

Livrable final

Réseau

20 JANVIER

Edwin TRENY
Mathis WAUTERS
Pierre MARTIN
Pierre LATORSE

Sommaire :

1. Introduction	3
1.1 Contexte projet	3
1.2 Problématique	3
1.3 Description livrable 1	3
1.4 Notre équipe	3
1.5 Expression du besoin	4
2. Plan d'adressage	4
2.1 Adressage privé des entreprises	4
2.1.1 Bibliothèque	4
2.1.2 eXia	4
2.1.3 Digiplex	5
2.1.4 Engie	5
2.2 Adressage vers le DSLAM FAI	6
2.3 Adressage du réseau maillé FAI	6
2.4 Tunnel IPV6 entre eXia et Datacenter	7
3. Paramétrage de la maquette	7
3.1 Exia	7
3.2 Bibliothèque	14
3.3 Engie	17
3.4 Digiplex	21
4. Plan de Déploiement	32
4.1 Organisation du déploiement	32
4.2 Schéma Visio Logique	33
5. Gestion de Projet	35
6. Conclusion	36
7. Annexes	36

1. Introduction

Ce document est le compte-rendu finale sur la conception d'une architecture réseau pour la ville de FunkyTown.

1.1 Contexte projet

L'entreprise ESN eXia s'implante à Funkytown. C'est l'occasion parfaite pour aider toutes les entreprises présentes à se développer numériquement. Notre mission est de répondre à des besoins précis avant le 21/01/2022. Nous devons déployer une architecture réseau pour l'ensemble des entreprises qui ont signé un contrat avec nous.

1.2 Problématique

Comment mettre en place et paramétré le réseau dans la ville ?

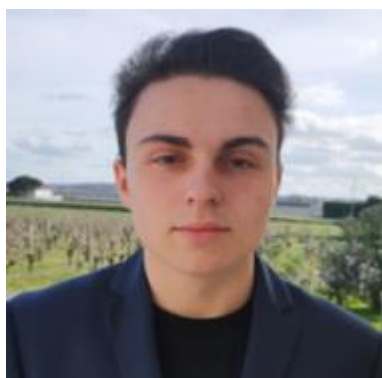
1.3 Description livrable 1

Après avoir déterminer l'adressage des équipements, nous allons maintenant paramétrer et tester les équipements afin d'assurer le bon fonctionnement du réseau. Nous établirons ensuite un plan de déploiement. Tout cela est possible en ayant établie au préalable une organisation minutieuse dans le groupe à l'aide de diagrammes GANTT et PERT.

1.4 Notre équipe



Pierre MARTIN



Pierre LATORSE



Mathis WAUTERS



Edwin TRENY

1.5 Expression du besoin

Durant le projet, plusieurs étapes sont demandées. Nous avons d'abord un plan d'adressage à établir. Nous calculerons ensuite toutes les adresses IP à utiliser ainsi que leur plage et le nombre d'hôtes maximum par réseau en fonction du cahier des charges et de la demande.

Dans un second temps nous créerons et paramétrons une maquette Packet Tracer afin que nos clients aient une visualisation de l'infrastructure réseau.

Pour finir, nous élaborerons un plan de déploiement du système réseau. Des diagrammes de gestion de projet nous aideront tout au long du projet pour une meilleure organisation entre les membres de l'équipe.

2. Plan d'adressage

2.1 Adressage privé des entreprises

2.1.1 Bibliothèque

Dans un premier temps nous allons faire le plan d'adressage de la bibliothèque. D'après le cahier des charges, nous avons déjà sur place 7 hôtes. Nous avons également la notation CIDR donnée. Nous pouvons alors déterminer le nombre d'hôtes disponibles ainsi que l'adresse de diffusion à partir de la plage utilisable et du masque. Nous obtenons alors ces données :

Nom du réseau	Nombre d'hotes souhaités	Nombre d'hôtes disponibles	Nombre d'IP restantes	Notation CIDR	Masque	Plage utilisable	Adresse réseau	Adresse de diffusion
Bibliothèque	7	254	247	/24	255.255.255.0	192.168.0.0 / 255.255.255.0	192.168.0.0	192.168.0.255

2.1.2 eXia

Concernant l'adressage privé de l'entreprise ESN eXia, nous avons réalisé ce dernier en suivant les informations précisées dans le cahier des charges fourni. Celui-ci précisait la présence des équipements suivants :

- 2 PC fixes
- 1 PC portable
- 1 Switch L2
- 1 Borne Wifi
- 1 Routeur
- 1 Serveur DNS & 1 serveur FTP local

De ce fait, nous avons un total de 8 équipements qui sont susceptibles d'avoir une adresse IPv4, soit un nombre d'hôtes souhaités de 8.

Par la suite, le cahier des charges nous précisait une adresse IPv4 privée de réseau tels que 192.168.1.0 avec un CIDR de 24 imposés.

Nous obtenons alors un masque de 255.255.255.0, soit un nombre d'hôtes disponibles de 254 qui est largement suffisant pour les 8 hôtes souhaités initialement. Enfin, nous obtenons l'adresse de réseau (192.168.1.0), l'adresse de broadcast (192.168.1.255) via l'utilisation des portes logiques & et la plage d'adresses IP utilisables (192.168.1.1 à 192.168.1.254).

Nom du réseau	Nombre d'hôtes souhaités	Nombre d'hôtes disponibles	Nombre d'IP restantes	Notation CIDR	Masque	Plage utilisable	Adresse réseau	Adresse de rediffusion
ESN EXIA	8	254	246	24	255.255.255.0	192.168.1.1 -> 192.168.1.254	192.168.1.0	192.168.1.255

2.1.3 Digiplex

Pour la partie du Digiplex nous avons suivis les demandes qui était listés.

Ensuite nous avons appliqué les masques adaptés à chaque réseau et attribuer les plages et adresses nécessaires.

Nom du réseau	Nombre d'hôtes souhaités	Nombre d'hôtes disponibles	Nombre d'IP restantes	Notation CIDR	Masque	Plage utilisable	Adresse réseau	Adresse de rediffusion
Conception	29	254	225	/24	255.255.255.0	192.168.10.0/255.255.255.0	192.168.10.0	192.168.10.255
Commercial	38	254	216	/24	255.255.255.0	192.168.20.0/255.255.255.0	192.168.20.0	192.168.20.255
Ressources Humaines	24	254	230	/24	255.255.255.0	192.168.30.0/255.255.255.0	192.168.30.0	192.168.30.255
Hotline	12	254	242	/24	255.255.255.0	192.168.40.0/255.255.255.0	192.168.40.0	192.168.40.255
Wifi Entreprise	28	254	226	/24	255.255.255.0	192.168.50.0/255.255.255.0	192.168.50.0	192.168.50.255
Wifi Invité	8	254	246	/24	255.255.255.0	192.168.60.0/255.255.255.0	192.168.60.0	192.168.60.255
Server	6	254	248	/24	255.255.255.0	192.168.70.0/255.255.255.0	192.168.70.0	192.168.70.255
Management	0	254	254	/24	255.255.255.0	192.168.80.0/255.255.255.0	192.168.80.0	192.168.80.255

2.1.4 Engie

Pour cette partie, nous avons d'abord déterminé le nombre d'hôtes dont nous avons besoin par vlan (fourni dans le cahier des charges), puis nous avons calculé le CIDR qui va nous servir pour le calcul du masque. Ensuite, nous avons calculé le masque inversé puis en découle l'adresse de Broadcast.

Voici un exemple pour le VLAN 10 :

Adresse réseau de base = 192.168.10.0

Il faut un réseau capable d'host $100 \times 1,3 = 130$ (ce choix s'explique par une marge de 30% au cas où il y aurait un ajout d'équipement dans le futur).

$$2^n - 2 \geq 130 \Leftrightarrow n = 7$$

$$\text{CIDR} : 32 - 7 = 25$$

Masque : 255.255.255.128

Masque inversé : 0.0.0.127

Adresse Broadcast : 192.168.12.127

Plage utilisable : 192.168.10.1 à 192.168.10.127

D'après le cahier des charges, nous devons définir un autre réseau à la suite des VLANs 10/11/12 qui permet une plage de seulement 2 adresses. Enfin, nous avons nommé ce dernier réseau VLAN 13 afin de rester dans une optique de VLANs.

Nom du réseau	Nombre d'hôtes souhaités	Nombre d'hôtes disponibles	Nombre d'IP restantes	Notation CIDR	Masque	Plage utilisable	Adresse réseau	Adresse de diffusion
VLAN 10	100	126	26	25	255.255.255.128	192.168.0.1 - 192.168.0.126	192.168.0.0	192.168.0.127
VLAN 11	60	62	2	26	255.255.255.192	192.168.10.1 - 192.168.10.191	192.168.10.0	192.168.10.63
VLAN 12	20	30	10	27	255.255.255.224	192.168.20.1 - 192.168.20.30	192.168.20.0	192.168.20.31
VLAN 13	2	6	4	29	255.255.255.248	192.168.20.32 - 192.168.20.37	192.168.20.31	192.168.20.38

2.2 Adressage vers le DSLAM FAI

Par rapport à toute la partie d'adressage au niveau du DataCenter, nous utiliserons des adresses IP publiques.

En effet, comme c'est principalement un adressage des interconnexions, nous devons définir le lien entre plusieurs réseaux soit sous forme publique.

De ce fait, nous avons commencé par analyser les différents liens présents entre le DSLAM et les entreprises, puis nous avons défini les adresses IP publiques avec la même méthode que les adressages précédents.

Comme les interconnexions se réalisent entre 2 routeurs, soit 2 équipements, nous avons un nombre d'hôtes souhaités de 2 auquel on n'ajoutera pas de marge car, nous pensons que ces connexions ne changeront pas à l'avenir (pas d'ajout d'équipements).

Finalement, nous obtenons des plages de 2 adresses disponibles pour chaque connexion, soit un CIDR de 30 et un masque de 255.255.255.252.

De plus, nous avons décidé de réaliser un adressage public de sorte qu'il soit clair en modifiant la première partie de l'adresse entre chaque réseau différent (par exemple : 41.0.0.0 & 42.0.0.0).

Nom du réseau	Nombre d'hôtes souhaités	Nombre d'hôtes disponibles	Nombre d'IP restantes	Notation CIDR	Masque	Plage utilisable	Adresse réseau	Adresse de diffusion
Engie/DSLAM	2	2	0	/30	255.255.255.252	41.0.0.1 -> 41.0.0.2	41.0.0.0	41.0.0.3
EXIA/DSLAM	2	2	0	/30	255.255.255.252	42.0.0.1 -> 42.0.0.2	42.0.0.0	42.0.0.3
Bibliothèque/DSLAM	2	2	0	/30	255.255.255.252	43.0.0.1 -> 43.0.0.2	43.0.0.0	43.0.0.3
Digiplex/DSLAM	2	2	0	/30	255.255.255.252	44.0.0.1 -> 44.0.0.2	44.0.0.0	44.0.0.3

2.3 Adressage du réseau maillé FAI

Pour cette partie, nous avons décidé de refaire tout l'adressage réseau. Étant dans le datacenter, nous avons choisi de mettre des adresses publiques commençant par 80.0.0.0. Ainsi, nous avons fait des réseaux pour chaque connexion entre les

différents routeurs du réseau maillé FAI. La méthode utilisée pour réaliser ce type d'adressage est la même que les précédentes utilisées.

Nom du réseau	Nombre d'hôtes souhaités	Nombre d'hôtes disponibles	Nombre d'IP restantes	Notation CIDR	Masque	Plage utilisable	Adresse réseau	Adresse de diffusion
Engie/DSLAM	2	2	0/30	255.255.255.252	41.0.0.1 -> 41.0.0.2	41.0.0.0	41.0.0.3	
EXIA/DSLAM	2	2	0/30	255.255.255.252	42.0.0.1 -> 42.0.0.2	42.0.0.0	42.0.0.3	
Bibliothèque/DSLAM	2	2	0/30	255.255.255.252	43.0.0.1 -> 43.0.0.2	43.0.0.0	43.0.0.3	
Digiplex/DSLAM	2	2	0/30	255.255.255.252	44.0.0.1 -> 44.0.0.2	44.0.0.0	44.0.0.3	
FAI01/FAI02	2	2	0/30	255.255.255.252	80.0.0.1 ->80.0.0.2	80.0.0.0	80.0.0.3	
FAI01/FAI04	2	2	0/30	255.255.255.252	80.0.0.5 ->80.0.0.6	80.0.0.4	80.0.0.7	
FAI02/FAI03	2	2	0/30	255.255.255.252	80.0.0.9 ->80.0.0.10	80.0.0.8	80.0.0.11	
FAI03/FAI04	2	2	0/30	255.255.255.252	80.0.0.13 ->80.0.0.14	80.0.0.12	80.0.0.15	
FAI03/FAI05	2	2	0/30	255.255.255.252	80.0.0.17 ->80.0.0.18	80.0.0.16	80.0.0.19	
FAI04/FAI05	2	2	0/30	255.255.255.252	80.0.0.21 ->80.0.0.22	80.0.0.20	80.0.0.23	
FAI02/WAN	2	2	0/30	255.255.255.252	80.0.0.25 ->80.0.0.26	80.0.0.24	80.0.0.27	
WAN/DNS	2	2	0/30	255.255.255.252	80.0.0.29 ->80.0.0.30	80.0.0.28	80.0.0.31	
WAN/GOOGLE	2	2	0/30	255.255.255.252	80.0.0.33 ->80.0.0.34	80.0.0.32	80.0.0.35	
FA01/DSLAM	2	2	0/30	255.255.255.252	80.0.0.37 ->80.0.0.38	80.0.0.36	80.0.0.39	
WAN/DSLAM	2	2	0/30	255.255.255.252	80.0.0.41 ->80.0.0.42	80.0.0.40	80.0.0.43	
FAI05/EXIA RT	2	2	0/30	255.255.255.252	80.0.0.45 ->80.0.0.46	80.0.0.44	80.0.0.47	

2.4 Tunnel IPV6 entre eXia et Datacenter

Pour le tunnel IPV6 nous avons repris les informations du sujet qui nous indiquent les adresses IPV6 des différents acteurs de cette partie.

On se retrouve donc avec 2 réseaux (un cloud et celui de l'EXIA), le tunnel et le serveur MERAKI avec leur adresse

Nom du réseau	Nombre d'hôtes souhaités	Nombre d'hôtes disponibles	Nombre d'IP restantes	Notation CIDR	Masque	Plage utilisable	Adresse réseau	Adresse de diffusion
MERAKI/EXIA RT (tunnel IPV6)				/64		2001:DB8:3000::		
Réseau local EXIA (IPV6)				/64		2001:DB8:2000::		
Réseau du cloud distant				/64		2001:DB8:1000::		
Serveur MERAKI				/64		2001:DB8:1000::1		

3. Paramétrage de la maquette

3.1 Exia

Premièrement, nous avons décidé de commencer la configuration de la maquette par le site Exia. Pour ce faire, nous avons débuté le site Exia par la configuration de la sécurisation des accès. Afin de pouvoir répondre aux attentes de sécurisation des accès au switch et au routeur du site Exia, nous avons décidé d'établir une sécurisation de l'accès à la console puis au mode privilégié. De ce fait, nous avons utilisé les commandes de configuration des mots de passes pour l'accès console et l'accès au mode privilégié comme suit :

Procédure pour définir un mot de pass sur l'accès via cable console

```
S1#conf t
S1(config)#line console 0
S1(config-line)#password cisco
S1(config-line)#login
S1(config-line)#exit
S1(config)#exit
```

Procédure pour sécuriser l'accès au mode privilégié

```
S1> en
S1# configure terminal
S1(config)# enable password cisco
S1(config)# exit
```

Afin d'améliorer notre sécurisation des accès sur les équipements, nous avons décidé d'encrypter les mots de passes dans le fichier de configuration de ces derniers via les commandes suivantes :

Procédure pour chiffrer les mots de passe d'activation (enable) et de console.

```
S1> en
S1# config t
S1(config)# service password-encryption
S1(config)# exit
```

Cependant, nous avons décidé de ne pas sécuriser les ports des équipements tels que le switch mais cela reste possible de façon dynamique en utilisant le mot clé Sticky dans les commandes suivantes :

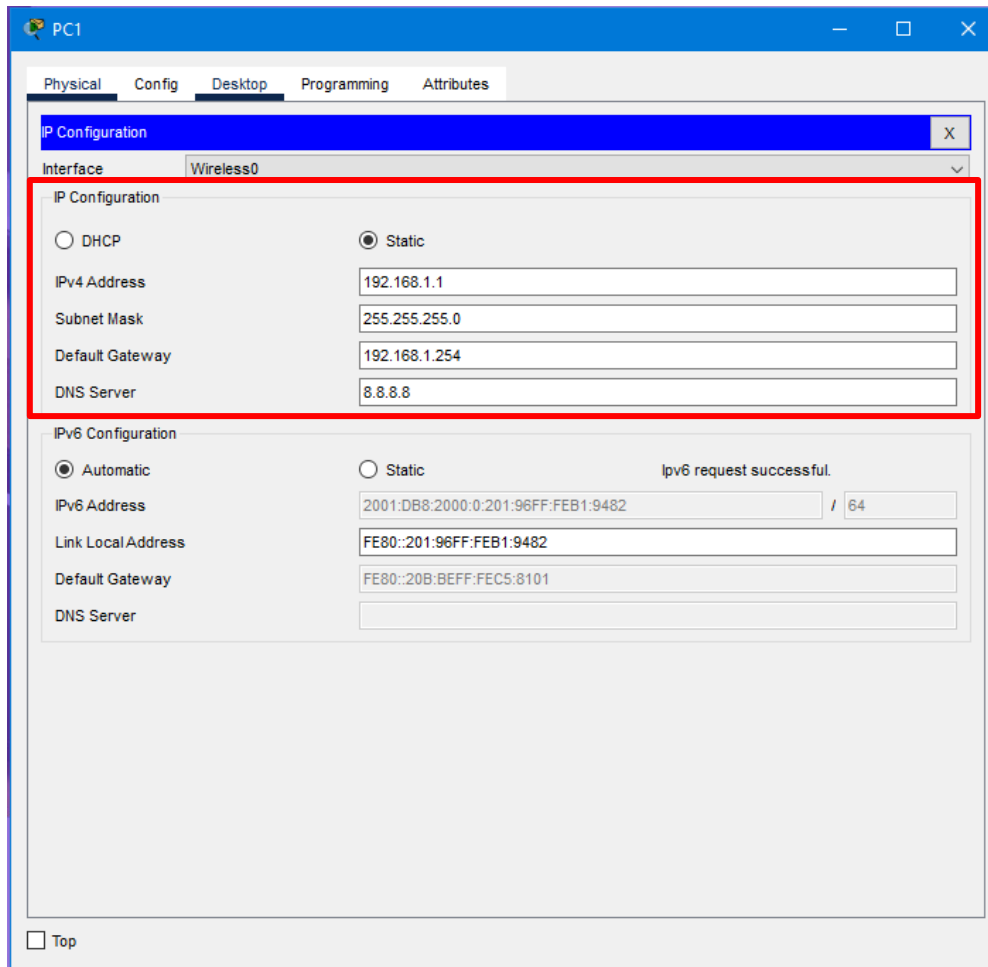
S2(config)#interface FastEthernet 0/2 ou encore S2(config)#interface range FastEthernet 0/1 - 24

S2(config-if)#switchport mode access

S2(config-if)#switchport port-security

S2(config-if)#switchport port-security mac-address sticky.

Ensuite, nous avons décidé de réaliser l'adressage fixe dans le réseau 192.168.1.0/24. De ce fait, nous avons pris chacun des 3 ordinateurs puis nous leur avons fourni une adresse ipv4 privée dans le réseau ainsi que sur le port du routeur qui accède au LAN d'Exia, soit un default gateway (ou passerelle par défaut). De plus, nous avons adressé le serveur DNS & FTP local en 192.168.1.200/24 comme précisé dans le cahier des charges.



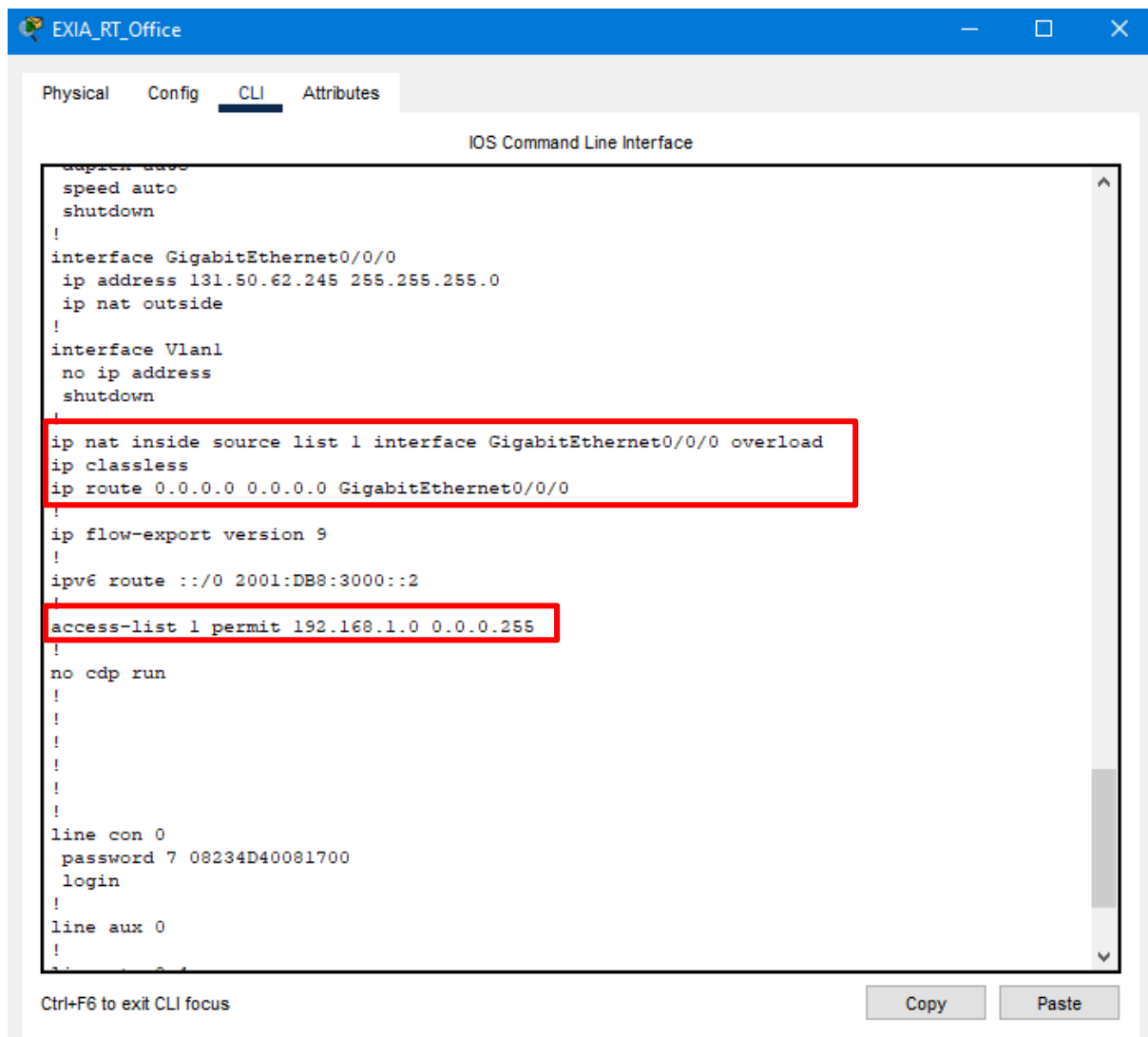
A la suite de ces étapes, il ne nous restait localement plus qu'à configurer l'accès WEB via une méthode de PAT surchargé via le mot clé « overload ». La méthode est la suivante :

Configurer les interfaces en fonction du nat inside et outside

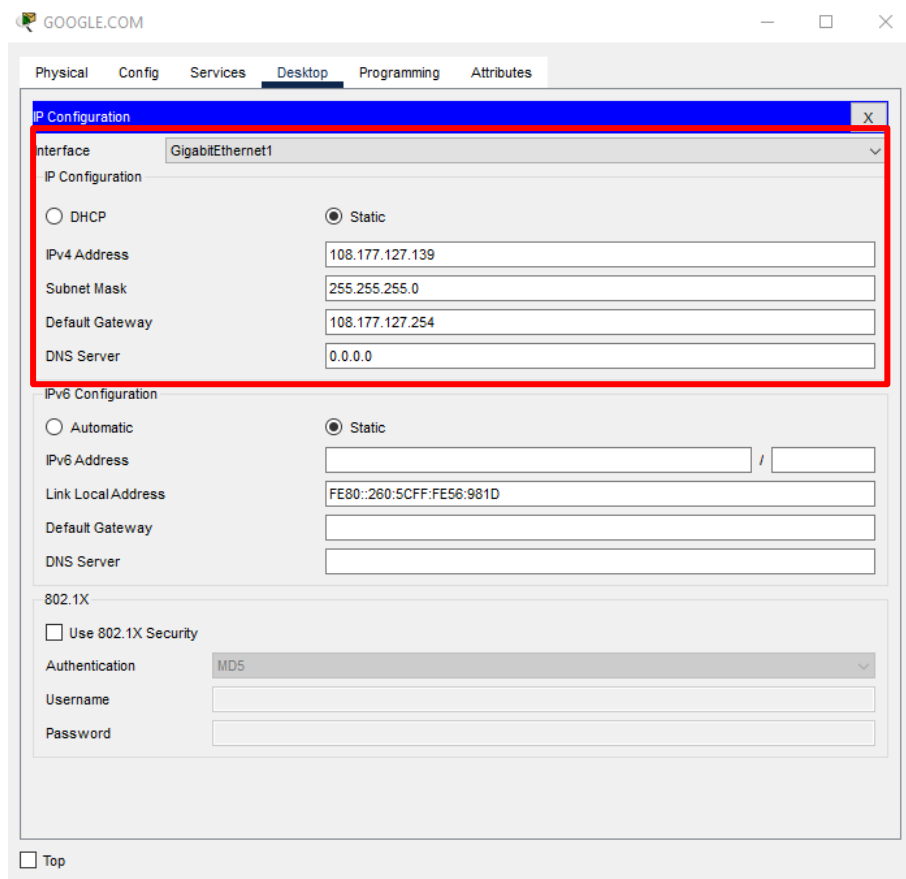
Configurer les access-list nécessaires

Configurer le PAT avec la commande requise

Définir une route statique par défaut



Cependant, nous n'arrivions pas à joindre le serveur Web du datacenter car ce dernier a été mal adressé de base sur la maquette. De ce fait, nous avons changé d'interface car ce n'était pas la bonne qui était adressé, et l'accès au Web fonctionnait.



En ce qui concerne le serveur FTP et le fait de pouvoir déposer et récupérer des images IOS d'équipement, nous avons dû configurer un compte utilisateur Exia avec un mot de passe auquel nous avons donné tous les droits possibles. Ensuite, nous avons cherché les différentes commandes pour récupérer et déposer des images qui sont les suivantes :

Depuis un équipement Cisco :

Pour déposer

-copy flash: tftp: (Préciser nom fichier flash à trouver grâce à commande suivante "show flash")

-copy startup-config tftp:

-copy running-config tftp:

Pour récupérer

-copy tftp: flash:

-copy tftp: startup-config

-copy tftp: running-config

Depuis un PC dans command prompt :

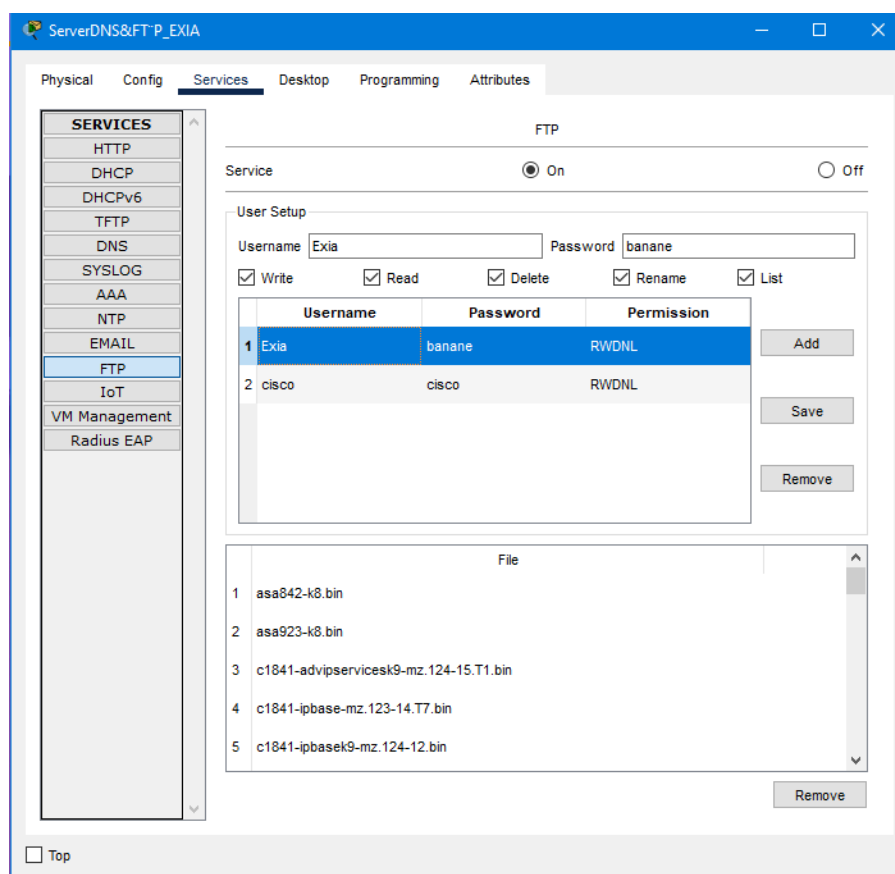
-ftp [adresse ip serveur FTP] => permet d'accéder via username et password au ftp

Depuis le mode ftp :

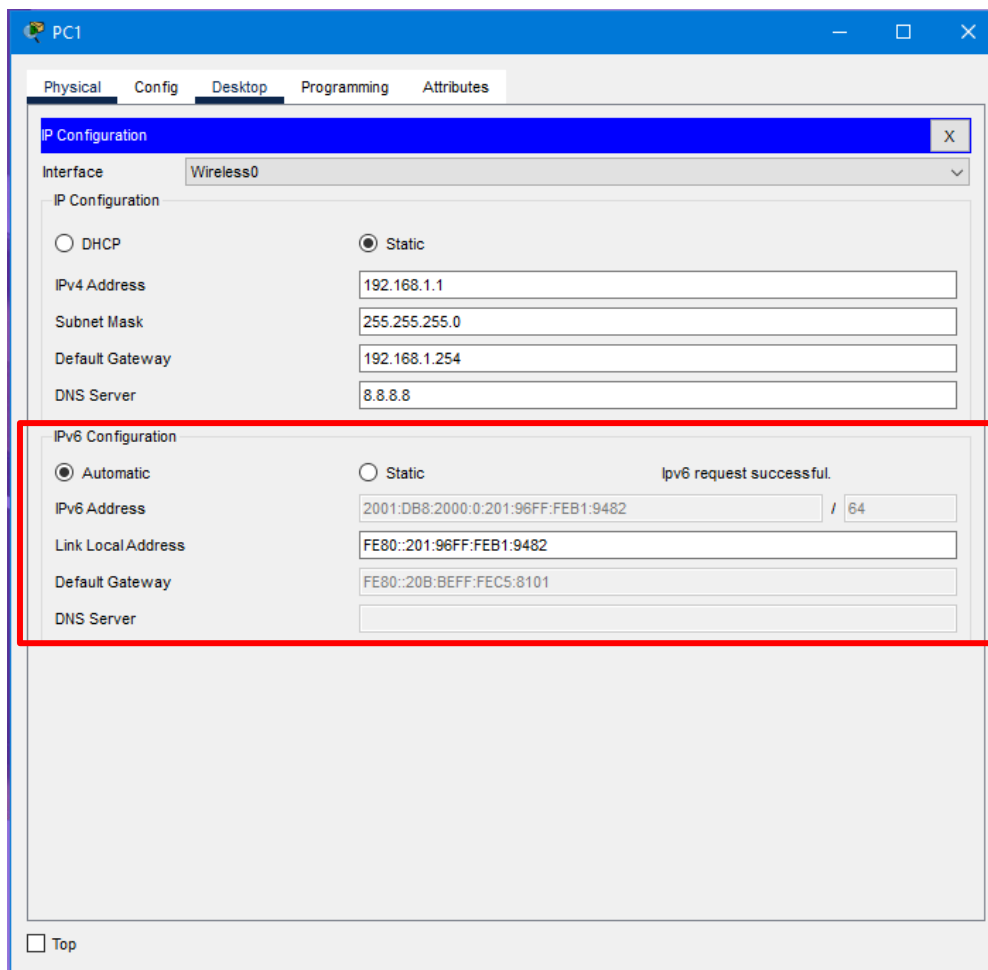
-put => Pour déposer un fichier

-get => Pour récupérer un fichier

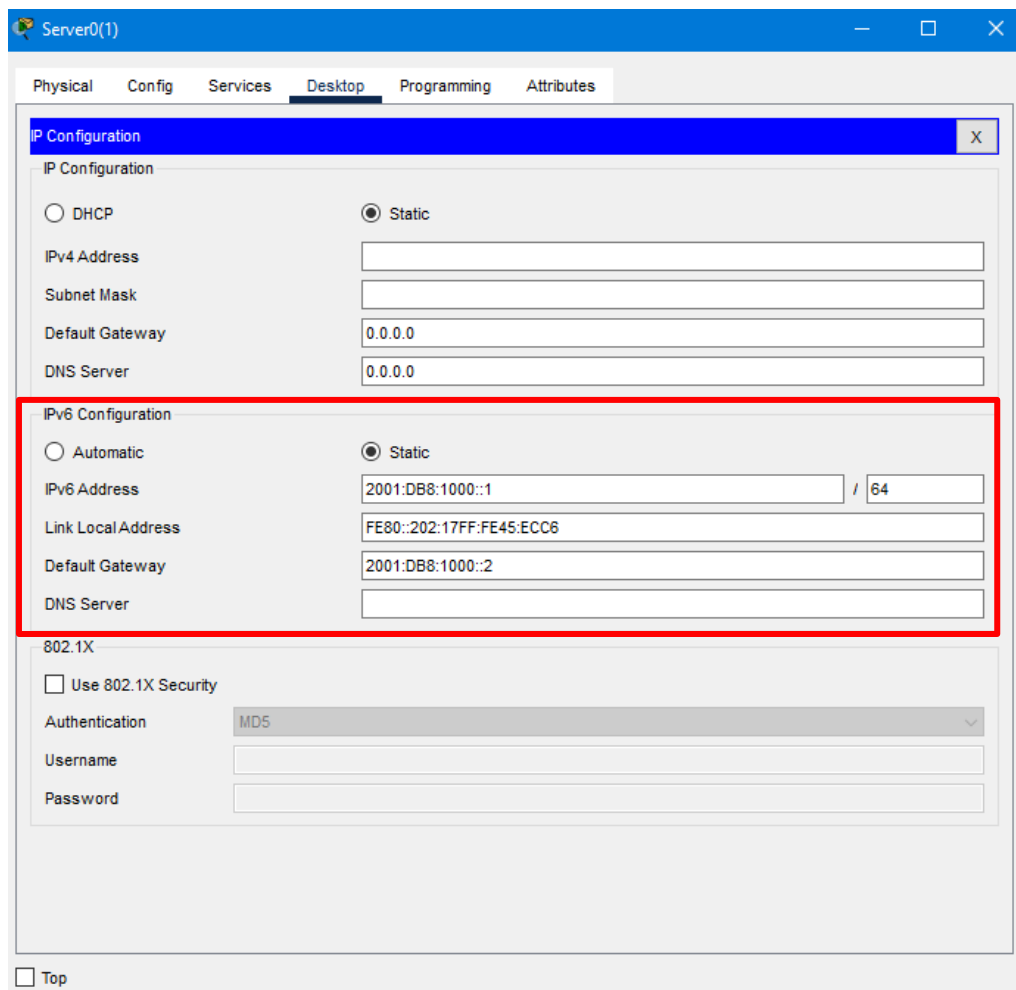
-dir => Pour afficher les fichiers dans le serveur FTP



Finalement, nous avons configuré le tunnel ipv6 entre le routeur Exia et le cloud du serveur Exia Meraki. Pour ce faire, nous avons commencé par configurer un adressage ipv6 en autoconfig stateless depuis le routeur Exia avec le préfixe 2001 :DB8 :2000 ::/64 en eui-64. Ensuite, nous avons configuré le tunnel ipv6 via les commandes que nous avons apprises lors du workshop dédié sur chacun des routeurs (Exia et ExiaMeraki). Enfin, nous avons configuré des routes ipv6 statiques par défaut sur chacun des routeurs afin de pouvoir atteindre le serveur Meraki.



Cependant, nous avons fait face à un problème car le serveur Meraki était mal adressé. En effet, ce l'adressage de ce dernier n'était pas cohérent avec le préfixe du réseau dans lequel il se trouvait. De ce fait, nous l'avons réadapté au routeur et notre tunnel ipv6 fonctionnait.



Nous avons alors un réseau fonctionnel et répondant entièrement au cahier des charges pour le site Exia.

3.2 Bibliothèque

En ce qui concerne la configuration du réseau de la bibliothèque, comme pour le site d'Exia, nous avons décidé de commencer par la sécurisation des accès, la méthode étant la même que celle employée précédemment.

Ensuite, pour la configuration de l'accès à distance, nous avons décidé d'employer un SSH via la méthode suivante :



Pour la partie adressage du routeur, nous avons simplement défini manuellement l'adresse ipv4 privée 192.168.0.254 en tant que default gateway.

Ensuite, comme nous devons configurer les adresses IP des PC de façon dynamique avec un DNS publique (soit 8.8.8.8 DNS du datacenter), nous avons décidé de configurer un serveur DHCP directement sur le routeur de la façon suivante :

```
RouterA#conf t
```

```
RouterA(config)# ip dhcp pool LAN
```

```
RouterA(dhcp-config)# network 192.168.0.0 255.255.255.0
```

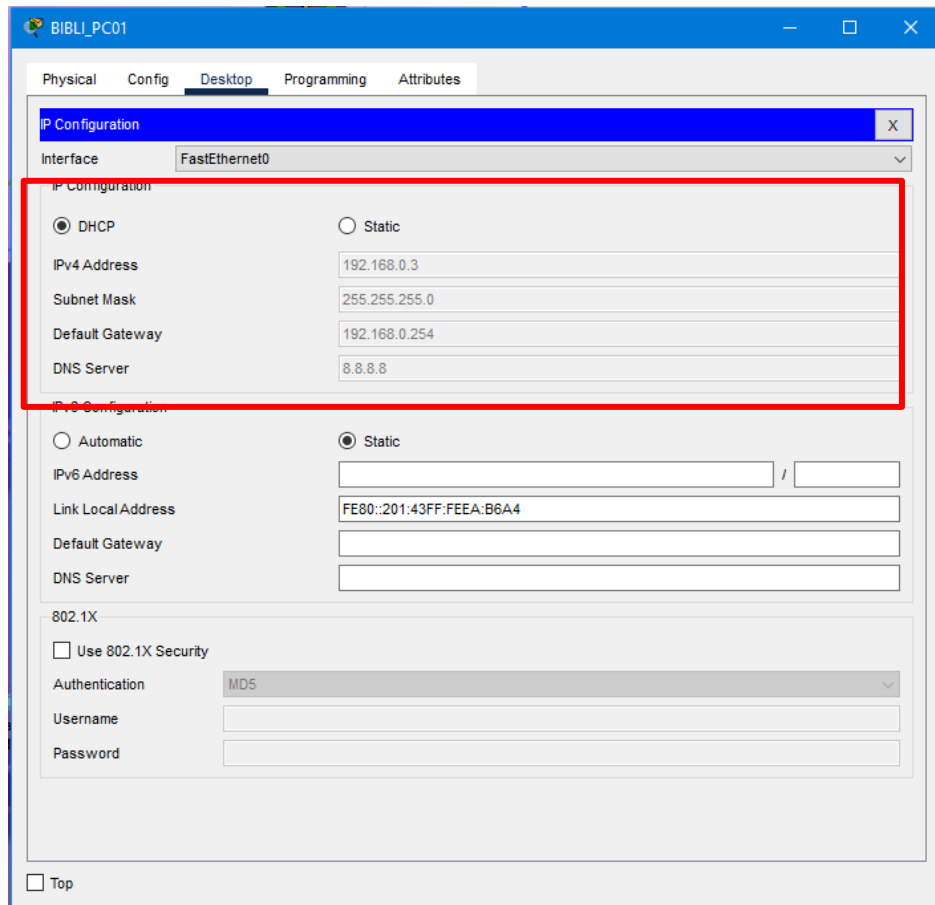
```
RouterA(dhcp-config)# default-router 192.168.0.254
```

```
RouterA(dhcp-config)# dns-server 8.8.8.8
```

```
RouterA(dhcp-config)# exit
```

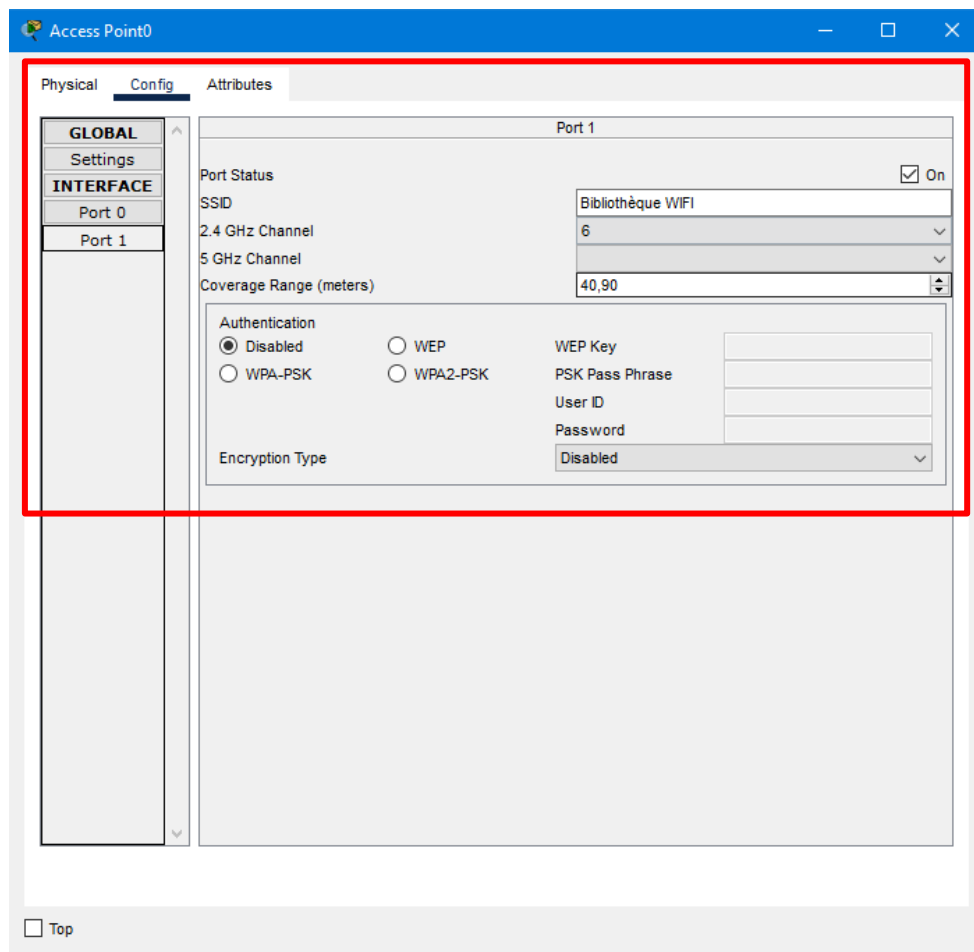
```
RouterA(config)# ip dhcp excluded-address 192.168.0.253 192.168.0.253
```

De plus, nous avons exclu l'adresse 192.168.0.253 car nous l'avons utilisé pour le SSH du switch.



Afin de permettre l'accès au WEB, nous avons utilisé la même méthode du PAT surchargé que pour le site d'Exia.

Finalement, nous devons configurer un SSID de la borne wifi de la bibliothèque avec un accès ouvert au public, soit sans mot de passe afin que n'importe qui puisse s'y connecter.

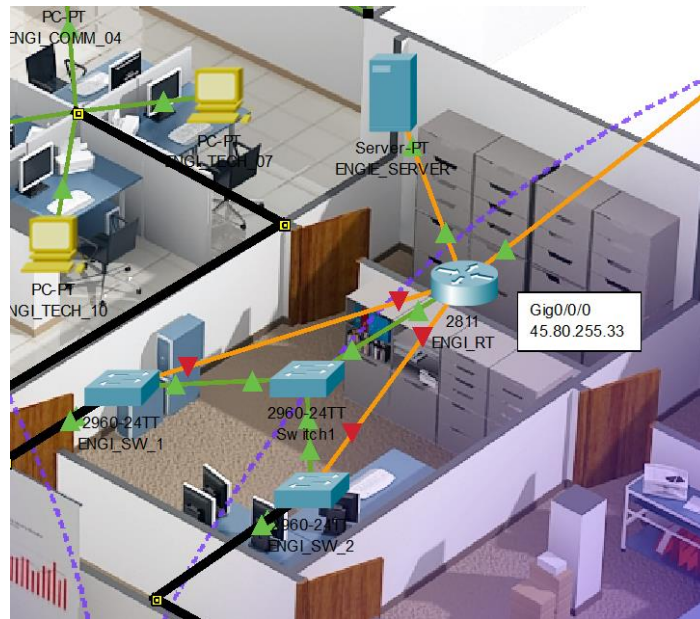


Enfin, nous avons un réseau totalement fonctionnel et répondant au cahier des charges pour le site de la bibliothèque.

3.3 Engie

Premièrement, lors de la configuration réseau du site Engie, nous avons paramétré les vlan sur le nouveau switch, switches que nous avons relié en mode trunk entre eux afin que chacun puisse communiquer les différents VLANs.

Ensuite, nous nous sommes rendu compte que le câblage avait un problème et qu'il n'était pas possible via les ports utilisés par les deux switches disponibles de paramétrer un VTP fonctionnel. De ce fait, nous avons décidé d'ajouter un 3ème switch du même modèle que les autres présents sur le Engie et branché sur le port fa0/1 éligible à la configuration d'un VTP fonctionnel car nous ne pouvions pas modifier le branchement des câbles, ni les supprimer.



Correction problème de câblage avec nouveau switch

```
Bl>en
Bl#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Bl(config)#vtp version 2
Bl(config)#vtp domain CESI
Changing VTP domain name from NULL to CESI
Bl(config)#vtp password CESI
Setting device VLAN database password to CESI
Bl(config)#vtp mode server
Device mode already VTP SERVER.
Bl(config)#exit
```

Méthode de configuration VTP

En ce qui concerne la configuration du VTP, nous avons défini le nouveau switch en tant que serveur et les deux autres qui y sont relié en mode client. Ce qui signifie que tout changement effectué sur le switch en mode serveur se répercutera sur les switches en mode client.

Nous avons donc créé le premier réseau VLAN 10, puis le second VLAN 11, le troisième VLAN 12 et pour finir le VLAN 13, correspondant respectivement au service Technique, au service Communication, au Wifi Invité et au Serveur.

Après avoir créé les vlan, nous avons paramétré tous les ports des switches en mode « access » pour différents vlan en fonction de quel pc était rattaché à ce port. Nous avons ainsi dû regarder à quel port chaque pc était relié en regardant tous les câbles qui portaient de chaque pc et leur port de destination.

Après cela, il nous a fallu faire le routage inter-VLAN afin que les ordinateurs puissent communiquer entre eux même en n'étant pas dans le même VLAN. Ainsi, nous configuré un router-on-a-stick à l'aide de la méthode suivante de création de sous-interfaces pour chaque VLAN :

```

Al>en
Al#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Al(config)#interface fa0/0.10
Al(config-subif)#encapsulation dot1q 10
Al(config-subif)#description Rouge
Al(config-subif)#ip address 192.168.10.254 255.255.255.0
Al(config-subif)#exit

```

Exemple de configuration de sous interface (issu d'une corbeille d'exercice)

Nous avons aussi ajouté une sécurité pour l'accès physique, comme nous l'avons fait sur l'exia et sur la bibliothèque, c'est-à-dire en rajoutant un mot de passe avant de pouvoir accéder à la console et au mode configuration du routeur.

Nous avons par la suite mis en place le DNS, le Domain Name System, qui permet de traduire les noms de domaine Internet en adresse IP par exemple. Pour cela, nous avons dû renseigner l'IP du serveur DNS.

The screenshot shows the 'ENGIE_SERVER' configuration window with the 'Desktop' tab selected. The 'IP Configuration' section is highlighted with a red box. It contains the following settings:

- IP Configuration:**
 - ☐ DHCP
 - ☒ Static
 - IPv4 Address: 192.168.12.33
 - Subnet Mask: 255.255.255.248
 - Default Gateway: 192.168.12.38
 - DNS Server: 0.0.0.0
- IPv6 Configuration:**
 - ☐ Automatic
 - ☒ Static
 - IPv6 Address: [empty] / [empty]
 - Link Local Address: FE80::260:70FF:FEC2:9956
 - Default Gateway: [empty]
 - DNS Server: [empty]
- 802.1X:**
 - ☐ Use 802.1X Security
 - Authentication: MD5
 - Username: [empty]
 - Password: [empty]

At the bottom left, there is a 'Top' button.

Configuration adresse ipv4 Serveur Engie DNS & DHCP

Ensuite, nous avons configuré un DHCP, c'est-à-dire un protocole réseau qui nous permet d'attribuer automatiquement les paramètres IP des ordinateurs selon notre plage d'adresse disponibles via un serveur physique contrairement à la bibliothèque.

The screenshot shows the 'Services' tab in the ENGIE_SERVER configuration window. The 'DHCP' service is selected in the sidebar. The main configuration area is titled 'DHCP' and shows settings for the 'FastEthernet0' interface. The 'Service' is set to 'On'. The configuration fields include:

- Interface: FastEthernet0
- Service: On
- Pool Name: Wifi_Invite
- Default Gateway: 192.168.12.30
- DNS Server: 192.168.12.33
- Start IP Address: 192.168.12.1
- Subnet Mask: 255.255.255.224
- Maximum Number of Users: 29
- TFTP Server: 0.0.0.0
- WLC Address: 0.0.0.0

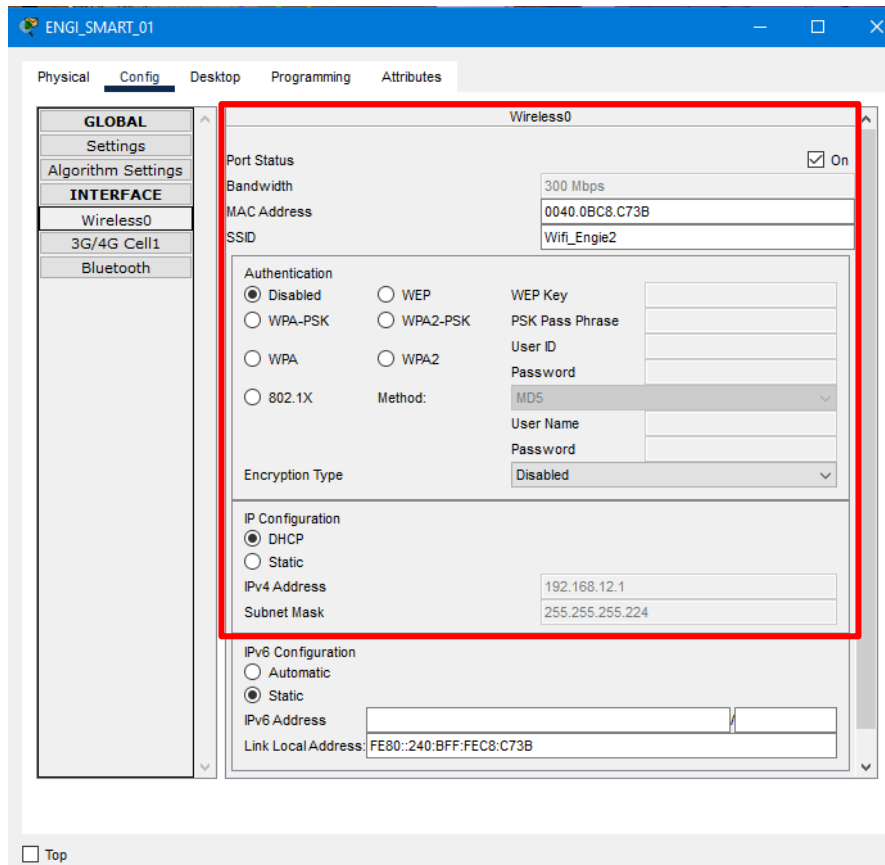
Below the configuration fields are 'Add', 'Save', and 'Remove' buttons. A table lists the configured DHCP pools:

Pool Name	Default Gateway	DNS Server	Start IP Address	Subnet Mask	Max User	TFTP Server	WLC Address
Wifi_Invite	192.168.12.30	192.168.12.33	192.168.12.1	255.255.255.224	29	0.0.0.0	0.0.0.0
Service_Comm...	192.168.12.30	192.168.12.33	192.168.12.1	255.255.255.224	61	0.0.0.0	0.0.0.0
Service_Tech...	192.168.12.30	192.168.12.33	192.168.12.1	255.255.255.224	125	0.0.0.0	0.0.0.0
serverPool	0.0.0.0	0.0.0.0	192.168.12.1	255.255.255.224	7	0.0.0.0	0.0.0.0

Configuration service DHCP

Afin de permettre un accès wifi aux Pc portables et aux téléphones portables, nous avons configuré les deux bornes wifi avec deux SSID différents sans sécurisation, donc un accès ouvert. Puis, nous avons configuré les ports du switch relié à chacune des bornes en mode access vers le vlan 12 dédié au réseau wifi.

Par la suite, nous avons connecté nos Pc portable et téléphones portables d'Engie en Wifi et leur adressage de façon dynamique.



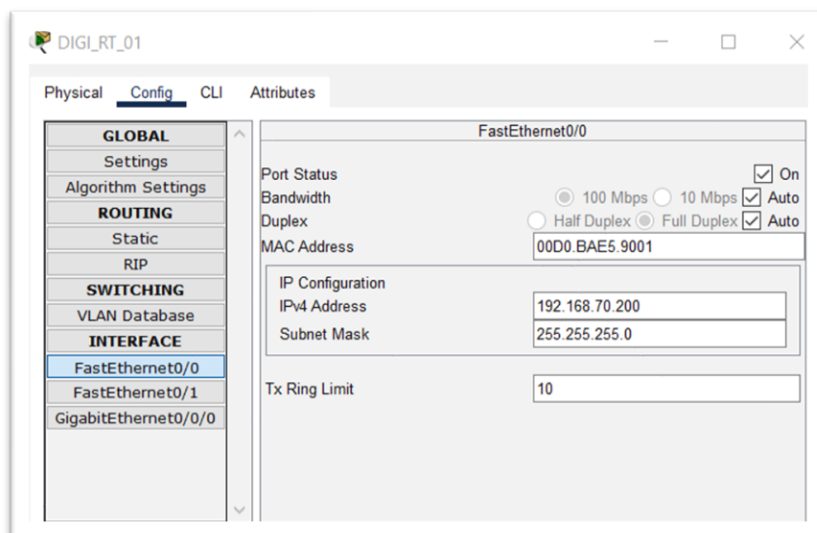
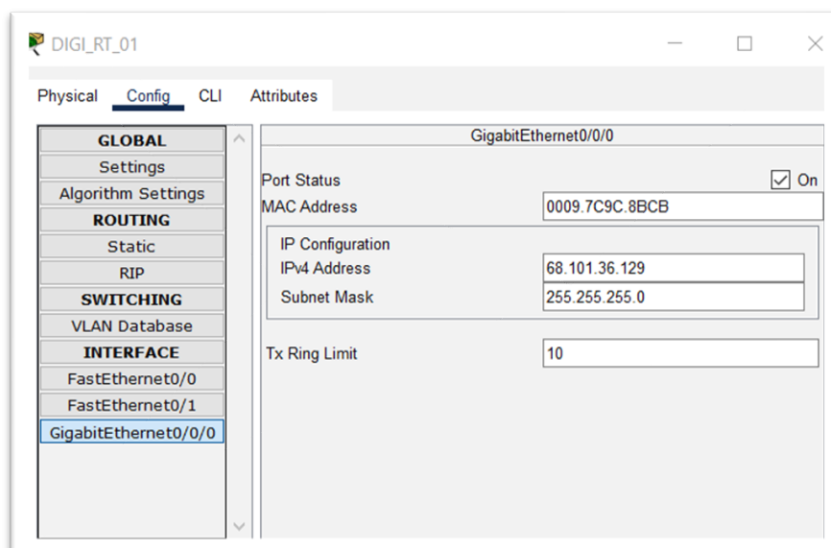
Connection téléphone portable au wifi et adressage dynamique

Finalement, nous avons configuré l'accès WEB via le routeur d'Engie et grâce, encore une fois, à la méthode du PAT.

Nous avons alors un réseau fonctionnel et répondant au cahier des charges dans son entièreté pour l'entreprise Engie.

3.4 Digiplex

Pour permettre à Digiplex de se développer durablement nous avons commencé par une chose indispensable : raccorder le Digiplex au Datacenter via son routeur. Pour cela, nous lui avons donné une adresse IPv4 comprise dans la plage d'adresse que nous avons attribué préalablement à cette connexion sur son port GigabitEthernet0/0/0 et une adresse IPv4 sur son port FastEthernet 0/0 pour faire le lien avec le switch de niveau 3 du RDC.



Pour l'Etherchannel des liaisons des switch de chaque étage, nous avons choisis d'utiliser la configuration Etherchannel avec un protocole LACP (Link Aggregation Control Protocol (protocole de contrôle d'agrégation des liens) sur le switch de niveau 3 par le biais des commandes suivantes :

```
B1>en
B1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
B1(config)#interface fa0/1
B1(config-if)#channel-protocol lacp
B1(config-if)#channel-group 1 mode active
B1(config-if)#
Creating a port-channel interface Port-channel 1

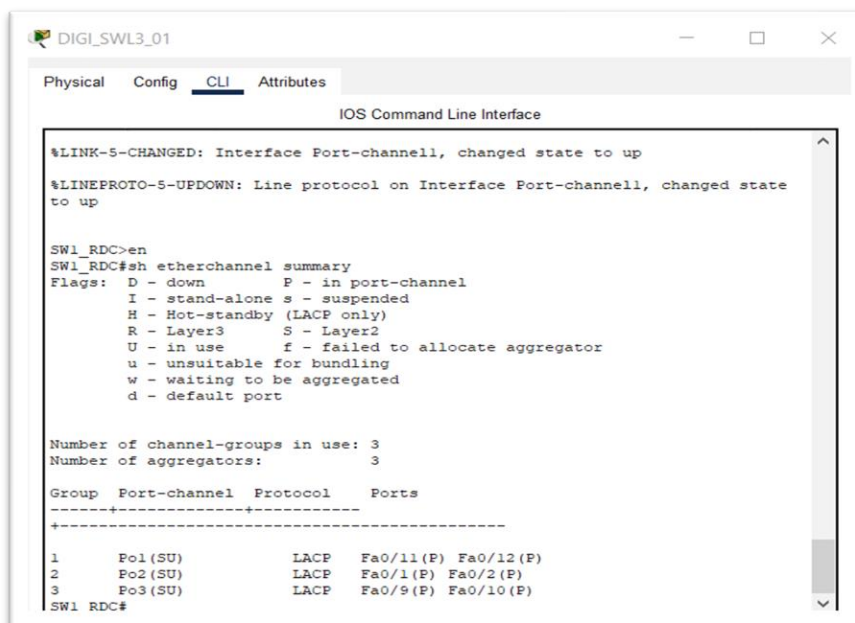
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1,
changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1,
changed state to up
no shutdown
B1(config-if)#exit
```

Exemple de configuration type d'un etherchannel (issu de la corbeille sur les VLANs)

Pour être plus précis, nous avons 3 groupes différents, un pour lier RDC et étage 1, un autre pour lier RDC et étage 2 et un dernier pour lier RDC et étage 3.

Pour vérifier que nos configurations de l'Etherchannel soient bien réussies nous avons regardé dans le switch de niveau 3 avec la commande suivante :



The screenshot shows a network switch CLI window titled 'DIGI_SWL3_01'. The 'CLI' tab is selected, and the 'IOS Command Line Interface' is active. The output of the 'show etherchannel summary' command is displayed, showing three channel-groups in use, all using the LACP protocol. The output includes a list of flags and a table of channel-groups.

```
%LINK-5-CHANGED: Interface Port-channel1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Port-channel1, changed state to up

SW1_RDC>en
SW1_RDC#sh etherchannel summary
Flags:  D - down          P - in port-channel
        I - stand-alone  S - suspended
        H - Hot-standby (LACP only)
        R - Layer3       S - Layer2
        U - in use       f - failed to allocate aggregator
        u - unsuitable for bundling
        w - waiting to be aggregated
        d - default port

Number of channel-groups in use: 3
Number of aggregators:          3

Group  Port-channel  Protocol    Ports
-----+-----+-----+-----
1      Po1(SU)        LACP       Fa0/11(P) Fa0/12(P)
2      Po2(SU)        LACP       Fa0/1(P)  Fa0/2(P)
3      Po3(SU)        LACP       Fa0/9(P)  Fa0/10(P)

SW1_RDC#
```

On peut donc observer ici qu'on a bien 3 channel-groups utilisant le protocole LACP utiliser par le switch de niveau 3 et qui réunis plusieurs ports à chaque fois.

Nous avons ensuite paramétré le VTP (VLAN Trunk Protocol) sur chacun des switchs présent dans le bâtiment. Pour faire cela, nous avons défini l'équipement serveur (celui qui va transmettre ses VLAN aux autres) et les équipements clients (ceux qui vont recevoir ces VLAN). Nous avons donc choisi le switch de niveau 3 comme équipement serveur. Pour pouvoir transmettre les données nous avons définis les ports transmettant les VLAN en mode « trunk » et ceux les recevant en mode « access ». Ceci nous a ainsi permis de transmettre paramètres sur tous les switchs des étages sans nous arrêter au switch communiquant seulement avec le niveau 3.

Issue this command in order to set the VTP domain name:

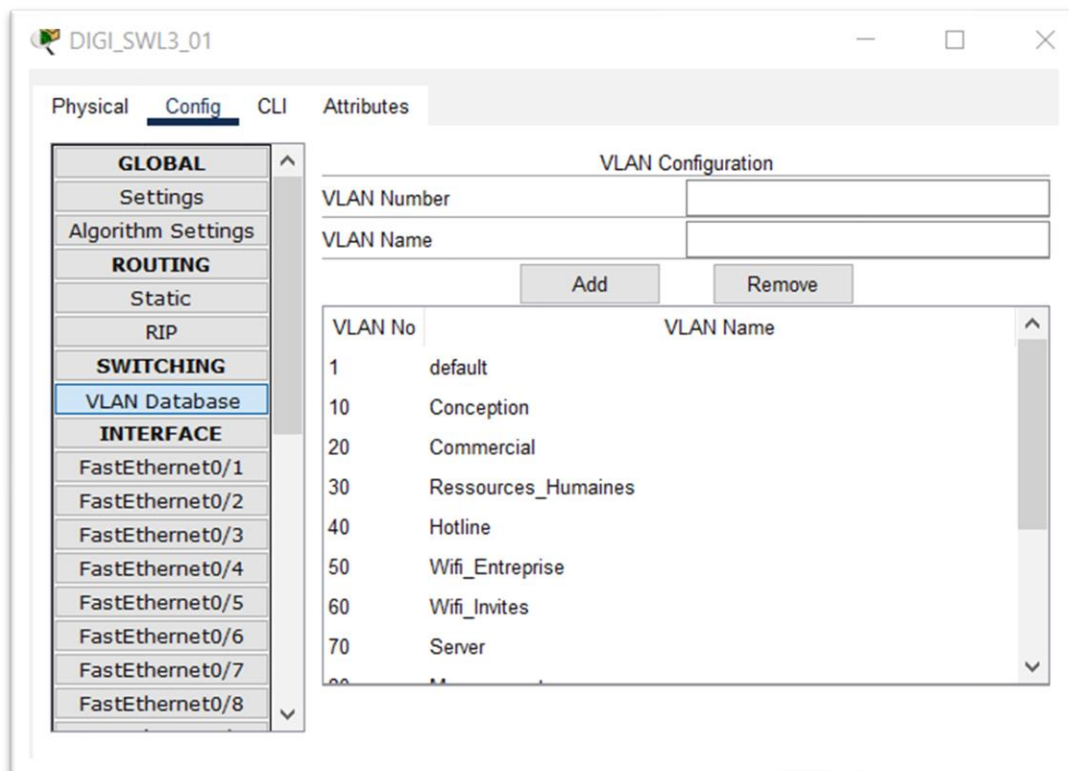
```
Router(vlan)#vtp domain domain-name
```

C.

Issue this command in order to set the VTP mode:

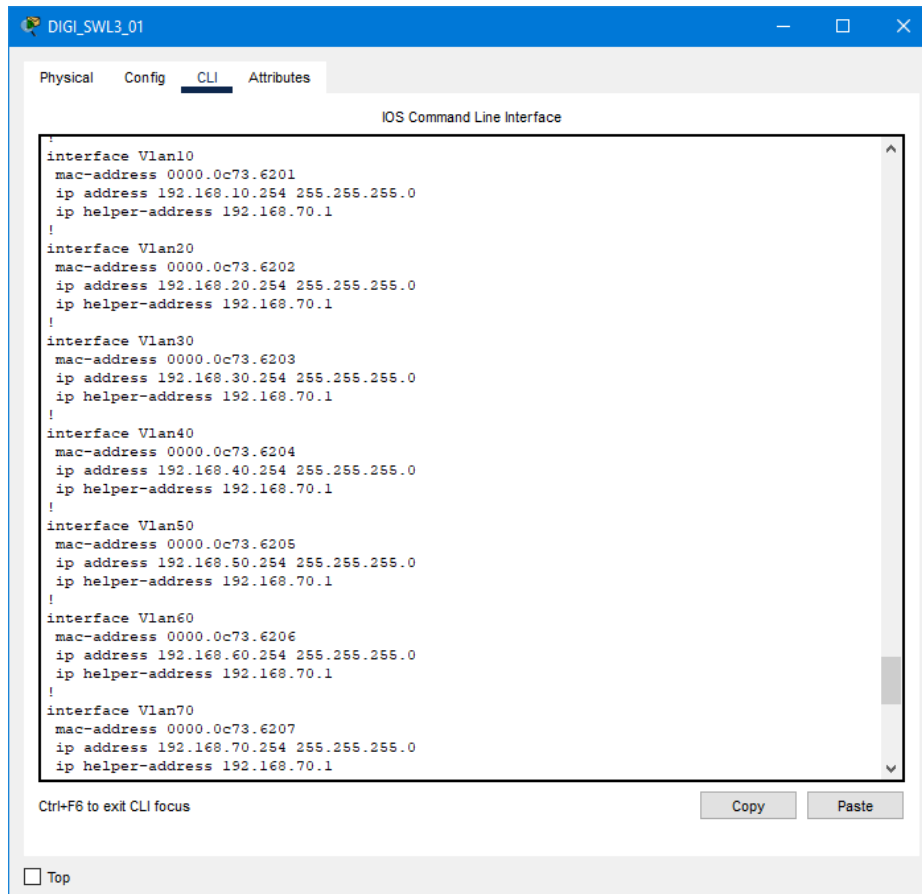
```
Router(vlan)#vtp {client | server | transparent}
```

Une fois cela fait nous avons créé les VLAN nécessaire sur notre niveau 3 comme ceci :



Ces vlan ce sont ainsi transmis à chaque appareil serveur ce qui permettra de les utiliser à chaque étage du bâtiment et de les mettre sur un VLAN commun.

Afin de permettre aux différents PC et VLAN à communiquer entre eux via grâce au switch central L3, nous avons décidé d'implémenter un routage inter-vlan sur ce dernier. Pour ce faire, nous avons commencé par implémenter des sous-interfaces pour chaque VLAN sur le switch L3. Puis, nous avons attribué une adresse à chacun étant leur default gateway (ou passerelle par défaut). Enfin, nous avons activé le routage inter-Vlan via la commande ip routing en mode configuration.



Configuration sous interfaces

Pour pouvoir nous connecter à nos switchs à distance nous avons décidé d'utiliser le protocole SSH pour chacun de nos commutateurs car il était plus sécurisé que Telnet grâce à l'utilisation d'une clé de chiffrement. Ainsi nous avons utilisé les mêmes commandes que pour les sites précédents.

Nous obtenons alors la configuration suivante :

```
:
hostname SW2_RDC
!
!
!
ip domain-name digiplex.com
!
username digiplex privilege 1 password 0 banane
!
```

```

!
line con 0
!
line vty 0 4
 login local
 transport input ssh
line vty 5 15
 login local
 transport input ssh
!

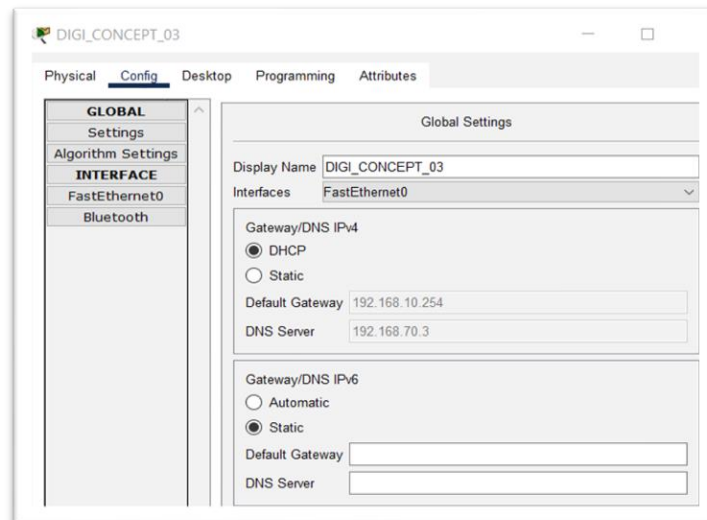
```

Pour pouvoir attribuer automatiquement les adresses des appareils sur les différents réseaux nous avons mis en place un serveur DHCP contenant les informations des différents réseaux utilisé par le Digiplex :

The screenshot shows the DIGI_SRV_DHCP configuration window with the 'Services' tab selected. The 'DHCP' service is configured for the 'FastEthernet0' interface. The configuration includes a pool name 'Commercial', a default gateway of 192.168.20.254, a DNS server of 192.168.70.3, and a start IP address of 192.168.20.1 with a subnet mask of 255.255.255.0. The maximum number of users is set to 253. The TFTP and WLC addresses are both 0.0.0.0. Below the configuration fields, there is a table listing the configured DHCP pools.

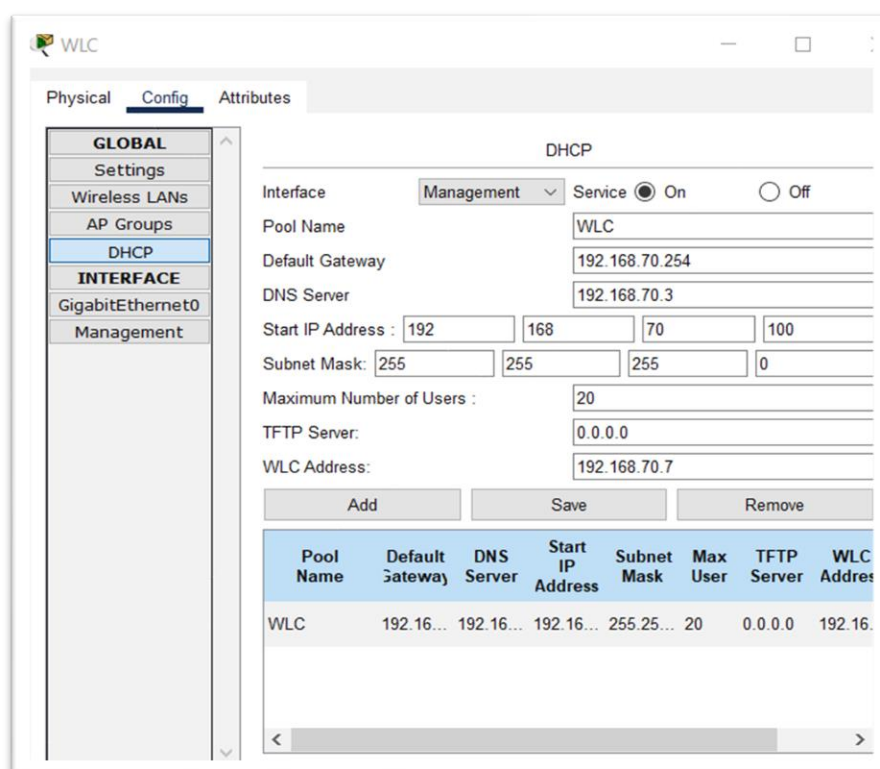
Pool Name	Default Gateway	DNS Server	Start IP Address	Subnet Mask	Max User	TFTP Server	WLC Address
Commercial	192.16...	192.16...	192.16...	255.25...	253	0.0.0.0	0.0.0.0
Conception	192.16...	192.16...	192.16...	255.25...	253	0.0.0.0	0.0.0.0
serverPool	0.0.0.0	0.0.0.0	10.0.0.1	255.25...	255	0.0.0.0	0.0.0.0

Comme nos switches ont été paramétrés en access pour les VLANs y compris le 70, nous avons plus qu'à configurer l'IP helper address sur le switch L3 via la commande du même nom et aller dans un PC régler son attribution d'adresse sur DHCP :



Cependant nos laptops étaient hors de portée de nos switches car ceux-ci n'utilisent pas la connexion filaire mais utilise une connexion wifi.

Nous avons donc besoin de faire appel à un Wireless LAN Controller ou WLC et des accesspoint pour pouvoir créer des zones de wifi. Nous avons donc dû définir des groupes d'accesspoint et définir les spécificités des réseaux wifi.



The screenshot shows the WLC configuration window with the 'Config' tab selected. The left sidebar has 'AP Groups' highlighted under the 'GLOBAL' section. The main area is titled 'AP Groups' and contains the following fields and tables:

- Select AP Group:** A dropdown menu set to 'default-group'.
- Name:** A text field containing 'default-group'.
- Wireless LANs:** A section with the text 'Each Wireless LAN can belong to multiple AP groups.' followed by a table:

In AP Gro	Name	SSID
<input checked="" type="checkbox"/>	Wifi_Invite	Wifi_Invite
<input checked="" type="checkbox"/>	Wifi_Enterprise	Wifi_Enterprise
- Access Points:** A section with the text 'Each Access Point can belong to one AP group.' followed by a table:

In AP Gro	Name	MAC Address	Status
<input checked="" type="checkbox"/>	DIGI3_AP_02	00D0.97A4.9101	Online
<input checked="" type="checkbox"/>	DIGI3_AP_04	000A.F397.9A01	Online

At the bottom of the main area are three buttons: 'New', 'Remove', and 'Save'.

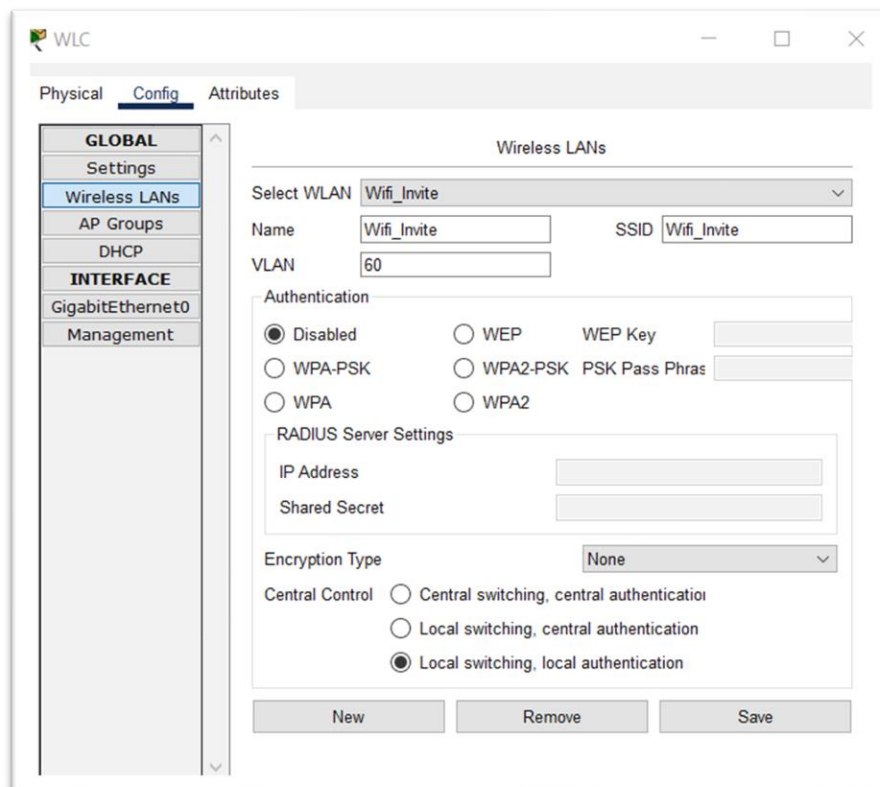
Configuration des groupes d'access-point

The screenshot shows the WLC configuration window with the 'Config' tab selected. The left sidebar has 'Wireless LANs' highlighted under the 'GLOBAL' section. The main area is titled 'Wireless LANs' and contains the following fields and sections:

- Select WLAN:** A dropdown menu set to 'Wifi_Enterprise'.
- Name:** A text field containing 'Wifi_Enterprise'.
- SSID:** A text field containing 'Wifi_Enterprise'.
- VLAN:** A text field containing '50'.
- Authentication:** A section with radio buttons for 'Disabled', 'WPA-PSK', 'WPA', 'WEP', 'WPA2-PSK', and 'WPA2'. 'WPA2-PSK' is selected.
 - WEP Key:** A text field (empty).
 - PSK Pass Phrase:** A text field containing 'banane2022'.
- RADIUS Server Settings:** A section with:
 - IP Address:** A text field containing '192.168.70.4'.
 - Shared Secret:** A text field containing 'banane'.
- Encryption Type:** A dropdown menu set to 'AES'.
- Central Control:** A section with radio buttons for 'Central switching, central authentication', 'Local switching, central authentication', and 'Local switching, local authentication'. 'Local switching, local authentication' is selected.

At the bottom of the main area are three buttons: 'New', 'Remove', and 'Save'.

Configuration du SSID d'entreprise en WPA2-PSK



Configuration du SSID des invités en accès ouvert

Ensuite, pour permettre aux bornes wifi de se connecter au WLC il nous a fallu configurer les différents liens reliés au WLC et aux access-point en mode trunk avec un vlan natif 70 car ce dernier fait partie du vlan 70.

```

interface FastEthernet0/14
 switchport trunk native vlan 70
 switchport trunk encapsulation dot1q
 switchport mode trunk
!

```

Configuration vlan natif 70 et mode trunk des différents liens

Enfin pour connecter les laptops aux réseaux, il nous a fallu aller sur un des laptops, dans la partie Desktop et dans l'option « PC Wireless ».



Connection au wifi sur les PC portables

Finalement, pour l'accès WEB, nous avons utilisé la même méthode que pour les autres sites (PAT) sur le routeur. Cependant, comme le routeur est configuré dans le réseau VLAN 70, nous avons rencontré un problème de communication. En effet, les PC n'arrivaient pas à communiquer avec le routeur et de même pour le switch L3 qui n'arrivait pas à communiquer avec ce dernier.

De ce fait, nous avons dû définir des routes statiques pour chaque VLAN sur le routeur en direction du switch L3, et une route statique par défaut sur le switch L3 allant vers le routeur permettant alors de transmettre au routeur les messages provenant des différents VLAN et de même pour le routeur de communiquer avec les différents VLAN (soit les différents PC).

```
ip helper-address 192.168.70.1
!
interface Vlan50
 mac-address 0000.0c73.6205
 ip address 192.168.50.254 255.255.255.0
 ip helper-address 192.168.70.1
!
interface Vlan60
 mac-address 0000.0c73.6206
 ip address 192.168.60.254 255.255.255.0
 ip helper-address 192.168.70.1
!
interface Vlan70
 mac-address 0000.0c73.6207
 ip address 192.168.70.254 255.255.255.0
 ip helper-address 192.168.70.1
!
interface Vlan80
 mac-address 0000.0c73.6208
 no ip address
 ip helper-address 192.168.70.1
!
ip classless
ip route 0.0.0.0 0.0.0.0 192.168.70.200
!
ip flow-export version 9
!
!
no cdp run
!
!
```

Configuration sur le switch L3

```
!
interface Vlan1
 no ip address
!
ip nat inside source list 10 interface GigabitEthernet0/0/0 overload
ip nat inside source list 20 interface GigabitEthernet0/0/0 overload
ip nat inside source list 30 interface GigabitEthernet0/0/0 overload
ip nat inside source list 40 interface GigabitEthernet0/0/0 overload
ip nat inside source list 50 interface GigabitEthernet0/0/0 overload
ip nat inside source list 60 interface GigabitEthernet0/0/0 overload
ip classless
ip route 0.0.0.0 0.0.0.0 GigabitEthernet0/0/0
ip route 192.168.10.0 255.255.255.0 FastEthernet0/0/0
ip route 192.168.20.0 255.255.255.0 FastEthernet0/0/0
ip route 192.168.30.0 255.255.255.0 FastEthernet0/0/0
ip route 192.168.40.0 255.255.255.0 FastEthernet0/0/0
ip route 192.168.50.0 255.255.255.0 FastEthernet0/0/0
ip route 192.168.60.0 255.255.255.0 FastEthernet0/0/0
ip route 192.168.70.0 255.255.255.0 FastEthernet0/0/0
!
ip flow-export version 9
!
!
access-list 10 permit 192.168.10.0 0.0.0.255
access-list 20 permit 192.168.20.0 0.0.0.255
access-list 30 permit 192.168.30.0 0.0.0.255
access-list 40 permit 192.168.40.0 0.0.0.255
access-list 50 permit 192.168.50.0 0.0.0.255
access-list 60 permit 192.168.60.0 0.0.0.255
!
!
!
```

Configuration sur le routeur

Nous avons alors un réseau fonctionnel et respectant le cahier des charges pour le site Digiplex.

4. Plan de Déploiement

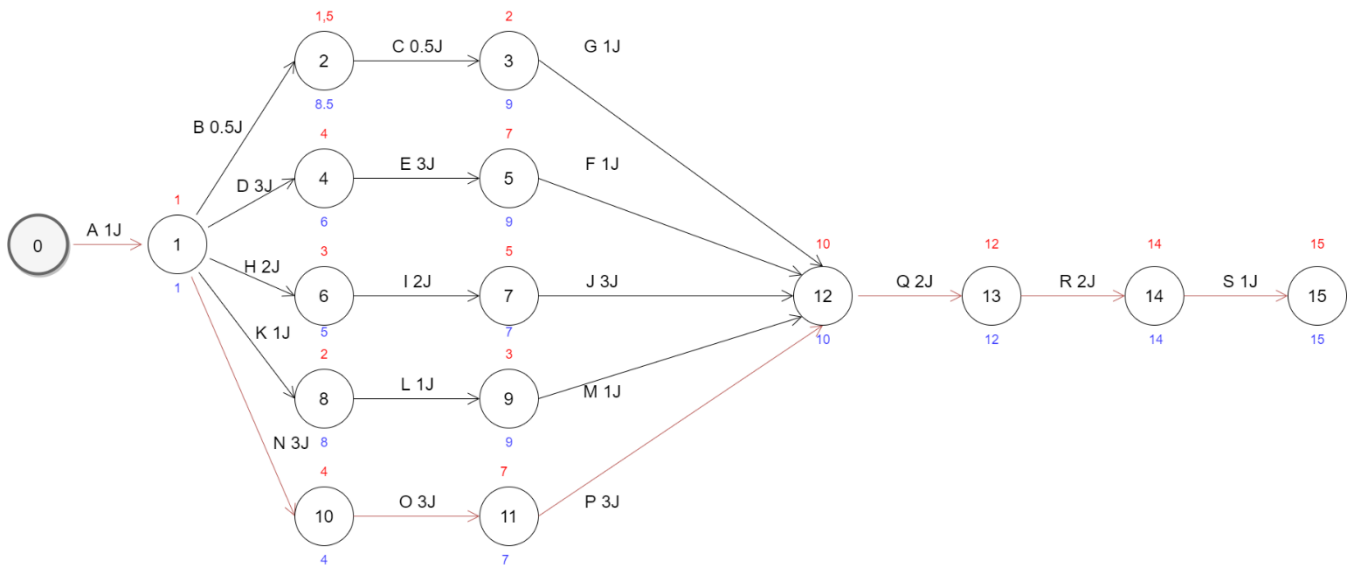
4.1 Organisation du déploiement

Une fois que la simulation est complètement paramétrée et fonctionnelle, nous pouvons maintenant passer à la phase de planification du déploiement sur site. Pour cela, nous avons dans un premier temps listé toutes les tâches à effectuer pour assurer cet objectif.

Voici la liste des tâches à effectuer, ainsi que leur effectif, leur durée et leur antécédant.

	Tâches	Effectif	Antériorité	Durée (J)
A	Réception du matériel	4	-	1
B	Installation du matériel Exia	1	A	0,5
C	Paramétrage réseau Exia	1	B	0,5
D	Installation du matériel Datacenter	2	A	3
E	Paramétrage réseau Datacenter	2	D	3
F	Test/troubleshooting réseau Datacenter	2	E	1
G	Test/Troubelshooting réseau Exia	1	C	1
H	Installation du matériel Engie	2	A	2
I	Paramétrage réseau Engie	2	H	2
J	Test/Troubelshooting réseau Engie	2	I	3
K	Installation du matériel bibliothèque	1	A	1
L	Paramétrage réseau bibliothèque	1	K	1
M	Test/Troubelshooting Réseau Bibliothèque	1	L	1
N	Installation du matériel Digiplex	2	A	3
O	Paramétrage réseau Digiplex	2	N	3
P	Test/Troubelshooting Réseau Digiplex	4	O	3
Q	Paramétrage tunnel IPV6	2	G - F - J - M - P	2
R	Test/Troubelshooting Tunnel IPV6	4	Q	2
S	Test Accès WEB général	4	R	1

Nous avons détaillé ces tâches afin de permettre une meilleure organisation au moment du déploiement. Ce tableau, nous emmène au diagramme Pert suivant :



Nous pouvons apercevoir le chemin critique en orange. Nous devons donc au moment du déploiement nous concentrer essentiellement sur la ponctualité de ces tâches.

Pour une meilleure répartition des tâches, nous avons conçu un diagramme Gant. Cela va nous permettre de mieux visualiser la durée de chaque tâche ainsi que leur date d'échéance. Voici le GANT du plan de déploiement :

[Dossier final](#)

4.2 Schéma Visio Logique

Étant donné la complexité de notre maquette finale, cela peut empêcher la compréhension ou la visualisation du réseau dans certains bâtiments comme par exemple, le Digiplex. C'est la raison pour laquelle nous avons produit un schéma Visio Logique de l'infrastructure réseau.

Il nous a permis de mieux situer les modifications et paramétrages au fur et à mesure du projet.

Pour représenter le réseau de la ville de manière plus simplifiée, et afin de pouvoir mieux comprendre quels seraient les enjeux d'un problème sur une ligne de communication précise, nous avons fait un schéma Visio logique. En effet, ce type de schéma nous permet de représenter les différentes parties qui composent nos bâtiments. Nous avons donc décidé de faire un schéma Visio logique de chaque bâtiment ainsi qu'un autre sur le plan général de la ville, soit le raccordement de chaque bâtiment au datacenter (ou DSLAM).

Pour ce faire, nous avons dû répertorier toutes les connexions entre les pc, les switchs, les routeurs et les points d'accès sans fil de chaque bâtiment. Par exemple, dans le cas de Digiplex, chacun des étages est visible sur un seul schéma.

De plus, pour simplifier la représentation des PC ou équipements finaux en trop grand nombre, nous avons décidé de les abréger et les regrouper en un seul signe les représentant.

[Dossier final](#)

5. Gestion de Projet

Afin de permettre une fluidité et une bonne organisation dans l'équipe, nous avons créé un Diagramme Pert ainsi qu'un Gantt. Ces tâches ont été effectuées pour les mêmes raisons que le plan de déploiement. Cela facilite la visualisation temporelle des tâches ainsi que le partage des tâches dans l'équipe. Nous avons d'abord effectué, comme précédemment, la liste des tâches nécessaires à ce projet.

	Tâches	Effectifs (Max)	Antériorités	Durée (J)
A	Analyse du sujet	4	-	1
B	Expression des besoins	4	A	1
C	Création du Pert + Gantt	4	B	2
D	Plan d'adressage Bibliothèque	1	C	3
E	Plan d'adressage Exia	1	C	3
F	Plan d'adressage Engie	1	C	3
G	Plan d'adressage Digiplex	1	C	3
H	Rédaction livrable 1 - Bibliothèque	1	D	1
I	Rédaction livrable 1 - Exia	1	E	1
J	Rédaction livrable 1 - Engie	1	F	1
K	Rédaction livrable 1 - Digiplex	1	G	1
L	Plan d'adressage Datacenter	4	D-E-F-G	2
M	Finalisation livrable 1 - Datacenter	4	L	1
N	Paramétrage réseau Datacenter	4	M	3
O	Essais maquette Datacenter	4	N	1
P	Paramétrage réseau bibliothèque	2	O	1
Q	Paramétrage réseau Exia	2	O	1
R	Paramétrage réseau Engie	2	O	1
S	Paramétrage réseau Digiplex	4	O	2
T	Essais maquette Bibliothèque	1	P	1
U	Essais maquette Exia	1	Q	1
V	Essais maquette Engie	2	R	1
W	Essais maquette Digiplex	4	S	1
X	Rédaction livrable 2	4	W	3
Y	Plan de déploiement	2	X	2
Z	Schéma Visio logique	2	X	2
AA	Rédaction livrable 3 - Plan déploiement	2	Y	1
AB	Rédaction livrable 3 - Schéma Visio	4	Z	1
AC	Rédaction Livrable 4	4	AB	1
AD	Préparation de la soutenance	4	AC	2
AE	Présentation	4	AD	1

Comme vous pouvez vous en apercevoir, nous avons également beaucoup détaillé les tâches et mis en avant leur répartition dans l'équipe.

Le Pert et le Gantt, sont trop grands pour être affichés. Vous pouvez alors visualiser ces documents ici :

[Dossier final](#)

6. Conclusion

Pour conclure, nous avons pu fournir une maquette complète et fonctionnelle suite au plan d'adressage établie dans un premier temps. Nous avons ensuite réalisé avec succès le plan de déploiement et l'organisation dans le groupe. Cela a permis d'accomplir le projet dans les temps et sans difficultés particulières mise à part quelques-unes rencontrées dans la maquette.

L'infrastructure réseau de notre client pourra alors commencer à être livrée et déployée dans les temps.

7. Annexes

Vous trouverez en pièce attachée la maquette finale, les tableaux Excel regroupant les Perts et Gantt du déploiement et du suivi de projet. Vous trouverez également les schémas Visio Logiques du projet.

[Dossier final](#)