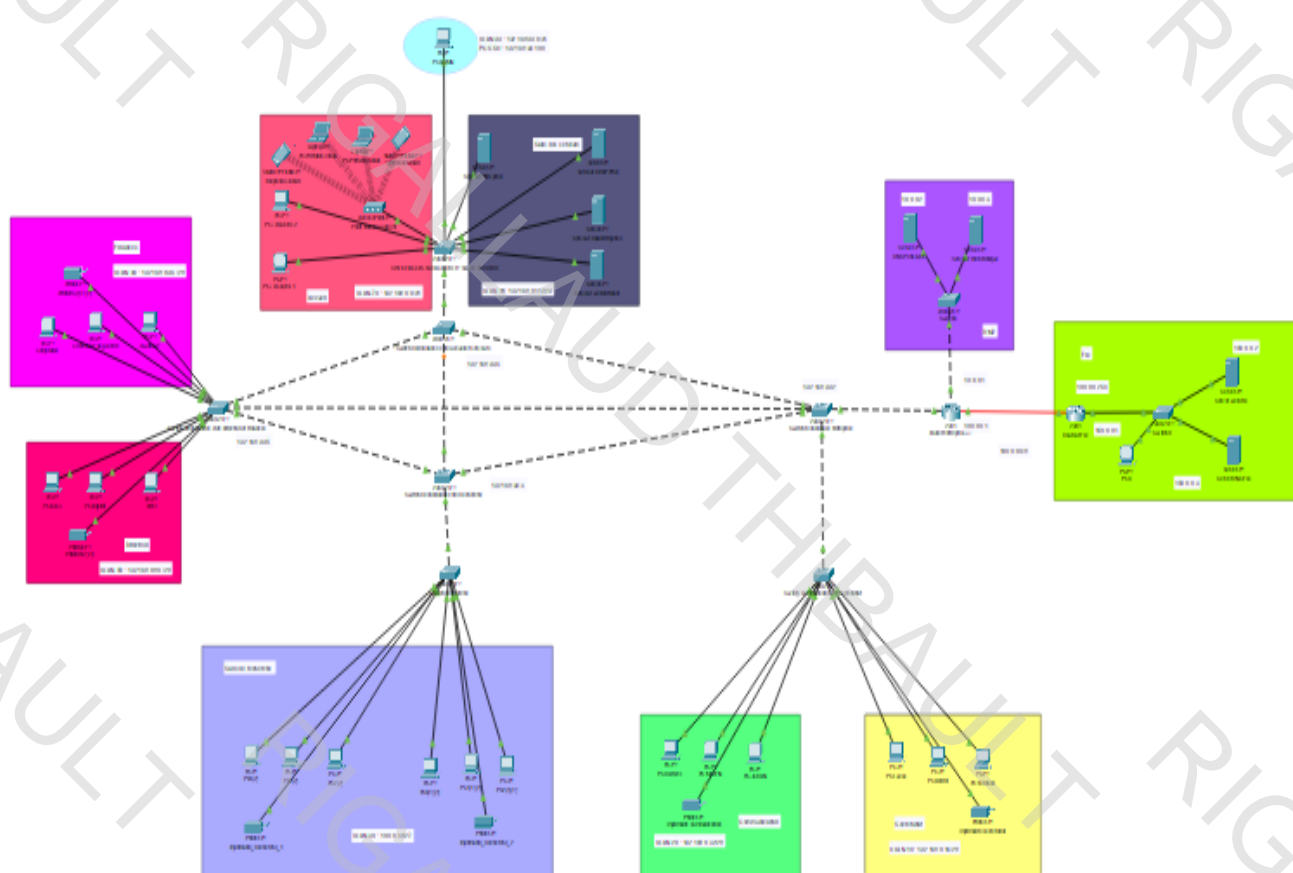


# COMPTE RENDU SAE201

Présentation du Travail effectué pour la SAE

Rigallaud Thibault Groupe C



IUT de Blois

SAE201- Construire un réseau informatique pour une petite entreprise

## Table des matières

I.	Présentation de la SAE .....	2
II.	Création du réseau de l'entreprise .....	4
	A. Mise en place de la redondance des switchs .....	9
	B. Mise en place des VLAN et du VLSM.....	9
	C. Configuration des serveurs privés à l'entreprise .....	14
	D. Configuration de la DMZ.....	26
III.	Partie FAI .....	28
	A. Adressage et configuration du routeur.....	28
	B. Configuration des serveurs du FAI.....	29
IV.	Configuration des équipements pour la communication inter-réseau.....	31
	A. NAT/PAT .....	31
	B. ROUTES.....	33
V.	Sécurité et Vérifications .....	33
	A. SSH et ACL de contrôle de flux.....	33
	B. Vérifications.....	38
VI.	Conclusion.....	40

## I. Présentation de la SAE

### Objectif :

Pour rappel, l'objectif de cette SAE est de faire une synthèse des connaissances en réseau que nous avons pu acquérir tout au long de notre première année de BUT R&T. De plus, elle permet d'évaluer nos compétences afin concevoir un réseau informatique entièrement fonctionnel pour une petite entreprise.

### Programme National :

Selon le programme national, le professionnel R&T peut être sollicité pour construire et mettre en place le réseau informatique d'une petite entreprise multisites. L'objectif est alors de répondre aux besoins pour construire et mettre en place le réseau de commutation, de routage, de services réseaux de base et de sécurité formulés pour la Structure. Ce réseau s'appuie sur des équipements et des services informatiques incontournables mais fondamentaux pour fournir à la structure un réseau fonctionnel et structuré.

De plus, le professionnel R&T doit comprendre et construire une architecture d'un réseau d'entreprise avec un accès à Internet, élaborer une méthode efficace pour tester progressivement la configuration réalisée : capturer le trafic ; prouver par différents points de vérification la validation des contraintes du cahier des charges.

### Les ressources utilisées lors de cette SAE :

- R101-Initiation aux réseaux informatiques
- R102-Principes et architecture des réseaux
- R103-Réseaux locaux et équipements actifs
- R108-Bases des systèmes d'exploitation
- R201-Technologies de l'internet
- R202-Administration système et fondamentaux de la virtualisation
- R203-Bases des services réseaux
- R210-Anglais technique 2
- R211-Expression-Culture-Communication Professionnelles : Renforcement de techniques de communication
- R212-Projet Personnel et Professionnel

### Cahier des charges :

Mettre en œuvre le réseau informatique d'une petite entreprise devant comporter :

- Plusieurs switchs en redondance
- Plusieurs VLANs
- Une architecture de sous-réseaux IPv4 privés en VLSM
- Un serveur public, un serveur web intranet, un serveur DNS public, un serveur DNS privé, un serveur DHCP donnant une configuration IP à certains clients
- Le raccordement au réseau public d'un FAI comportant au minimum le serveur web et le serveur DNS du FAI et un client dans le FAI
- Les PC de l'entreprise doivent accéder au site web du FAI, le FAI doit pouvoir accéder au site web de l'entreprise
- Tous les équipements d'interconnexion doivent être sécurisés et accessibles du PC administrateur de l'entreprise en SSH
- Double adressage : IPv4 obligatoire, IPv6 apprécié
- D'autres services et fonctionnalités peuvent être ajoutés au choix, l'architecture et l'étendue de votre réseau d'entreprise ne dépend que de vous. Mais inutile d'élaborer un réseau complexe si les fonctionnalités de base n'y sont pas !
- Les noms des VLANs, des PC, des serveurs et du FAI ainsi que les contenus des sites web doivent être personnalisés : pas de nom générique du style PC1, PC2, SRV1, VLAN1...

## II. Création du réseau de l'entreprise

Avant de commencer à développer toutes les étapes passées afin d'aboutir à la création d'un réseau d'entreprise, nous allons vous exposer le matériel utilisé ainsi que le schéma global du réseau.

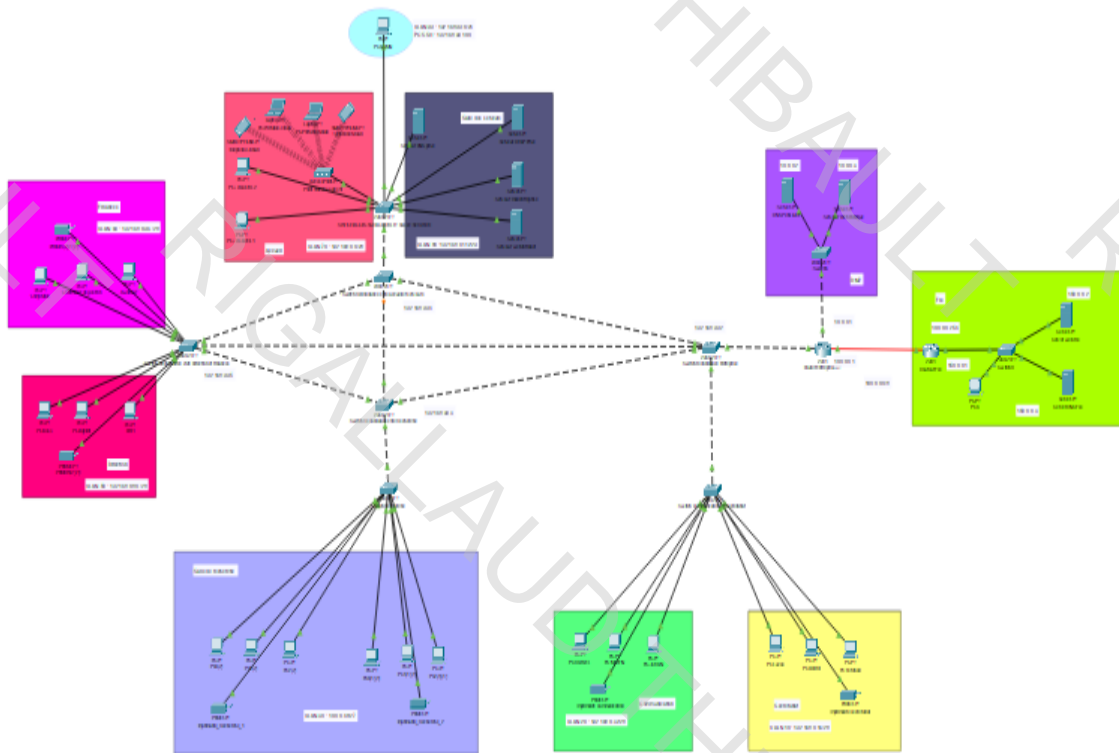


Figure 1 : Réseau de l'entreprise

Ainsi, nous avons ici l'architecture complète du réseau, il est composé de 6 salles configurées via des VLANs auquel nous ajoutons la DMZ et un petit réseau représentant le FAI comportant un PC client, un serveur DNS et un serveur WEB.

Pour créer notre réseau, nous avons donc besoin de matériels permettant sa gestion et son fonctionnement (interconnexion, routage...), les voici :

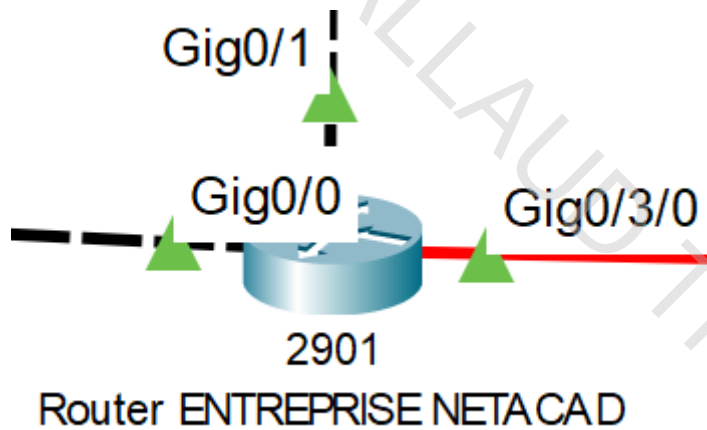


Figure 2 : Routeur Entreprise

On remarque que le routeur est connecté sur 3 interfaces, cela s'explique par l'architecture du réseau. En effet, l'interface de gauche est connectée au réseau privé de l'entreprise sur le port GigabitEthernet0/0, l'interface du haut est connectée à la DMZ de l'entreprise sur le port GigabitEthernet0/1 quant à l'interface de droite, elle est connectée au routeur du FAI via l'interface GigabitEthernet0/3/0 avec une liaison fibre.

Pour rajouter cette liaison fibre, nous avons du rajouter un module sur le routeur 2901 car le port fibre n'est pas présent par défaut sur cet équipement. Voici les différentes étapes pour le faire.

Tout d'abord, il faut se rendre dans l'interface physique du routeur (rond rouge) puis dans un second temps l'éteindre (rond bleu).

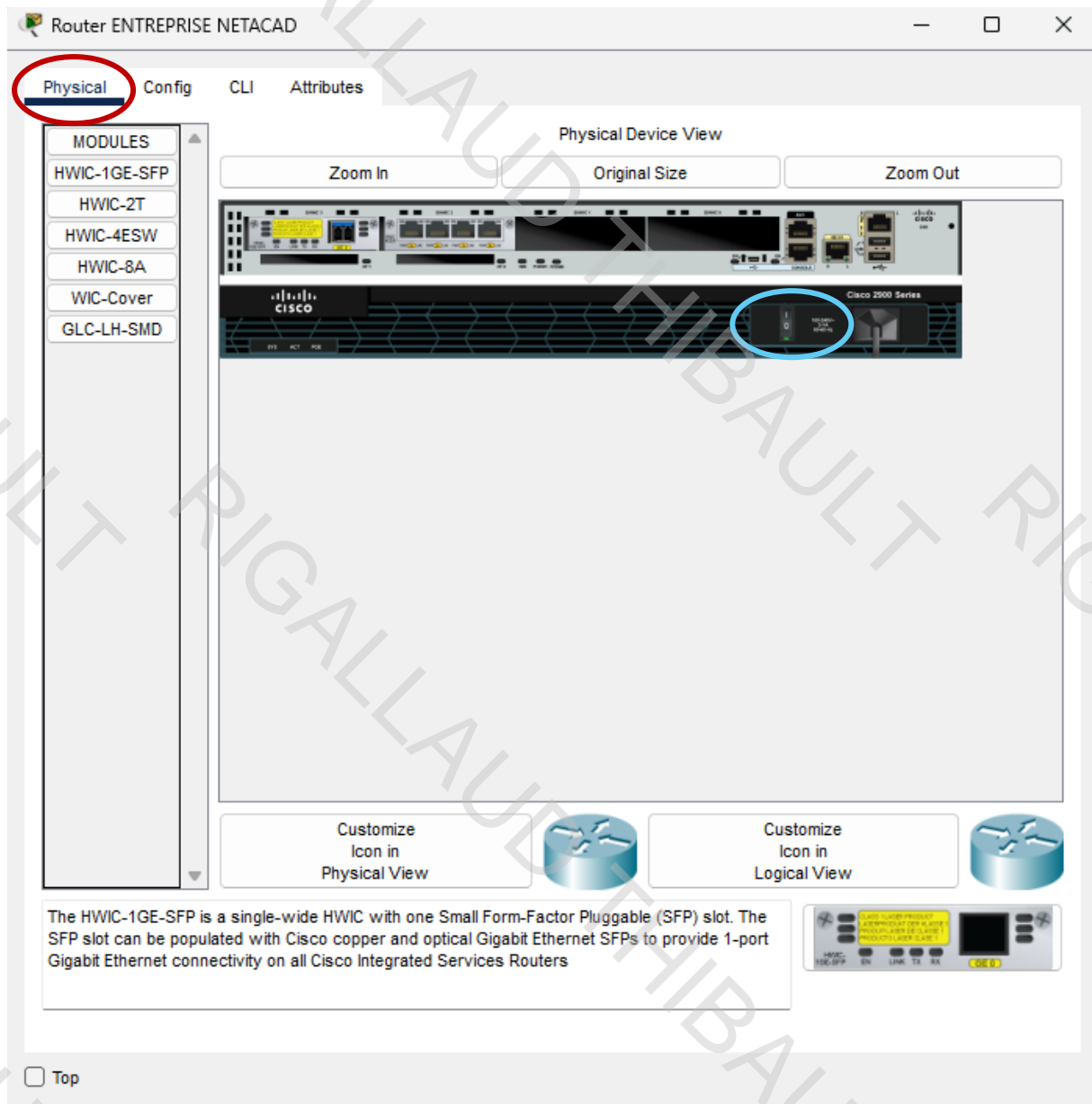


Figure 3 : Fenêtre physique routeur

Une fois que le routeur est éteint, nous pouvons rajouter les 2 modules suivants :

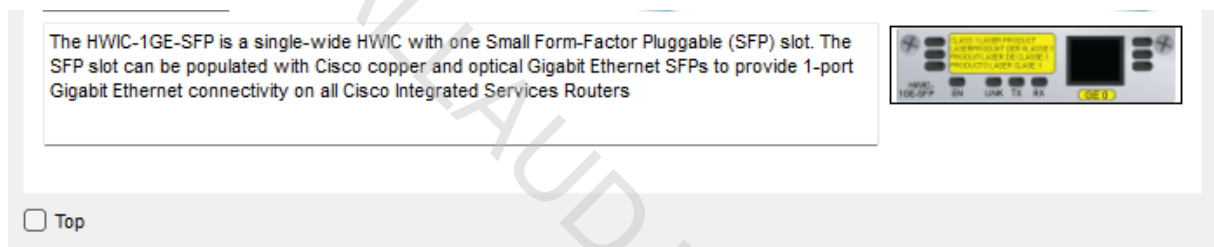


Figure 4 : Module HWIC

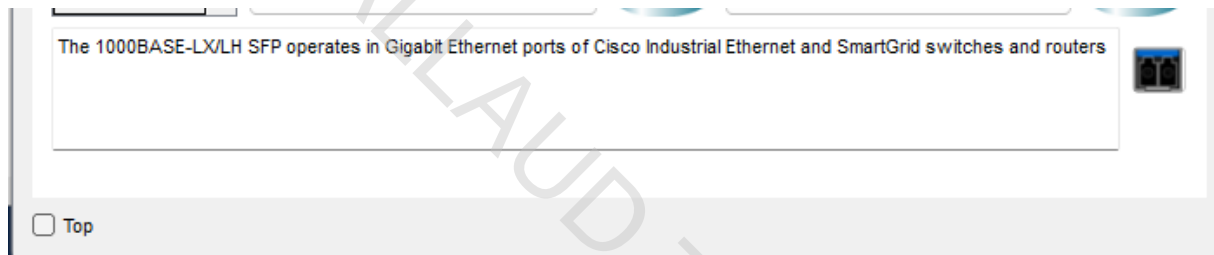


Figure 5 : Module GLC-LH-SMD

Le premier module va permettre d'ajouter un port pour la fibre sur le routeur. Le second module est le port fibre à implémenter dans le premier module. Voyons comment s'y prendre :



Figure 6 : Routeur Vide face arrière

Nous avons ici un routeur 2901 sans aucun module ajouté.

Nous allons ainsi pouvoir y rajouter le module HWIC-1GE-SFP dans un des « trous » qui permettent son installation (cercle rose)



Figure 7 : Routeur Face arrière avec module HWIC

Ainsi, on a bien ajouté au routeur le module permettant de rajouter dans un second temps le port fibre. Pour le port fibre, il suffit de le faire glisser dans l'espace qui lui est laissé par le module HWIC (cercle violet).



Figure 8 : Routeur Face arrière prêt à être connecté en fibre sur le port GigabitEthernet0/3/0

Ainsi, une fois ces deux modules ajoutés, le routeur va pouvoir accueillir une liaison fibre. Il est tout de même important de notifier que nous aurions aussi pu utiliser un câble Serial DTE que l'on aurait connecté sur le port Serial de notre routeur mais ce n'est pas le moyen de connexion inter-routeur que nous avons choisi.

Ensuite, nous allons aussi retrouver des serveurs qui permettront d'avoir des services à l'intérieur de l'entreprise tel qu'un le DNS, le DHCP, WEB, SMTP/POP3 (mail).

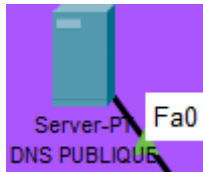


Figure 9 : Serveur sur Cisco

Voici la représentation graphique d'un serveur sur Cisco Packet Tracer. A noter que dans un serveur nous y retrouvons tous les services utilisables sur Packet Tracer et qu'il n'y a pas de serveurs particuliers à choisir pour un service en particulier (voir Figure 10 : Interface Graphique serveur sur Packet Tracer)

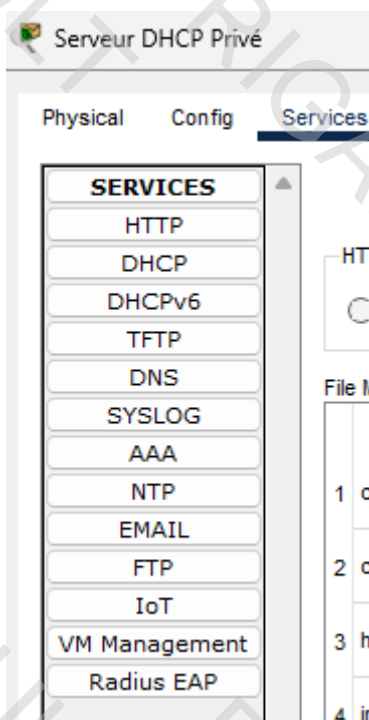
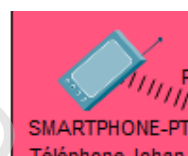
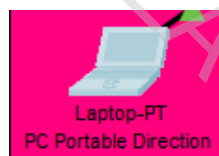


Figure 10 : Interface Graphique serveur sur Packet Tracer

De plus, nous retrouverons dans notre réseau tout un ensemble d'équipement client tel que des PC, Smartphones, Imprimantes, Ordinateurs Portable.



Afin de pouvoir garantir un réseau sans fil dans certaines salles, nous avons aussi utilisé des ACCESS-POINT permettant de mettre en place un WiFi sécurisé.



Enfin, nous avons aussi utilisé une multitude de switch dans le réseau permettant de relier plusieurs équipements au sein du LAN. Nous allons voir leur configuration.

#### A. Mise en place de la redondance des switches

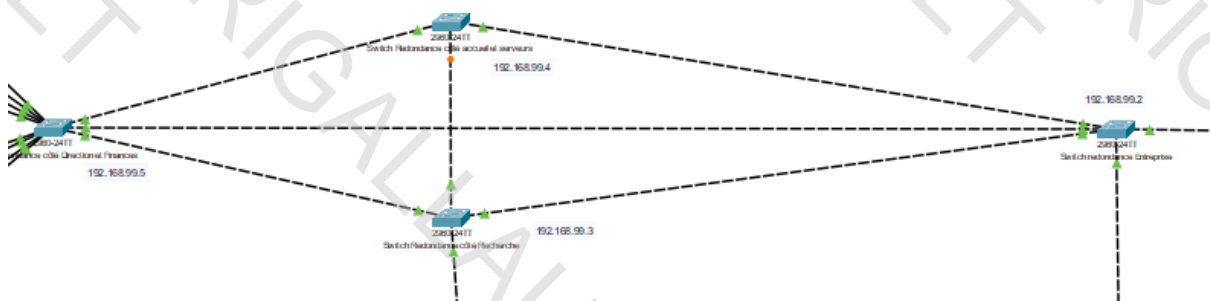


Figure 11 : Redondance des SW

Ainsi, pour le réseau de l'entreprise nous avons décidé de former un triangle de switches afin d'avoir une redondance sur le réseau privé. Cette configuration permet d'avoir des routes de secours en cas de pannes d'un des switches. Cependant, il y réside quand même un problème de fiabilité car il n'y a qu'un seul switch qui relie le reste du réseau au routeur de l'entreprise.

#### B. Mise en place des VLAN et du VLSM

Pour la création du réseau d'entreprise, il était inscrit dans le cahier des charges que nous devons mettre en place plusieurs VLANs ainsi qu'un adressage en VLSM.

Ainsi, nous avons ci-dessous l'ensemble de VLANs que nous avons dû créer lors de la mise en place du réseau.

1	default	active
10	Secretariat	active
20	Communication	active
30	Salle_de_Recherche_1	active
50	Direction	active
60	Finances	active
70	Accueil	active
80	Salle_serveur	active
99	Admin	active

Figure 12 : Tous les VLANs du réseau

Ainsi pour chaque VLANs nous avons dû les créer dans les switchs correspondant ainsi que dans le routeur. Pour cela voici les commandes utilisées dans le CLI pour le mettre en place :

```
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#vlan 20
Switch(config-vlan)#name Communication
Switch(config-vlan)#exit
Switch(config)#int
Switch(config)#interface vlan 20
Switch(config-if)#
```

Figure 13 : Création du VLAN20 dans le switch racine

Les commandes inscrites sur la capture d'écran ci-dessus permettent de créer le VLAN 20 et de le renommer avec un nom plus explicite tel que Communication. Cela va permettre de se repérer de façon plus aisée lors des modifications dans le réseau.

```
Switch(config-if-range)#interface range fastEthernet0/2-5
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan 20
Switch(config-if-range)#exit
Switch(config)#exit
```

Figure 14 : Attribution de certains ports du switch pour le VLAN 20

Ainsi, les commandes suivantes permettent de passer les ports du switch en mode access (port qui achemine uniquement le trafic vers et depuis le VLAN spécifique qui lui a été attribué).

Pour configurer l'ensemble des switchs dont nous avons besoin nous avons adapté ces commandes en fonction du nom du VLAN voulu, son numéro et les ports qui lui sont attribués.

Malgré tout, la configuration des switchs n'est pas terminée. Afin que le réseau puisse bien communiquer, il est important de mettre en place des ports en mode trunk. Pour rappel, un trunk est généralement un lien entre deux équipements réseaux (ici switch et routeur). Il permet de transporter du trafic pour plusieurs VLANs.

```
interface GigabitEthernet0/1
  switchport mode trunk
```

Figure 15 : Interface switch mode trunk

Ainsi la commande `switchport mode trunk` permet de passer le port de l'interface souhaité en mode trunk permettant ainsi le transport du trafic des VLANs. Bien évidemment, pour que le transport marche, il faut que le mode trunk soit activé sur les deux côtés du lien.

De plus, pour que notre configuration fonctionne avec des VLANs nous avons dû configurer des sous interfaces sur le routeur. En effet voici un exemple de sous interface configurées sur le routeur pour le VLAN10

```
Router>en
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#go
Router(config)#i
Router(config)#in
Router(config)#interface gi
Router(config)#interface gigabitEthernet 0/0.10
Router(config-subif)#enc
Router(config-subif)#encapsulation dot1Q
% Incomplete command.
Router(config-subif)#encapsulation dot1Q 10
Router(config-subif)#ip add
Router(config-subif)#ip address 192.168.0.7 255.255.255.240
```

Figure 16 : Configuration d'une sous interface sur le routeur

Ici l'objectif est de mettre en place une sous-interface sur un routeur Cisco afin de permettre le routage inter-VLAN". Nous avons donc créé la sous-interface GigabitEthernet 0/0.10 ce qui signifie qu'elle est destinée au VLAN 10. Pour que cette sous-interface puisse gérer le trafic de ce VLAN l'encapsulation IEEE 802.1Q est configurée avec l'identifiant du VLAN (dot1Q 10). Enfin nous avons attribué à cette sous-interface, une adresse IP (ici 192.168.0.7) et un masque de sous-réseau (255.255.255.240) ce qui permettra au routeur de communiquer avec les hôtes du VLAN 10. Cette configuration est essentielle pour permettre à différents VLANs, isolés sur un switch, de communiquer entre eux via le routeur.

De cette manière, nous avons répété ces actions pour chaque VLAN en attribuant une IP qui respecte notre adressage IP VLSM<sup>1</sup>.

Comme dis précédemment, pour organiser le réseau et séparer les différents services de l'entreprise nous avons mis en place plusieurs VLANs. Chaque service (comme la direction, le secrétariat, la salle de recherche, etc.) est associé à un VLAN spécifique ce qui permet d'isoler logiquement les communications et de mieux gérer la sécurité. Nous avons utilisé le VLSM pour adapter la taille des sous-réseaux selon le nombre de machines par service. Par exemple, les services avec peu de postes (comme la direction) ont un sous-réseau en /28 pouvant accueillir au maximum 14 machines.

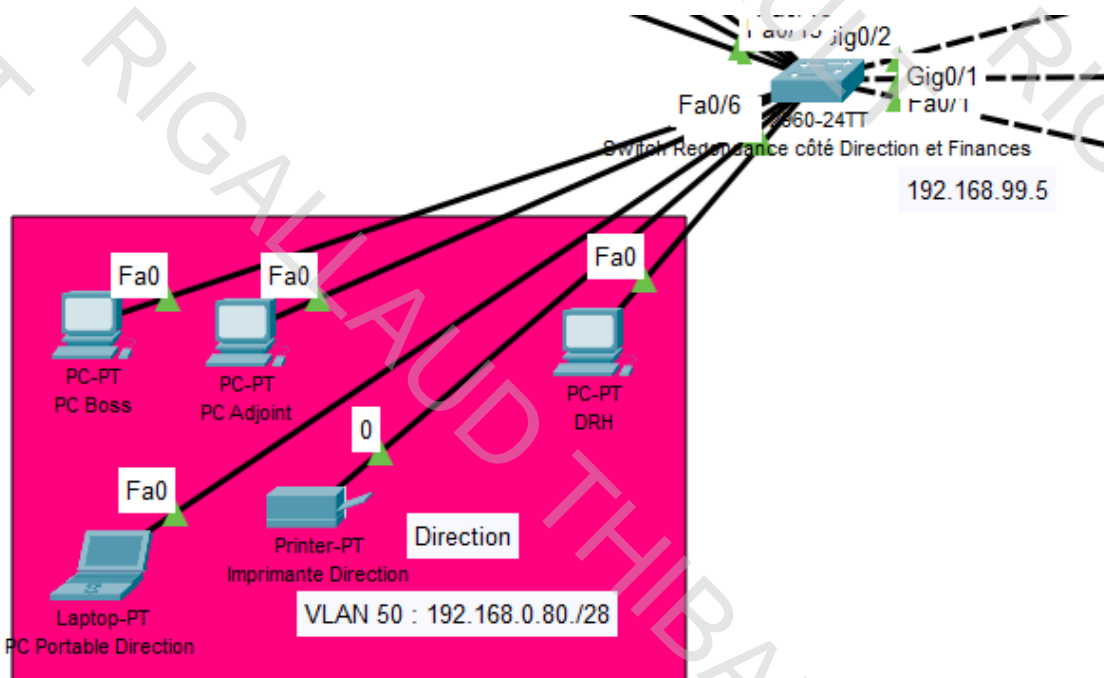


Figure 17 : VLAN 50

En effet, on remarque que pour la direction, nous avons 5 machines (3 PC, 1 PC portable et une imprimante). Ceci nous oblige à avoir un minimum de 6 adresses car nous en utilisons une de plus pour celle de la sous-interface du routeur. Voici les raisons qui nous ont poussé à choisir un masque en /28. Malgré le peu de machines dans la direction un masque en /29 n'aurait pas été adapté car on a  $2^3 - 2 = 6$  IP disponibles pour un /29 et qu'il est important de garder au moins une adresse de libre en cas d'ajout de matériel imprévu.

Au contraire pour la salle de recherche qui a plus de machines nous avons choisi un sous-réseau en /27.

<sup>1</sup> Variable Length Subnet Mask

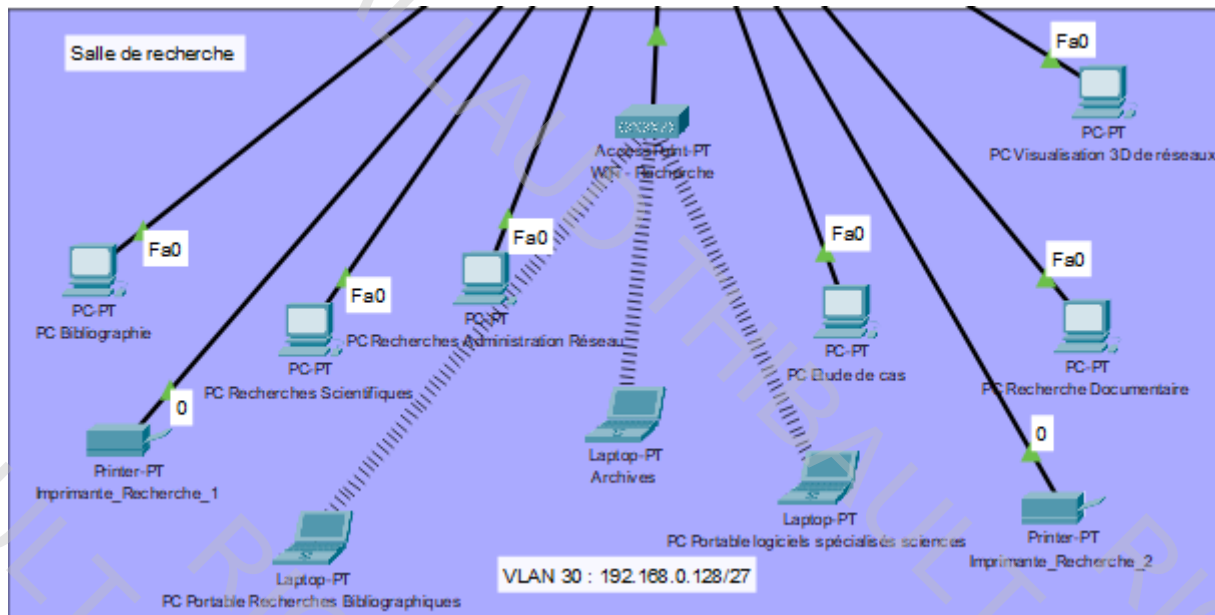


Figure 18 : VLAN 30

On peut facilement expliquer ce choix car nous avons beaucoup plus de machines présentes sur ce VLAN. En effet on recense 12 machines sur ce réseau + la passerelle par défaut. Avec 13 machines au total il est vrai que nous aurions pu opter pour un sous réseau en /28 car nous aurions eu  $2^4 - 2 = 14$  IP disponibles. Cependant nous avons opté pour un réseau en /27 pour avoir des adresses plus flexibles permettant de rajouter des machines dans la salle de recherche en cas de besoin ( $2^5 - 2 = 30$ ).

Vous pouvez d'ailleurs remarquer que l'on passe du VLAN 30 au 50. Cela s'explique car pendant la confection du réseau nous avons d'abord séparé la salle de recherche en 2 VLANs, cependant après réflexion cela n'était pas réellement utile. Nous avons de plus pris le choix de ne pas modifier tous les n° de VLANs car leur n° tel quel ne change pas vraiment le réseau en lui-même.

Pour résumer pour que tous ces VLANs puissent communiquer nous avons donc configuré un routage inter-VLAN en créant des sous-interfaces sur le routeur, chacune associée à un VLAN avec l'encapsulation dot1Q. Ensuite, nous avons attribué une adresse IP à chaque sous-interface qui sert de passerelle pour les postes du VLAN concerné. Grâce à cette configuration les machines peuvent communiquer entre elles même si elles sont sur des VLANs différents tout en gardant une structure réseau claire et optimisée.

Voici un tableau qui représente l'adressage LAN du réseau de l'entreprise

Interface	VLAN	Adresse IP	Masque	Adresse réseau	Plage d'adresses utilisables	Broadcast
GigabitEthernet0/0.70	70	192.168.0.1	255.255.255.240 (/28)	192.168.0.0	192.168.0.1 – 192.168.0.14	192.168.0.15
GigabitEthernet0/0.10	10	192.168.0.17	255.255.255.240 (/28)	192.168.0.16	192.168.0.17 – 192.168.0.30	192.168.0.31
GigabitEthernet0/0.20	20	192.168.0.33	255.255.255.240 (/28)	192.168.0.32	192.168.0.33 – 192.168.0.46	192.168.0.47
GigabitEthernet0/0.30	30	192.168.0.129	255.255.255.224 (/27)	192.168.0.128	192.168.0.129 – 192.168.0.158	192.168.0.159
GigabitEthernet0/0.50	50	192.168.0.81	255.255.255.240 (/28)	192.168.0.80	192.168.0.81 – 192.168.0.94	192.168.0.95
GigabitEthernet0/0.60	60	192.168.0.97	255.255.255.240 (/28)	192.168.0.96	192.168.0.97 – 192.168.0.110	192.168.0.111
GigabitEthernet0/0.80	80	192.168.0.113	255.255.255.248 (/29)	192.168.0.112	192.168.0.113 – 192.168.0.119	192.168.0.120
GigabitEthernet0/0.99	99	192.168.99.1	255.255.255.0 (/24)	192.168.99.0	192.168.99.1 – 192.168.99.254	192.168.99.255

### C. Configuration des serveurs privés à l'entreprise

Ainsi, nous avons mis en place plusieurs serveurs privés à l'entreprise tel qu'un DNS privé, un DHCP privé, un serveur mail, et un web intranet.

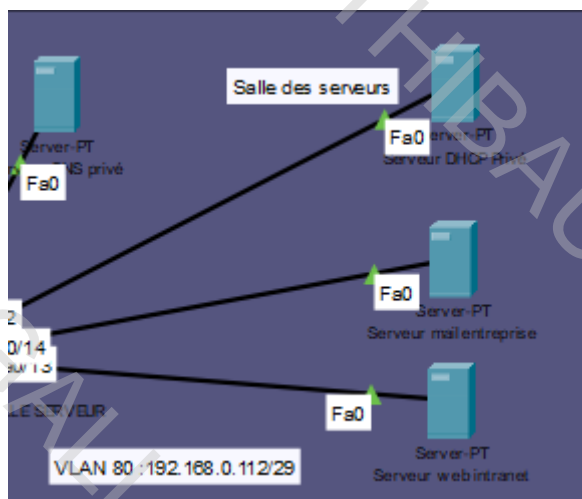


Figure 19 : VLAN 80, serveurs

Dans cette partie, nous allons voir leur création et leur mise en place dans le LAN de l'entreprise.

Ces serveurs figurent tous dans le VLAN 80 qui a pour adresse réseau 192.168.0.112/29. Nous justifions ce /29 par le peu de machines présentes dans ce VLAN.

Passons maintenant à la configuration du serveur DNS privé :

Afin de configurer notre DNS, nous nous retrouvons dans l'interface graphique fournie par Cisco Packet Tracer lorsque l'on clique sur l'icône d'un serveur. Nous y retrouvons donc tous les services utilisables sur Packet Tracer comme dis précédemment et nous choisissons le DNS.

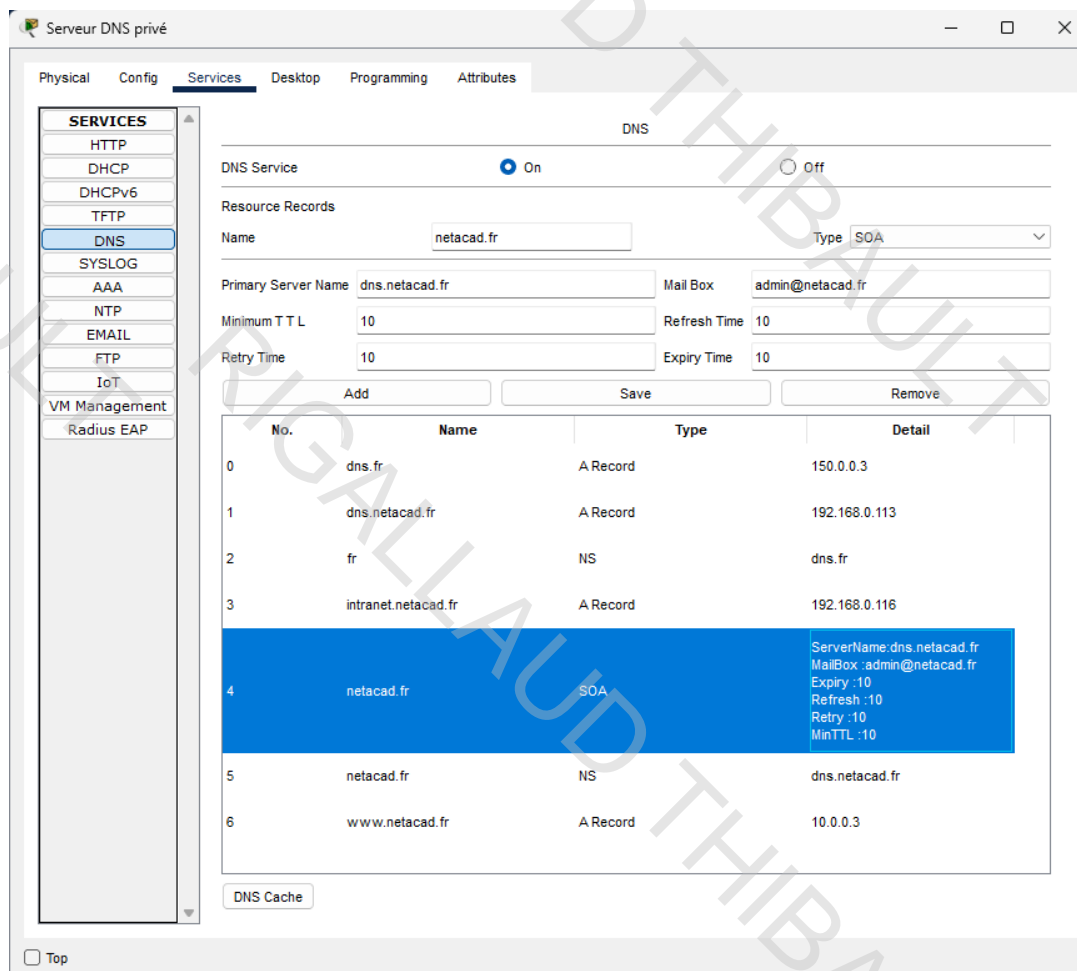


Figure 20 : DNS privé de l'entreprise

Pour rappel, le rôle principal d'un serveur DNS est de faire la correspondance entre un nom de domaine comme [www.netacad.fr](http://www.netacad.fr) et une adresse IP comme 10.0.0.3. Cela permet aux utilisateurs d'accéder facilement à des ressources sur le réseau sans avoir à retenir les adresses IP. Dans cette configuration le service DNS est activé pour le domaine netacad.fr. Son adresse IP est 192.168.0.114/29 et on y retrouve différents types d'enregistrements : les A Record associent un nom à une adresse IP par exemple dns.netacad.fr pointe vers 192.168.0.113, dns.fr pointe 150.0.0.3 et [www.netacad.fr](http://www.netacad.fr) pointe vers 10.0.0.3 Les NS désignent les serveurs responsables du domaine ici dns.fr et dns.netacad.fr relié respectivement à fr et netacad.fr. Enfin le SOA (Start of Authority) indique que le serveur principal est dns.netacad.fr, avec un administrateur admin@netacad.fr. Ce dernier enregistrement contient aussi des informations comme le TTL, le temps de rafraîchissement, d'expiration et de tentative en cas d'échec.

Comme pour la configuration du DNS, nous nous retrouvons sur l'interface graphique des serveurs via Packet Tracer où nous choisissons le service DHCP afin de mettre en place ce service dans notre salle d'accueil

**Serveur DHCP Privé**

Physical Config **Services** Desktop Programming Attributes

**SERVICES**

- HTTP
- DHCP**
- DHCPv6
- TFTP
- DNS
- SYSLOG
- AAA
- NTP
- EMAIL
- FTP
- IoT
- VM Management
- Radius EAP

**DHCP**

Interface: FastEthernet0 Service: ☒ On ☐ Off

Pool Name: serverPool

Default Gateway: 192.168.0.1

DNS Server: 192.168.0.2

Start IP Address: 192 168 0 5

Subnet Mask: 255 255 255 240

Maximum Number of Users: 8

TFTP Server: 0.0.0.0

WLC Address: 0.0.0.0

Add Save Remove

Pool Name	Default Gateway	DNS Server	Start IP Address	Subnet Mask	Max User	TFTP Server	WLC Address
serverPool	192.168.0.1	192.168.0.2	192.168.0.5	255.255.255.240	8	0.0.0.0	0.0.0.0

Figure 21 : Serveur DHCP Entreprise

Pour rappel, le service DHCP permet d'attribuer automatiquement une adresse IP aux machines qui se connectent à un réseau comme ici aux équipements connectés à l'access-point dans la salle d'accueil. Ici, le serveur DHCP est activé sur l'interface FastEthernet0. Le pool nommé serverPool permet de délivrer une passerelle par défaut définie sur 192.168.0.1 et un serveur DNS sur 192.168.0.2 avec une plage d'adresses commençant à 192.168.0.5 avec un masque de sous-réseau 255.255.255.240 ce qui permet de gérer jusqu'à 8 utilisateurs (comme précisé dans le champ "Maximum Number of Users"). Ainsi chaque machine connectée au point d'accès de la salle d'accueil recevra automatiquement une configuration réseau correcte (adresse IP, passerelle, DNS) sans intervention manuelle.

Avant de passer à la création du serveur web Intranet de l'entreprise ainsi que la création du serveur mail, nous allons profiter de l'explication de la confection du DNS pour parler de l'intégration de l'access-point dans l'accueil.

Pour que l'access-point fonctionne dans notre salle d'accueil, nous avons donc branché le port Ethernet de l'access-point sur un port du switch appartenant au VLAN 70 correspondant au VLAN des appareils de la salle d'accueil. Nous avons fait de même pour le serveur DHCP en le connectant en Ethernet à un port du VLAN70 afin qu'il puisse délivrer un adressage automatique aux appareils se connectant au réseau via l'access-point. Cette manière de faire marche que notre serveur est connecté au même switch que l'access-point, cependant si ce n'était pas le cas nous aurions pu utiliser la commande `ip helper-address 192.168.0.3` pour que le routeur puisse relayer les requêtes DHCP et que l'on puisse ainsi obtenir un adressage dynamique. Une fois ceci fait, nous avons mis en place en réseau sans fil grâce à l'interface graphique fournie par Packet Tracer.

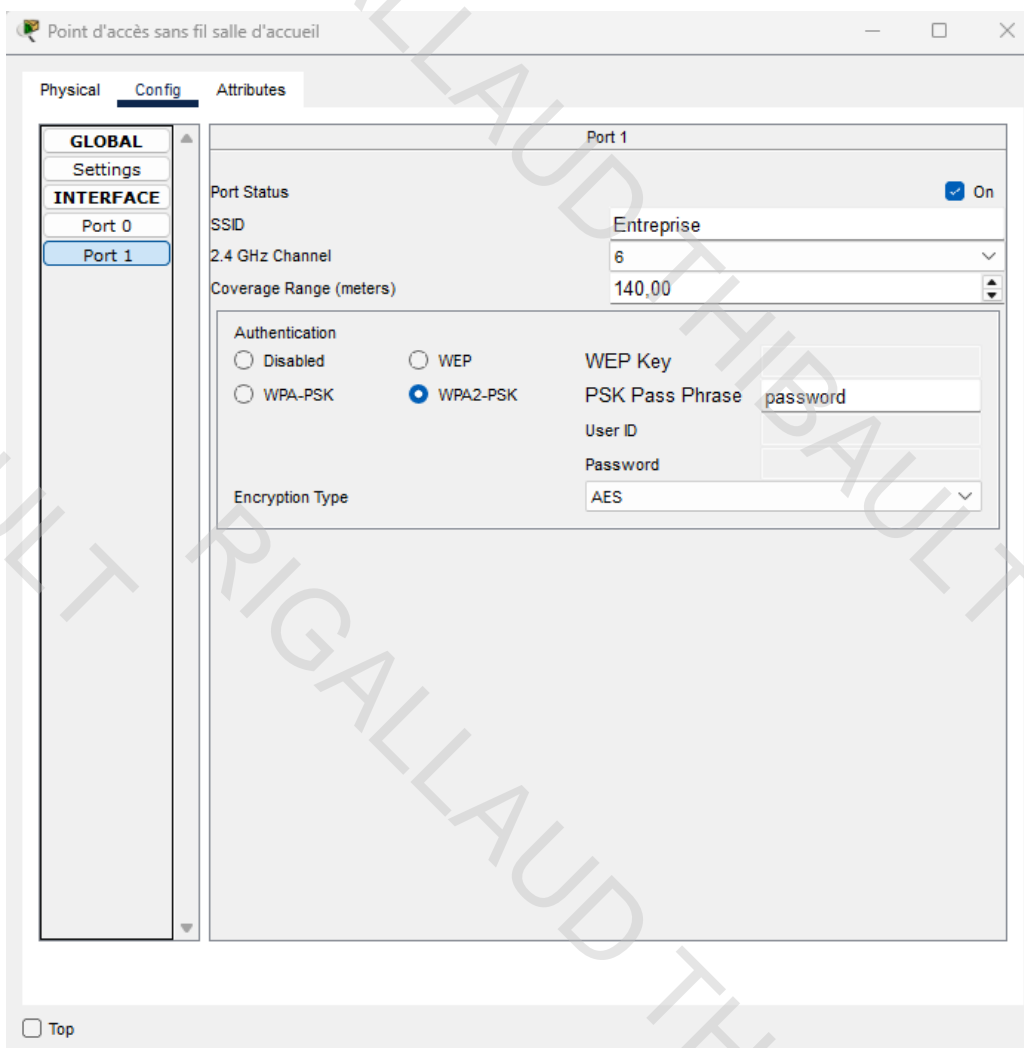


Figure 22 : Configuration réseau sans fil accueil

Ainsi comme l'indique la Figure 22 : Configuration réseau sans fil accueil, nous avons configuré le SSID de notre réseau sans-fil que nous avons nommé simplement « Entreprise ». Ensuite, nous avons choisi la méthode d'authentification à notre réseau sans fil (ici, WPA2-PSK) et nous avons choisi le mot de passe « password » afin de pouvoir se connecter à notre réseau. Ensuite pour vérifier que notre installation fonctionne, il suffit de prendre un équipement doté d'une connexion sans fil : Smartphone et vérifier qu'il à accès au réseau et qu'il obtient bien un adressage dynamique :

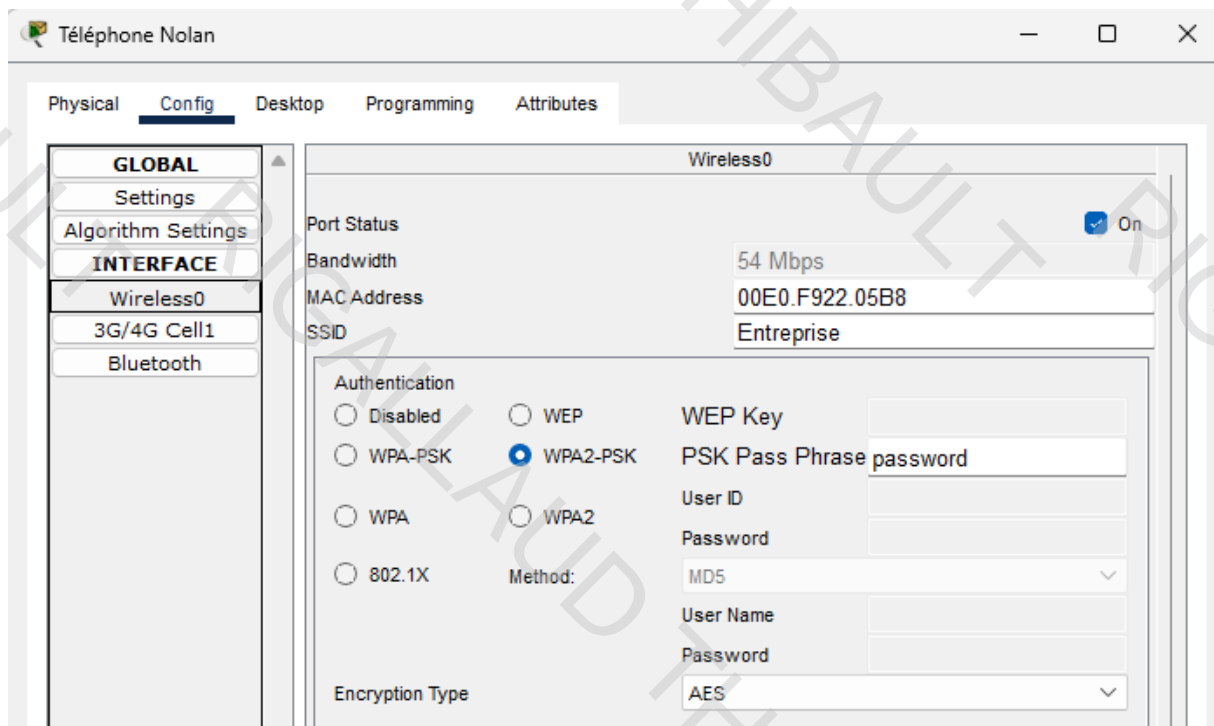


Figure 23 : Accès au WiFi de l'entreprise via Smartphone

Ainsi sur la figure ci-dessus, on observe que le SSID et le mot de passe sont bien renseignés.

Sur la figure suivante, nous observons aussi que le DHCP est fonctionnel car le smartphone à été doter d'une adresse IP de manière dynamique qui figure dans le POOL du DHCP.

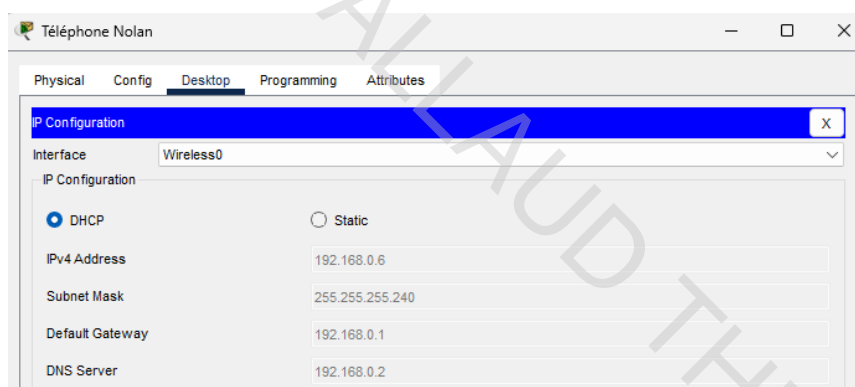


Figure 24 : Adressage Dynamique Smartphone

On en profite pour vérifier la connectivité du téléphone avec un autre équipements du réseau (ici un ordinateur de la salle de recherche).

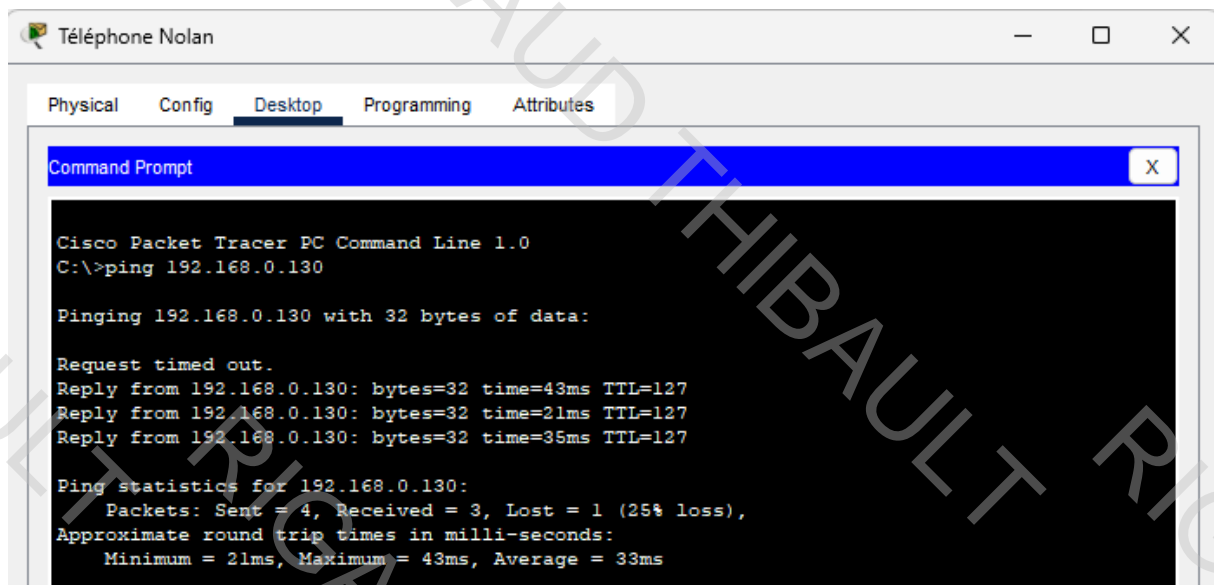


Figure 25 : Connectivité Smartphones vers autre équipement du réseau

Passons maintenant à la configuration du serveur web Intranet de l'entreprise. Dans le cadre de ce travail se limitant à la sphère éducative, j'ai pris la liberté d'appeler mon entreprise NETACAD et donc de baser le site de l'entreprise sur ce nom.

Ainsi, pour configurer le serveur web, nous nous retrouvons une fois de plus sur l'interface graphique des serveurs via Packet Tracer où nous choisissons le service HTTP.

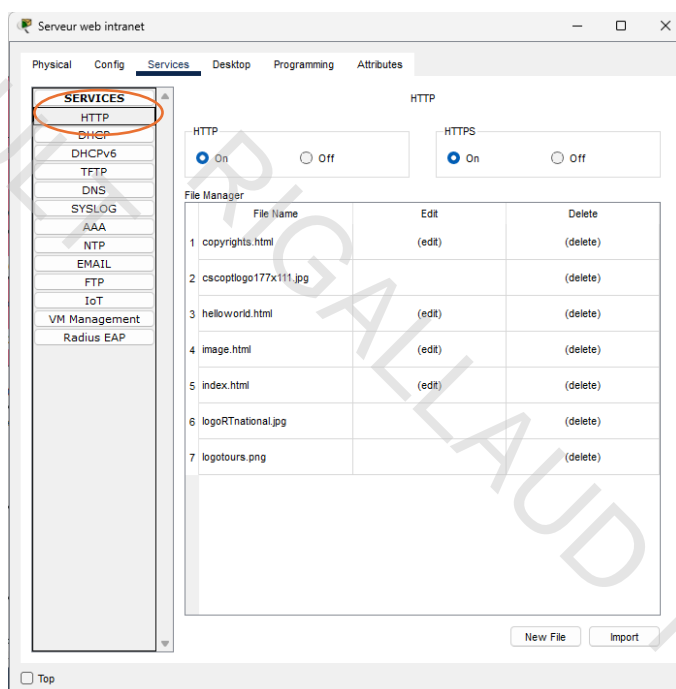


Figure 26 : Interface Graphique Packet Tracer http

Ainsi, une fois sur le bon service, il est important d'activer le service http afin que nous puissions accéder à notre Intranet. Pour la configuration du site, nous avons modifié le fichier par défaut produit par Packet Tracer en appuyant sur le bouton « edit ». Une fois le bouton appuyé, nous avons pu créer notre site en html/css :

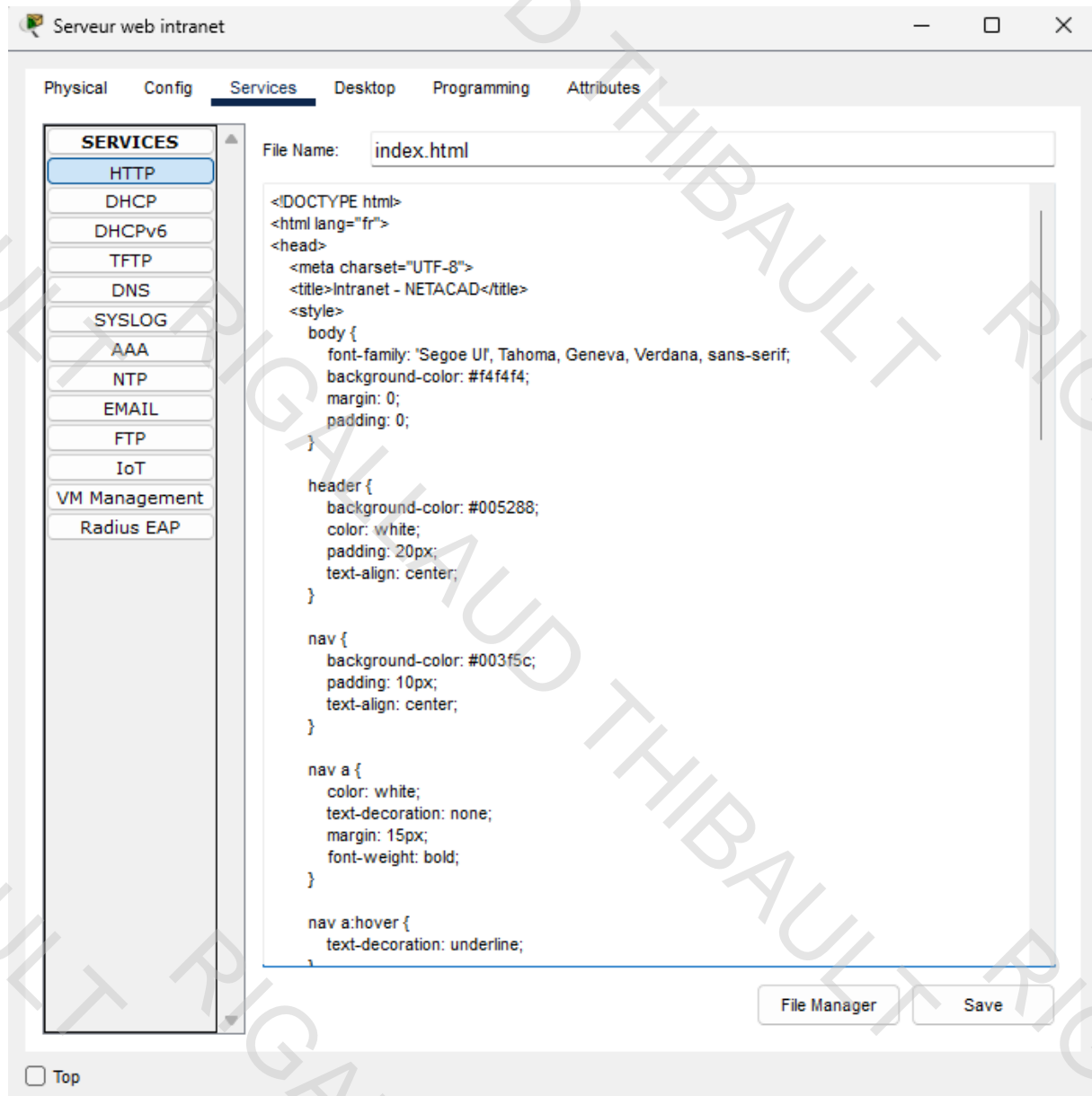


Figure 27 : Extrait css de l'intranet

Ainsi, voici l'intranet que nous avons confectionné pour l'entreprise.



Figure 28 : Intranet Netacad

Enfin, pour conclure avec les serveurs privés de l'entreprise, nous avons mis en place un serveur de mail communiquant uniquement sur le LAN de l'entreprise. Comme pour les autres serveurs nous l'avons configuré via l'interface graphique de Packet Tracer.

Pour ce serveur, il est important de penser à activer le protocole SMTP (expédition/acheminement du mail) ainsi que le protocole POP3 (réception des messages).

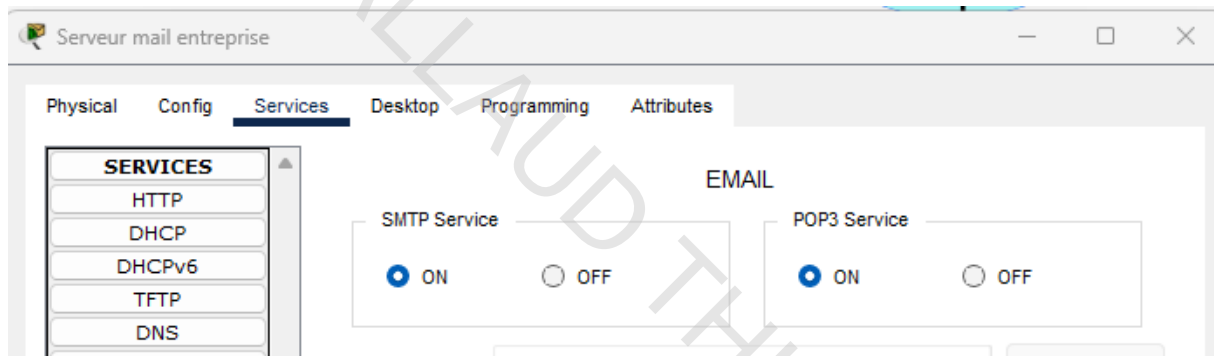


Figure 29 : Vérification que les protocoles de messagerie sont activés

Une fois que les protocoles sont bien activés sur le serveur, nous avons ensuite dû entrer le nom de domaine du serveur mail afin de pouvoir créer une base pour les adresses mail. Nous avons donc choisi netacad.fr. Après ça, nous avons ajoutés des utilisateurs dans le serveur web avec un nom d'utilisateur et un mot de passe.

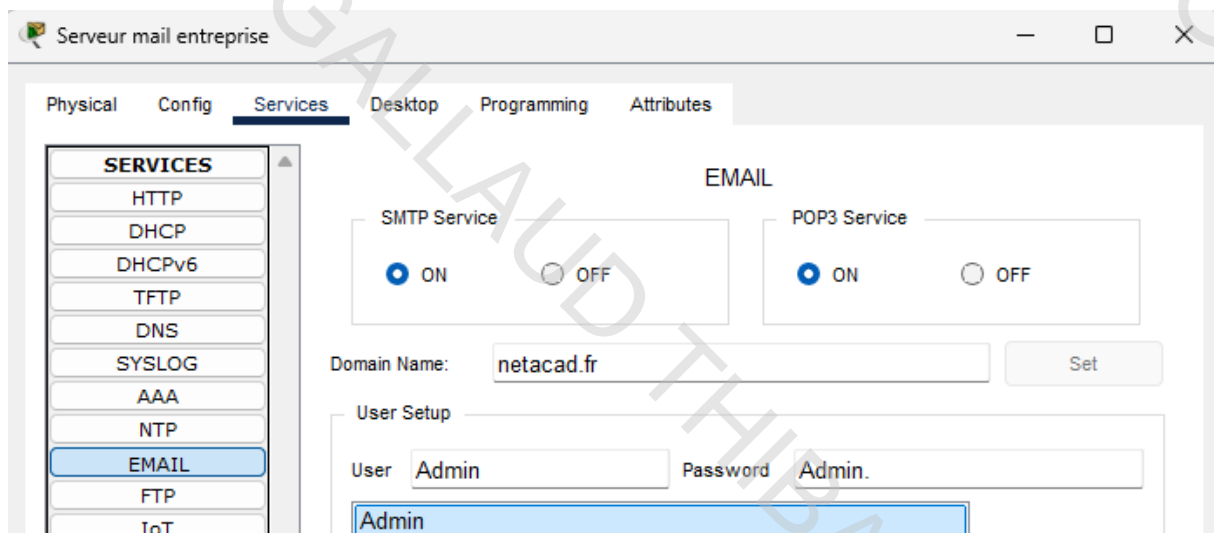


Figure 30 : Compte Admin email

Ainsi on observe ici le compte Admin avec le mot de passe Admin. lui permettant de se connecter à sa messagerie sur sa machine.

Figure 31 : Configuration Mail PC Admin

Voici les informations à rentrer sur un ordinateur pour se connecter à son compte mail. On y retrouve l'adresse mail de l'utilisateur, le serveur d'envoi, le serveur de réception ainsi que son nom d'utilisateur et son mot de passe. Une fois cela renseigné, on se retrouve sur l'interface suivante :

Figure 32 : Messagerie Mail Vide

Via cette interface, nous pouvons recevoir un mail, en écrire et y répondre. Voici un exemple de l'envoi d'un mail.

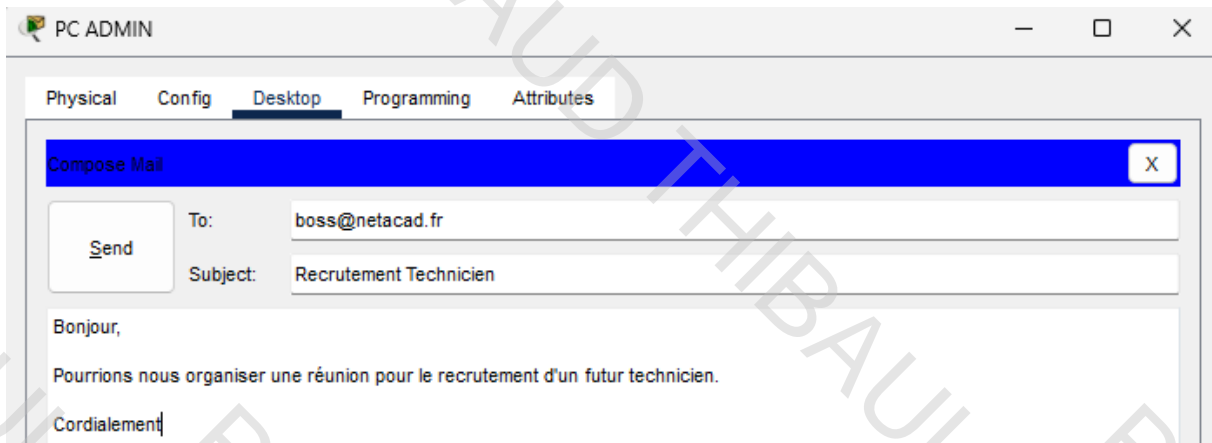


Figure 33 : Envoi de mail

Une fois le mail envoyé, une petite validation se présente en bas de la page :

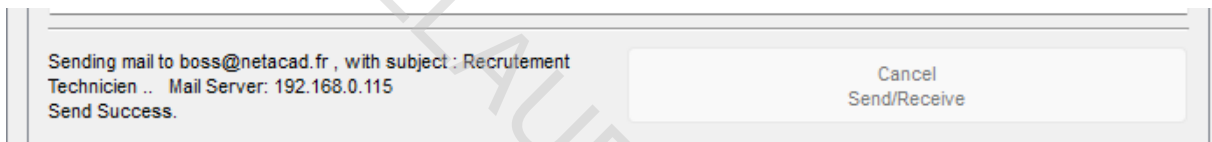


Figure 34 : Confirmation envoi mail

Ensuite, nous nous dirigeons sur l'ordinateur du destinataire dans l'objectif de vérifier la réception du mail.

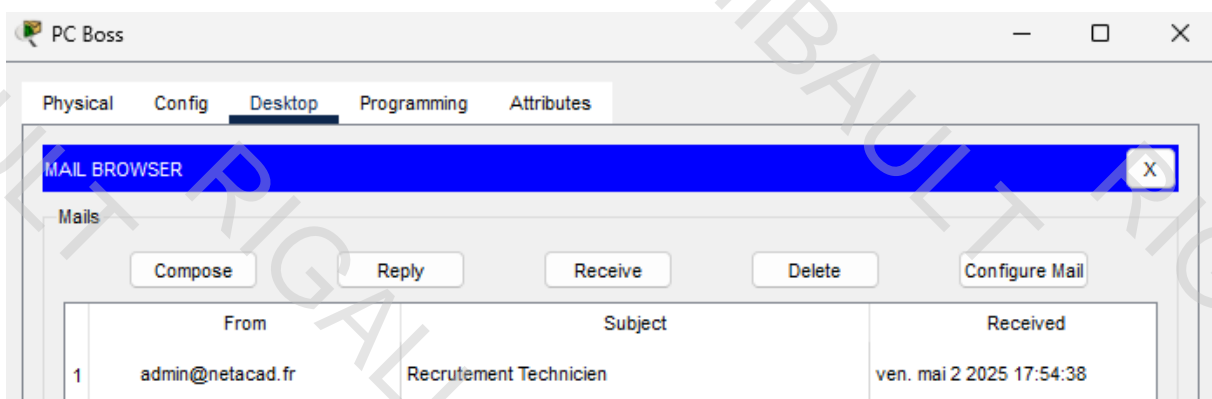


Figure 35 : Réception mail

Voici comment s'affiche la réception d'un mail, on y retrouve l'expéditeur, le sujet et la date de réception. Une fois le mail ouvert, voici les interfaces de lecture proposée par Packet Tracer :

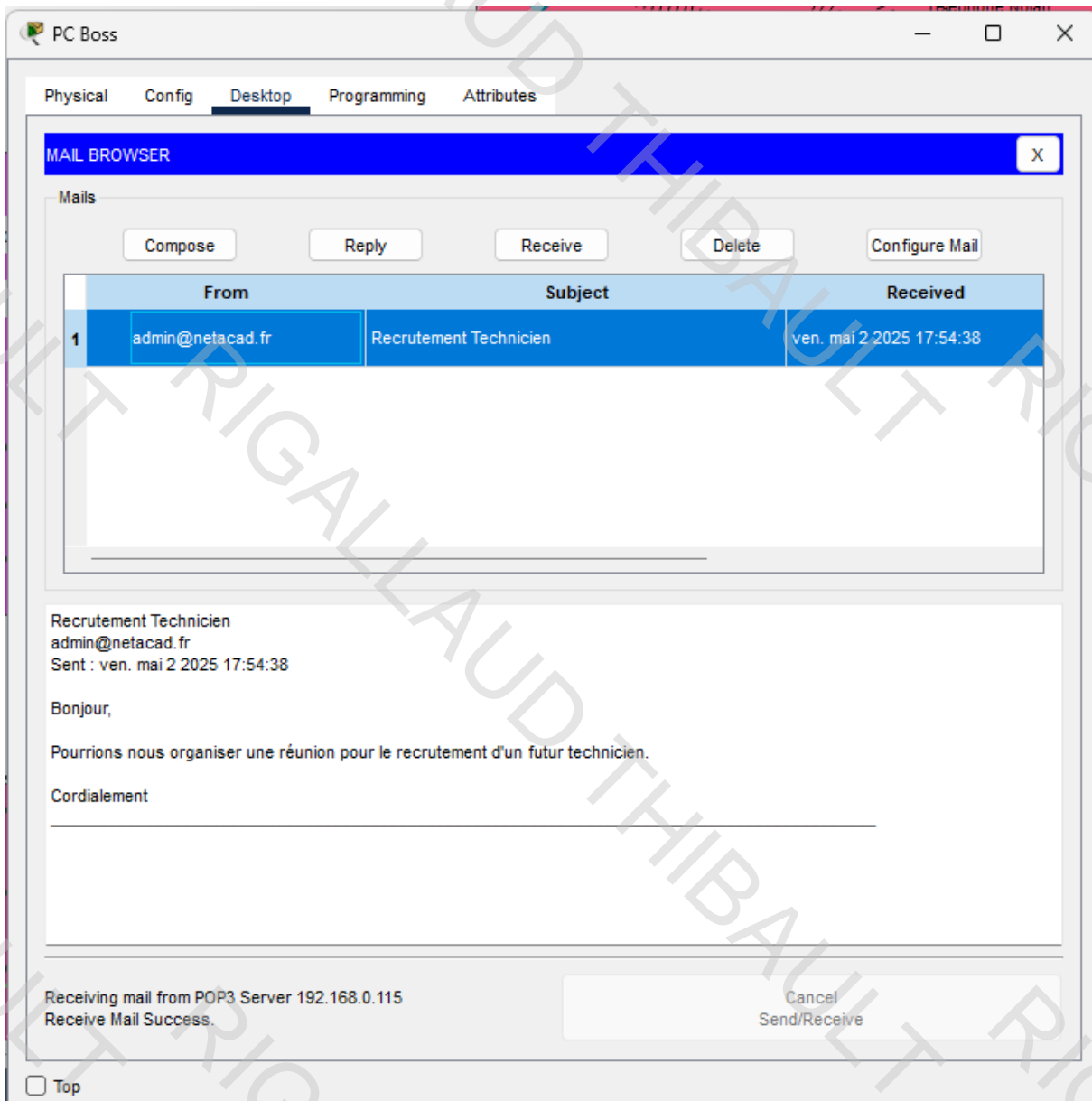


Figure 36 : Affichage au premier clic sur le mail

Lorsque l'on double clique sur le mail, une nouvelle page s'ouvre avec le mail en plus grand et les informations d'expédition affichée d'une autre manière :

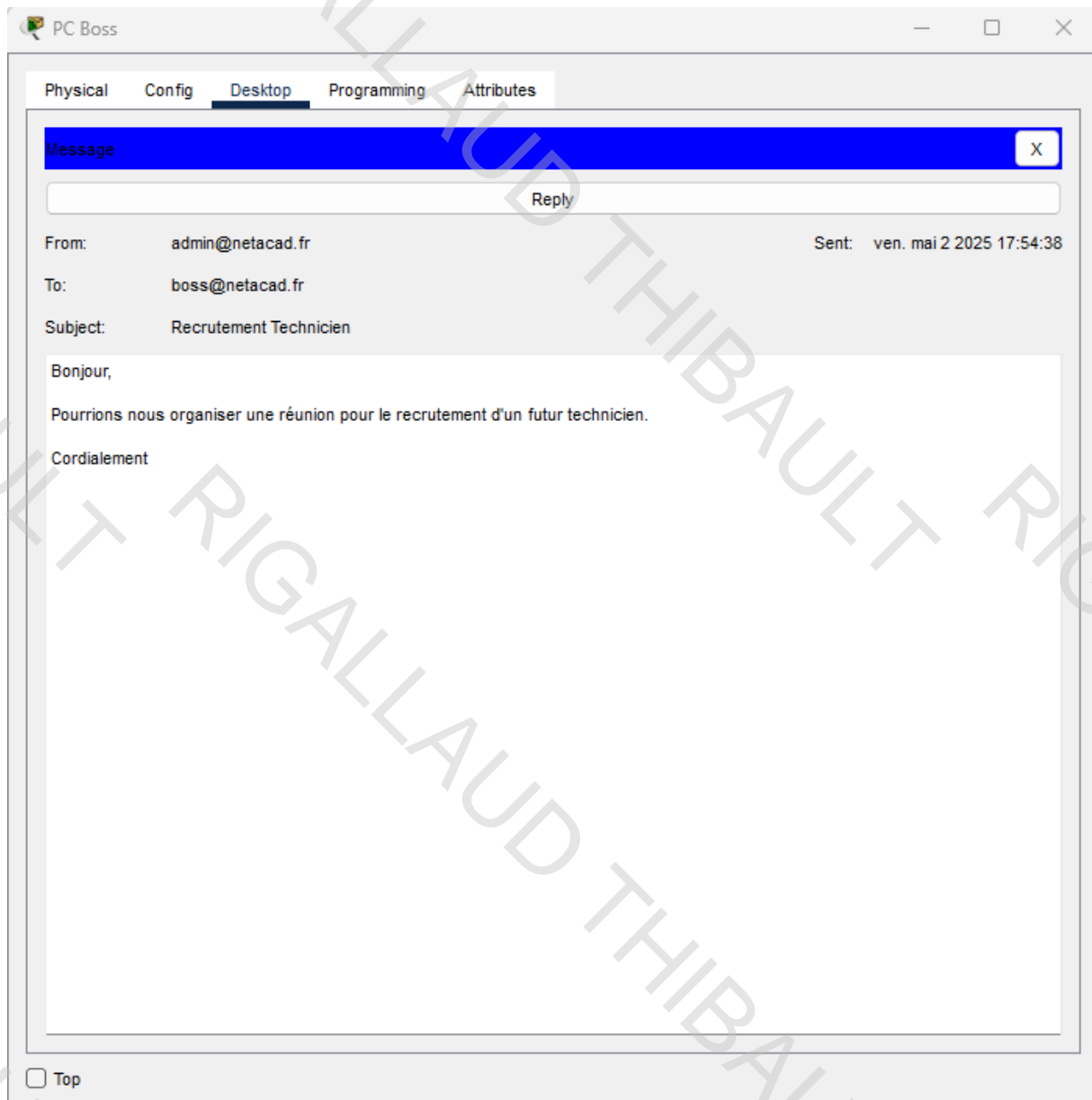


Figure 37 : Interface mail grand

#### D. Configuration de la DMZ

Pour rappel, la DMZ est une partie du réseau informatique qui permet de sécuriser l'accès aux services de l'entreprise. Elle est située entre le réseau local et Internet et est reliée à une autre interface du routeur que le réseau interne de l'entreprise. Son rôle principal est d'accueillir des serveurs accessibles depuis l'extérieur comme un site web ou un serveur DNS public tout en empêchant l'accès au réseau privé de l'entreprise. Ainsi, en cas d'attaque si le réseau de la DMZ est compromis, ce ne sera pas le cas pour le LAN privé de l'entreprise. Dans notre architecture, la DMZ est constitué du DNS public et du serveur WEB public.

Ainsi, pour la configuration de notre DMZ, nous avons attribué une adresse IP à l'interface GigabitEthernet0/1 ainsi qu'un début de configuration pour le nat que nous verrons ensuite.

```
interface GigabitEthernet0/1
 ip address 10.0.0.1 255.255.255.240
 ip nat inside
 duplex auto
 speed auto
```

Figure 38 : Interface DMZ

Afin de mieux se repérer dans le réseau, nous avons décidé de choisir un adressage différent pour la DMZ. Dans cette idée, nous sommes partis pour un adressage en 10.0.0.0/28 avec l'adresse du routeur en 10.0.0.1/28, le serveur DNS en 10.0.0.2/28 et le serveur web en 10.0.0.3/28

Pour le serveur DNS, nous avons suivi les mêmes étapes que pour celui privé en y rajoutant les données du FAI :

The screenshot shows the 'DNS PUBLIC' configuration window. The 'Services' tab is active, and the 'DNS' service is turned 'On'. Below this, there is a section for 'Resource Records' with a table listing several records. The table has columns for 'No.', 'Name', 'Type', and 'Detail'.

No.	Name	Type	Detail
0	dns.fr	A Record	150.0.0.3
1	dns.netacad.fr	A Record	100.0.0.1
2	fr	NS	dns.fr
3	netacad.fr	SOA	ServerName: dns.neta... MailBox: admin@netacad.fr Expiry: 10 Refresh: 10 Retry: 10 MinTTL: 10
4	netacad.fr	NS	dns.netacad.fr
5	www.netacad.fr	A Record	100.0.0.1

At the bottom of the window, there is a 'DNS Cache' button and a 'Top' link.

Figure 39 : DNS PUBLIC

Pour le serveur web, nous avons aussi utilisé la même technique pour le créer. Ainsi, voici le site web public de l'entreprise :

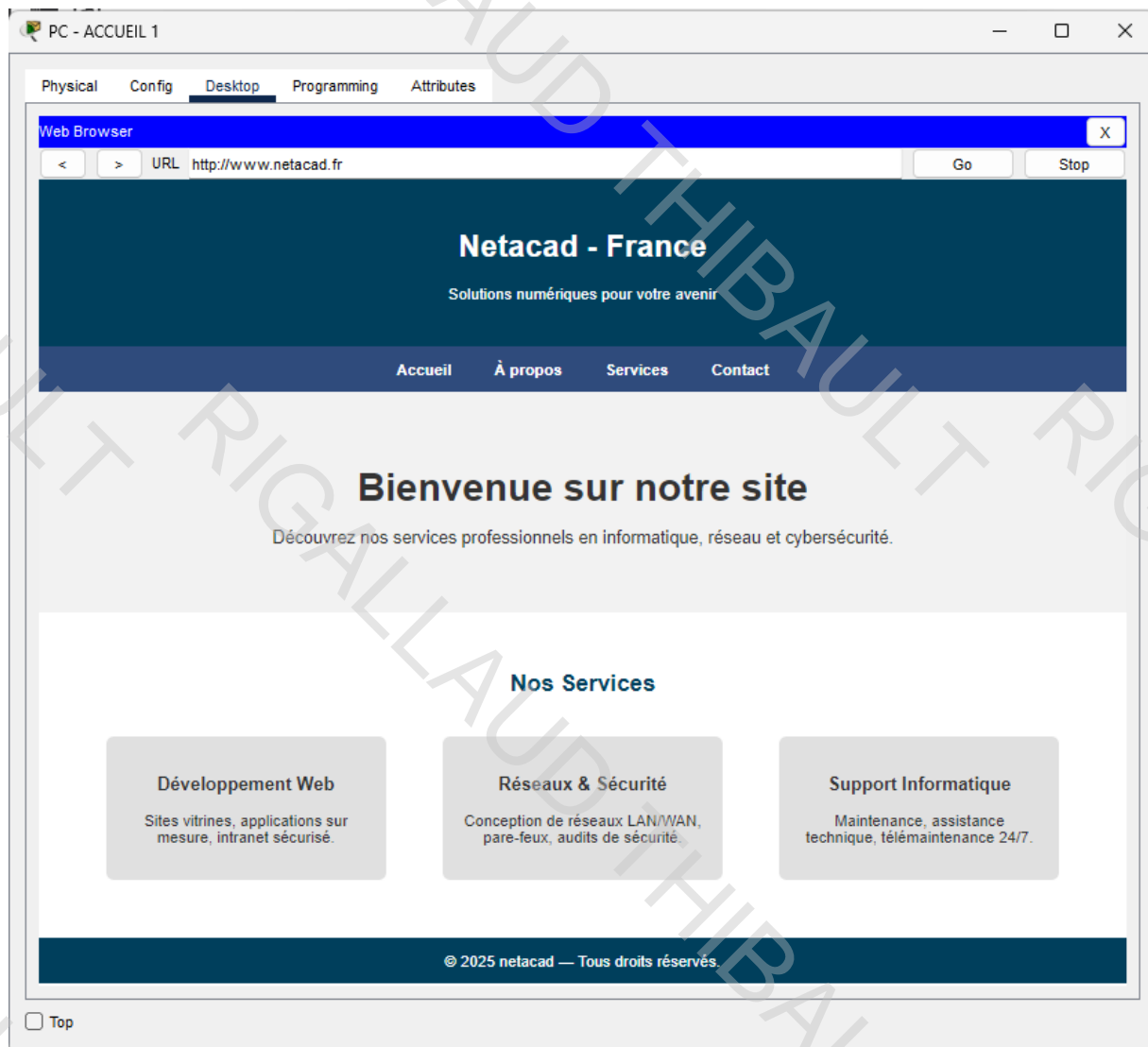


Figure 40 : Site Internet Entreprise

### III. Partie FAI

#### A. Adressage et configuration du routeur

Pour la partie FAI, nous sommes donc partis sur un adressage public en 100.0.0.0/8 entre le routeur FAI et le routeur entreprise ainsi qu'un adressage en 150.0.0.0/16 pour le réseau du FAI. Ainsi, nous avons configuré l'interface GigabitEthernet0/3/0 (fibre vers l'entreprise) avec 100.0.0.254 255.0.0.0 en adresse IP et l'interface GigabitEthernet0/0 avec 150.0.0.1 255.255.0.0 pour le côté FAI.

```
interface GigabitEthernet0/0
 ip address 150.0.0.1 255.255.0.0
 duplex auto
 speed auto
```

Figure 42 : Interface FAI --> Entreprise

```
interface GigabitEthernet0/3/0
 ip address 100.0.0.254 255.0.0.0
```

Figure 41 : Interface FAI

Contrairement aux switchs du LAN entreprise, nous n'avons pas besoin de faire de configuration particulière car nous n'utilisons pas de VLANs pour ce réseau.

## B. Configuration des serveurs du FAI

Ainsi, concentrons-nous sur la configuration des deux serveurs du FAI : Serveur Web et Serveur DNS

Voici le site web du FAI que nous avons mis en place :



Figure 43 : Site web FAI

Pour le serveur DNS, voici sa configuration :

Server DNS FAI

Physical Config **Services** Desktop Programming Attributes

**SERVICES**

- HTTP
- DHCP
- DHCPv6
- TFTP
- DNS**
- SYSLOG
- AAA
- NTP
- EMAIL
- FTP
- IoT
- VM Management
- Radius EAP

**DNS**

DNS Service ☒ On ☐ Off

Resource Records

Name  Type **A Record** ▼

Address

No.	Name	Type	Detail
0	dns.fr	A Record	150.0.0.3
1	dns.netacad.fr	A Record	10.0.0.2
2	fr	SOA	ServerName: dns.fr MailBox : admin@dns.fr Expiry : 10 Refresh : 10 Retry : 10 MinTTL : 10
3	fr	NS	dns.fr
4	netacad.fr	NS	dns.netacad.fr
5	www.bouygues.fr	A Record	150.0.0.2

☐ Top

Figure 44 : DNS FAI

Ainsi, le serveur DNS ci-dessus comporte de la résolution de nom (NS) avec fr pour le dns.fr et netacad.fr pour le dns.netacad.fr. On y retrouve aussi des enregistrement A pour ces 2 DNS ainsi que pour accéder au site web du FAI au nom [www.bouygues.fr](http://www.bouygues.fr) à l'adresse 150.0.0.2.

## IV. Configuration des équipements pour la communication inter-réseau

Jusqu'ici, nous avons configuré, les services basiques pour le LAN, la DMZ et le FAI. En effet, pour le LAN nous avons configuré les services de mail, intranet, dhcp, dns ainsi que le VLSM et les VLANs. Cela permet au LAN de fonctionner. Cependant, en laissant la configuration telle quelle, il est impossible de communiquer avec l'extérieur à partir du réseau privé de l'entreprise. En effet, les adresses de notre réseau étant privées ne sont pas routable et ne peuvent donc pas accéder au réseau du FAI et inversement. C'est dans cette idée que nous mettons en place du NAT ainsi que du PAT.

### A. NAT/PAT

Pour rappel le NAT et le PAT sont des fonctions permettant à un réseau privé d'utiliser des adresses IP non routables tout en accédant à Internet. Le NAT traduit une adresse IP privée en une adresse publique, masquant ainsi l'adresse interne des appareils du LAN. Par exemple, le poste du BOSS configuré avec l'adresse IP 192.168.0.82 peut communiquer avec le FAI via l'IP publique de l'entreprise 100.0.0.1. Le PAT quant à lui, étend cette fonctionnalité en permettant à plusieurs appareils du réseau privé de partager une seule adresse publique grâce à l'utilisation de ports distincts. Par exemple, les machines du secrétariat (192.168.0.18 et 192.168.0.19) peuvent accéder simultanément à Internet via la même IP publique (100.0.0.1), mais avec des ports différents (100.0.0.1:5001 et 100.0.0.1:5002). De plus le PAT permet aussi d'accéder à des services de l'entreprise dans la DMZ de l'extérieur en redirigeant l'adresse privée et son port à l'adresse public du réseau et le port adapté au service. Ces technologies assurent non seulement la connectivité vers l'extérieur, mais aussi une meilleure gestion des adresses IP publiques et une couche supplémentaire de sécurité en masquant les adresses internes du réseau.

Ainsi nous allons voir la mise en place de NAT puis du PAT.

Comme dis précédemment, nous devons faire de la traduction d'adresse sur le routeur entreprise afin de pouvoir communiquer avec l'extérieur. Pour cela, la première étape est de définir les interfaces d'entrées et de sortie du NAT via les commandes ip nat inside ou outside.

```
interface GigabitEthernet0/0
no ip address
ip nat inside
duplex auto
speed auto
```

Figure 45 : Interface inside côté LAN entreprise

Sur cette figure, la commande `ip nat inside` agit sur toutes les sous interfaces se trouvant sur l'interface `GigabitEthernet0/0`. Cela représente donc un nat sur l'ensemble du réseau privé de l'entreprise.

```
interface GigabitEthernet0/1
ip address 10.0.0.1 255.255.255.240
ip nat inside
duplex auto
speed auto
```

Figure 46 : Interface inside côté DMZ

```
interface GigabitEthernet0/3/0
ip address 100.0.0.1 255.0.0.0
ip nat outside
```

Figure 47 : Interface outside côté Entreprise --> FAI

Toujours dans l'optique de communiquer avec l'extérieur, nous rajoutons un ACL afin de d'autoriser toutes les adresses comprises entre 192.168.0.1 et 192.168.0.254 à communiquer.

```
access-list 99 permit 192.168.0.0 0.0.0.255
```

Figure 48 : ACL pour le LAN

Enfin, la commande ci-dessous permet d'utiliser l'ACL, de prendre l'interface `GigabitEthernet0/1` comme adresse publique pour toutes les traductions et le mot `overload` permet de faire du PAT afin que plusieurs machines puissent communiquer avec l'extérieur en même temps.

À la suite de ça, nous rajoutons d'autres commandes cisco afin de produire de la redirection de port, plus précisément la redirection du trafic arrivant sur notre IP public au port 80 vers notre IP privé de site internet de l'entreprise. Nous faisons la même chose mais pour le DNS et cette fois ci sur le port TCP et UDP car le port UDP est le port par défaut pour le DNS mais le port TCP est parfois utilisé pour le transfert de zone DNS.

```
ip nat inside source static tcp 10.0.0.3 80 100.0.0.1 80
ip nat inside source static tcp 10.0.0.2 53 100.0.0.1 53
ip nat inside source static udp 10.0.0.2 53 100.0.0.1 53
```

Figure 49 : PAT Routeur Entreprise

## B. ROUTES

Une fois que le NAT et le PAT sont configurés, nous nous rendons compte que la communication vers l'extérieur n'est toujours pas possible. Cela se justifie par le manque de route statique et de route par défaut en absence de protocole de routage comme l'OSPF. Ainsi, sur le routeur entreprise, nous mettons en place les routes suivantes :

```
ip route 150.0.0.0 255.255.0.0 100.0.0.254
ip route 0.0.0.0 0.0.0.0 100.0.0.254
```

Figure 50 : Routeur Entreprise route statique

Ainsi, le réseau est configuré avec deux routes principales. La première est une route statique qui dirige le trafic vers le réseau du FAI en spécifiant la passerelle à utiliser pour atteindre ce réseau. La seconde correspond à la route par défaut du routeur : si ce dernier ne connaît pas la localisation du réseau de destination, il redirige les données vers l'adresse IP définie dans cette route par défaut. Dans cette configuration, on remarque que la passerelle est identique pour la route statique et la route par défaut. Cette similitude s'explique par le fait que le réseau ne dispose que d'une seule liaison vers l'extérieur centralisant ainsi tout le trafic externe via cette unique passerelle.

## V. Sécurité et Vérifications

### A. SSH et ACL de contrôle de flux

Voyons maintenant comment se fait la configuration des équipements d'interconnexion pour les sécuriser et les rendre accessibles du PC administrateur de l'entreprise en SSH

```
Switch(config)#vlan 99
Switch(config-vlan)#name Admin
Switch(config-vlan)#exit
Switch(config)#int
Switch(config)#interface vlan99
Switch(config-if)#
%LINK-5-CHANGED: Interface Vlan99, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan99, changed state to up

Switch(config-if)#ip adre
Switch(config-if)#ip add
Switch(config-if)#ip address 192.168.99.4 255.255.255.0
Switch(config-if)#no sh
Switch(config-if)#no shutdown
Switch(config-if)#end
Switch#
%SYS-5-CONFIG_I: Configured from console by console
```

Figure 51: VLAN 99 ADMIN

Comme illustré sur la Figure 51: VLAN 99 ADMIN, nous avons créé un nouveau VLAN nommé Admin qui a pour objectif principal d'isoler et de sécuriser la gestion des équipements réseau. En attribuant une interface VLAN avec l'adresse 192.168.99.4/24, nous permettons au PC administrateur d'accéder aux switches et routeur via SSH de manière sécurisée. Cette séparation renforce la sécurité en limitant les risques d'accès non autorisés tout en simplifiant la maintenance puisque les configurations peuvent être effectuées à distance de façon centralisée.

```
interface GigabitEthernet0/0.99
 encapsulation dot1Q 99
 ip address 192.168.99.1 255.255.255.0
```

Figure 52 : sous-interface VLAN99

Comme pour les autres VLAN, nous avons aussi rajouté une sous-interface sur le routeur pour le VLAN99 avec l'encapsulation DOT1Q et une adresse IP.

Une fois la création du VLAN, ainsi que l'adressage de chaque switchs sur le VLAN terminés, nous sommes passés à la sécurisation des équipements :

```
Switch(config)#hostname SW-SSH-ACCUEIL-SERVEUR
SW-SSH-ACCUEIL-SERVEUR(config)#ip domain-name netacad.fr
SW-SSH-ACCUEIL-SERVEUR(config)#crypto key generate rsa
The name for the keys will be: SW-SSH-ACCUEIL-SERVEUR.netacad.fr
Choose the size of the key modulus in the range of 360 to 4096 for your
General Purpose Keys. Choosing a key modulus greater than 512 may take
a few minutes.

How many bits in the modulus [512]: 128
% A decimal number between 360 and 4096
How many bits in the modulus [512]: 4096
% Generating 4096 bit RSA keys, keys will be non-exportable...[OK]

SW-SSH-ACCUEIL-SERVEUR(config)#ip ssh version 2
*Mar 1 1:14:15.465: %SSH-5-ENABLED: SSH 1.99 has been enabled
SW-SSH-ACCUEIL-SERVEUR(config)#username admin privilege 15 secret Admin.
SW-SSH-ACCUEIL-SERVEUR(config)#line vty 0 4
SW-SSH-ACCUEIL-SERVEUR(config-line)#trn
SW-SSH-ACCUEIL-SERVEUR(config-line)#tra
SW-SSH-ACCUEIL-SERVEUR(config-line)#transport input ssh
SW-SSH-ACCUEIL-SERVEUR(config-line)#login local
SW-SSH-ACCUEIL-SERVEUR(config-line)#acc
SW-SSH-ACCUEIL-SERVEUR(config-line)#access-class 10 in
SW-SSH-ACCUEIL-SERVEUR(config-line)#exit
SW-SSH-ACCUEIL-SERVEUR(config)#acc
SW-SSH-ACCUEIL-SERVEUR(config)#access-list 1i
SW-SSH-ACCUEIL-SERVEUR(config)#access-list 1is
SW-SSH-ACCUEIL-SERVEUR(config)#access-list 10 per
SW-SSH-ACCUEIL-SERVEUR(config)#access-list 10 permit 192.168.99.0 0.0.0.255
SW-SSH-ACCUEIL-SERVEUR(config)#end
```

Figure 53 : Configuration SSH

Ainsi selon la Figure 53 : Configuration SSH, nous avons réalisé en plusieurs étapes la configuration du SSH pour garantir un accès sécurisé. D'abord, nous avons renommé le switch en "SW-SSH-ACCUEIL-SERVEUR" et nous l'avons associé au domaine "netacad.fr". Ensuite nous avons généré des clés RSA aléatoires de 4096 bits pour sécuriser les échanges. Puis nous avons activé la version 2 du protocole SSH pour renforcer la sécurité. Après ça nous avons créé un compte administrateur avec des

privileges maximum protégé par un mot de passe chiffré. Nous avons aussi configuré l'accès distant pour n'accepter que les connexions SSH via les lignes VTY avec authentification locale. Enfin une ACL a été mise en place pour restreindre les connexions SSH au seul réseau administratif 192.168.99.0/24 assurant ainsi que seuls les utilisateurs autorisés puissent accéder au switch de manière sécurisée.

Voici un exemple d'accès au routeur de l'entreprise en SSH via le CLI d'un ordinateur :

```
C:\>ssh -l admin 192.168.99.1

Password:

ROUTEUR-NETACAD#sh r
Building configuration...

Current configuration : 2236 bytes
!
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname ROUTEUR-NETACAD
!
!
!
!
!
!
!
no ip cef
no ipv6 cef
!
!
--More-- |
```

Figure 54 : SSH via CLI

Et voici comment accéder au SSH via l'interface graphique offerte par Packet Tracer :

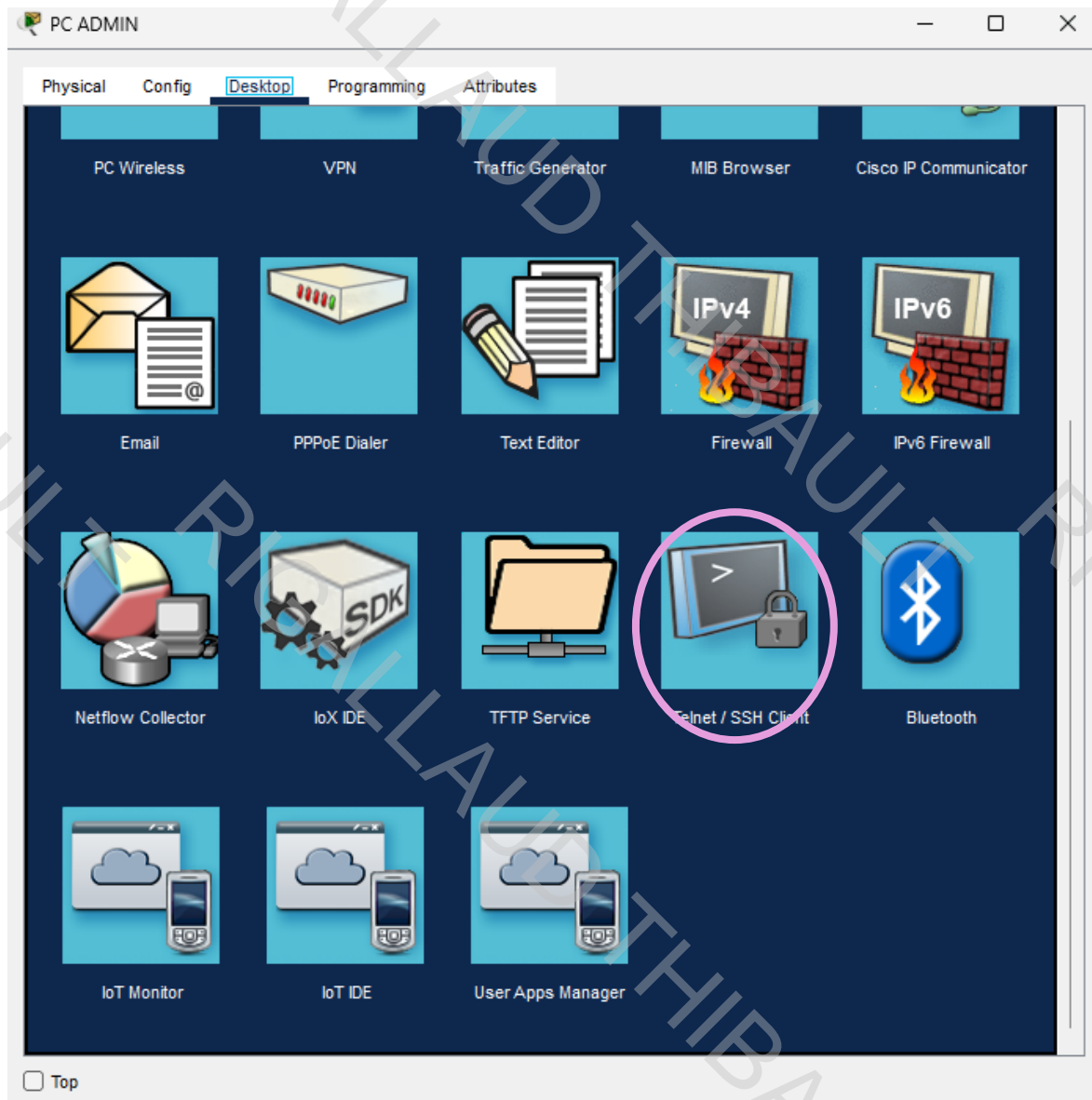


Figure 55 : SSH Graphique

On se retrouve donc sur l'ordinateur Admin de l'entreprise, on clique sur « Desktop » et on retrouve ainsi l'espace dédié à Telnet/SSH en cliquant dessus.

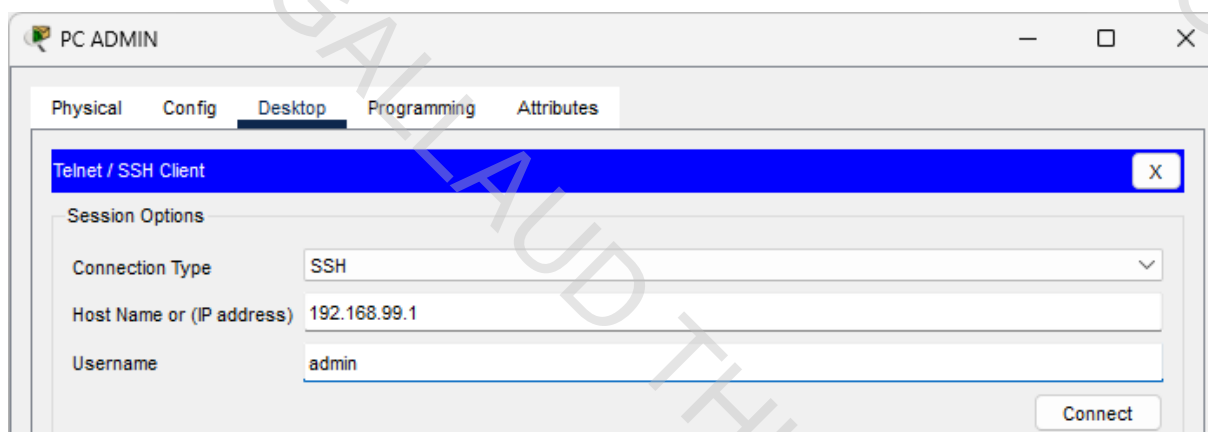


Figure 56 : Connexion SSH interface graphique

Ainsi, cisco nous permet de rentrer le type de connexion, l'adresse IP de la machine et le nom d'utilisateur voulu pour se connecter. Une fois que les bonnes données sont entrées on se retrouve avec cette interface :

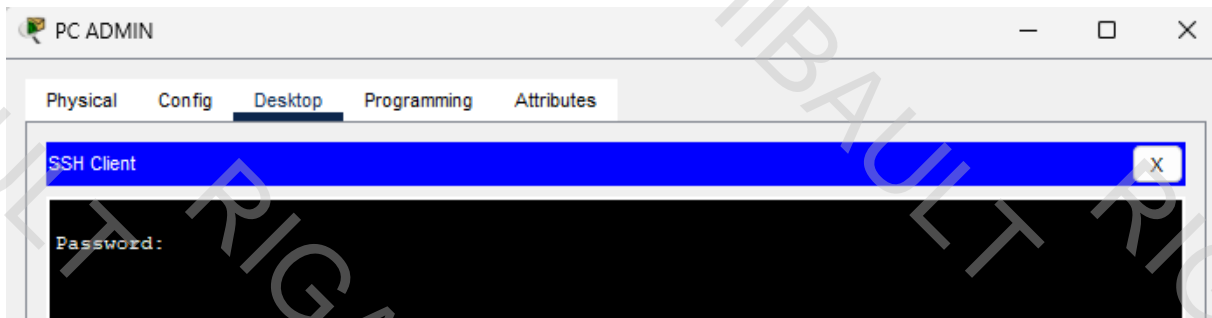


Figure 57 : Connexion SSH graphique

On y rentre donc le mot de passe de la session afin de se connecter à l'équipement :



Figure 58 : SSH connecté

Une fois le mot de passe entré nous sommes bien connecté via une liaison SSH au routeur de l'entreprise.

Maintenant, voyons les ACL de contrôle de flux que nous avons mis en place :

```
access-list 101 permit tcp any host 10.0.0.3 eq www
access-list 101 permit tcp any host 10.0.0.3 eq 443
access-list 101 permit udp any host 10.0.0.2 eq domain
access-list 101 deny ip any 10.0.0.0 0.0.0.255
access-list 101 permit ip any any
```

Figure 59 : ACL de contrôle

L'ACL 101 que nous avons configuré à pour but de filtrer le trafic réseau de manière précise. Elle autorise d'abord les connexions TCP vers le serveur web (10.0.0.3) sur les ports HTTP (80) et HTTPS (443) permettant ainsi l'accès aux services web. Les requêtes DNS utilisant le protocole UDP vers le serveur 10.0.0.2 sur le port 53 (domain) sont également permises. Ensuite, l'ACL bloque explicitement tout autre trafic IP à destination du sous-réseau 10.0.0.0/24. Enfin une dernière règle autorise tout autre trafic non précédemment filtré assurant ainsi que seules les communications spécifiées sont contrôlées tandis que le reste du trafic peut circuler normalement.

## B. Vérifications

Ainsi, maintenant que nous avons configuré tout notre réseau nous allons vérifier que les PC entreprises peuvent accéder au site web FAI et que le FAI à accès au site web de l'entreprise.

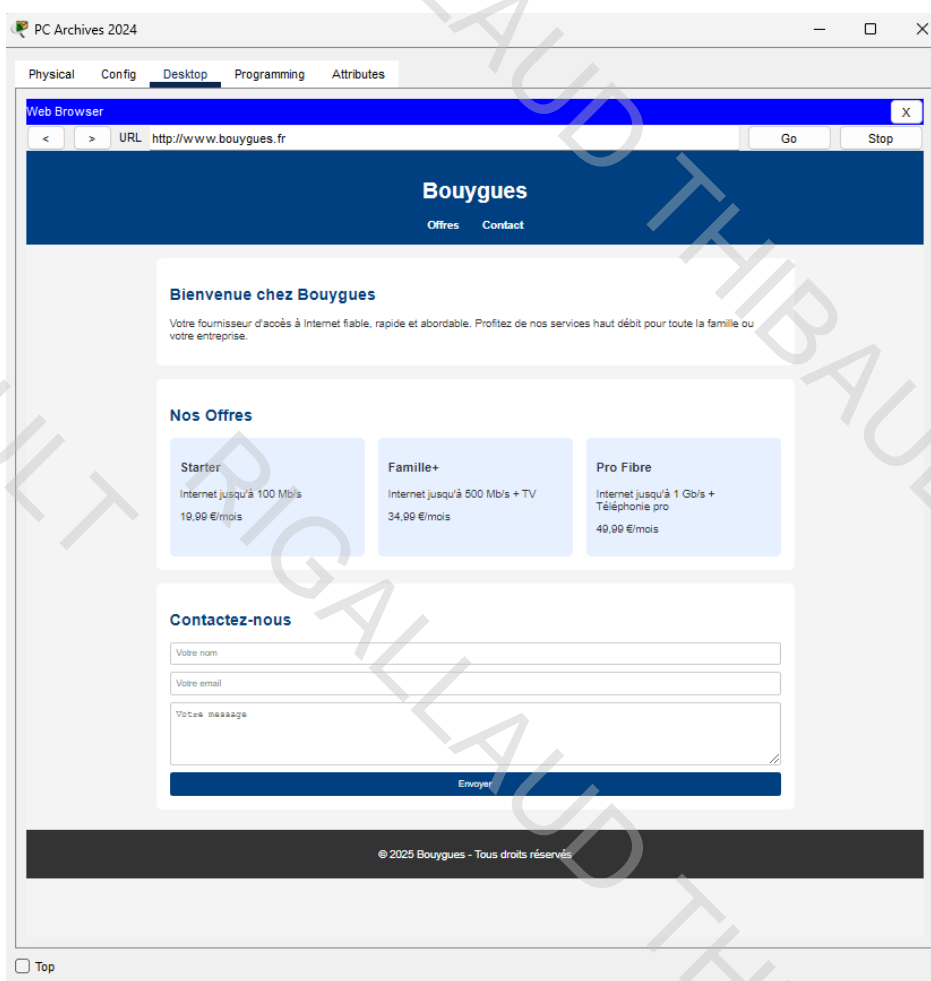


Figure 60 : Accès au site du FAI via un ordinateur de l'entreprise

On observe sur la Figure 60 : Accès au site du FAI via un ordinateur de l'entreprise qu'en prenant un PC au hasard il a bien accès au site du FAI.

Maintenant regardons si le PC se trouvant côté FAI a bien accès au site internet de l'entreprise :

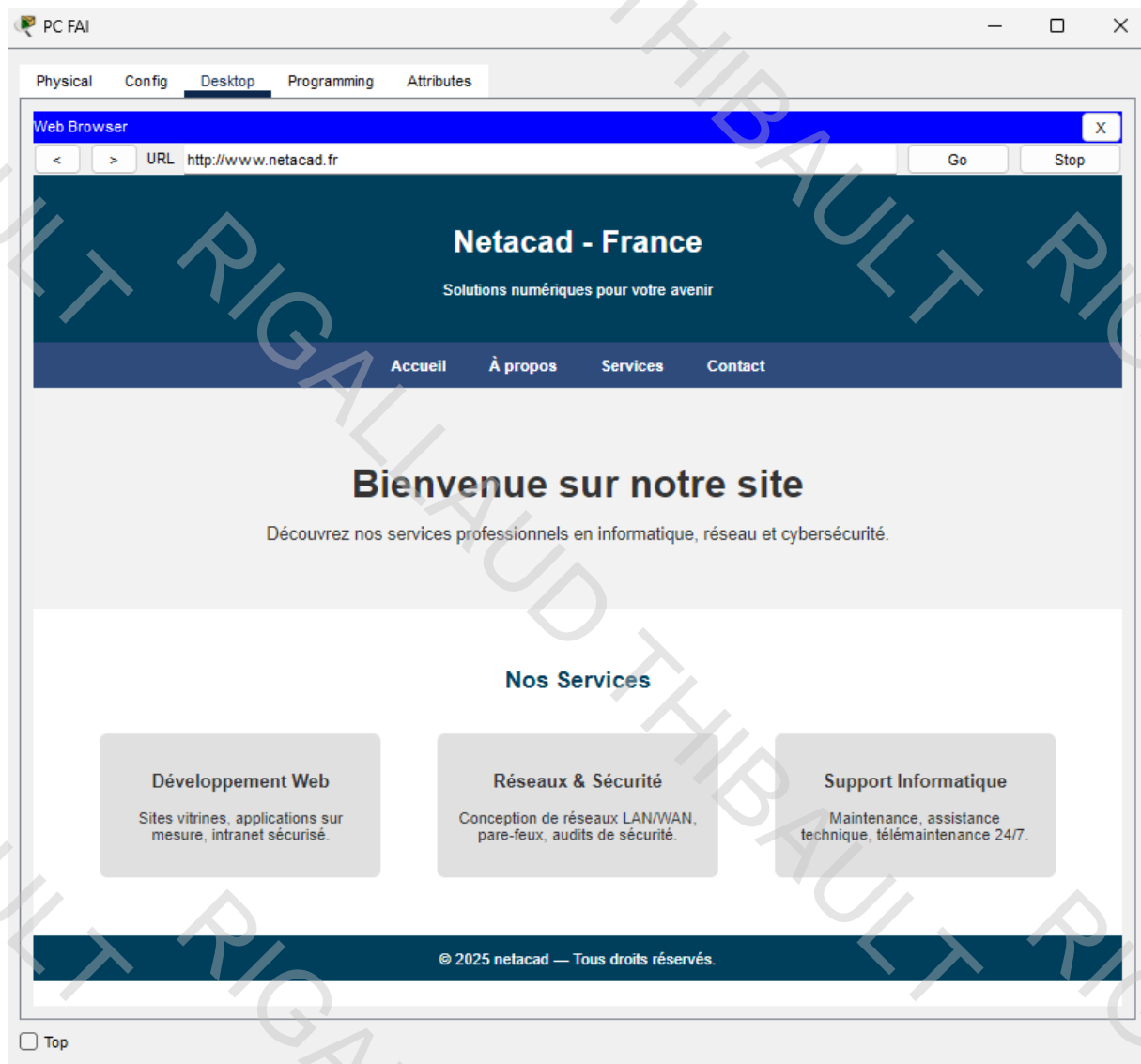


Figure 61 : Accès au site internet entreprise depuis le PC côté FAI

## VI. Conclusion

En tenant compte des contraintes et des exigences, nous avons mis en place une infrastructure réseau redondante avec des switches, assurant une résilience contre les pannes potentielles. Les serveurs dédiés pour le web, mail, DNS, et DHCP, ont été configurés pour garantir une gestion efficace des ressources réseau et des services de l'entreprise. L'intégration avec le réseau public via le FAI permet à la fois un accès externe contrôlé aux ressources de l'entreprise et une navigation sécurisée pour les utilisateurs internes. Le cloisonnement des accès notamment avec le site intranet accessible uniquement depuis le réseau interne protège les informations sensibles de l'entreprise. Chaque équipement d'interconnexion a été sécurisé et est accessible uniquement depuis le PC administrateur via SSH assurant une gestion centralisée et sécurisée des configurations. Le plan d'adressage IPv4 et les VLANs ont été soigneusement planifiés pour segmenter le réseau en sous-réseaux fonctionnels facilitant la gestion du trafic et améliorant la sécurité. En conclusion, ce projet illustre notre capacité à concevoir et configurer un réseau informatique complexe pour une petite entreprise en combinant redondance, sécurité, et efficacité opérationnelle. Les compétences acquises au cours du semestre 1 et 2 ont été appliquées pour créer une infrastructure réseau robuste capable de soutenir les activités actuelles et futures de l'entreprise.

Figure 1 : Réseau de l'entreprise .....	4
Figure 2 : Routeur Entreprise .....	5
Figure 3 : Fenêtre physique routeur .....	6
Figure 4 : Module HWIC .....	6
Figure 5 : Module GLC-LH-SMD .....	7
Figure 6 : Routeur Vide face arrière .....	7
Figure 7 : Routeur Face arrière avec module HWIC .....	7
Figure 8 : Routeur Face arrière prêt à être connecté en fibre sur le port GigabitEthernet0/3/0 .....	7
Figure 9 : Serveur sur Cisco .....	8
Figure 10 : Interface Graphique serveur sur Packet Tracer .....	8
Figure 11 : Redondance des SW .....	9
Figure 12 : Tous les VLANs du réseau .....	10
Figure 13 : Création du VLAN20 dans le switch racine .....	10
Figure 14 : Attribution de certains ports du switch pour le VLAN 20 .....	10
Figure 15 : Interface switch mode trunk .....	11
Figure 16 : Configuration d'une sous interface sur le routeur .....	11
Figure 17 : VLAN 50 .....	12
Figure 18 : VLAN 30 .....	13

Figure 19 : VLAN 80, serveurs .....	14
Figure 20 : DNS privé de l'entreprise.....	15
Figure 21 : Serveur DHCP Entreprise .....	16
Figure 22 : Configuration réseau sans fil accueil .....	17
Figure 23 : Accès au WiFi de l'entreprise via Smartphone.....	18
Figure 24 : Adressage Dynamique Smartphone .....	18
Figure 25 : Connectivité Smartphones vers autre équipement du réseau .....	19
Figure 26 : Interface Graphique Packet Tracer http .....	19
Figure 27 : Extrait css de l'intranet .....	20
Figure 28 : Intranet Netacad .....	21
Figure 29 : Vérification que les protocoles de messagerie sont activés .....	22
Figure 30 : Compte Admin email .....	22
Figure 31 : Configuration Mail PC Admin.....	23
Figure 32 : Messagerie Mail Vide .....	23
Figure 33 : Envoi de mail.....	24
Figure 34 : Confirmation envoi mail.....	24
Figure 35 : Réception mail.....	24
Figure 36 : Affichage au premier clic sur le mail.....	25
Figure 37 : Interface mail grand.....	26
Figure 38 : Interface DMZ .....	27
Figure 39 : DNS PUBLIC .....	27
Figure 40 : Site Internet Entreprise .....	28
Figure 41 : Interface FAI.....	29
Figure 42 : Interface FAI --> Entreprise .....	29
Figure 43 : Site web FAI .....	29
Figure 44 : DNS FAI .....	30
Figure 45 : Interface inside côté LAN entreprise .....	32
Figure 46 : Interface inside côté DMZ .....	32
Figure 47 : Interface outside côté Entreprise --> FAI.....	32
Figure 48 : ACL pour le LAN .....	32
Figure 49 : PAT Routeur Entreprise .....	32
Figure 50 : Routeur Entreprise route statique .....	33
Figure 51 : VLAN 99 ADMIN .....	33
Figure 52 : sous-interface VLAN99 .....	34
Figure 53 : Configuration SSH .....	34
Figure 54 : SSH via CLI .....	35
Figure 55 : SSH Graphique.....	36
Figure 56 : Connexion SSH interface graphique.....	36
Figure 57 : Connexion SSH graphique.....	37
Figure 58 : SSH connecté .....	37
Figure 59 : ACL de contrôle.....	37

Figure 60 : Accès au site du FAI via un ordinateur de l'entreprise .....	38
Figure 61 : Accès au site internet entreprise depuis le PC côté FAI.....	39