

OMARI SABER

Institut Universitaire de Technologie de Blois
BUT Réseaux & Télécommunications

SAE21 Concevoir le réseau informatique d'une petite structure

Enseignant

Ludovic Fontaine, Pascal Bourquin & Remi Rouffaud

Sommaire

Introduction	3
I Mise en place du Réseau	4
1 VLSM	4
2 Spanning-tree	5
3 Les VLANs et Inter-VLANs	6
4 Sécurité & SSH	13
5 Serveur, DNS & FAI	17
Conclusion	28

Introduction

Dans ce compte rendu de SAE21, je vais expliciter les différentes commandes, configuration que j'ai mis en place pour concevoir mon petit réseau d'entreprise ainsi que la FAI. On a eu donc pour but de concevoir un réseau sous packet tracer avec tout ce que l'on a appris tout au long de l'année. Le cahier des charges étant le suivant : plusieurs switch en redondance, plusieurs VLANs, IPv4 en VLSM, serveur web intranet et public ainsi que celui du FAI, de même pour le DNS ainsi qu'un client dans le FAI, les pc doivent joindre le FAI et le FAI doit accéder au site web de l'entreprise, tout équipement d'interconnexion joignable via ssh depuis le pc admin et de l'IPv6.

I Mise en place du Réseau

1 VLSM

Le VLSM (Variable Length Subnet Mask) est un masque de sous-réseau à longueur variable. Il permet l'économie d'adresses IP dans une entreprise. Etant donné que mon entreprise comprendra que 40 machines en comptant les sous-interfaces du routeur à configurer comme passerelle par défaut pour mes sous-réseaux, il est aucunement nécessaire d'utiliser un réseau en /8, /16 ou /24 qui peuvent contenir plus de 254 machines, dans mon cas à moi, il n'en est pas du tout nécessaire car je configure une petite entreprise.

Le VLSM se présente donc ainsi :

Emplacement sous-réseaux :	Nombre d'équipements	Adresse Réseau	Masque	Plage d'adresses
Administration	9	192.168.1.0	255.255.255.240	192.168.1.1 à 192.168.1.14
DMZ	6	192.168.1.16	255.255.255.248	192.168.1.17 à 192.168.1.22
Bureau d'études techniques	6	192.168.1.24	255.255.255.248	192.168.1.25 à 192.168.1.30
Bureau d'études architecte	6	192.168.1.32	255.255.255.248	192.168.1.33 à 192.168.1.38
Direction	5	192.168.1.40	255.255.255.248	192.168.1.41 à 192.168.1.46
Salle de réunion	5	192.168.1.48	255.255.255.248	192.168.1.49 à 192.168.1.54
Salle serveur privé	3	192.168.1.56	255.255.255.248	192.168.1.57 à 192.168.1.62

FIGURE 1 – VLSM

J'ai par la même occasion mis en place de l'IPv6, j'ai utilisé le prefix 2001 :41d0 :fe7e : : /48, auxquelles les adresses que j'ai crée pour mon réseau se présente sous cette forme :

Réseaux	Adresse IPv6	Masque IPv6
Administration	2001 :41d0 :fe7e :6000::	/51
DMZ	2001 :41d0 :fe7e ::	/51
Bureau d'études techniques	2001 :41d0 :fe7e :c000 ::	/51
Bureau d'études architecte	2001 :41d0 :fe7e :a000 ::	/51
Direction	2001 :41d0 :fe7e :2000 ::	/51
Salle de réunion	2001 :41d0 :fe7e :4000 ::	/51
Salle serveur privé	2001 :41d0 :fe7e :8000 ::	/51

FIGURE 2 – Réseau IPv6

2 Spanning-tree

Le Spanning Tree Protocol (aussi appelé STP) est un protocole réseau de niveau 2 permettant de déterminer une topologie réseau sans boucle (appelée algorithme de l'arbre recouvrant) dans les LAN avec ponts. Il est défini dans la norme IEEE 802.1D et est basé sur un algorithme décrit par Radia Perlman en 1985. Il permet donc des switch en redondance, sur packet tracer, l'élection du switch racine se fait automatiquement via le mode pvst (Per-VLAN Spanning Tree) c'est un mode propriétaire cisco.

Comme on peut le voir sur le switch du bureau d'études, le mode pvst est automatiquement généré :

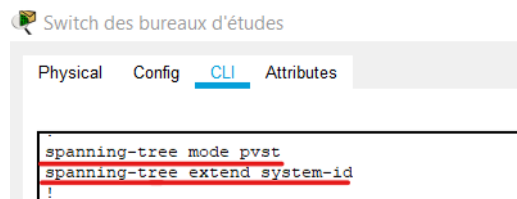


FIGURE 3 – Spanning-tree

L'architecture est celle-ci :

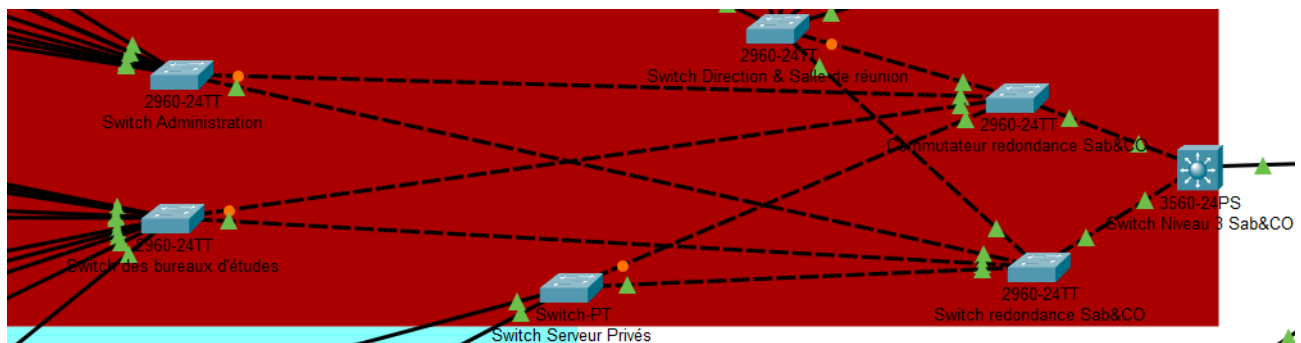


FIGURE 4 – STP

3 Les VLANs et Inter-VLANs

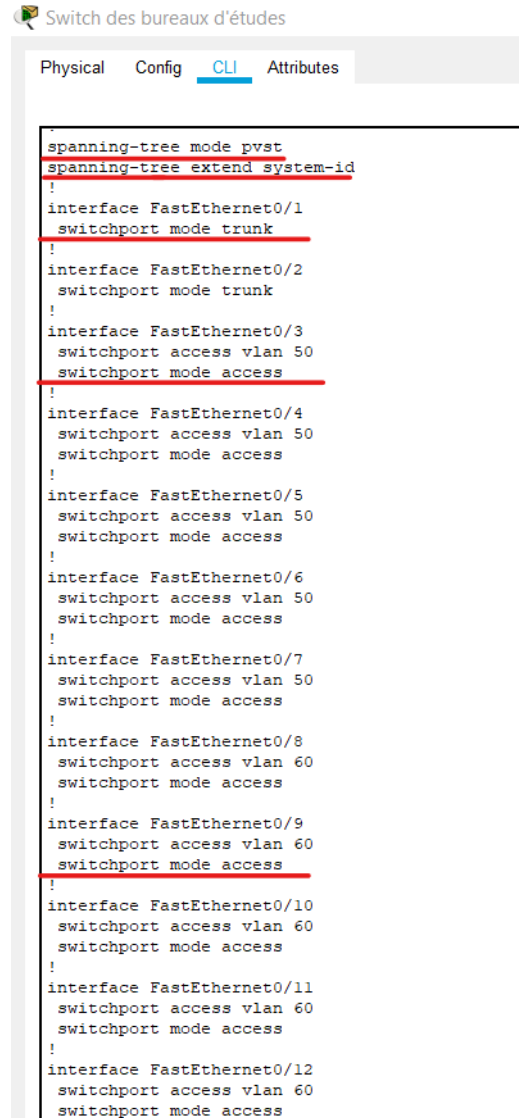
Un réseau local virtuel, communément appelé VLAN (pour Virtual LAN), est un réseau informatique logique indépendant. Il permet de séparer les flux et permet la sécurité car il crée un ensemble logique isolé et le seul moyen de pouvoir joindre un équipement/machine dans un vlan, est de passer par un routeur. C'est ce qu'on appelle la communication inter-vlan.

J'ai créée autant de vlan que j'ai de sous-réseaux donc 7 au total. Qui se présente donc ainsi :

- DMZ : vlan 10
- Direction : vlan 20
- Salle de réunion : vlan 30
- Administration : vlan 40
- Bureau d'études architecte : vlan 50
- Bureau d'études techniques : vlan 60
- Serveur privé : vlan 70

Pour pouvoir les configurer et qu'ils soient utilisable dans le réseau. Il faut configurer les différents interfaces des switchs mis en place, en "switchport mode access, switchport access vlan x" pour les interfaces entrantes donc côtés machines et "switchport mode trunk" sur les interfaces sortantes côtés routeur/switch.

Ce qui donne sur le switch des bureaux d'études :



Switch des bureaux d'études

Physical Config CLI Attributes

```
!
spanning-tree mode pvst
spanning-tree extend system-id
!
interface FastEthernet0/1
switchport mode trunk
!
interface FastEthernet0/2
switchport mode trunk
!
interface FastEthernet0/3
switchport access vlan 50
switchport mode access
!
interface FastEthernet0/4
switchport access vlan 50
switchport mode access
!
interface FastEthernet0/5
switchport access vlan 50
switchport mode access
!
interface FastEthernet0/6
switchport access vlan 50
switchport mode access
!
interface FastEthernet0/7
switchport access vlan 50
switchport mode access
!
interface FastEthernet0/8
switchport access vlan 60
switchport mode access
!
interface FastEthernet0/9
switchport access vlan 60
switchport mode access
!
interface FastEthernet0/10
switchport access vlan 60
switchport mode access
!
interface FastEthernet0/11
switchport access vlan 60
switchport mode access
!
interface FastEthernet0/12
switchport access vlan 60
switchport mode access
```

FIGURE 5 – Configuration des VLAN 50 et 60 sur un même switch

Sur les switches en redondance il suffit simplement de déclarer les vlan créer et configurer toutes les interfaces en mode trunk. la configuration est différente pour le switch de niveau 3, en effet il faut une encapsulation pour qu'il puisse supporter la topologie.

Ce qui nous donne :

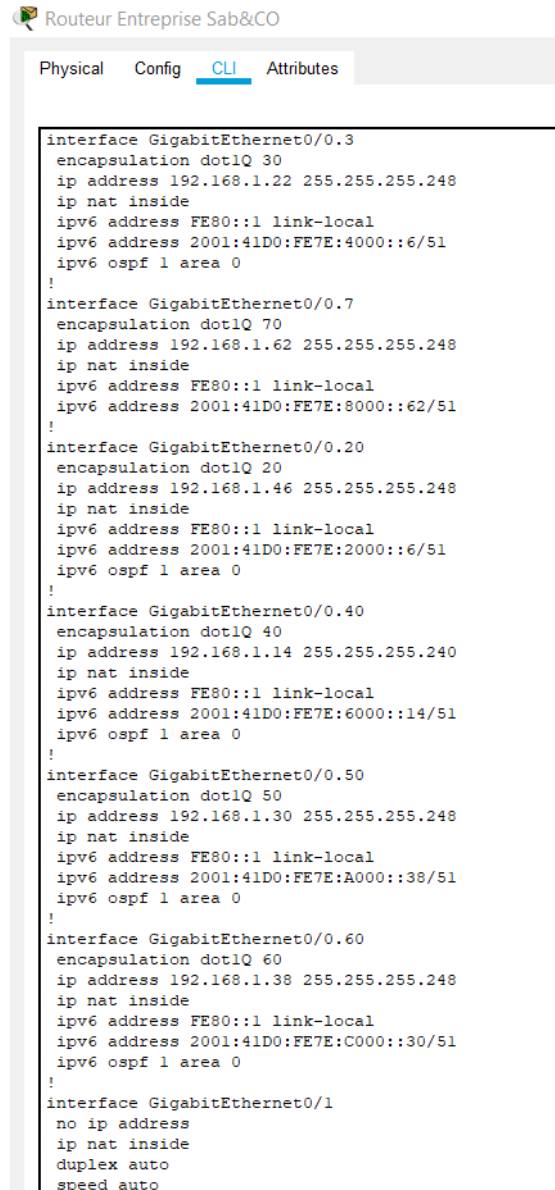


```
!
!
!
!
!
interface FastEthernet0/1
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface FastEthernet0/2
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface FastEthernet0/3
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface FastEthernet0/4
!
interface FastEthernet0/5
!
interface FastEthernet0/6
.
```

FIGURE 6 – Configuration des interfaces du switch niveau 3

Pour permettre la communication entre VLAN, il est obligatoire de créer des sous-interfaces sur le routeur et d'attribuer des adresses. Ici dans mon cas, chaque adresse du routeur est une passerelle par défaut, j'ai utilisé la dernière adresse du sous-réseau. J'ai par la même occasion attribuer les adresses IPv6.

La configuration finale se présente sous cette forme :



```

Routeur Entreprise Sab&CO
Physical Config CLI Attributes

interface GigabitEthernet0/0.3
 encapsulation dot1Q 30
 ip address 192.168.1.22 255.255.255.248
 ip nat inside
 ipv6 address FE80::1 link-local
 ipv6 address 2001:41D0:FE7E:4000::6/51
 ipv6 ospf 1 area 0
!
interface GigabitEthernet0/0.7
 encapsulation dot1Q 70
 ip address 192.168.1.62 255.255.255.248
 ip nat inside
 ipv6 address FE80::1 link-local
 ipv6 address 2001:41D0:FE7E:8000::62/51
!
interface GigabitEthernet0/0.20
 encapsulation dot1Q 20
 ip address 192.168.1.46 255.255.255.248
 ip nat inside
 ipv6 address FE80::1 link-local
 ipv6 address 2001:41D0:FE7E:2000::6/51
 ipv6 ospf 1 area 0
!
interface GigabitEthernet0/0.40
 encapsulation dot1Q 40
 ip address 192.168.1.14 255.255.255.240
 ip nat inside
 ipv6 address FE80::1 link-local
 ipv6 address 2001:41D0:FE7E:6000::14/51
 ipv6 ospf 1 area 0
!
interface GigabitEthernet0/0.50
 encapsulation dot1Q 50
 ip address 192.168.1.30 255.255.255.248
 ip nat inside
 ipv6 address FE80::1 link-local
 ipv6 address 2001:41D0:FE7E:A000::38/51
 ipv6 ospf 1 area 0
!
interface GigabitEthernet0/0.60
 encapsulation dot1Q 60
 ip address 192.168.1.38 255.255.255.248
 ip nat inside
 ipv6 address FE80::1 link-local
 ipv6 address 2001:41D0:FE7E:C000::30/51
 ipv6 ospf 1 area 0
!
interface GigabitEthernet0/1
 no ip address
 ip nat inside
 duplex auto
 speed auto

```

FIGURE 7 – Attribution des passerelles par défaut sur le routeur

Sur l'IPv6, j'ai privilégié un routage dynamique avec ospfv3 comme on peut le voir dans la figure 7, avec les commandes "ipv6 ospf 1 area 0" faites sur toutes les interfaces.

DHCP

J'ai mis en place un DHCP pour la salle de réunion, qui est elle comprise dans le vlan 30. J'ai directement configuré le serveur DHCP, depuis le routeur cisco. Les configurations sont les suivantes pour la mise en place du DHCP :

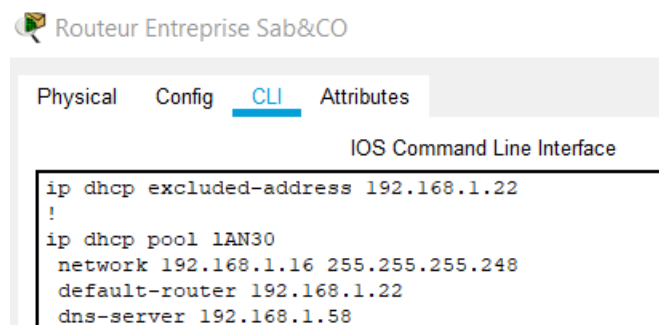


FIGURE 8 – Configuration du DHCP sur routeur Cisco 2911

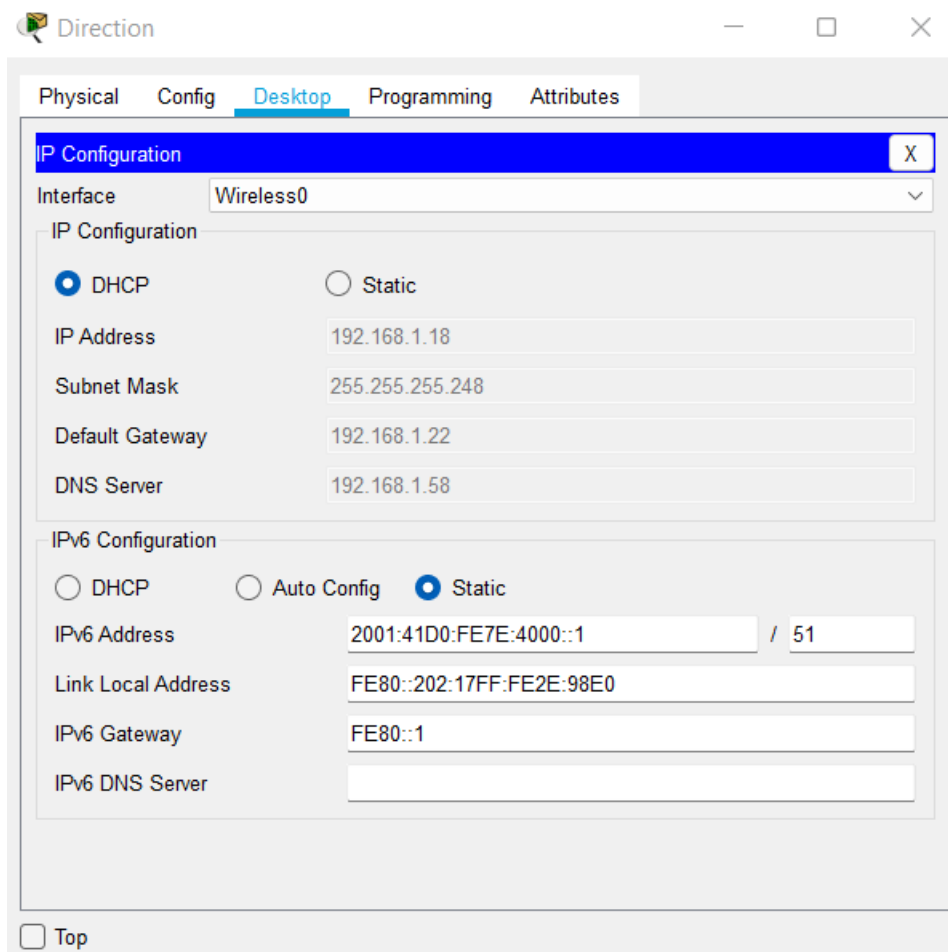


FIGURE 9 – Attribution d'adresses via DHCP

Vérification du routage inter-vlan en IPv6 et IPv4

Depuis le VLAN direction, on a tenté un ping vers le VLAN administration :

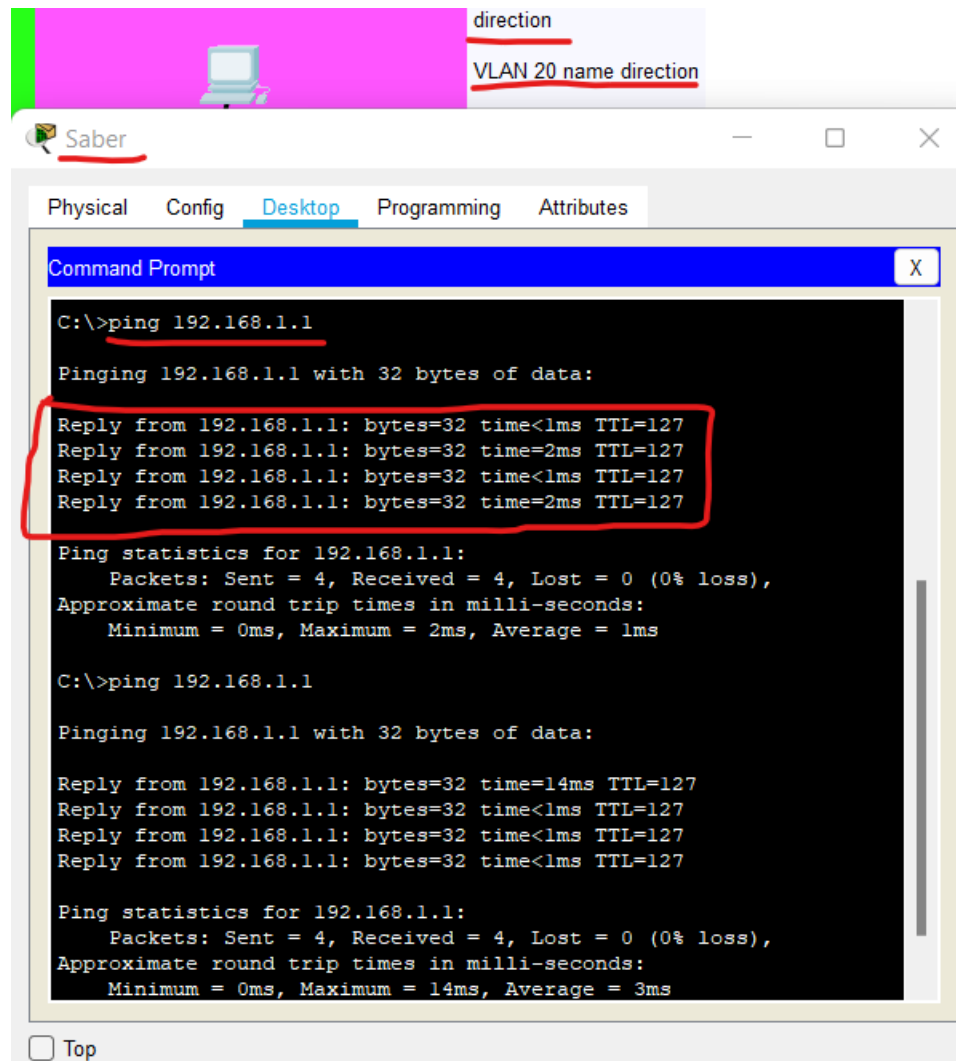


FIGURE 10 – IPv4 ping abouti

Depuis le VLAN direction, on a tenté un ping vers le VLAN bureauetu :

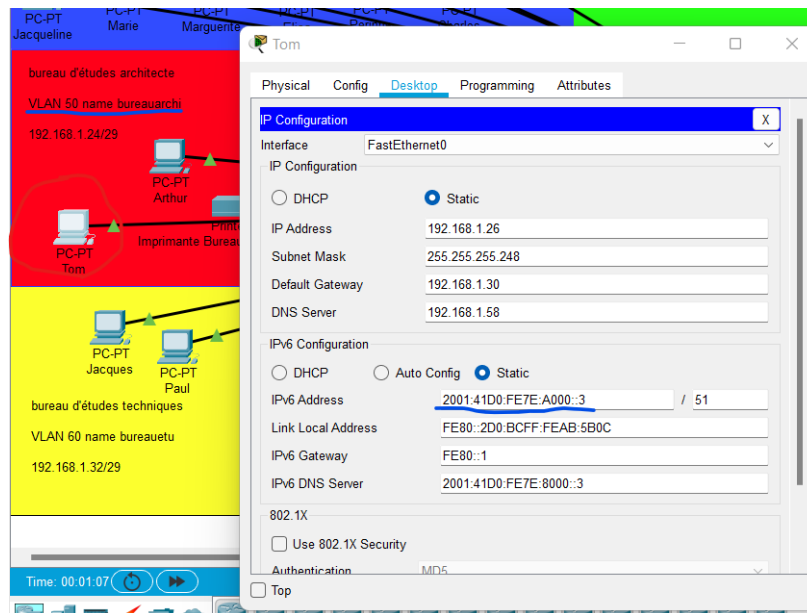


FIGURE 11 – Configuration IPv6 & IPv4 de TOM

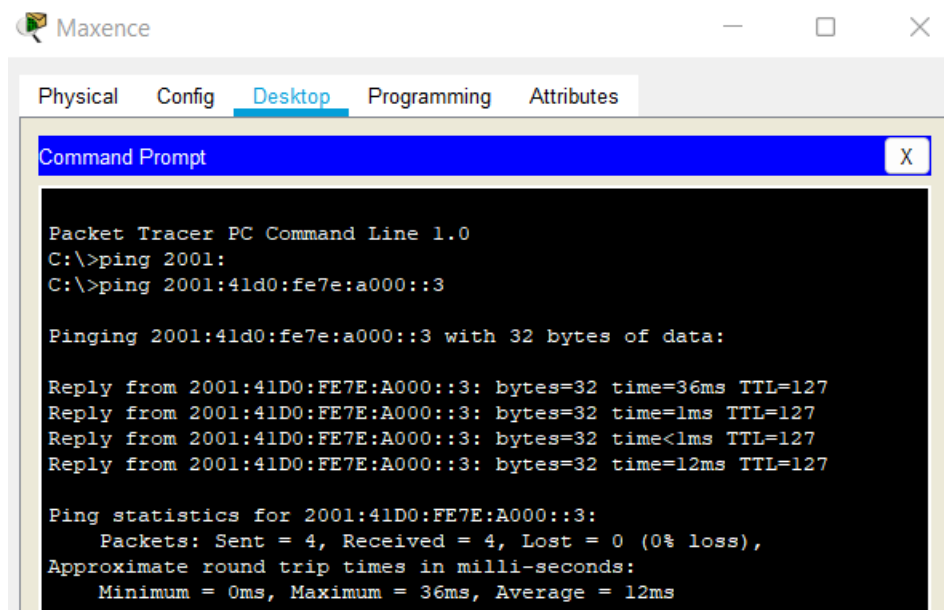


FIGURE 12 – Ping abouti depuis direction vers bureauetu

4 Sécurité & SSH

Après avoir configuré toute la partie routage, je vais maintenant sécuriser la connexion des switch et du routeur et assurer la connexion ssh uniquement entre les équipements d'interconnexion et le pc admin.

Pour ce faire, prenons un exemple d'un switch pour voir tout le procédé mis en place :

```

service password-encryption
!
hostname SwEntrepriseRed1
!
enable secret 5 $1$mERr$bUgaq3R/91B7pfyU8SR6F0
!
!
!
ip ssh version 2
ip ssh authentication-retries 2
ip ssh time-out 75
no ip domain-lookup
ip domain-name entreprisesab&co.fr
!
username administrateur secret 5 $1$mERr$hX5rVt7rPNoS4wqbXKX7m0

```

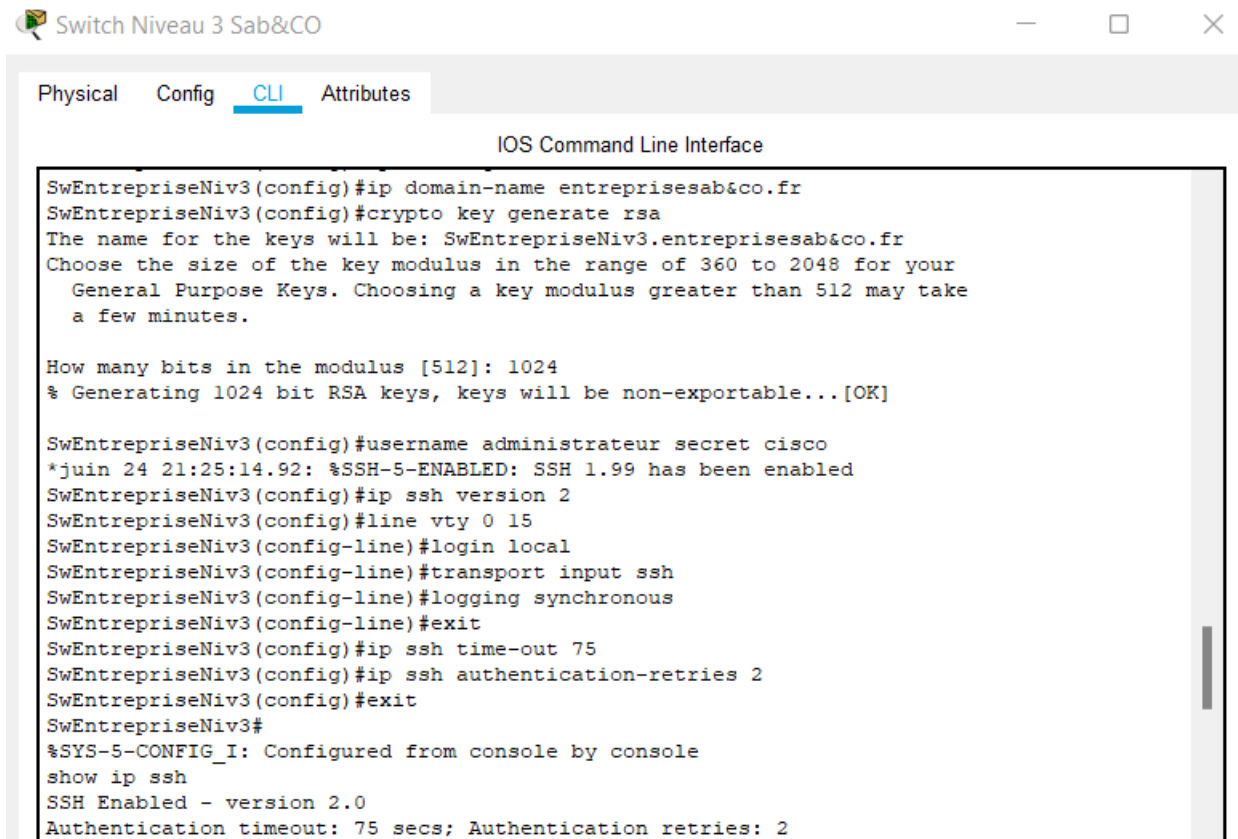
FIGURE 13 – Configuration des mots de passe à entrer lors de la connexion exex mode et ligne à distance

```

access-list 12 permit host 192.168.1.49
line con 0
!
line vty 0 4
access-class 12 in
exec-timeout 60 0
password 7 0822455D0A16061B13181F
logging synchronous
login local
transport input ssh
line vty 5 15
access-class 12 in
exec-timeout 60 0
password 7 0822455D0A16061B13181F
logging synchronous
login local
transport input ssh

```

FIGURE 14 – Configuration des mots de passe à entrer lors de la connexion exec mode et ligne à distance



Switch Niveau 3 Sab&CO

Physical Config **CLI** Attributes

IOS Command Line Interface

```
SwEntrepriseNiv3(config)#ip domain-name entreprisesab&co.fr
SwEntrepriseNiv3(config)#crypto key generate rsa
The name for the keys will be: SwEntrepriseNiv3.entreprisesab&co.fr
Choose the size of the key modulus in the range of 360 to 2048 for your
General Purpose Keys. Choosing a key modulus greater than 512 may take
a few minutes.

How many bits in the modulus [512]: 1024
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]

SwEntrepriseNiv3(config)#username administrateur secret cisco
*juin 24 21:25:14.92: %SSH-5-ENABLED: SSH 1.99 has been enabled
SwEntrepriseNiv3(config)#ip ssh version 2
SwEntrepriseNiv3(config)#line vty 0 15
SwEntrepriseNiv3(config-line)#login local
SwEntrepriseNiv3(config-line)#transport input ssh
SwEntrepriseNiv3(config-line)#logging synchronous
SwEntrepriseNiv3(config-line)#exit
SwEntrepriseNiv3(config)#ip ssh time-out 75
SwEntrepriseNiv3(config)#ip ssh authentication-retries 2
SwEntrepriseNiv3(config)#exit
SwEntrepriseNiv3#
%SYS-5-CONFIG_I: Configured from console by console
show ip ssh
SSH Enabled - version 2.0
Authentication timeout: 75 secs; Authentication retries: 2
```

FIGURE 15 – Configuration ssh

Pour garantir uniquement la connexion ssh depuis le PC admin, il faut entrer dans la configuration “line vty 0 15” et entrer les commandes suivante “access-list 12 permit 192.168.1.49(ip du pc admin)” puis access-class 12 in” et attribué une adresse IP au VLAN 1, permettant ainsi la liaison à distance. Pour les switchs et le routeur j’ai choisi une adresse en 10.0.0.0/8.

On vérifie si cela a été pris en compte :

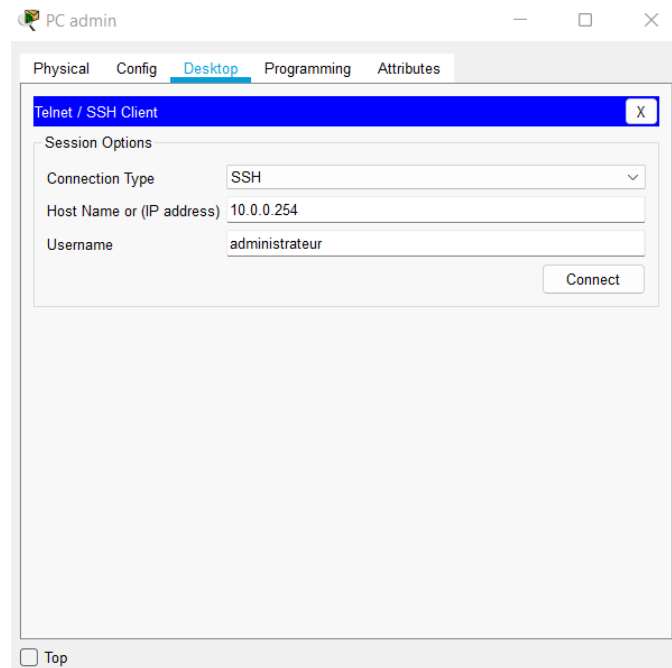


FIGURE 16 – Connexion ssh au routeur depuis PC Admin

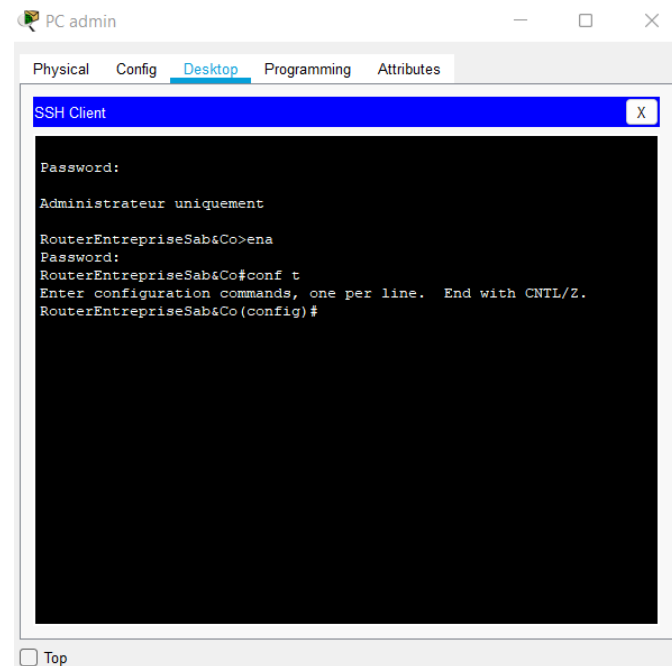


FIGURE 17 – Connexion ssh au routeur réussi depuis pc Admin

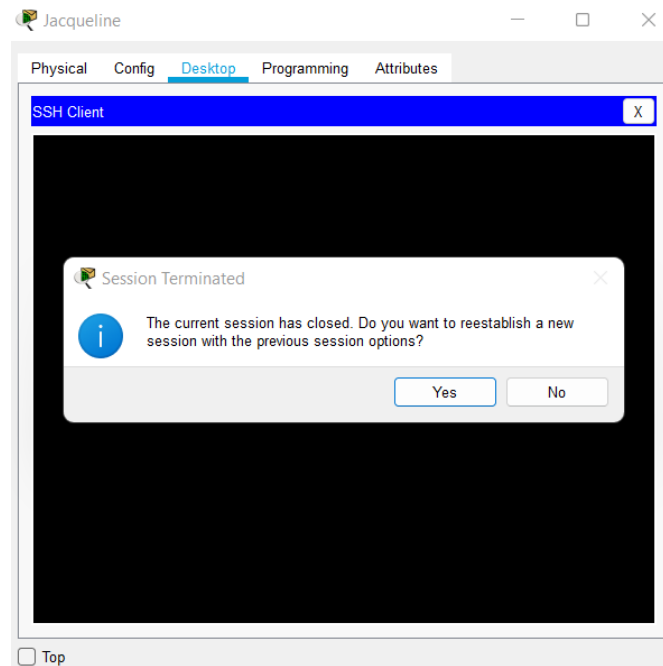


FIGURE 18 – Connexion ssh au routeur depuis le poste jacqueline refusé

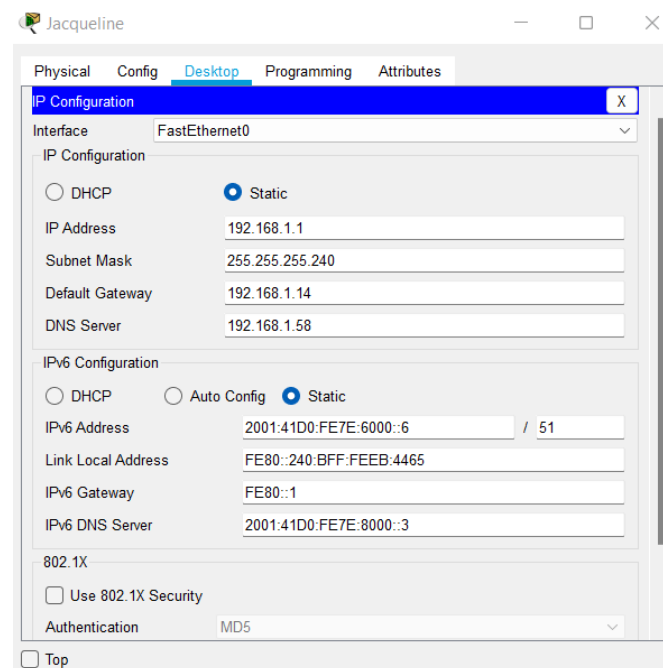


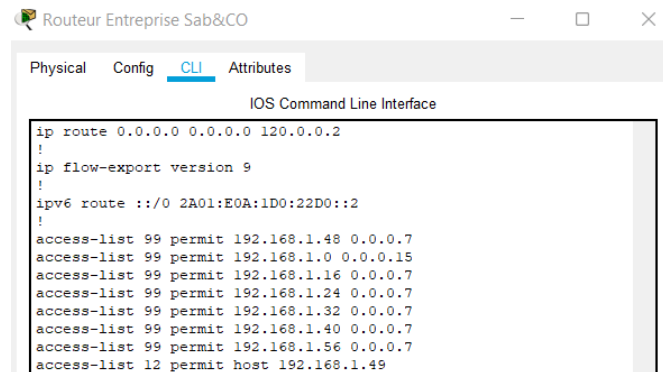
FIGURE 19 – Configuration poste de jacqueline

Comme on peut le voir le poste de jacqueline n'a pas l'autorisation de se connecter au routeur à distance en ssh car son adresse IP est rejeté grâce aux access-list précédemment intégré à la configuration.

5 Serveur, DNS & FAI

J'ai créé un réseau FAI que j'ai joint à mon réseau d'entreprise via les routeurs, dans ce FAI, j'ai procédé à la même configuration que le réseau d'entreprise, c'est-à-dire, ipv4, ipv6, le tout sans vlsm avec des adresses public, j'ai procédé au routage ospfv3 sans faire de routage statique en ipv4. Par la même occasion j'ai attribué une route par défaut à mon routeur d'entreprise qui va vers le routeur FAI ainsi que des ACL, pour que les machines du réseau puisse joindre le FAI et ses serveurs.

Ce qui donne comme configuration :



```
Router Entreprise Sab&CO
Physical Config CLI Attributes
IOS Command Line Interface
ip route 0.0.0.0 0.0.0.0 120.0.0.2
!
ip flow-export version 9
!
ipv6 route ::/0 2A01:E0A:1D0:22D0::2
!
access-list 99 permit 192.168.1.48 0.0.0.7
access-list 99 permit 192.168.1.0 0.0.0.15
access-list 99 permit 192.168.1.16 0.0.0.7
access-list 99 permit 192.168.1.24 0.0.0.7
access-list 99 permit 192.168.1.32 0.0.0.7
access-list 99 permit 192.168.1.40 0.0.0.7
access-list 99 permit 192.168.1.56 0.0.0.7
access-list 12 permit host 192.168.1.49
```

FIGURE 20 – Configuration des acl et route par défaut pour accéder au FAI

J'ai intégré dans mon réseau d'entreprise plusieurs serveurs, notamment :

- Serveur web intranet
- Serveur DNS privé
- Serveur web public
- Serveur DNS public
- Serveur TFTP
- Serveur Mail & NTP

Nous verrons comment nous avons pu les configurer tout au long de cette partie.

Dans le FAI j'ai intégré plusieurs serveurs aussi comme :

- Serveur web FAI
- Serveur DNS FAI pour délégation
- Serveur DNS FAI
- Serveur Mail & NTP

Pour commencer, les serveurs web intranet et dns privé :

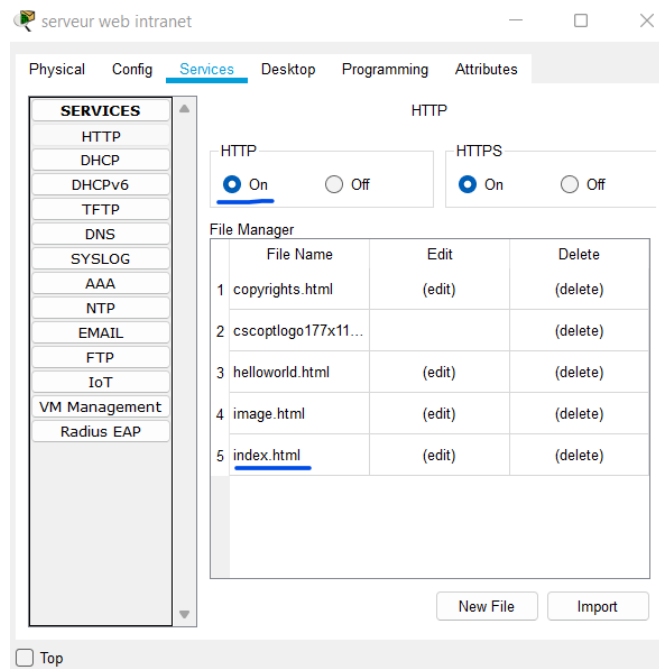


FIGURE 21 – Configuration serveur web intranet

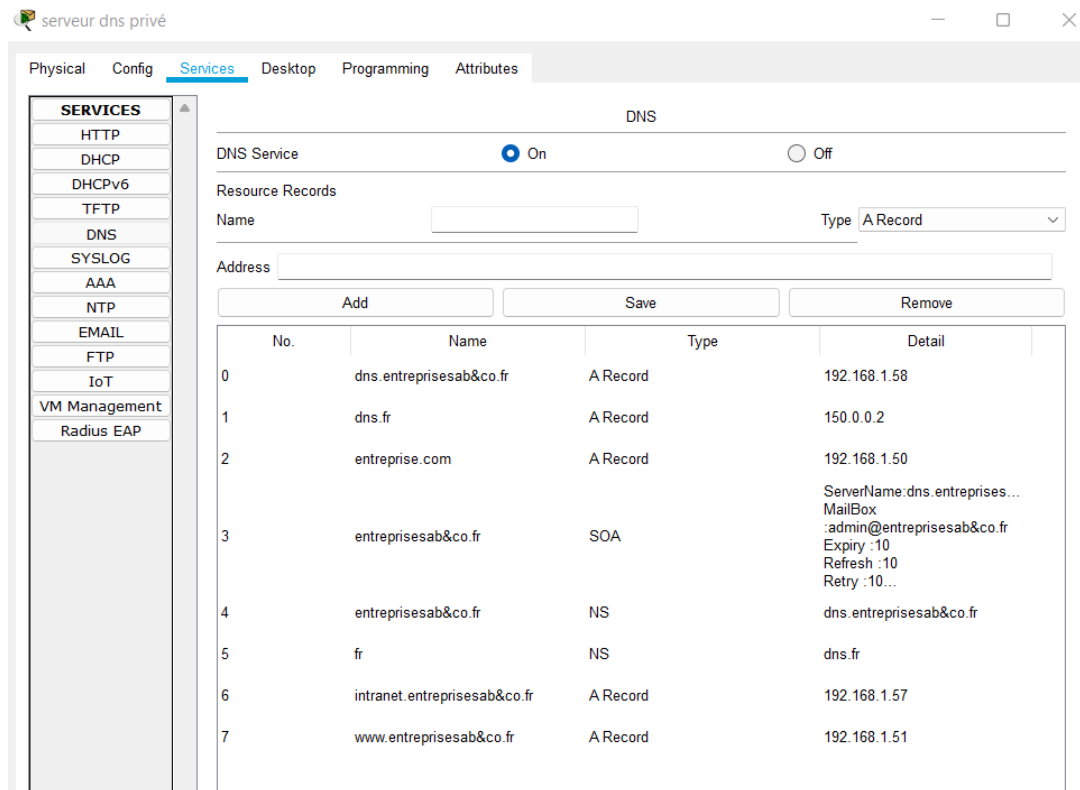


FIGURE 22 – Configuration serveur dns privé

Après les avoir configuré correctement, nous pouvons joindre le serveur web et dns depuis un pc du réseau d'entreprise avec le fqdn "intranet.entreprisesab&co.fr" :

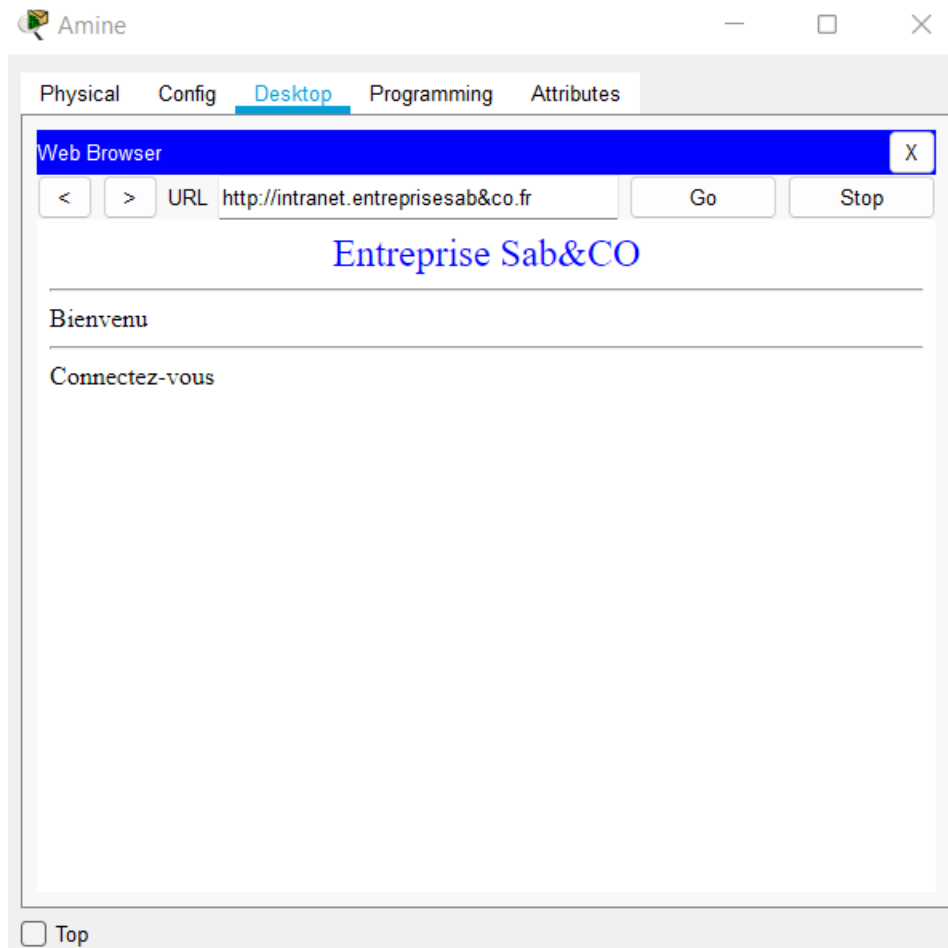


FIGURE 23 – Le serveur DNS privé fonctionne

Maintenant que les serveurs du domaine privé fonctionne, nous allons configurer les serveurs DNS public et serveur web public :

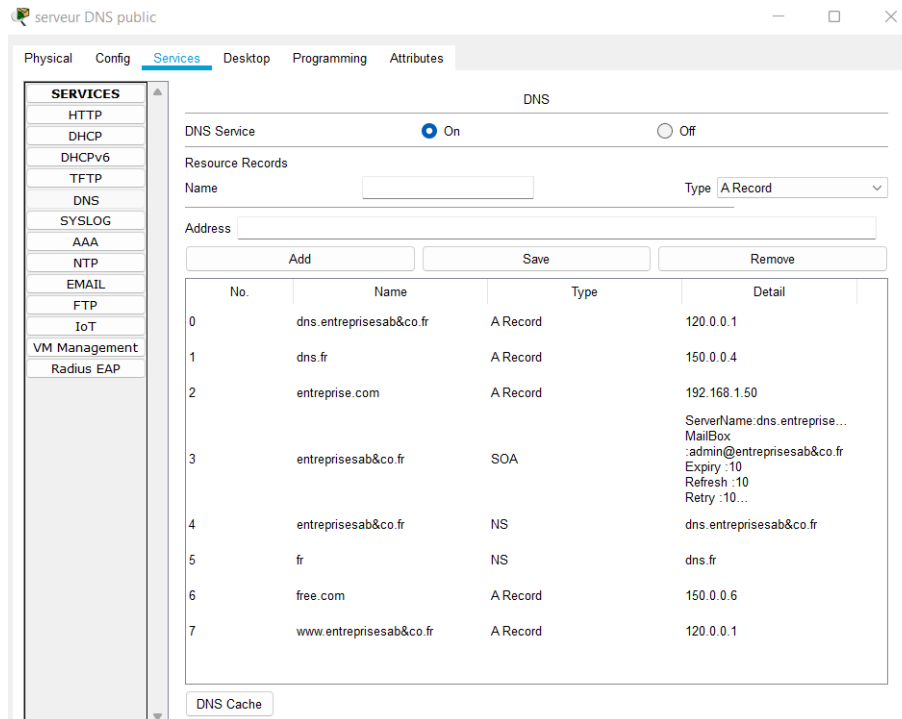


FIGURE 24 – Configuration serveur dns public

Vérification du fqdn “www.entreprisesab&co.fr” :

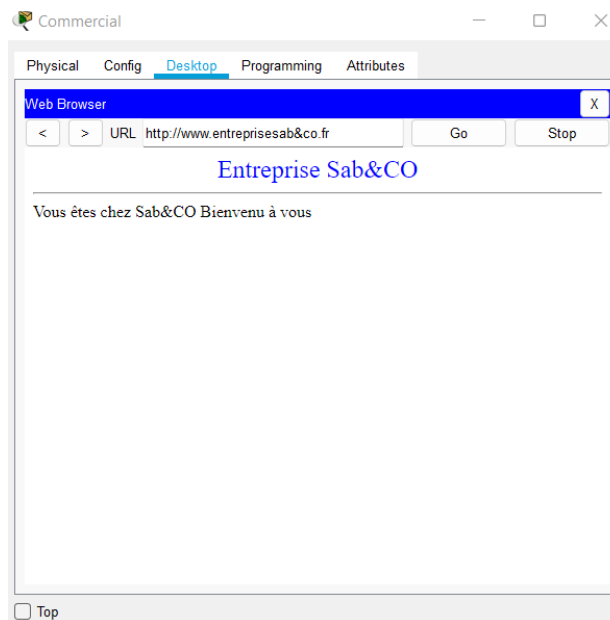


FIGURE 25 – Le serveur DNS public fonctionne

Configuration des serveurs DNS FAI pour la délégation et DNS FAI :

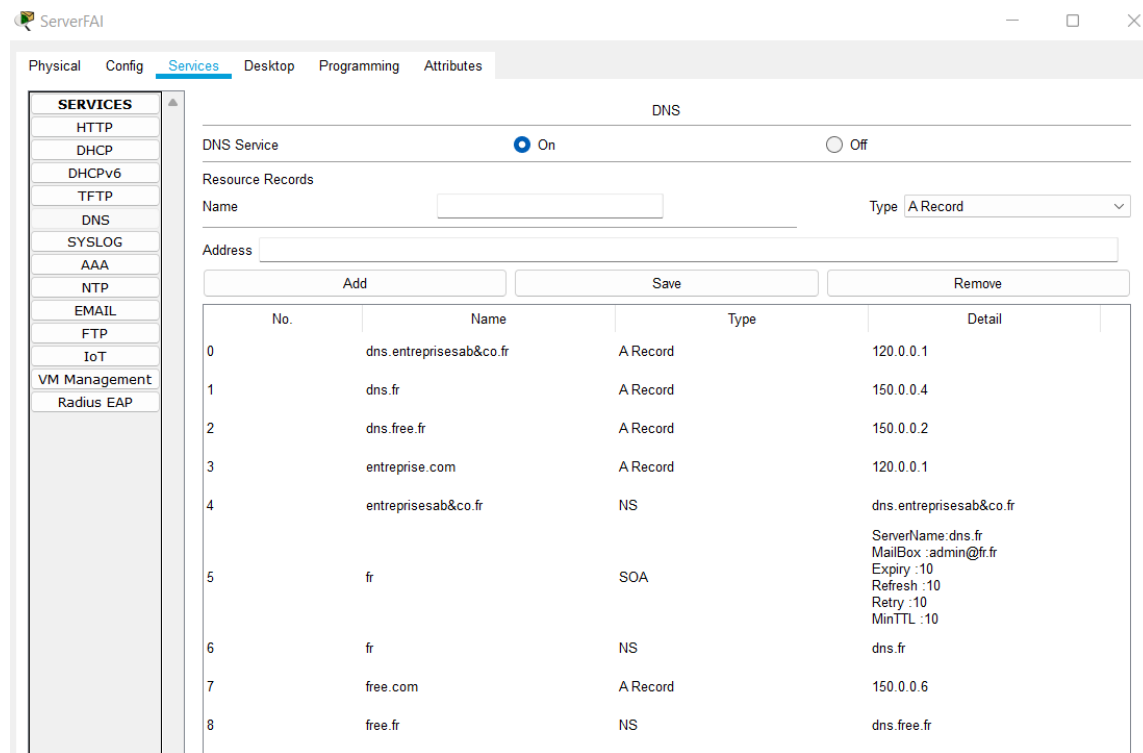


FIGURE 26 – Config DNS FAI delegation

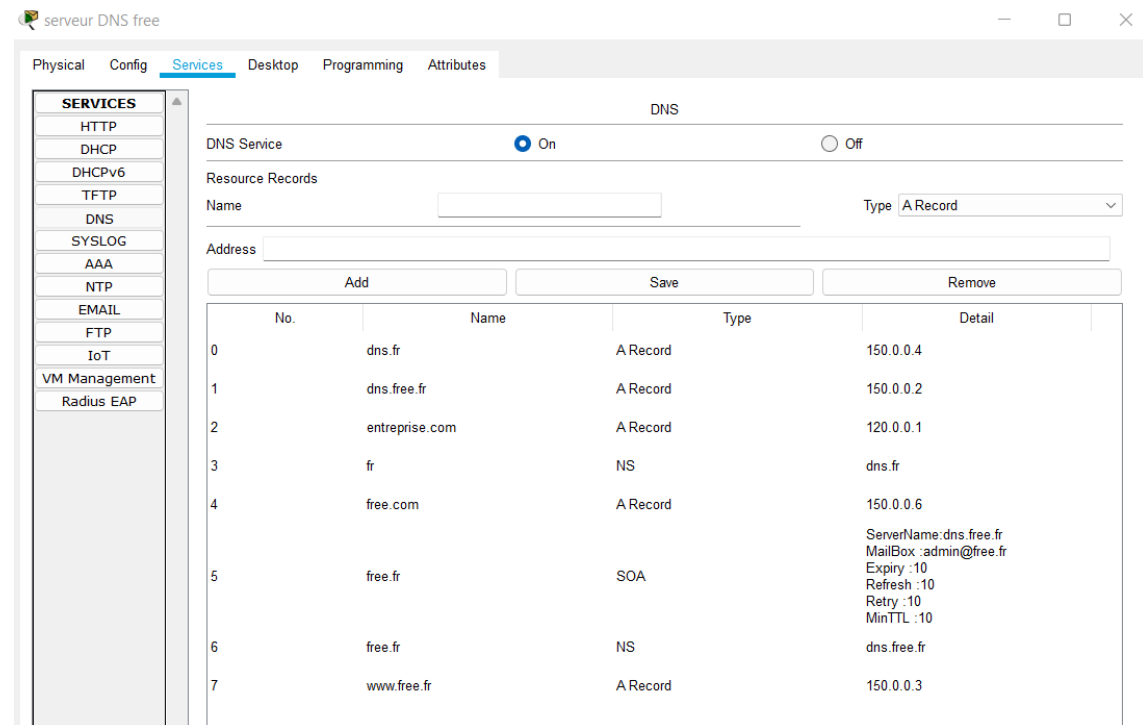


FIGURE 27 – Config DNS FAI

Vérification du fqdn “www.free.fr” sur le pc du client FAI :

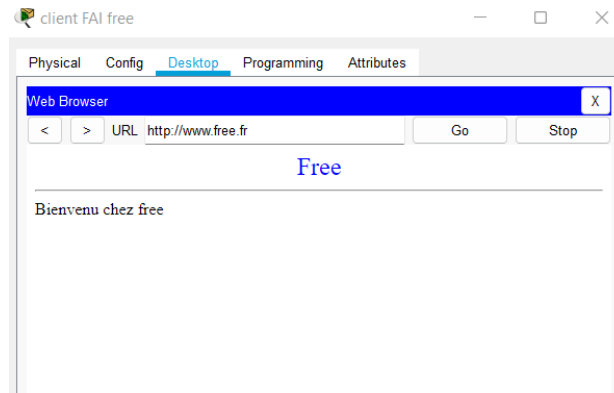


FIGURE 28 – Fqdn FAI fonctionne

Maintenant que les DNS, fqdn fonctionne bien, il faut configurer des redirection de port sur le routeur pour pouvoir joindre les pages web en dehors des réseaux, pour ce faire voici la configuration sur le routeur de l'entreprise :

```
-  
ip nat inside source static tcp 192.168.1.51 80 120.0.0.1 80  
ip nat inside source static udp 192.168.1.52 53 120.0.0.1 53
```

FIGURE 29 – Redirection de port

Donc maintenant depuis le client FAI, il est possible de joindre la page web de l'entreprise :

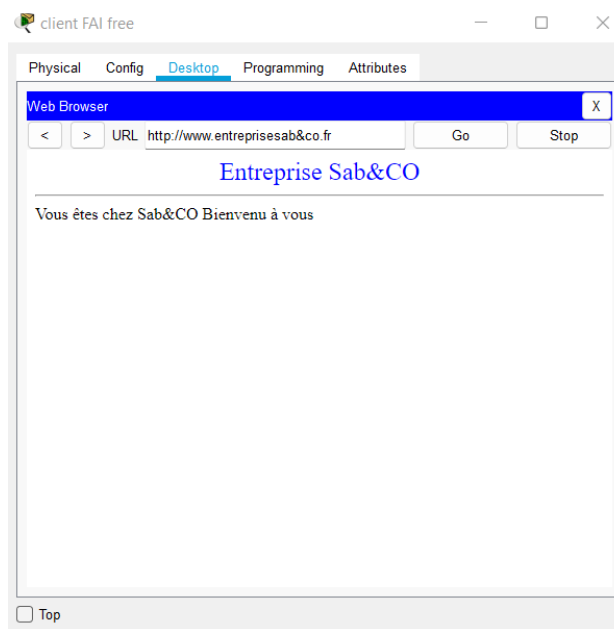


FIGURE 30 – La redirection de port marche

Serveur FTP :

```
routerentreprisesab&co#copy startup-config tftp:
Address or name of remote host []? 192.168.1.53
Destination filename [routerentreprisesab&co-config]?

Writing startup-config...!!
[OK - 2997 bytes]

2997 bytes copied in 0.077 secs (38922 bytes/sec)
```

FIGURE 31 – Configuration du routeur transféré vers TFTP

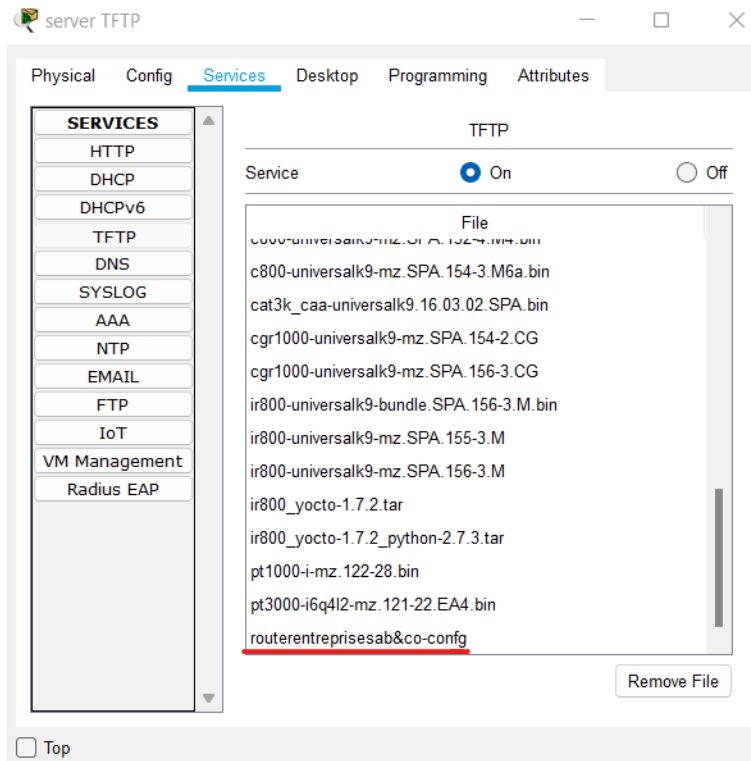


FIGURE 32 – Configuration du routeur transféré vers TFTP avec succès

Configuration du serveur Mail & NTP côté entreprise :

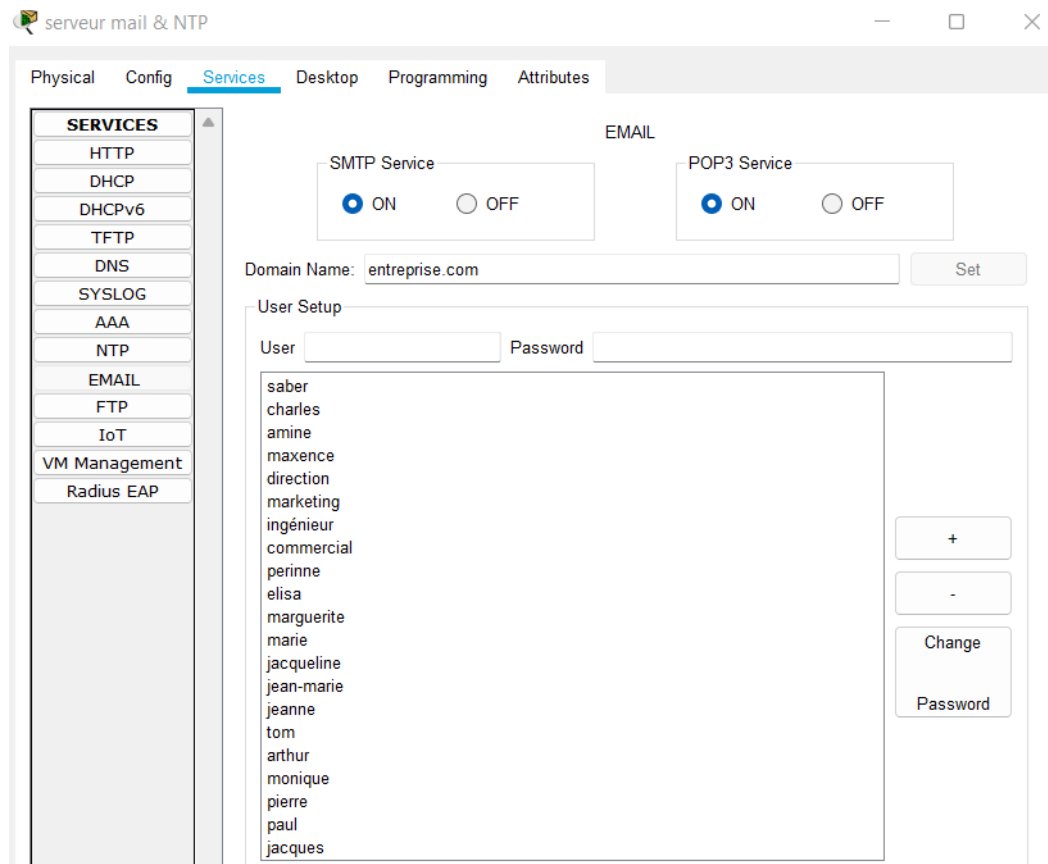


FIGURE 33 – Configuration du serveur Mail

J’ai entré tous les utilisateurs du réseau d’entreprise avec une adresse mail ici avec comme @ “entreprise.com”, on observe si la configuration fonctionne et si les utilisateurs peuvent s’envoyer des mails mutuellement.

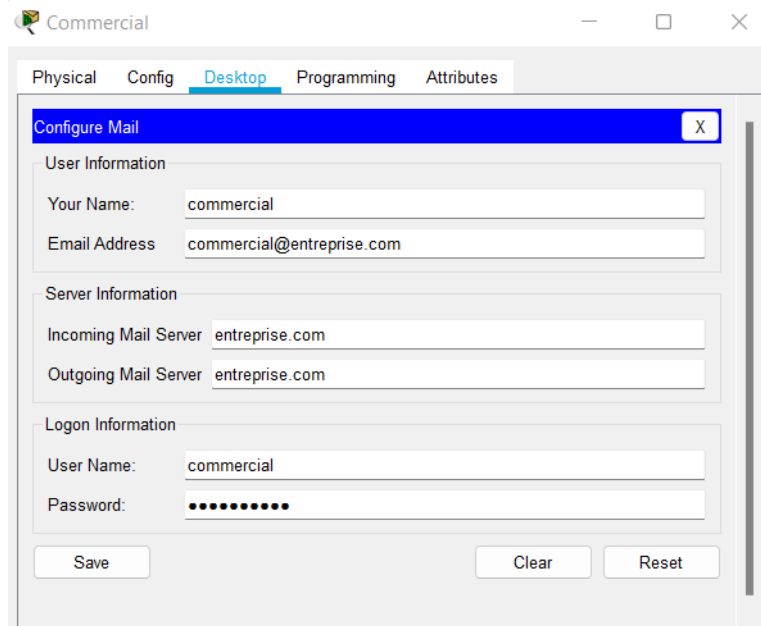


FIGURE 34 – Configuration du mail côté PC

“Entreprise.com” grâce au serveur DNS, que j’ai configuré précédemment avec le A record vers “Entreprise.com” évite d’entrer l’adresse IP du serveur mail, mais simplement le nom de domaine.

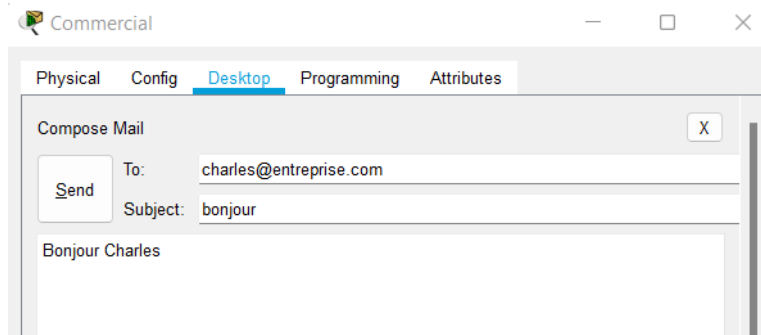


FIGURE 35 – Envoi mail à Charles depuis Commercial

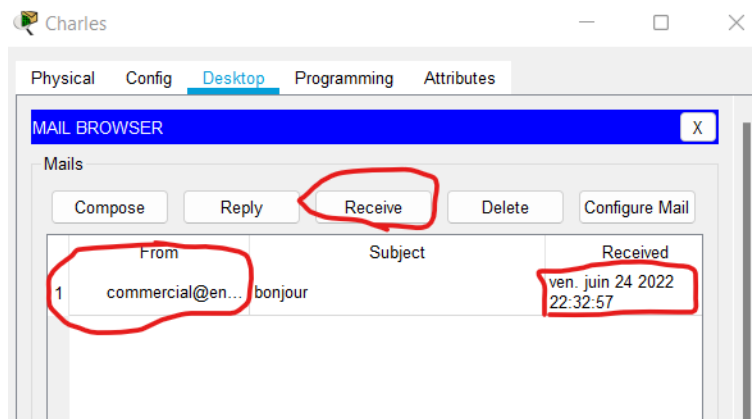


FIGURE 36 – Charles reçoit bien le mail

Charles reçoit bien le mail avec la bonne date et la bonne heure grâce au serveur NTP configuré :

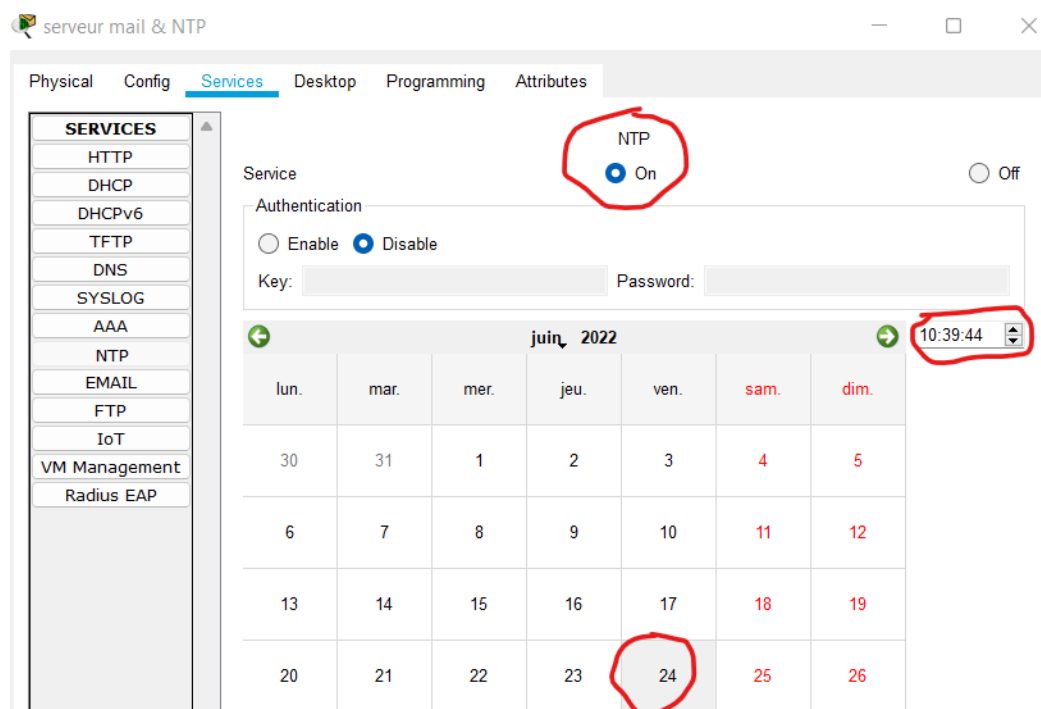


FIGURE 37 – Configuration serveur NTP

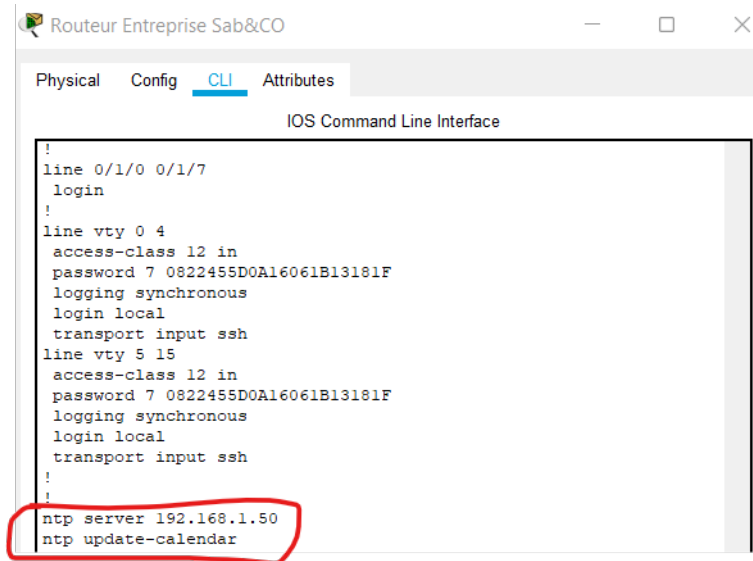


FIGURE 38 – NTP pris en compte sur le routeur entreprise

La configuration du serveur mail du FAI et NTP est sensiblement la même. Maintenant ce que l'on veut, c'est pouvoir envoyer des mails entre FAI et pc entreprise. On fait pour ça des redirection de port sur POP3 et SMTP, ce qui donne :

```

ip nat inside source static tcp 192.168.1.50 25 120.0.0.1 25
ip nat inside source static tcp 192.168.1.50 110 120.0.0.1 110
    
```

FIGURE 39 – PAT pour POP3 et SMTP

On vérifie si cela marche bien :

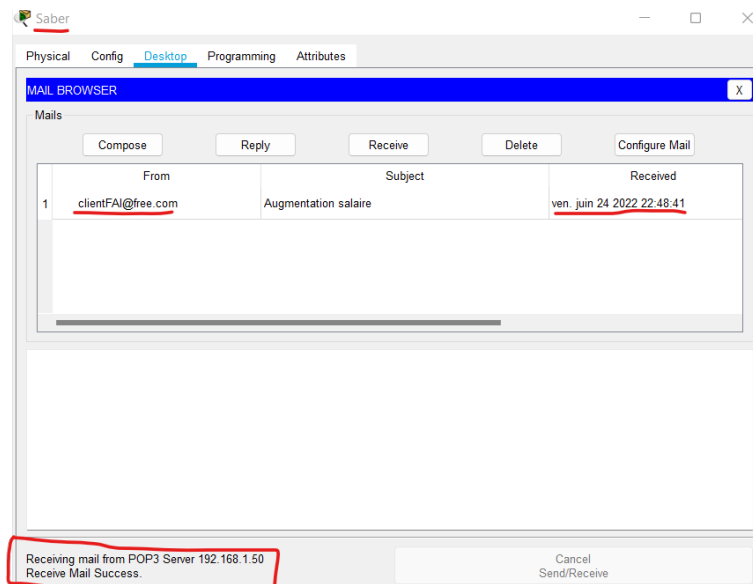


FIGURE 40 – Le PAT marche parfaitement

Conclusion

Dans cette SAE, nous avons pu mettre en place en réseau avec toutes les notions, configurations apprises tout au long de l'année, VLANs, ACL, NAT, PAT, DNS, HTTP etc... J'ai pu assurer tout le cahier des charges en plus de configurer en plus un serveur NTP & Mail. J'aurai pu configurer des règles de filtrage pour permettre la sécurité, ça n'a malheureusement pas abouti et j'ai préféré configurer au mieux les autres configurations demandés dans le cahier des charges.

Table des figures

1	VLSM	4
2	Réseau IPv6	4
3	Spanning-tree	5
4	STP	5
5	Configuration des VLAN 50 et 60 sur un même switch	7
6	Configuration des interfaces du switch niveau 3	8
7	Attribution des passerelles par défaut sur le routeur	9
8	Configuration du DHCP sur routeur Cisco 2911	10
9	Attribution d'adresses via DHCP	10
10	IPv4 ping abouti	11
11	Configuration IPv6 & IPv4 de TOM	12
12	Ping abouti depuis direction vers bureauetu	12
13	Configuration des mots de passe à entrer lors de la connexion exex mode et ligne à distance	13
14	Configuration des mots de passe à entrer lors de la connexion exec mode et ligne à distance	13
15	Configuration ssh	14
16	Connexion ssh au routeur depuis PC Admin	15
17	Connexion ssh au routeur réussi depuis pc Admin	15
18	Connexion ssh au routeur depuis le poste jacqueline refusé	16
19	Configuration poste de jacqueline	16
20	Configuration des acl et route par défaut pour accéder au FAI	17
21	Configuration serveur web intranet	18
22	Configuration serveur dns privé	18
23	Le serveur DNS privé fonctionne	19
24	Configuration serveur dns public	20
25	Le serveur DNS public fonctionne	20
26	Config DNS FAI delegation	21
27	Config DNS FAI	21
28	Fqdn FAI fonctionne	22
29	Redirection de port	22
30	La redirection de port marche	22
31	Configuration du routeur transféré vers TFTP	23
32	Configuration du routeur transféré vers TFTP avec succès	23
33	Configuration du serveur Mail	24
34	Configuration du mail côté PC	25
35	Envoi mail à Charles depuis Commercial	25

36	Charles reçoit bien le mail	26
37	Configuration serveur NTP	26
38	NTP pris en compte sur le routeur entreprise	27
39	PAT pour POP3 et SMTP	27
40	Le PAT marche parfaitement	27