous appliquons les routes au routeur -
conf) access-list 10 permit 172.16.0.0 0.0.255.255
conf) access-list 10 deny any
                                    - Nous ajoutons les ACL -
```

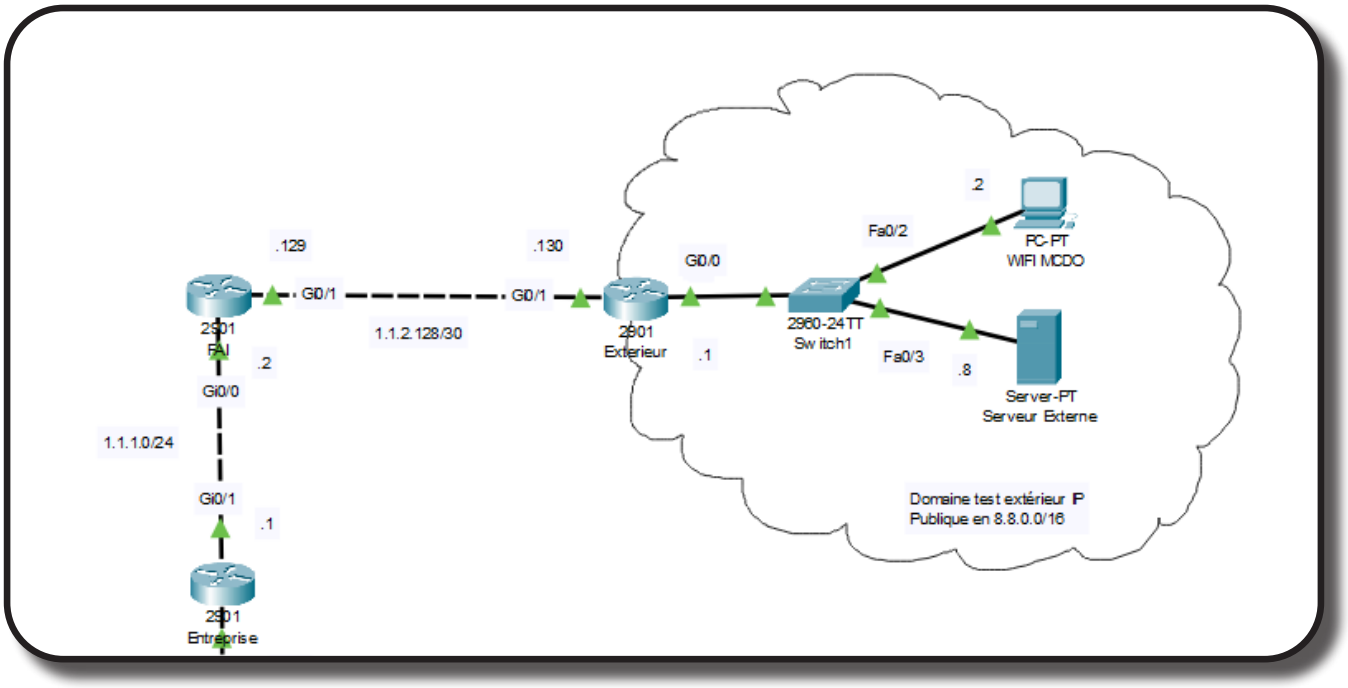
Dès à présent, les clients locaux peuvent sortir en NAT dynamique vers l'extérieur.

Cette partie à été faite un peu plus tôt et comme nous pouvons ping l'extérieur, cela fonctionne en vérifiant : debug ip nat

l'ASA 5506 ne supportant pas les VLAN, nous ne pourrons pas mettre et faire passer des VLAN au niveau de la DMZ.

IV) Ajout du réseau publique interconnecté avec FAI

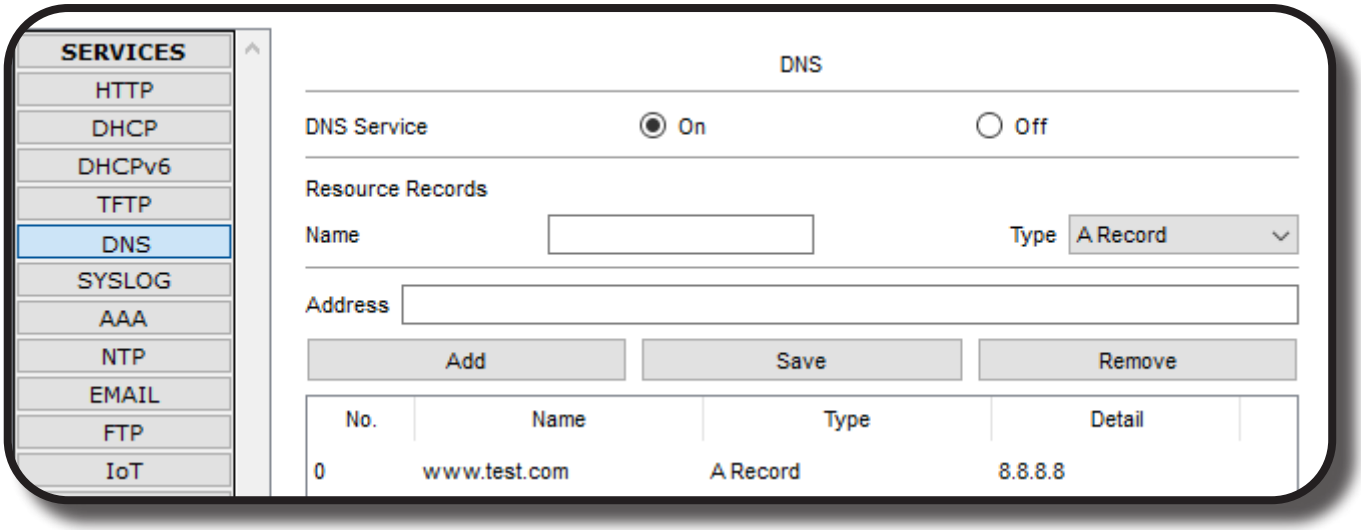
Nous allons passer à l'ajout du réseau publique, il à pour @IP 8.8.0.0/16 c'est pourquoi nous allons rajouter à notre réseau un serveur externe ainsi qu'un PC qui, pour représenter le réseau extérieur sera connecté depuis le Wifi du McDo.



Nous ajoutons donc les @IP aux machines :

- PC WIFI MCDO : 8.8.8.2
- Serveur Externe : 8.8.8.1

Après avoir mis les @IP aux machines il nous reste donc à rajouter le nom de domaine Serveur Web.



Après cette étape il nous reste à configurer le routeur FAI de notre fournisseur d'accès internet et le routeur Exterieur.

Avant de configurer le routeur extérieur, nous savons que le routage entre les routeurs devra se faire en EIGRP pour l'échange des réseaux, c'est pourquoi nous allons rajouter les commandes EIGRP pour déclarer les réseaux.

```
-en
#conf t
conf) hostname exterieur
conf) int gi0/0
conf-if) ip add 8.8.8.1 255.255.255.0
conf-if) no sh
conf-if) ex
conf) int gi0/1
conf-if)  ip add 1.1.2.130 255.255.255.252
conf-if) no sh
conf-if) ex
                                    - Nous ajoutons l'ip route vers le FAI -
conf) ip route 0.0.0.0 0.0.0.0 1.1.2.129
conf) routeur eigrp 100
conf-routeur) network 8.8.0.0 0.0.255.255
conf-routeur) network 1.1.2.128 0.0.0.3
conf-routeur) ex
                                    - Ajout des réseaux eigrp -
```

Nous allons ensuite passer à la configuration du routeur FAI :

```
-en
#conf t
conf) hostname FAI
conf) int gi0/0
conf-if) ip address 1.1.1.2 255.255.255.0
conf-if) no sh
conf-if) ex
conf) int gi0/1
conf-if)  ip address 1.1.2.129 255.255.255.252
conf-if) no sh
conf-if) ex
                                    - Ajout des @ip aux interfaces -
```

```
conf) routeur eigrp 100
conf) network 1.1.2.128 0.0.0.3
conf) network 1.1.1.0 0.0.0.255
conf) ip route 8.8.0.0 255.255.0.0 1.1.2.130
conf) ip route 0.0.0.0 0.0.0.0 1.1.1.1
```

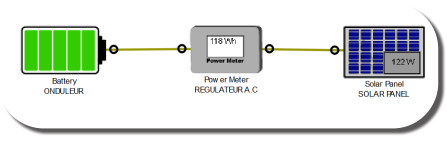
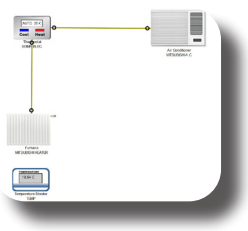
- Ajout des routes statiques -

V) Conclusion

Pour conclure, grâce à cette SAE cela nous a permis de faire évoluer nos connaissance en CISCO IOS, cela nous a permis également de découvrir l'environnement des firewall, on a du faire face à de nombreuses contrainte, pour pouvoir les réglées nous avons du nous renseigner sur internet, chercher, débugger, cela nous a pris beaucoup de temps.

Nous avons la quasi totalités des pings qui fonctionnent sauf, malheuresement, l'extérieur vers la DMZ qui, malgrè tout nos éfforts, n'avons pas réussi à faire fonctionner le ping.

Le DHCP fonctionne très bien, ou que vous soyez dans le réseau interne, le client n'aura qu'a juste cliquer sur le mode DHCP ce qui facilitera l'installation des postes de travail.

En bonus, nous nous sommes permis d'installer au seins de l'établissement, un système de climatisation qui permettra de pouvoir refroidir en été les différents serveur web, qui eux même sont alimentés par des panneaux solaire afin d'être le plus sobre possible écologiquement.

Merci de votre attention.