SAE201
Construire un réseau informatique pour une petite structure

Compte Rendu Technique : Création du réseau informatique de l'entreprise fictive « TechnoLink »

Table des Matières

Présentation du projet 3
Cahier des charges 4
1) Analyse et conception du réseau physique 5
1.1) Organisation spatiale des locaux 5
1.2) Inventaire et disposition des équipements informatiques 6
2) Conception de l'architecture logique du réseau 7
2.1) Structuration du réseau en VLAN 7
2.2) Adressage IPv4 et VLSM 11
3) Configuration des services internes de l'entreprise 16
3.1) Configuration des serveurs internes 16
3.2) Mise en place des services internes 17
4) Mise en place de la DMZ 21
4.1) Conception et configuration physique de la DMZ 21
4.2) Configuration logique de la DMZ 21
4.3) Configuration des services accessibles publiquement 23
5) Connexion au réseau externe (FAI) 25
5.1) Mise en place de la connectivité vers le FAI 25
5.2) Création et organisation du réseau du FAI 26
5.3) Mise en service des équipements du FAI 26
6) Configuration avancée : NAT et PAT 29
6.1) Configuration du NAT 29
6.2) Configuration de la redirection de ports (PAT) 30
7) Mise en service des serveurs DNS 31
7.1) Configuration des serveurs DNS 31
7.2) Vérification du fonctionnement des serveurs DNS 34
8) Mise en place de la sécurité des équipements 37
8.1) Mise en place des ACL (Access Control List) 37
8.2) Mise en place de la protection par SSH 39
Conclusion 43
Table des illustrations 44

Présentation du projet

Dans le cadre de notre formation en BUT – Réseaux et Télécommunications en première année, nous avons été amenés à concevoir l'architecture réseau complète d'une petite entreprise dans le cadre du projet SAE201. Ce projet a pour objectif de mobiliser l'ensemble des compétences acquises au cours des semestres 1 et 2 afin d'évaluer notre capacité à construire un réseau informatique opérationnel, sécurisé et structuré qui répond aux besoins primordiaux d'une entreprise.

À travers cette mise en situation, nous avons appliqué des principes essentiels tels que la commutation, le routage, l'usage des VLANs, l'adressage en VLSM, la gestion de plusieurs services, la sécurité et l'accès à internet. Le projet inclut également une zone DMZ, la mise en œuvre du NAT et de la redirection de ports, la mise en place de serveurs publics et privés. Tous ces éléments seront intégrés dans une architecture informatique simulée à l'aide de Cisco Packet Tracer.

Ce compte-rendu présente donc l'ensemble des étapes de la réalisation de notre projet, depuis l'analyse du cahier des charges jusqu'aux tests de fonctionnements finaux.

Cahier des charges

Afin de mettre en œuvre notre réseau informatique d'une petite entreprise, nous devons respecter un cahier des charges précis afin d'avoir les fonctionnalités de bases d'une architecture d'entreprise. Voici le cahier des charges que nous devons respecter :

- Plusieurs Switchs en redondance
- Plusieurs VLANs
- Une architecture de sous-réseaux IPv4 privés en VLSM
- Utilisation de plusieurs serveurs :
  - Serveur WEB public
  - Serveur WEB intranet
  - Serveur DNS public
  - Serveur DNS privé
  - Serveur DHCP
- Un raccordement au réseau public d'un FAI comportant :
  - Serveur WEB
  - Serveur DNS
  - Un client
- Tous 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 de l'administrateur de l'entreprise en SSH
- Double adressage : IPv4 obligatoire et IPv6 apprécié
- Le nom des VLANs, des PC, des serveurs et du FAI ainsi que les contenus des sites web doivent être personnalisés.

1) Analyse et conception du réseau physique

1.1) Organisation spatiale des locaux

Pour ce projet, nous allons créer le réseau informatique de l'entreprise « TechnoLink » . Plusieurs bureaux composent cette entreprise :

- Pôle des ingénieurs (2 bureaux : 8 employés)
- Pôle des chargés de Communication (4 employés)
- Pôle Administratif (5 employés)
- Secrétariat (2 employés)
- Accueil (2 employés)
- Direction (4 employés)
- Salle des serveurs (1 administrateur)
- Salle de réunion (jusqu'à 25 utilisateurs)

Afin d'isoler les services publics et les services privés, nous allons créer une DMZ (Demilitarized Zone), un sous-réseau séparé du réseau local et isolé de celui-ci qui abritera les services pouvant être accessibles depuis internet afin d'ajouter une couche de protection au réseau local. Dans notre cas, cette DMZ sera composée du serveur WEB et DNS publics de l'entreprise, ces services pouvant être accessibles depuis internet.

Grâce à cette composition, on peut ainsi créer le schéma de notre entreprise :

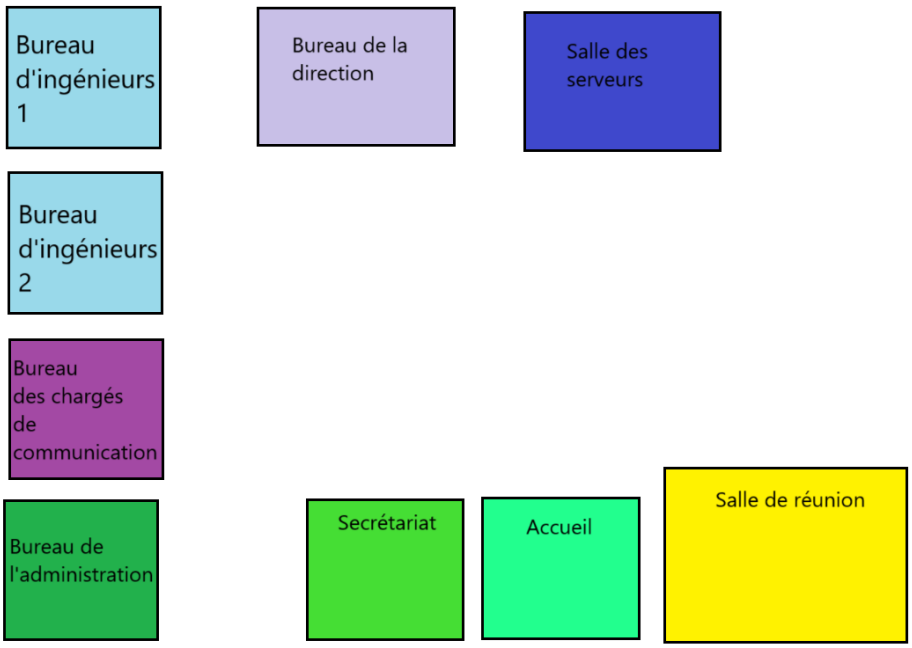

Figure 1 : Schéma de la disposition des salles composant les locaux de TechnoLink

1.2) Inventaire et disposition des équipements informatiques

Ainsi, après avoir créé le schéma des locaux, nous pouvons créer le schéma de notre réseau informatique. Sur ce schéma, nous allons pouvoir ajouter les différents équipements utilisés, la DMZ et l'accès au FAI. Voici le schéma :

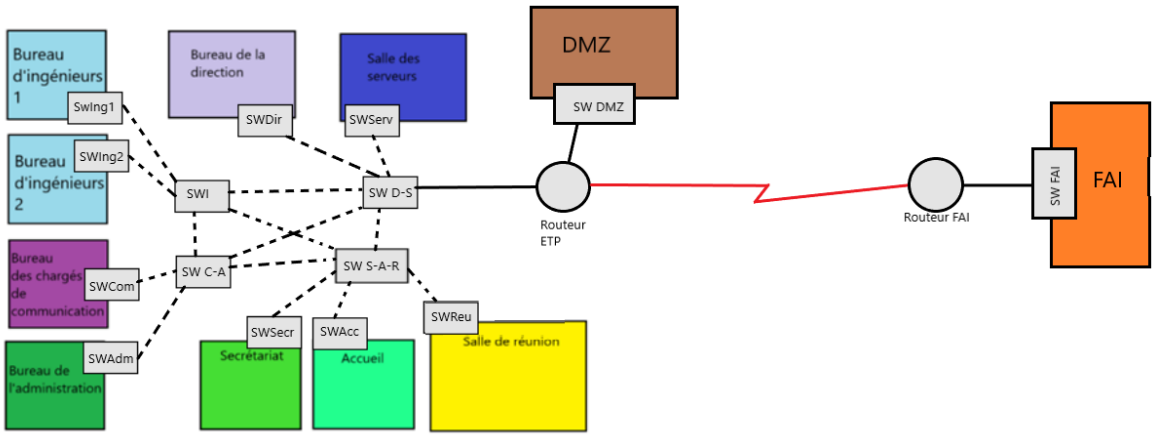

Figure 2 : Schéma de la mise en place du réseau informatique de TechnoLink

Maintenant que nous avons notre schéma, on peut créer un tableau récapitulatif des équipements que nous allons utiliser pour la partie Entreprise :

	PC :	Imprimantes
Bureau d'ingénieurs 1	4	1
Bureau d'ingénieurs 2	4	1
Bureau des chargés de communication	4	1
Bureau de l'administration	5	1
Secrétariat	2	1
Accueil	2	
Salle de réunion	10	
Direction	4	
Salle des serveurs	1	
Total	36	5

Figure 3 : Tableau récapitulatif du nombre de PC et d'imprimantes en fonction des salles

Equipements	Nombres
Routeurs	1
Switchs	13
Serveurs	5

Figure 4 : Tableau récapitulatif des équipements utilisé du coté entreprise

A cela, nous pouvons ajouter un PC « client FAI » et deux Serveurs du côté du FAI.

Maintenant que nous savons quels équipements nous allons utiliser et comment nous allons les disposer, nous pouvons commencer à configurer notre réseau. Pour ce faire nous allons commencer par mettre en place les Routeurs ainsi que les Switchs centraux :

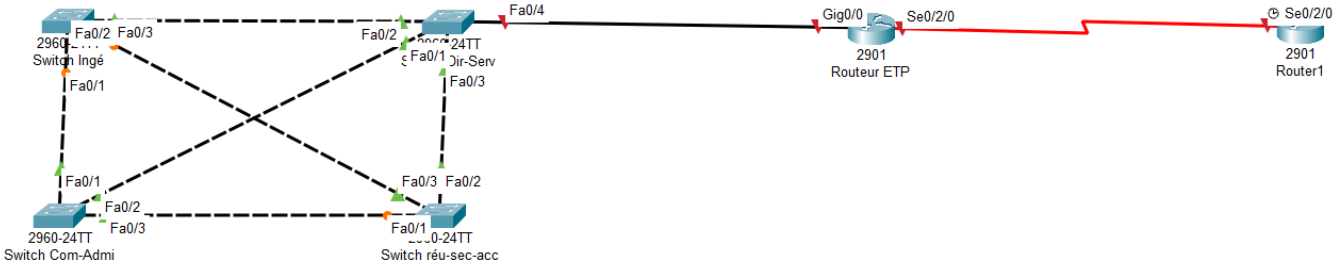

Figure 5 : Mise en place des Switchs et des Routeurs

Afin de respecter le cahier des charges, nous avons connecté les Switches centraux entre eux et nous avons activé le spanning-tree afin d'avoir notre redondance de Switchs.

2) Conception de l'architecture logique du réseau

2.1) Structuration du réseau en VLAN

La base de notre réseau ayant été créée, nous pouvons désormais nous concentrer sur son adressage logique. Afin de respecter le cahier des charges, nous avons choisi de segmenter le réseau à l'aide de VLAN. Cette méthode permet de renforcer la sécurité et d'améliorer la lisibilité de l'architecture réseau.

La création des VLAN a été réalisée de manière logique, en fonction de l'organisation des locaux et des services :

- VLAN_Inge : regroupe les deux salles dédiées aux ingénieurs.
- VLAN_Com : attribué à la salle des chargés de communication.
- VLAN_Adm : affecté aux hôtes du pôle administratif.
- VLAN_Serv : dédié à la salle des serveurs.
- VLAN_Reu : mis en place pour la salle de réunion
- VLAN_Acc : commun à la salle d'accueil et au secrétariat

Nous avons cependant un cas particulier pour la salle de la Direction. Dans cette salle, se trouvent quatre employés : le PDG, le PDG adjoint, le directeur des ingénieurs et le directeur de la communication.

- Un VLAN_Dir a été spécifiquement créé pour le PDG et le PDG adjoint.

- Le directeur des ingénieurs est rattaché au VLAN_Inge.
- Le directeur de la communication est rattaché au VLAN_Com.

Cette organisation va permettre à chaque hôte de fonctionner sur un réseau isolé tout en ayant une cohérence avec la structure de l'entreprise. On peut donc dresser le tableau récapitulatif suivant avec la numérotation de chaque VLAN :

Numéro :	Vlan :	Salles	Nombre d'équipements :
10	VLAN_Reu	Salle de reunion	10
20	VLAN_Inge	2 salles d'ingénieurs + Directeur Ingénieur	11
30	VLAN_COM	Salle des chargés de communication + Directeur communication	6
40	VLAN_Serv	Salle des serveurs	4
50	VLAN_Adm	Salle de l'administration	6
60	VLAN_Acc	Secrétariat + Accueil	5
70	VLAN_Dir	PDG + PDG adjoint	2

Figure 6 : Tableau récapitulatif des VLAN du réseau de TechnoLink

On peut désormais ajouter les VLANs sur les Switchs. Pour ce faire, on saisit les commandes suivantes sur chacun des Switchs de l'entreprise :

```
Switch(config)#vlan 10
Switch(config-vlan)# name Vlan_Reu
Switch(config-vlan)#vlan 20
Switch(config-vlan)# name Vlan_Inge
Switch(config-vlan)#vlan 30
Switch(config-vlan)# name Vlan_Com
Switch(config-vlan)#vlan 40
Switch(config-vlan)# name Vlan_Serv
Switch(config-vlan)#vlan 50
Switch(config-vlan)# name Vlan_Adm
Switch(config-vlan)#vlan 60
Switch(config-vlan)# name Vlan_Acc
Switch(config-vlan)#vlan 70
Switch(config-vlan)# name Vlan_Dir
```

Figure 7 : Ajout des VLANs sur les Switchs de l'entreprise TechnoLink

Ensuite, pour les Switchs de salles, nous devons mettre les ports connectés aux hôtes en mode « Access » sur le VLAN spécifique de la salle.

Voici l'exemple des commandes effectuées sur les Switchs Ingénieurs :

```
Switch(config)#interface FastEthernet0/1
Switch(config-if)#
Switch(config-if)#
Switch(config-if)#switchport access vlan 20
Switch(config-if)#
Switch(config-if)#exit
Switch(config)#interface FastEthernet0/2
Switch(config-if)#
Switch(config-if)#
Switch(config-if)#switchport access vlan 20
Switch(config-if)#
Switch(config-if)#exit
Switch(config)#interface FastEthernet0/3
Switch(config-if)#
Switch(config-if)#
Switch(config-if)#switchport access vlan 20
Switch(config-if)#
Switch(config-if)#exit
Switch(config)#interface FastEthernet0/4
Switch(config-if)#
Switch(config-if)#
Switch(config-if)#
Switch(config-if)#switchport access vlan 20
Switch(config-if)#
Switch(config-if)#exit
Switch(config)#interface FastEthernet0/5
Switch(config-if)#
Switch(config-if)#
Switch(config-if)#switchport access vlan 20
```

Figure 8 : Exemple de la configuration en mode Access des ports des Switchs Ingénieurs

Voici un autre exemple sur le Switch de la salle des chargés de communication :

```
Switch(config)#interface FastEthernet0/1
Switch(config-if)#
Switch(config-if)#
Switch(config-if)#switchport access vlan 30
Switch(config-if)#
Switch(config-if)#exit
Switch(config)#interface FastEthernet0/2
Switch(config-if)#
Switch(config-if)#
Switch(config-if)#switchport access vlan 30
Switch(config-if)#
Switch(config-if)#exit
Switch(config)#interface FastEthernet0/3
Switch(config-if)#
Switch(config-if)#
Switch(config-if)#switchport access vlan 30
Switch(config-if)#
Switch(config-if)#exit
Switch(config)#interface FastEthernet0/4
Switch(config-if)#
Switch(config-if)#
Switch(config-if)#switchport access vlan 30
Switch(config-if)#
Switch(config-if)#exit
Switch(config)#interface FastEthernet0/5
Switch(config-if)#
Switch(config-if)#
Switch(config-if)#switchport access vlan 30
Switch(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/6, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/6, changed state to up
```

Figure 9 : Exemple de configuration en mode Access des ports du Switch Comm'

En revanche, sur les autres ports utilisés sur les Switchs (liaison Switch-Switch ou Switch-Routeur), on doit activer le mode « trunk » afin de faire

passer tous les VLAN et assurer l'interconnexion entre les VLANs au sein de notre réseau.

Pour ce faire, on réalise la commande « switchport mode trunk » sur l'interface concernée. Voici un exemple de configuration effectuée sur un Switch central de notre réseau :

```
Switch(config)#interface FastEthernet0/1
Switch(config-if)#
%SYS-5-CONFIG_I: Configured from console by console

Switch(config-if)#switchport mode trunk

Switch(config-if)#
%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

Switch(config-if)#exit
Switch(config)#interface FastEthernet0/2
Switch(config-if)#
Switch(config-if)#switchport mode trunk

Switch(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/2, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/2, changed state to up

Switch(config-if)#exit
Switch(config)#interface FastEthernet0/3
Switch(config-if)#
Switch(config-if)#switchport mode trunk

Switch(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3, changed state to up

Switch(config-if)#exit
```

Figure 10 : Exemple de configuration en mode Trunk du switch «Com-Admi »

2.2) Adressage IPv4 et VLSM

Après avoir créé les VLANs, nous devons nous pencher sur la manière dont nous allons attribuer les plages d'adressage IPv4 à chacun des VLANs pour pouvoir ensuite configurer les hôtes statiques, notre routeur et notre DHCP.

Pour l'adressage de notre réseau, et comme demandé dans le cahier des charges, nous allons utiliser le VLSM (Variable Lenght Subnet Mask), ce qui implique que nous allons faire varier chaque masque de sous réseau en fonction du nombre d'hôtes. Nous avons donc réalisé le tableau suivant :

VLAN	Équipements	Hôtes + GW	Sous-réseau	Passerelle	Plage Utilisable (Hôtes)	Masque	Broadcast
VLAN_Reu	4 PC fixes + 6 portables + 1 AP	12	10.0.0.0/27	10.0.0.1	10.0.0.2 - 10.0.0.30	255.255.255.224	10.0.0.31
VLAN_Ingé	8 PC + 2 impr. + 1 PC Dir	12	10.0.0.32/28	10.0.0.33	10.0.0.34 - 10.0.0.46	255.255.255.240	10.0.0.47
VLAN_Com	4PC + 1 impr. + 1 PC Dir	9	10.0.0.48/28	10.0.0.49	10.0.0.50 - 10.0.0.62	255.255.255.240	10.0.0.63
VLAN_Serv	1 PC admin + 3 serveurs	5	10.0.0.64/29	10.0.0.65	10.0.0.66 - 10.0.0.70	255.255.255.248	10.0.0.71
VLAN_Admin	5 PC + 1 impr.	7	10.0.0.80/28	10.0.0.81	10.0.0.82 - 10.0.0.94	255.255.255.240	10.0.0.95
VLAN_Acc	2 PC accueil + 2 PC secrétariat	5	10.0.0.96/29	10.0.0.97	10.0.0.98 - 10.0.0.102	255.255.255.248	10.0.0.103
VLAN_Dir	2 PC dirigeants	3	10.0.0.104/29	10.0.0.105	10.0.0.106 - 10.0.0.110	255.255.255.248	10.0.0.111

Figure 11 : Tableau récapitulant l'adressage IP des VLANs

Ce tableau résume le nombre d'équipements présents sur chaque VLAN ainsi que les informations clés d'adressage (sous-réseau, passerelle, masque, plage IP, etc.). Il nous permet de planifier les sous-réseaux adaptés à chaque VLANs, d'avoir l'adresse de la passerelle par défaut, et de planifier les plages IP.

Ce tableau nous permet donc d'avoir une vision d'ensemble sur les plages d'adressages que nous allons attribuer à nos VLANs

On obtient ainsi le réseau de TechnoLink suivant :

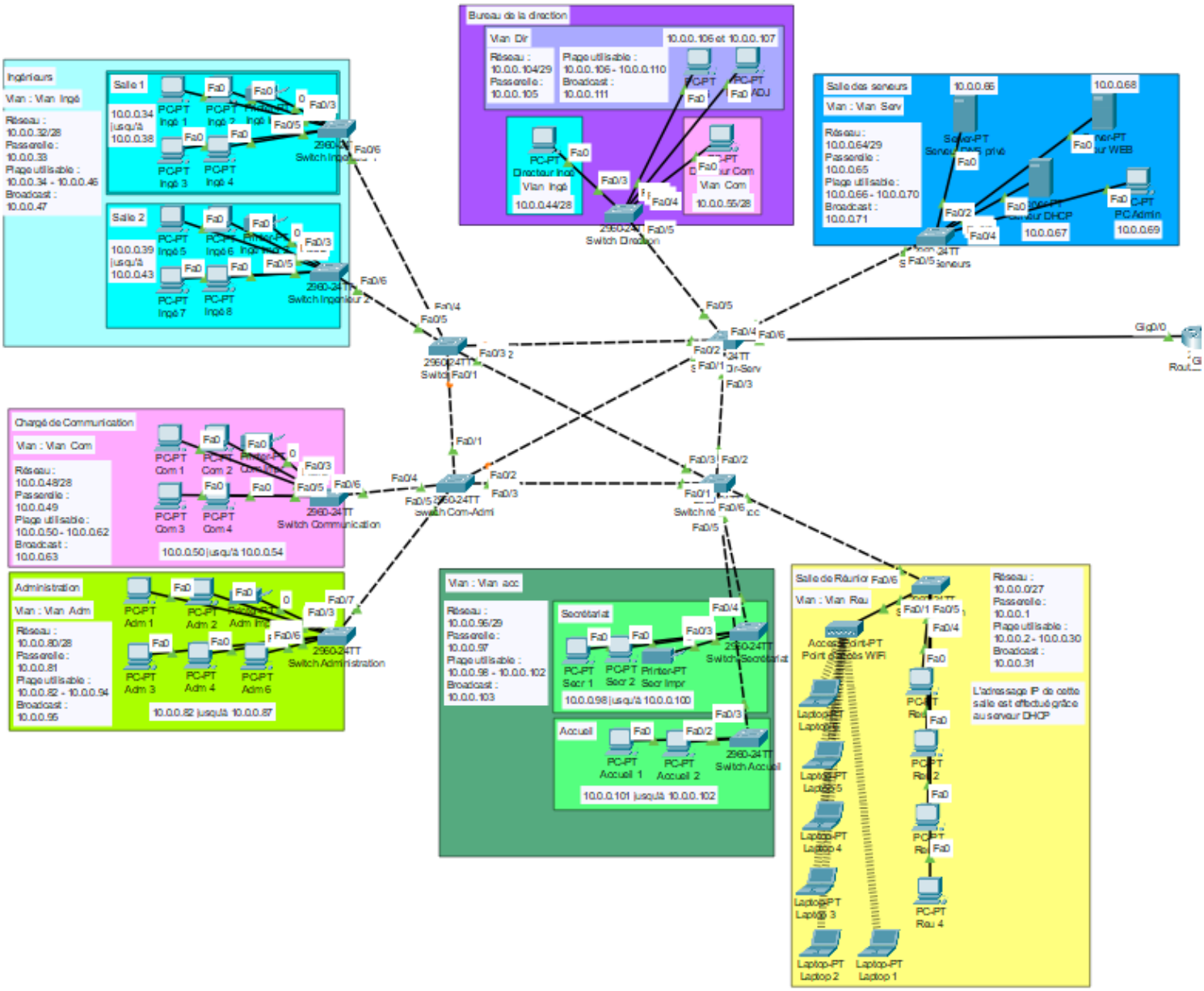

Figure 12 : Représentation du réseau de TechnoLink

On peut donc commencer l'attribution statique des adresses IP sur chacune des salles, sauf la salle de réunion qui sera gérée par le serveur DHCP. L'attribution des adresses IP se fait sur les interfaces de chaque hôte : on saisit l'adresse IP de l'hôte ainsi que son masque puis on lui indique sa passerelle par défaut.

Voici un exemple de configuration IP sur un PC d'Ingénieur :

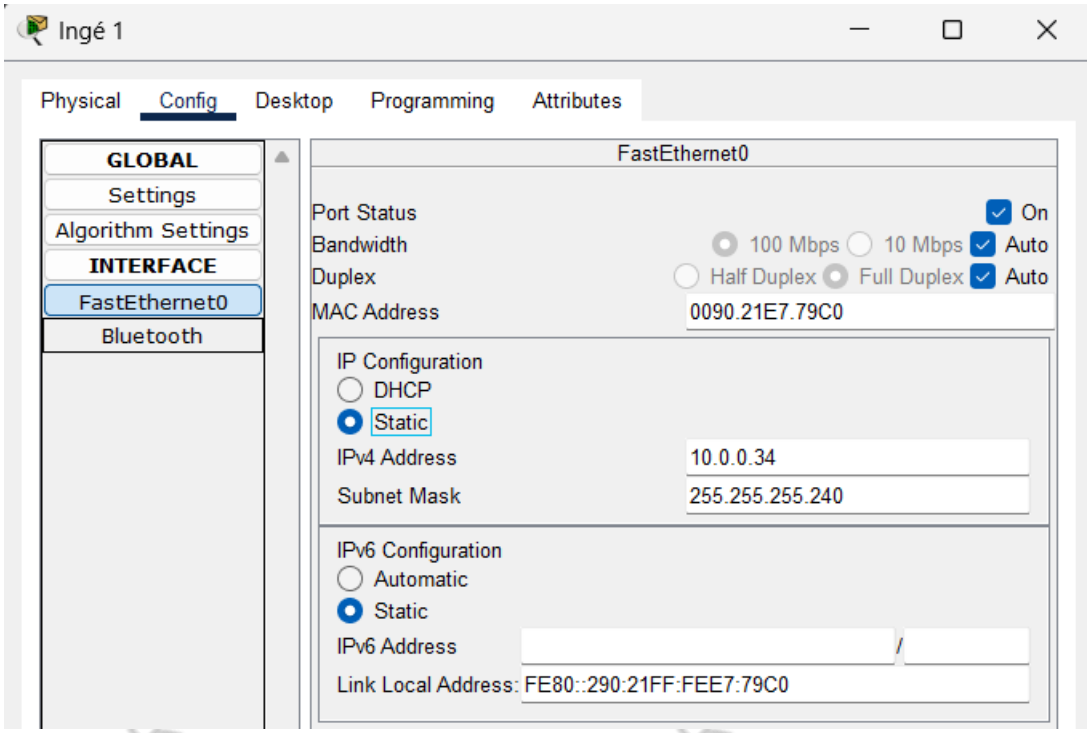

Figure 13 : Exemple de configuration IP statique sur un PC d'ingénieur

On réitère ces étapes sur tous les reste des postes nécessitant un adressage statique en veillant à respecter les plages indiquées dans le tableau vu précédemment (figure 11).

Après avoir fini l'adressage Statique, on doit configurer le routeur et les passerelles par défaut afin d'assurer la communication inter-VLAN et l'accès à l'extérieur du réseau. Cette configuration permettra le bon routage des paquets entre les différents sous-réseaux et assure une connectivité entre tous les postes de TechnoLink.

Afin d'assurer la communication inter-VLAN nous devons donc configurer des sous-interfaces sur le routeur. Chaque sous-interface correspondra à un VLAN spécifique, et sera associée à une adresse IP (passerelle par défaut) définie précédemment dans le tableau d'adressage (figure 13). Pour chaque sous interface, il est également nécessaire de configurer une ligne d'encapsulation « dot1Q » qui permet d'associer la sous-interface au VLAN correspondant.

On a donc la configuration CLI suivante :

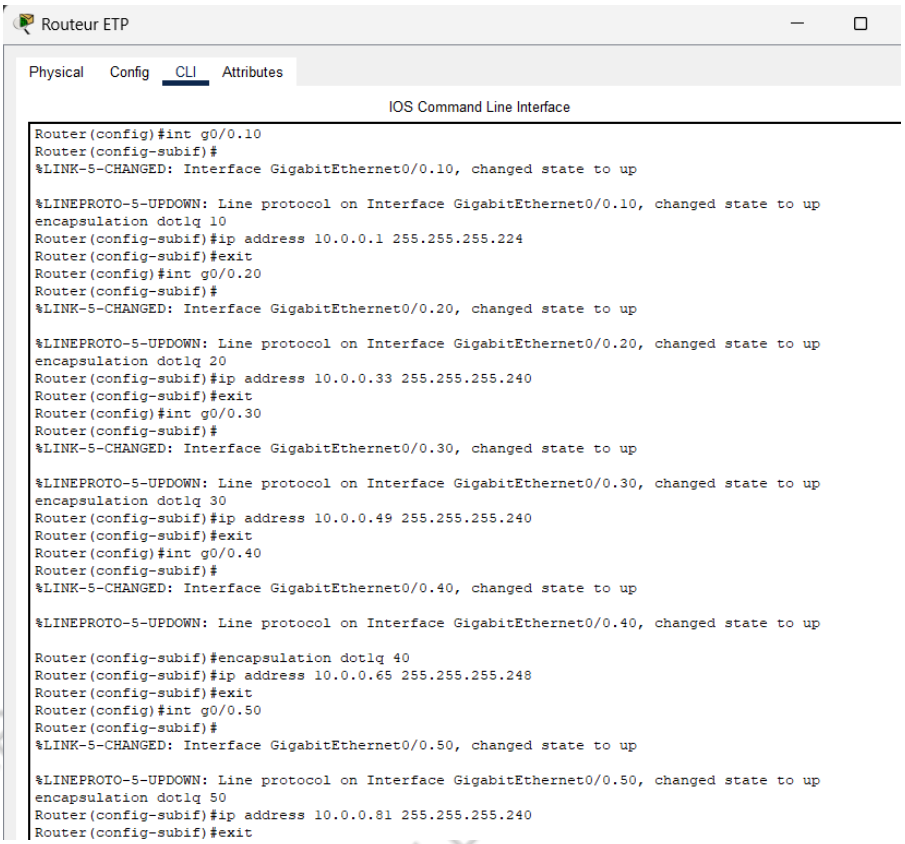

Figure 14 : Configuration des sous-interfaces sur le routeur + encapsulation (photo 1)

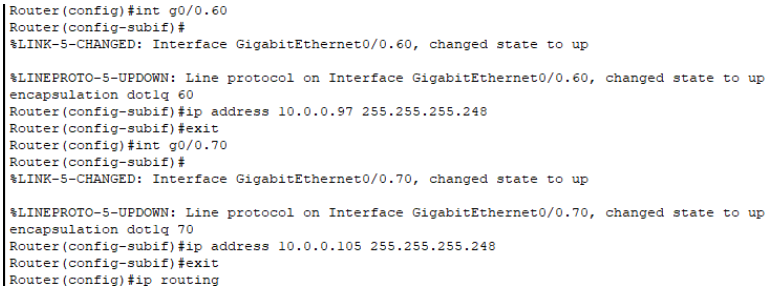

Figure 15 : Configuration des sous-interfaces sur le routeur + encapsulation (photo 2)

Bien sûr, on n'oublie pas la commande « ip routing » afin d'activer le routage sur le routeur.

On peut désormais vérifier notre configuration en essayant un ping depuis un PC de la salle Ingénieur vers un pc du secrétariat. On va donc prendre le pc ingénieur 10.0.0.34 et tenter un ping vers le pc 10.0.0.98 du secrétariat :

```
C:\>ipconfig

FastEthernet0 Connection:(default port)

   Connection-specific DNS Suffix..:
   Link-local IPv6 Address.....: FE80::290:21FF:FEE7:79C0
   IPv6 Address.....: ::
   IPv4 Address.....: 10.0.0.34
   Subnet Mask.....: 255.255.255.240
   Default Gateway.....: ::
                                 10.0.0.33

Bluetooth Connection:

   Connection-specific DNS Suffix..:
   Link-local IPv6 Address.....: ::
   IPv6 Address.....: ::
   IPv4 Address.....: 0.0.0.0
   Subnet Mask.....: 0.0.0.0
   Default Gateway.....: ::
                                 0.0.0.0

C:\>ping 10.0.0.98

Pinging 10.0.0.98 with 32 bytes of data:

Request timed out.
Reply from 10.0.0.98: bytes=32 time=3ms TTL=127
Reply from 10.0.0.98: bytes=32 time=10ms TTL=127
Reply from 10.0.0.98: bytes=32 time=1ms TTL=127

Ping statistics for 10.0.0.98:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 10ms, Average = 4ms
```

Figure 16 : Test de ping inter-VLAN

3) Configuration des services internes de l'entreprise

3.1) Configuration des serveurs internes

Maintenant que notre adressage IPv4 est fait, nous allons mettre en place les différents services utilisés au sein de l'entreprise. Nous allons donc configurer le serveur WEB, le serveur DNS et le serveur DHCP.

Commençons tout d'abord par leur affecter leur IPv4 statique, en respectant la plage d'adressage du VLAN_Serv :

Serveur DNS :

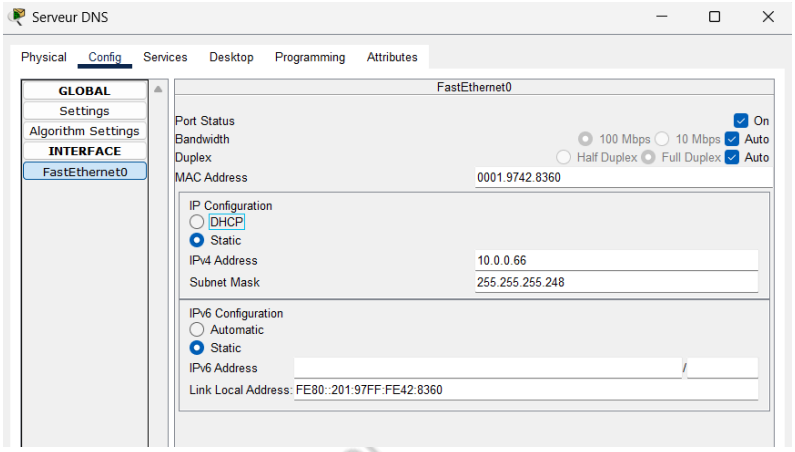

Figure 17 : Adressage IPv4 statique du serveur DNS privé

Serveur WEB :

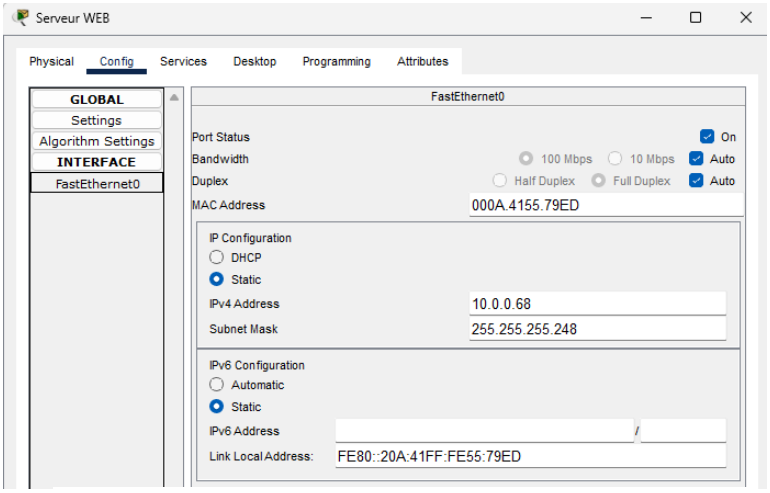

Figure 18 : Adressage IPv4 du serveur Intranet de TechnoLink

Serveur DHCP :

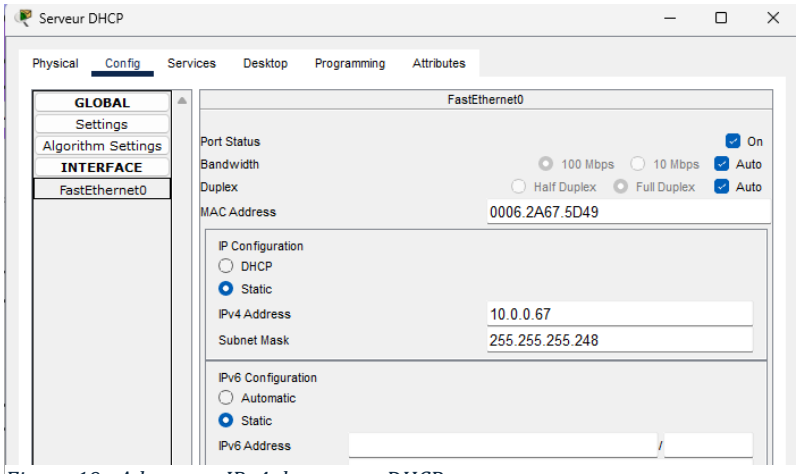

Figure 19 : Adressage IPv4 du serveur DHCP

3.2) Mise en place des services internes

On peut donc commencer la configuration des différents services :

Serveur WEB :

Pour configurer le service WEB, on active donc le service http et on saisit notre code HTML et CSS dans l'index.html présent dans les fichiers du serveur.

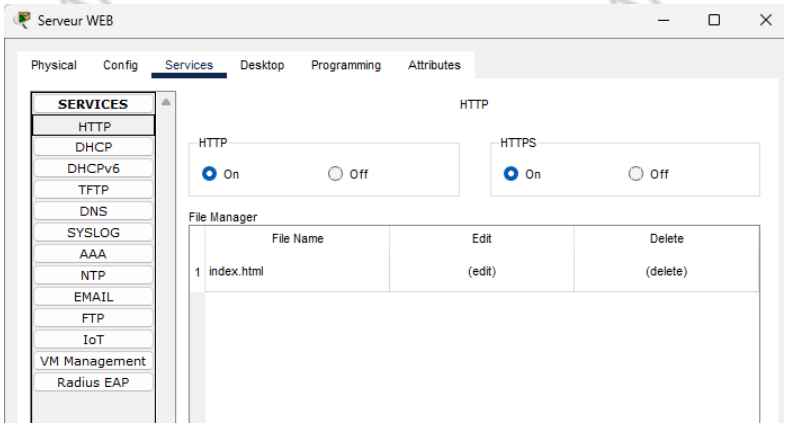

Figure 20 : Activation du service HTTP/HTTPS sur le serveur WEB privé de TechnoLink

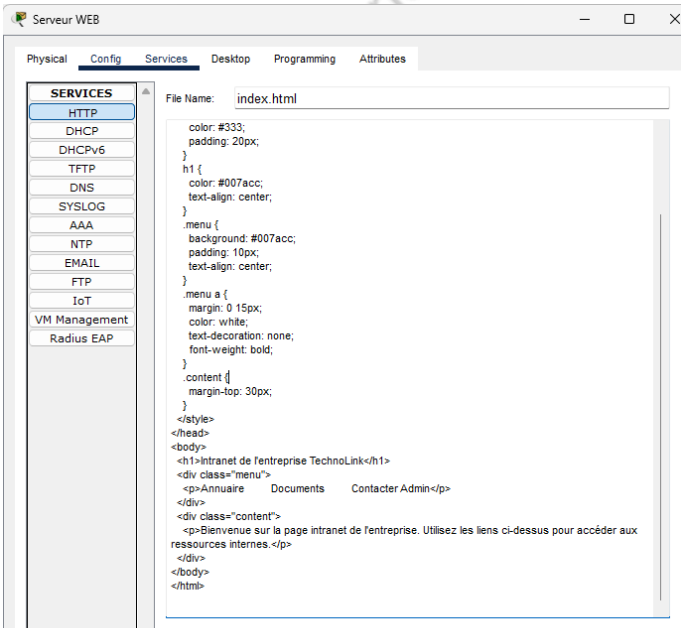

Figure 21 : Saisie du code HTML de la page intranet de TechnoLink

On peut vérifier que notre serveur WEB fonctionne en tapant l'adresse IP de notre serveur dans la barre de recherche d'un PC du réseau. Par exemple depuis le PC du PDG :

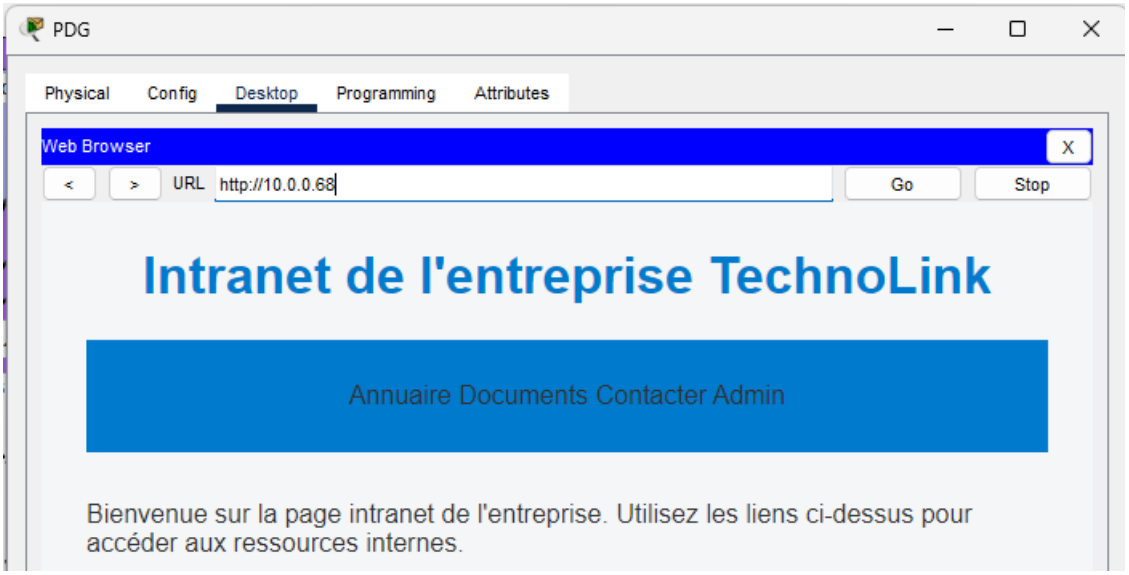

Figure 22 : Vérification du serveur Intranet de TechnoLink depuis le PC du PDG

Serveur DHCP :

Afin de configurer le service DHCP, on active le service sur le serveur puis on configure un pool DHCP pour notre salle de réunion. Grâce au tableau des adressages, on peut définir la passerelle par défaut, le serveur DNS, la première adresse IP du réseau, le masque de sous-réseau ainsi que le nombre maximum d'utilisateurs. Voici donc la configuration du « Pool_Reu » :

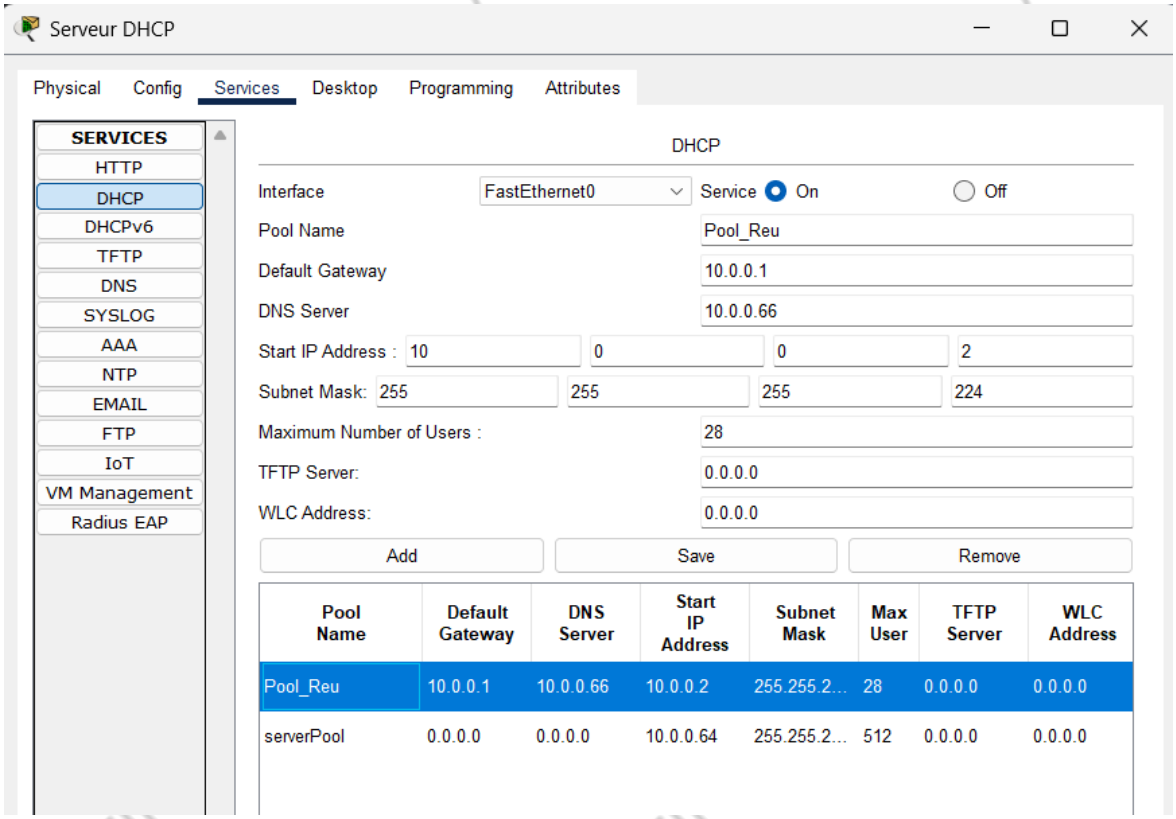

Figure 24 : Configuration du Pool DHCP "Pool_Reu" donnant la configuration IPv4 des PC présents dans la salle de réunion

A cela, il faut ajouter une ligne dans le CLI du routeur de l'entreprise pour que le DHCP fonctionne dans le VLAN_Reu :

```
Router(config)#int g0/0.10
Router(config-subif)#ip helper-address 10.0.0.67
Router(config-subif)#exit
Router(config)#exit
```

Figure 23 : Commande du routeur d'entreprise pour que le DHCP fonctionne dans le VLAN_Reu

Cette ligne est saisie dans la sous-interface 0.10 du routeur correspondant au VLAN_Reu et permet d'indiquer l'adresse IP du serveur DHCP à contacter en cas de demande de configuration via DHCP.

On peut ainsi vérifier le fonctionnement de notre DHCP en prenant un PC de la salle de réunion et en demandant une configuration IP via DHCP :

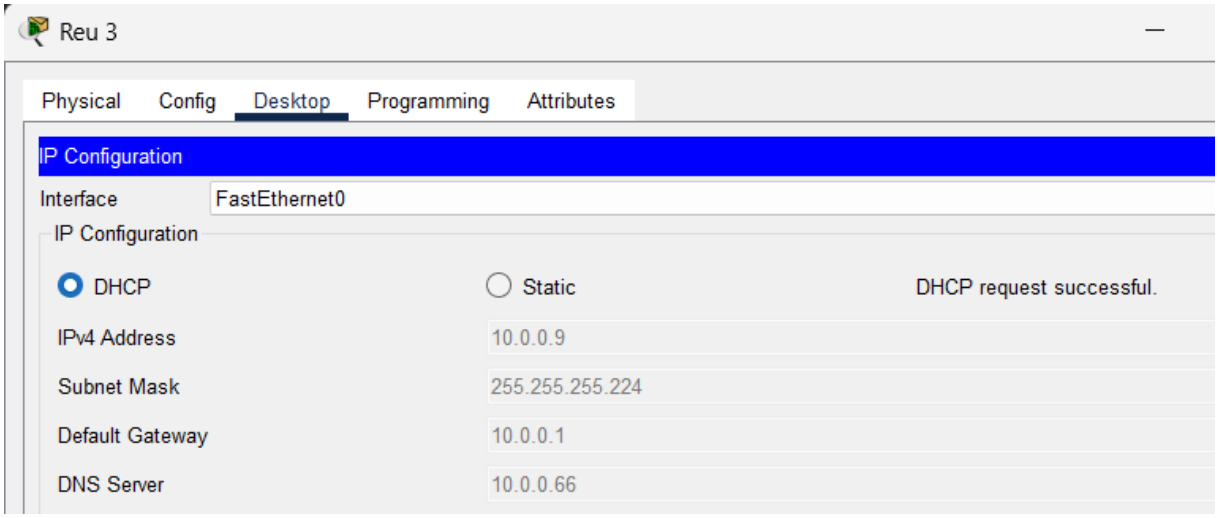

Figure 25 : Demande de configuration IPv4 via DHCP depuis un PC de la salle de réunion

On voit donc que le PC 3 présent dans la salle de réunion obtient bien une adresse IP cohérente avec la plage d'adresse attribué au VLAN_REU.

Serveur DNS :

La configuration du serveur DNS sera réalisée une fois l'ensemble du réseau, de la DMZ et du FAI configurés. Cela nous permettra d'effectuer une configuration complète incluant les redirections, les délégations de zones, ainsi que les tests de bon fonctionnement.

4) Mise en place de la DMZ

4.1) Conception et configuration physique de la DMZ

Nous allons donc ajouter les éléments nécessaires pour la DMZ, on relie donc deux serveurs à un « Switch DMZ », puis on relie ce Switch à une nouvelle interface de notre routeur d'entreprise, l'interface G0/1. On obtient donc le câblage suivant :

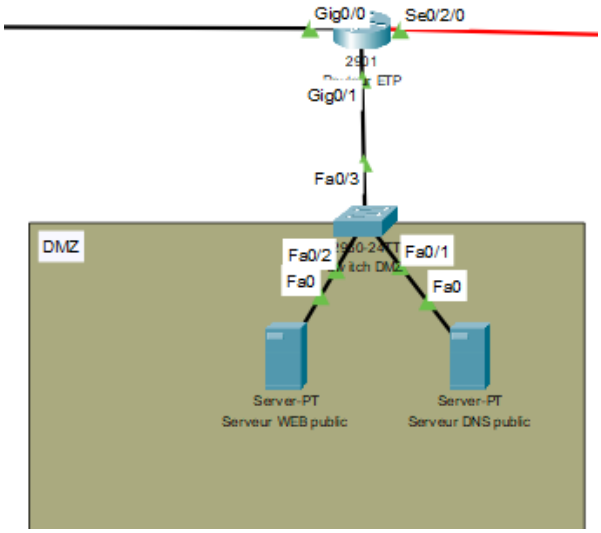

Figure 26 : Ajout de la DMZ sur une interface (G0/1) de notre routeur d'entreprise

4.2) Configuration logique de la DMZ

Puis de la même manière que pour le réseau local de TechnoLink, nous allons créer un VLAN dédié à la DMZ, lui attribuer un sous-réseau spécifique et y intégrer les serveurs concernés.

Commençons donc par le VLAN, nous allons donc créer un vlan 80 qui sera composé de deux serveurs uniquement. En suivant le même principe que le tableau d'adressage des VLAN du réseau local, on peut établir les informations du VLAN 80 de la DMZ que nous appellerons VLAN_DMZ :

VLAN	Équipements	Hôtes + GW	Sous-réseau	Passerelle	Plage Utilisable (Hôtes)	Masque	Broadcast
VLAN_DMZ	Gateway + 2 serveurs	3	10.1.0.0/29	10.1.0.1	10.1.0.2 - 10.1.0.6	255.255.255.248	10.1.0.7

Figure 27 : Adressage IP du VLAN 80 de la DMZ

Maintenant que nous avons l'adressage de notre VLAN, on peut créer la sous-interface G0/1.80 sur notre routeur qui sera la passerelle par défaut de notre VLAN.

On peut ensuite ajouter le vlan sur le Switch DMZ :

```
Switch(config)#vlan 80
Switch(config-vlan)# name VLAN_DMZ
```

Figure 29 : Ajout du VLAN_DMZ sur le Switch DMZ

```
interface GigabitEthernet0/1.80
 encapsulation dot1Q 80
 ip address 10.1.0.1 255.255.255.248
```

Figure 28 : Configuration de la sous-interface du VLAN_DMZ sur le routeur d'entreprise

On peut désormais configurer l'adressage IPv4 des serveurs. Pour cela on utilise les adresses IP présentes dans la plage d'adresses utilisables de notre tableau. On obtient ainsi la configuration suivante :

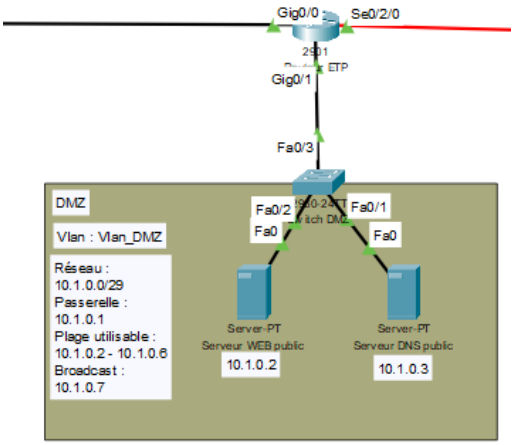

Figure 30 : Adressage des serveurs présents dans la DMZ

4.3) Configuration des services accessibles publiquement

Maintenant que notre DMZ est complètement configurée, on doit mettre en place les services publics qui y sont hébergé.

Commençons par le serveur WEB public, la configuration globale reste la même. On active le service HTTP/HTTPs puis on crée le site HTML de notre entreprise et on l'ajoute sur le fichier index.html présent dans le gestionnaire de fichiers de notre serveur WEB.

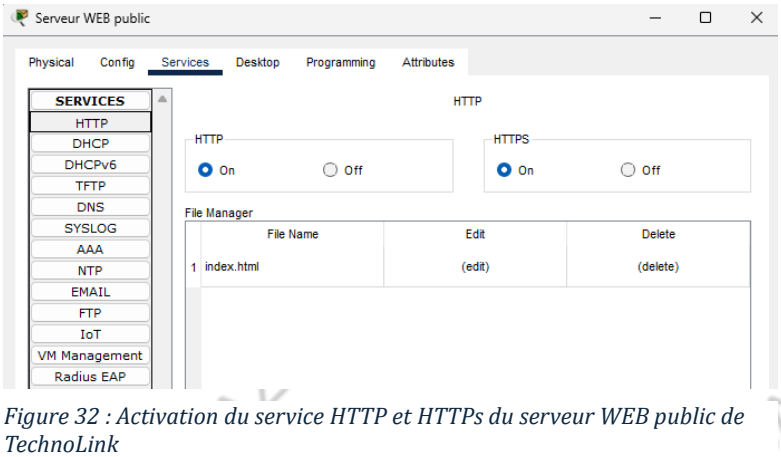

Figure 32 : Activation du service HTTP et HTTPs du serveur WEB public de TechnoLink

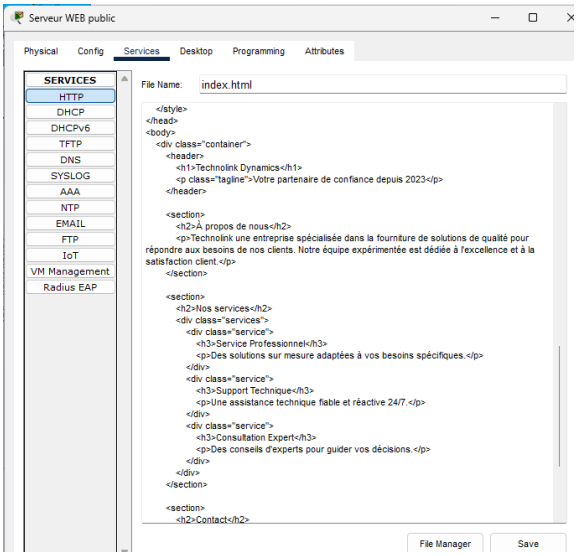

Figure 31 : Extrait du code HTML/CSS du site internet public de TechnoLink

On peut vérifier que notre site web fonctionne en essayant d'y accéder depuis un pc du réseau local. Pour ce faire, nous allons prendre le PC du PDG et nous allons accéder au site web en saisissant l'adresse IP du serveur.

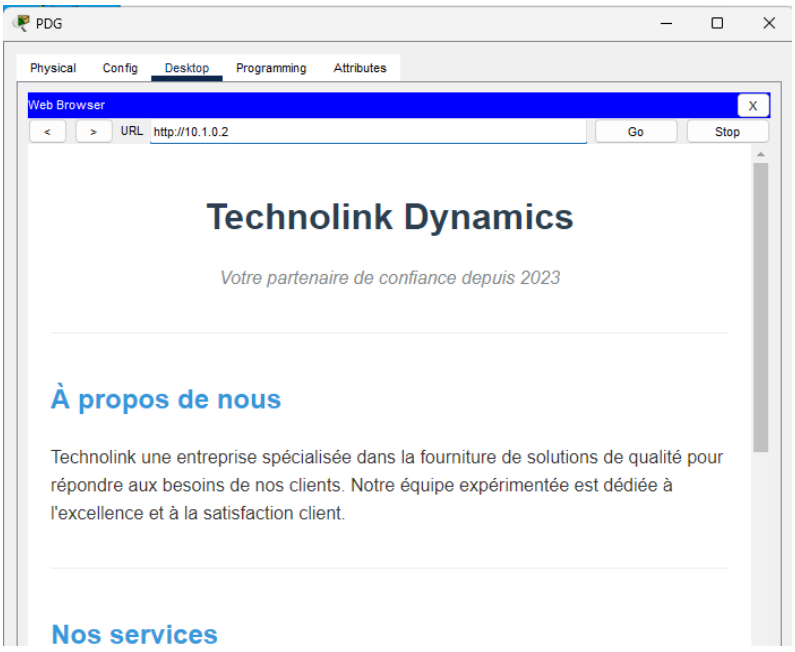

Figure 33 : Vérification du serveur WEB public de TechnoLink depuis le PC du PDG

On voit donc par cette capture que le serveur WEB public de TechnoLink fonctionne parfaitement.

Serveur DNS :

De même que pour le Serveur DNS privé, la configuration du serveur DNS sera réalisée une fois l'ensemble du réseau, de la DMZ et du FAI configurés. Cela nous permettra d'effectuer une configuration complète incluant les redirections, les délégations de zones, ainsi que les tests de bon fonctionnement.

5) Connexion au réseau externe (FAI)

5.1) Mise en place de la connectivité vers le FAI

Maintenant que le réseau de l'entreprise a été correctement configuré, nous allons procéder à la mise en place du Fournisseur d'Accès Internet (FAI) Orange. Pour cela, nous commencerons par configurer les interfaces publiques entre le routeur de l'entreprise et celui du FAI. Ensuite, nous procéderons à la configuration des serveurs et du client, conformément aux exigences du cahier des charges. Enfin, nous mettrons en place les services sur chacun des serveurs, puis nous effectuerons les tests de fonctionnement de la zone FAI.

Nous allons donc nous pencher dans un premier temps sur le réseau public présente entre le routeur de l'entreprise et celui du FAI. Nous savons que dans ce réseau, seuls deux équipements seront présents, nos deux Routeurs. Nous avons donc choisi le réseau publique 203.0.113.0 dont le masque de sous-réseau sera 255.255.255.252 soit le réseau 203.0.113.0/30. Ceci nous permet donc de configurer deux hôtes qui seront nos deux Routeurs.

On commence donc par configurer l'interface publique de notre routeur qui sera branchée en Serial, donc sur le port Serial0/2/0.

```
Router(config)#interface Serial0/2/0
Router(config-if)#ip address 203.0.113.2 255.255.255.252
Router(config-if)#no shutdown
```

Figure 34 : Configuration IPv4 de l'interface publique du routeur de l'entreprise

Nous devons aussi ajouter une route par défaut sur le routeur de l'entreprise vers le routeur du FAI avec la commande :
ip route 0.0.0.0 0.0.0.0 203.0.113.1

On continue par la configuration de l'interface du routeur FAI qui sera reliée à notre routeur d'entreprise.

```
Router(config)#interface Serial0/2/0
Router(config-if)#ip address 203.0.113.1 255.255.255.252
```

Figure 35 : Configuration IPv4 de l'interface publique du routeur FAI reliée au routeur de l'entreprise

5.2) Création et organisation du réseau du FAI

On peut désormais passer à la mise en place de la partie FAI en respectant les éléments du cahier des charges. Pour cela, nous allons devoir établir le réseau public dans lequel seront adressé les équipements du FAI. Nous avons ainsi pris le réseau 198.51.100.0 et le masque 255.255.255.0 soit 198.51.100.0/24. Nous avons choisi 198.51.100.1 comme passerelle par défaut, 198.51.100.10 pour le serveur WEB, 198.51.100.20 pour le serveur DNS d'Orange, 198.51.100.30 pour le client et 198.51.100.40 pour le serveur DNS racine (.com). Ce qui nous donne la zone suivante :

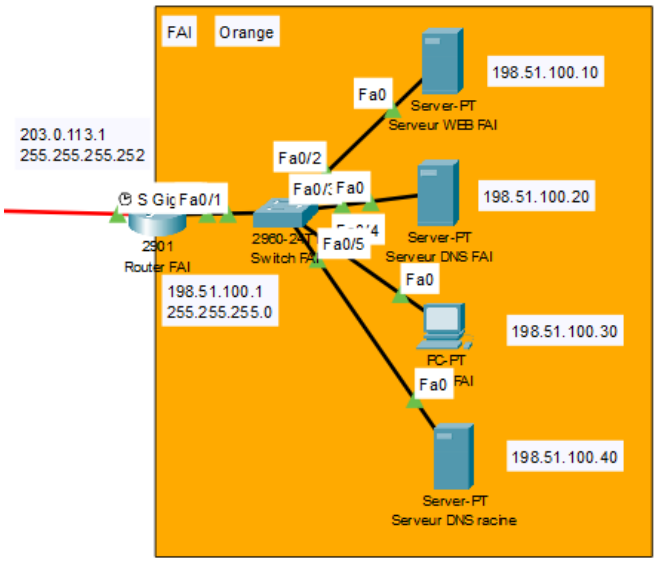

Figure 36 : Zone du FAI avec l'adressage choisi

5.3) Mise en service des équipements du FAI

Nous allons désormais passer à la mise en place des services et de équipements présents dans le FAI.

Client FAI :

De la même manière que nous avons fait l'adressage statique de nos réseaux dans notre entreprise. Il nous suffit de configurer l'IP du client indiqué précédemment, puis d'y préciser sa passerelle par défaut (198.51.100.1) ainsi que son serveur DNS (198.51.100.20). Pour vérifier le fonctionnement de notre client, on effectue un ping sur sa passerelle par défaut :

```
Pinging 198.51.100.1 with 32 bytes of data:

Reply from 198.51.100.1: bytes=32 time<1ms TTL=255
Reply from 198.51.100.1: bytes=32 time<1ms TTL=255
```

Figure 37 : Ping de la passerelle par défaut depuis le client FAI

Le client est donc bien configuré.

Serveur WEB :

Encore une fois, la configuration se fait de la même manière que sur les serveurs Web de l'entreprise il suffit d'adapter le code HTML/CSS pour qu'il soit cohérent.

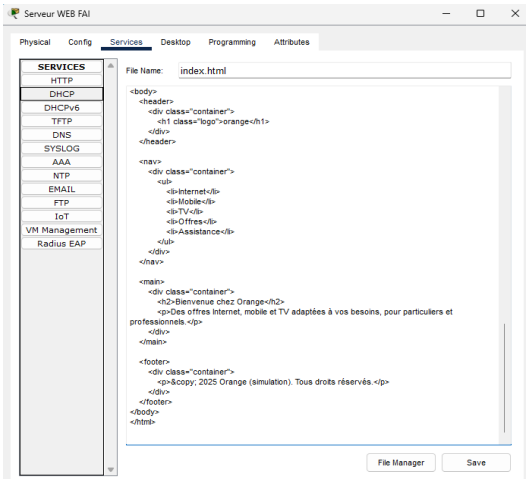

Figure 39 : Extrait du code HTML/CSS du site web simulé d'orange (FAI)

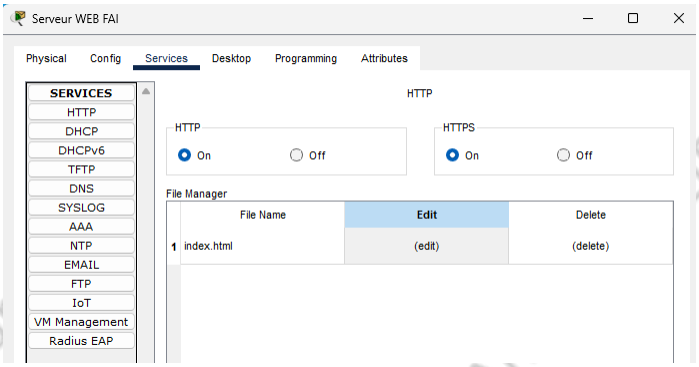

Figure 38 : Activation du service HTTP et HTTPs sur le serveur WEB du FAI

On peut ainsi vérifier le fonctionnement de notre site web en saisissant l'IP du Serveur Web sur notre client FAI :

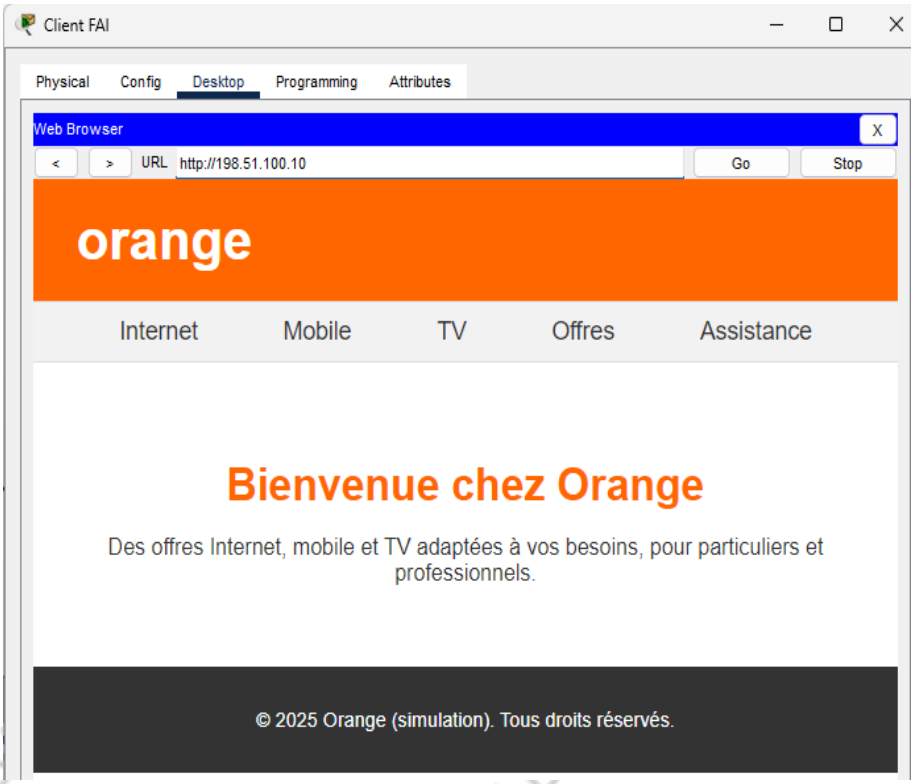

Figure 40 : Vérification du fonctionnement du site WEB du FAI depuis le client FAI

Serveurs DNS :

La configuration des serveur DNS sera réalisée une fois l'ensemble du réseau, de la DMZ et du FAI configurés. Cela nous permettra d'effectuer une configuration complète incluant les redirections, les délégations de zones, ainsi que les tests de bon fonctionnement.

6) Configuration avancée : NAT et PAT

Dans le but de permettre à notre réseau privé d'entreprise de communiquer avec le réseau public, il est nécessaire de mettre en place un mécanisme de NAT (Network Address Translation), accompagné d'une redirection de ports. Le NAT permet d'associer les adresses IP privées internes à une adresse IP publique, facilitant ainsi l'accès à Internet. La redirection de ports, quant à elle, permet de diriger les requêtes entrantes vers les services internes appropriés, dans notre cas le serveur WEB et DNS public de l'entreprise, tout en assurant leur accessibilité depuis l'extérieur.

6.1) Configuration du NAT

Tout d'abord, pour configurer le NAT, nous allons reprendre l'ensemble de nos sous-interfaces sur le routeur, y compris celle de la DMZ, puis ajouter la ligne « ip nat inside » à chacune.

```
interface GigabitEthernet0/0.10
 encapsulation dot1Q 10
 ip address 10.0.0.1 255.255.255.224
 ip helper-address 10.0.0.67
 ip nat inside
!
interface GigabitEthernet0/0.20
 encapsulation dot1Q 20
 ip address 10.0.0.33 255.255.255.240
 ip nat inside
!
interface GigabitEthernet0/0.30
 encapsulation dot1Q 30
 ip address 10.0.0.49 255.255.255.240
 ip nat inside
```

Figure 41 : Exemple de 3 sous-interfaces ayant la mention "ip nat inside"

Ensuite, nous allons créer une ACL (Access Control List) afin d'autoriser l'ensemble des réseaux associés à nos sous-interfaces, en utilisant des masques inversés. On identifiera cette ACL par le nombre 99.

```
Router(config)#access-list 99 permit 10.0.0.0 0.0.0.31
Router(config)#access-list 99 permit 10.0.0.32 0.0.0.15
Router(config)#access-list 99 permit 10.0.0.48 0.0.0.15
Router(config)#access-list 99 permit 10.0.0.64 0.0.0.7
Router(config)#access-list 99 permit 10.0.0.80 0.0.0.15
Router(config)#access-list 99 permit 10.0.0.96 0.0.0.7
Router(config)#access-list 99 permit 10.0.0.104 0.0.0.7
Router(config)#access-list 99 permit 10.1.0.0 0.0.0.7
```

Figure 43 : Lignes CLI permettant de créer l'ACL contenant les réseaux associés à nos sous interfaces

Cette ACL sera ensuite utilisée pour spécifier les adresses IP internes autorisées à être traduites par le NAT. Nous devons donc ajouter la commande suivante afin d'activer la traduction des adresses privées vers l'adresse publique de l'interface serial0/2/0, en mode surcharge (overload), ce qui permet à plusieurs hôtes internes de partager une seule adresse IP publique :

```
Router(config)#ip nat inside source list 99 interface Serial0/2/0 overload
```

Figure 42 : Commande permettant l'activation de la traduction des adresses privées vers l'adresse publique du routeur de l'entreprise

6.2) Configuration de la redirection de ports (PAT)

Nous allons maintenant mettre en place la redirection de ports afin que les services hébergés dans la DMZ soient accessibles depuis l'extérieur (Internet). Pour ce faire, nous allons utiliser le mécanisme de PAT (Port Address Translation), qui permet d'associer un port public de l'adresse IP du routeur à une adresse IP et un port interne spécifiques. Concrètement, cela consiste à rediriger les requêtes externes reçues sur un certain port vers l'adresse IP privée du serveur correspondant dans la DMZ. Cette configuration se fait à l'aide des commandes suivantes, dans lesquelles nous précisons le protocole (TCP ou UDP), l'IP privée du serveur, le port interne, ainsi que le port public utilisé sur l'interface extérieure.

```
Router(config)#ip nat inside source static tcp 10.1.0.2 80 203.0.113.2 80
Router(config)#ip nat inside source static udp 10.1.0.3 53 203.0.113.2 53
```

Figure 44 : Commandes permettant la redirection de ports sur le routeur de l'entreprise

La première commande permet de rediriger les requêtes HTTP reçues sur le port 80 de l'adresse publique 203.0.113.2 vers le serveur web local situé à l'adresse 10.1.0.2.

La seconde commande redirige les requêtes DNS envoyées en UDP sur le port 53 vers le serveur DNS interne 10.1.0.3.

7) Mise en service des serveurs DNS

7.1) Configuration des serveurs DNS

Maintenant que notre réseau d'entreprise, notre DMZ et notre FAI sont bien configurés, nous pouvons passer à la configuration des serveurs DNS. Nous allons donc avoir à configurer le serveur DNS privé et public de l'entreprise, le serveur DNS du FAI Orange et nous allons ajouter un serveur DNS racine (.com).

Nous allons donc devoir effectuer des délégations et des redirections entre chaque serveur DNS pour que chaque site internet puisse être accéder par son nom de domaine. Nous avons ainsi les configurations suivantes :

Serveur DNS privé :

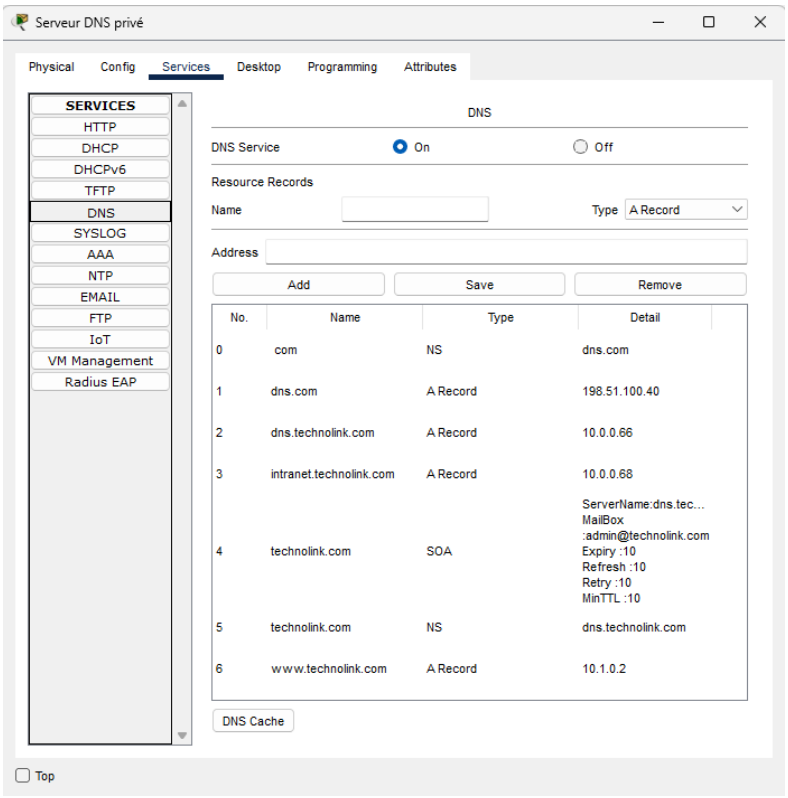

Figure 45 : Configuration DNS du serveur privé de l'entreprise

Dans cette configuration, on retrouve les informations du DNS privé de l'entreprise (dns.technolink.com), le nom de domaine que porte l'intranet (intranet.technolink.com) et le nom de domaine du site web public de l'entreprise (www.technolink.com). Les informations du DNS racine sont également présentes et pointent vers son IP dans la zone du FAI (dns.com – 198.51.100.40).

Serveur DNS public :

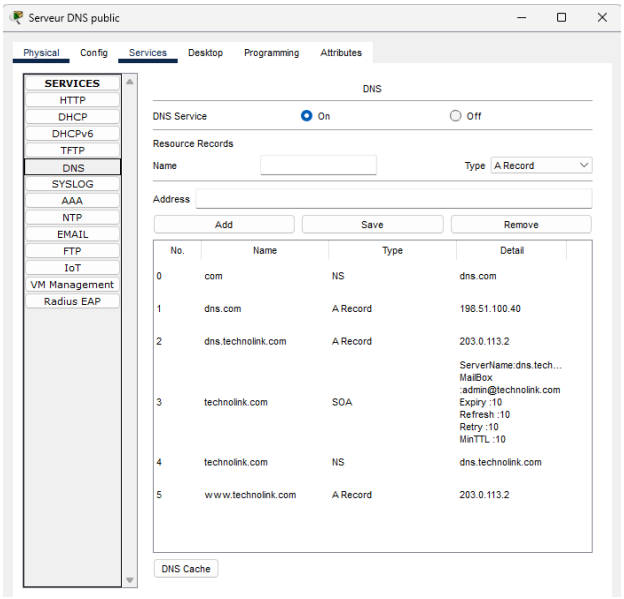

Figure 46 : Configuration du DNS public de l'entreprise

Dans cette configuration, on retrouve les informations du DNS public de l'entreprise (dns.technolink.com), le nom de domaine utilisé pour le site web public (www.technolink.com) ainsi que le nom de domaine associé au DNS racine (dns.com – 198.51.100.40). Le serveur DNS principal est configuré pour gérer la zone technolink.com, avec une adresse publique (203.0.113.2) attribuée à la fois au domaine principal et à son sous-domaine web. Les informations du DNS racine sont également présentes et orientent les requêtes vers le serveur DNS .com du FAI.

Serveur DNS racine :

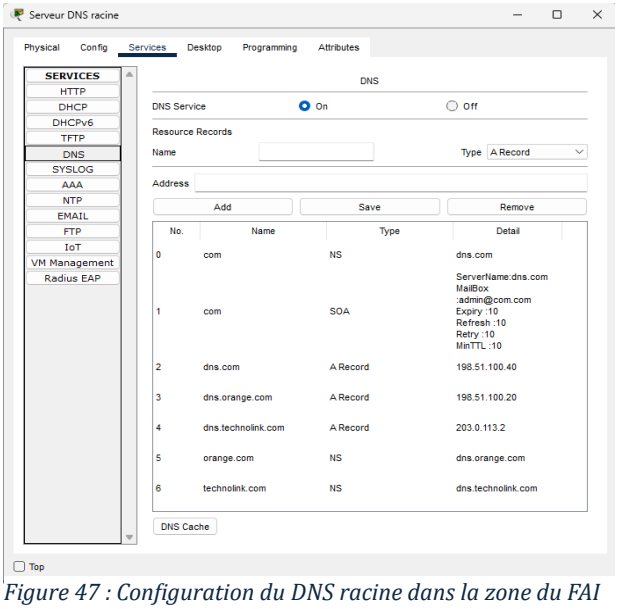

Figure 47 : Configuration du DNS racine dans la zone du FAI

Dans cette configuration, on retrouve les informations du serveur DNS racine utilisé pour diriger les requêtes vers les serveurs de noms responsables des domaines publics. Le domaine com est géré par ce serveur dns.com, dont l'adresse IP est 198.51.100.40. Des enregistrements de type A sont présents pour rediriger les requêtes vers les serveurs DNS publics des fournisseurs, comme dns.orange.com (198.51.100.20) pour le domaine orange.com, et dns.technolink.com (203.0.113.2) pour le domaine technolink.com. Cette configuration permet d'assurer la résolution hiérarchique des noms de domaine à partir de la racine jusqu'aux serveurs DNS des différentes entreprises.

Serveur DNS FAI (orange) :

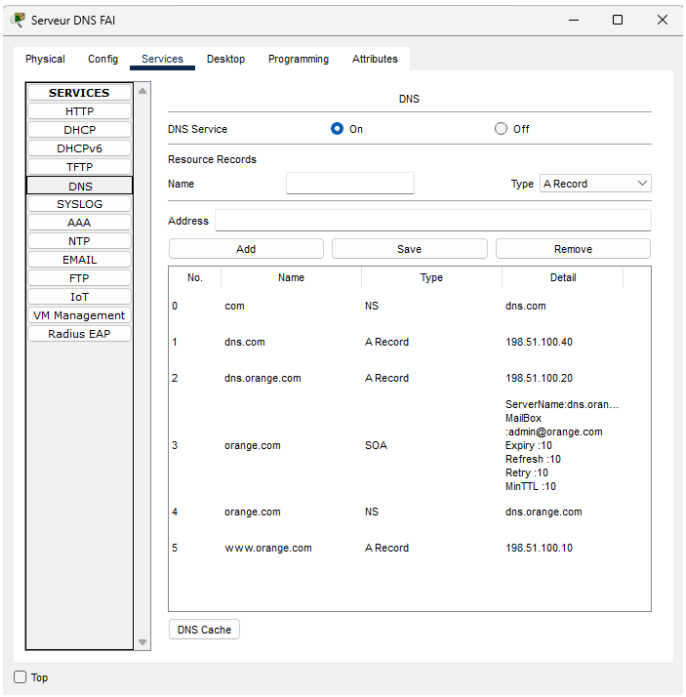

Figure 48 : Configuration du DNS FAI Orange

Dans cette configuration, on retrouve les informations du serveur DNS du fournisseur d'accès à Internet (FAI). Le domaine orange.com est géré par le serveur dns.orange.com, dont l'adresse IP est 198.51.100.20. Ce serveur DNS est responsable de la résolution des noms associés à l'infrastructure du FAI, notamment le site web public www.orange.com accessible à l'adresse 198.51.100.10. On y retrouve également un enregistrement NS pour le domaine com, pointant vers dns.com, et un enregistrement SOA qui définit les paramètres d'autorité du domaine orange.com, incluant l'adresse de contact de l'administrateur (admin@orange.com).

7.2) Vérification du fonctionnement des serveurs DNS

La configuration des serveurs DNS ayant été effectuée, nous pouvons vérifier leurs fonctionnements. Pour cela, nous allons tenter d'accéder à nos différents sites WEB depuis un hôte de l'entreprise et depuis le client FAI.

Nous allons donc commencer par l'hôte dans l'entreprise.

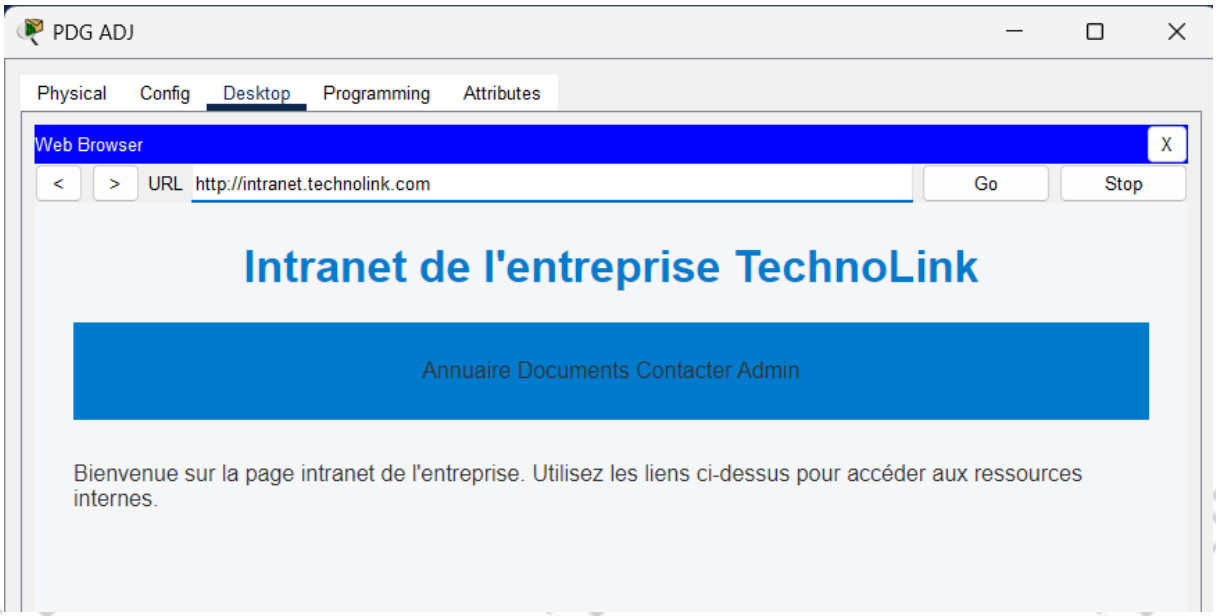

Figure 49 : Vérification du fonctionnement du site Intranet de TechnoLink depuis le PC du PDG ADJ

Nous voyons donc que le site intranet est bien accessibles par son nom de domaine.

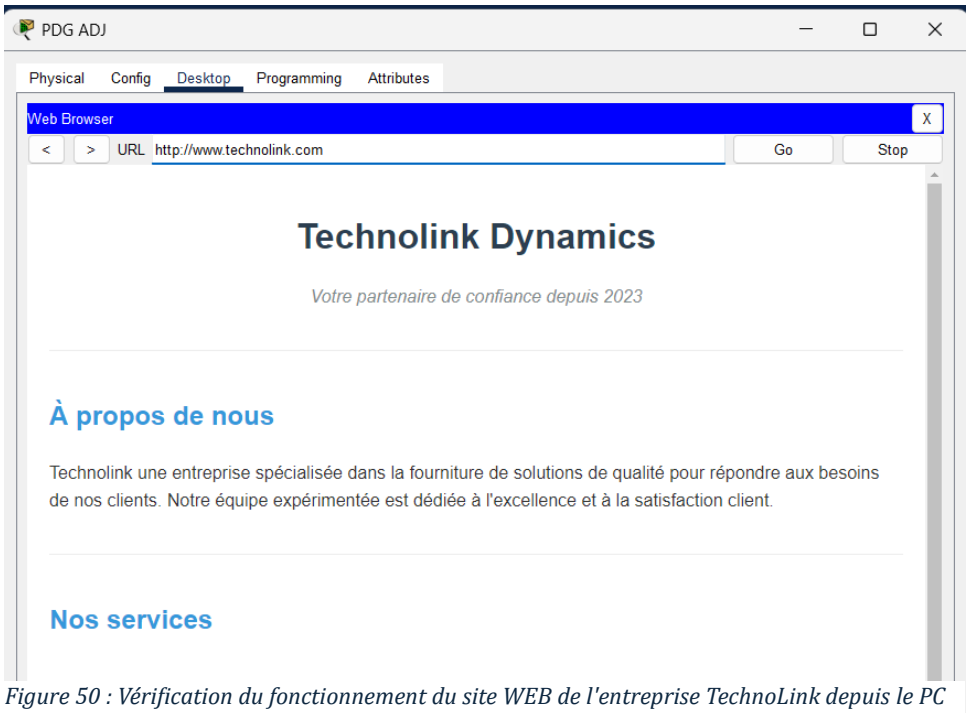

Figure 50 : Vérification du fonctionnement du site WEB de l'entreprise TechnoLink depuis le PC du PDG ADJ

Ainsi, on voit que l'accessibilité du site web public de l'entreprise par son nom de domaine fonctionne.

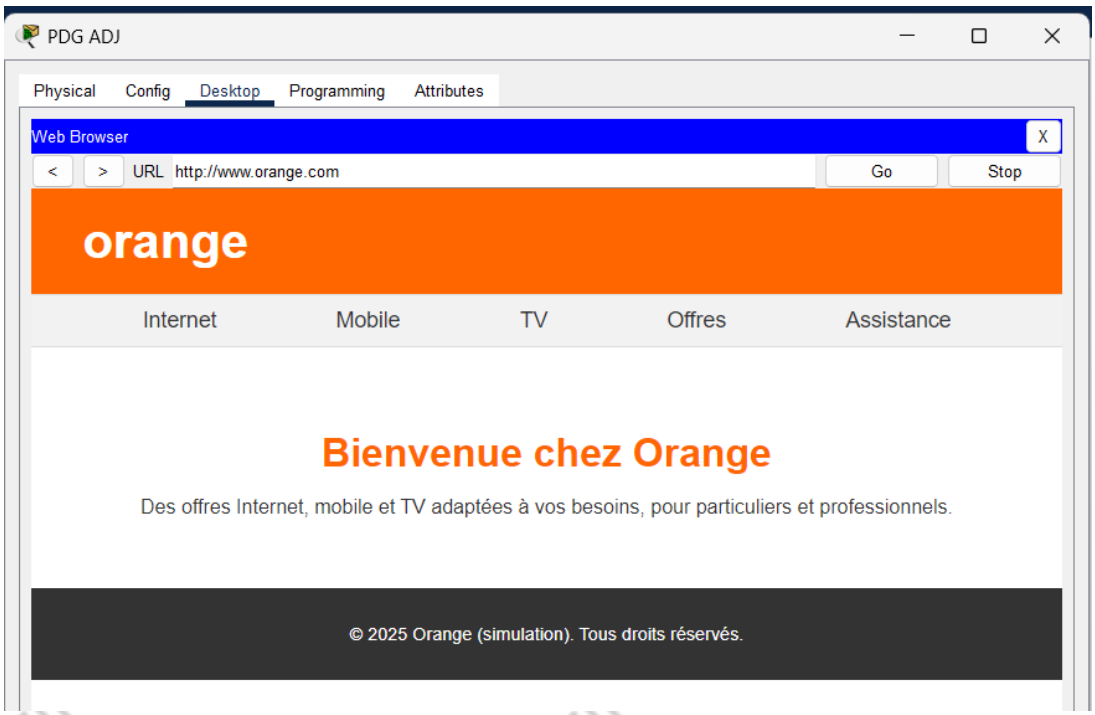

Figure 51 : Vérification du fonctionnement du site du FAI (Orange) depuis le PC du PDG ADJ

On voit donc que le site web d'orange est accessible par son nom de domaine.

On peut maintenant vérifier le fonctionnement de ces sites web depuis le client du FAI.

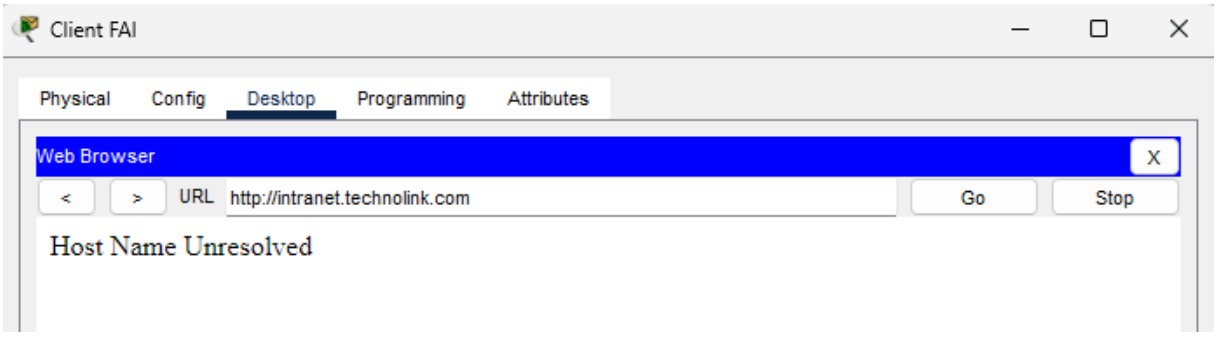

Figure 52 : Vérification du serveur Intranet de l'entreprise depuis le client FAI

Sur cette capture, on voit «Host Name Unresolved » ce qui est tout à fait normal puisque le site web intranet n'est accessible que depuis le réseau local de l'entreprise.

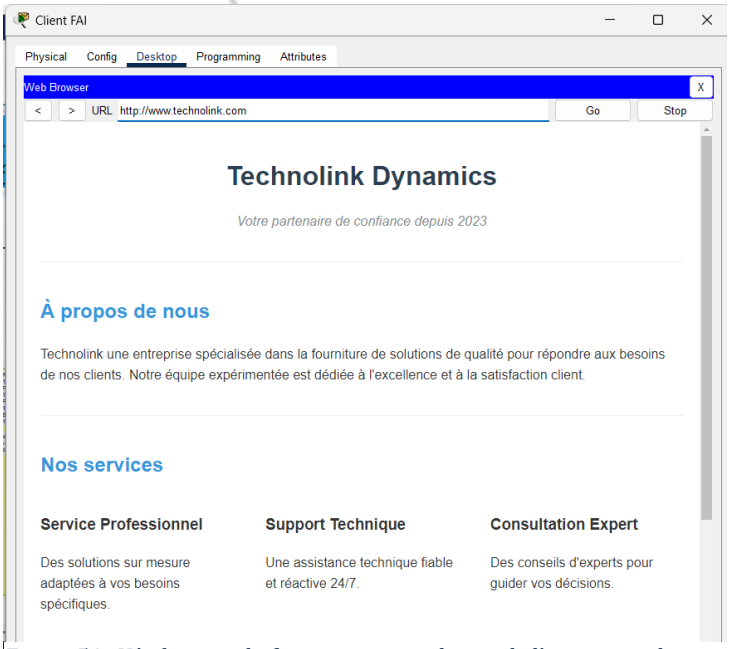

Figure 54 : Vérification du fonctionnement du site de l'entreprise depuis le client FAI

Cette capture nous montre que le site de l'entreprise est bien accessible par son nom de domaine depuis internet (client FAI).

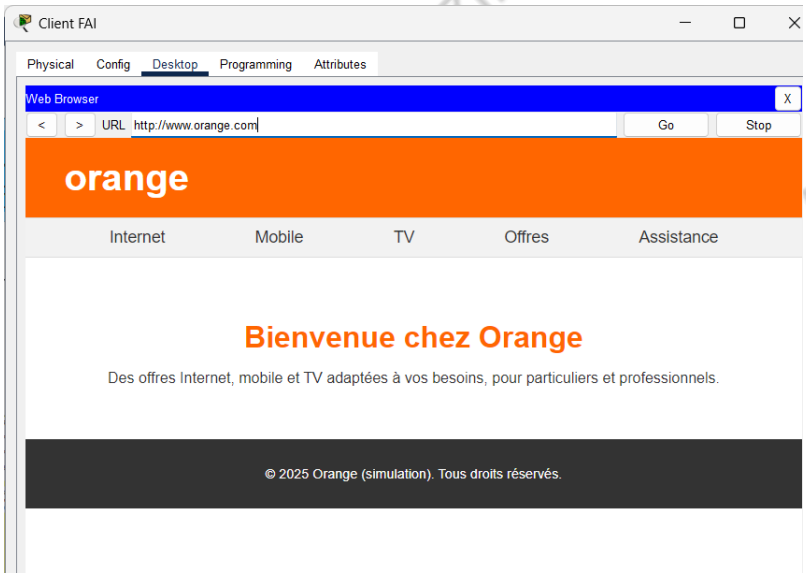

Figure 53 : Vérification du fonctionnement du Site du FAI (Orange) depuis le Client FAI

Enfin, on voit que le site du FAI est bien accessible par son nom de domaine depuis internet.

De manière générale, on voit donc que nos configurations DNS appliquées sur les différents serveurs DNS fonctionnement parfaitement.

8) Mise en place de la sécurité des équipements

8.1) Mise en place des ACL (Access Control List)

Pour renforcer la sécurité de notre réseau d'entreprise, nous allons mettre en place des ACL afin de filtrer le trafic non autorisé. Idéalement, une approche rigoureuse consisterait à utiliser des ACL avec état, permettant un filtrage intelligent des connexions en autorisant les retours de requêtes légitimes.

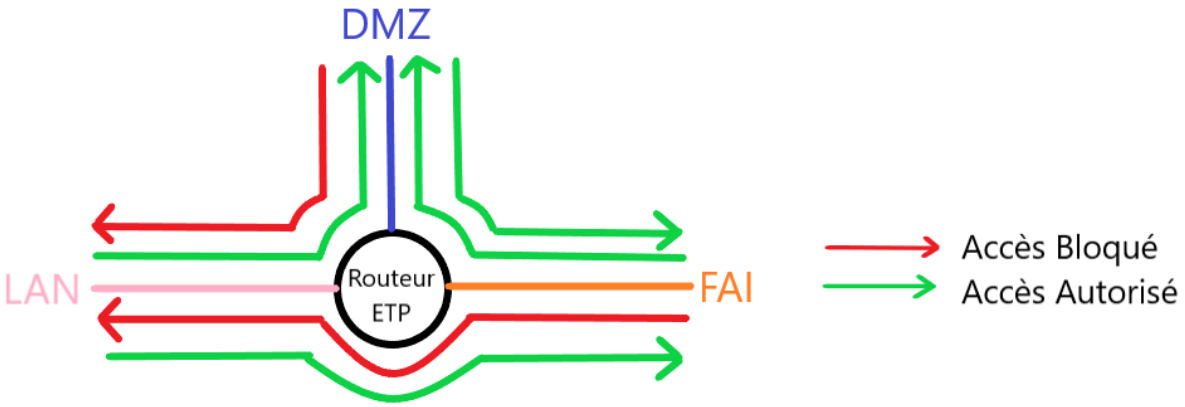

Figure 55 : Schéma illustrant le filtrage appliqué par des ACL avec états

Cependant, dans le cadre de ce projet et avec les connaissances acquises en fin de première année de BUT, nous nous limiterons à des ACL sans état. Celles-ci seront appliquées uniquement au niveau de la DMZ, car les appliquer ailleurs risquerait de bloquer le bon fonctionnement de services essentiels (le filtrage sans état n'autorisant pas automatiquement les réponses aux requêtes). Nous allons donc créer une ACL qui autorise uniquement l'accès aux services DNS et HTTP de la DMZ, tout en bloquant tout autre type de communication, y compris les pings, même en provenance du réseau local.

Pour ce faire, nous allons créer une ACL étendue que nous appliquerons en sortie de l'interface reliant le routeur à la DMZ. Cette ACL sera conçue de manière à n'autoriser que les services nécessaires (DNS et HTTP) en bloquant tout autre type de trafic non indispensable.

```
ip access-list extended VERS_DMZ
 permit udp any host 10.1.0.3 eq domain
 permit tcp any host 10.1.0.2 eq www
 deny ip any any
```

Figure 56 : Création de l'access-list VERS_DMZ

```
interface GigabitEthernet0/1.80
 encapsulation dot1Q 80
 ip address 10.1.0.1 255.255.255.248
 ip access-group VERS_DMZ out
 ip nat inside
```

Figure 57 : Attribution de l'ACL VERS_DMZ à la sous-interface de la DMZ.

Dans cette configuration, nous avons définis une ACL nommée VERS_DMZ.
La première ligne autorise le trafic UDP en provenance de n'importe quelle source vers l'hôte 10.1.0.3 sur le port 53, correspondant au service DNS.
La deuxième ligne autorise le trafic TCP vers l'hôte 10.1.0.2 sur le port 80, utilisé par le service HTTP (web).
La troisième ligne bloque tout autre trafic avec l'instruction deny ip any any.
Enfin, l'ACL est appliquée en sortie (out) de l'interface G0/1.80, qui correspond à la sous-interface connectée à la DMZ. Cela garantit que seuls les services explicitement autorisés dans la DMZ restent accessibles, même depuis le LAN, renforçant ainsi la sécurité de cette zone exposée.

8.2) Mise en place de la protection par SSH

Le protocole SSH permet d'établir une connexion sécurisée entre un poste administrateur et un équipement réseau comme un switch ou un routeur. Ce protocole est donc essentiel pour sécuriser l'administration des équipements, notamment lorsqu'ils sont accessibles à distance.

Pour configurer le SSH sur les équipements, plusieurs étapes sont nécessaires. Tout d'abord, nous allons affecter une adresse IP à une interface VLAN dédiée à l'administration, dans notre cas ce sera le VLAN 99.

Pour notre VLAN dédiée à l'administration des équipements, nous utiliserons le réseau 192.168.99.0/24. Nous attribuerons l'adresse IP 192.168.99.1 a la sous interface du vlan sur le routeur.

```
Router(config)#int G0/0.99
Router(config-subif)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0.99, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0.99, changed state to up
encapsulation dot1q 99
Router(config-subif)#ip address 192.168.99.1 255.255.255.0
Router(config-subif)#no shutdown
Router(config-subif)#exit
```

Figure 58 : Création de la sous-interface Vlan Admin 99

On peut configurera ensuite le SSH sur le routeur d'entreprise avec les commandes suivantes :

```
Router# conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname RTR-ETP
RTR-ETP(config)#ip domain-name technolink.com
RTR-ETP(config)#crypto key generate rsa
The name for the keys will be: RTR-ETP.technolink.com
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]: 4096
% Generating 4096 bit RSA keys, keys will be non-exportable...[OK]

RTR-ETP(config)#ip ssh version 2
*Mar 1 1:15:37.330: %SSH-5-ENABLED: SSH 1.99 has been enabled
RTR-ETP(config)#username admin privilege 15 secret Admin!
RTR-ETP(config)#line vty 0 4
RTR-ETP(config-line)#transport input ssh
RTR-ETP(config-line)#login local
RTR-ETP(config-line)#access-class 10 in
RTR-ETP(config-line)#exit
RTR-ETP(config)#access-list 10 permit 192.168.99.0 0.0.0.255
RTR-ETP(config)#end
RTR-ETP#
%SYS-5-CONFIG_I: Configured from console by console
write
Building configuration...
[OK]
RTR-ETP#
```

Figure 59 : Configuration du SSH sur le routeur d'entreprise

Ensuite, nous pouvons configurer les Switchs de la même manière. Nous commençons par attribuer une adresse IP unique sur l'interface VLAN 99 de chaque switch. Puis on met en place le SSH sur l'équipement.

On aura donc par exemple la configuration suivante sur le Switch Ingénieur 1 :

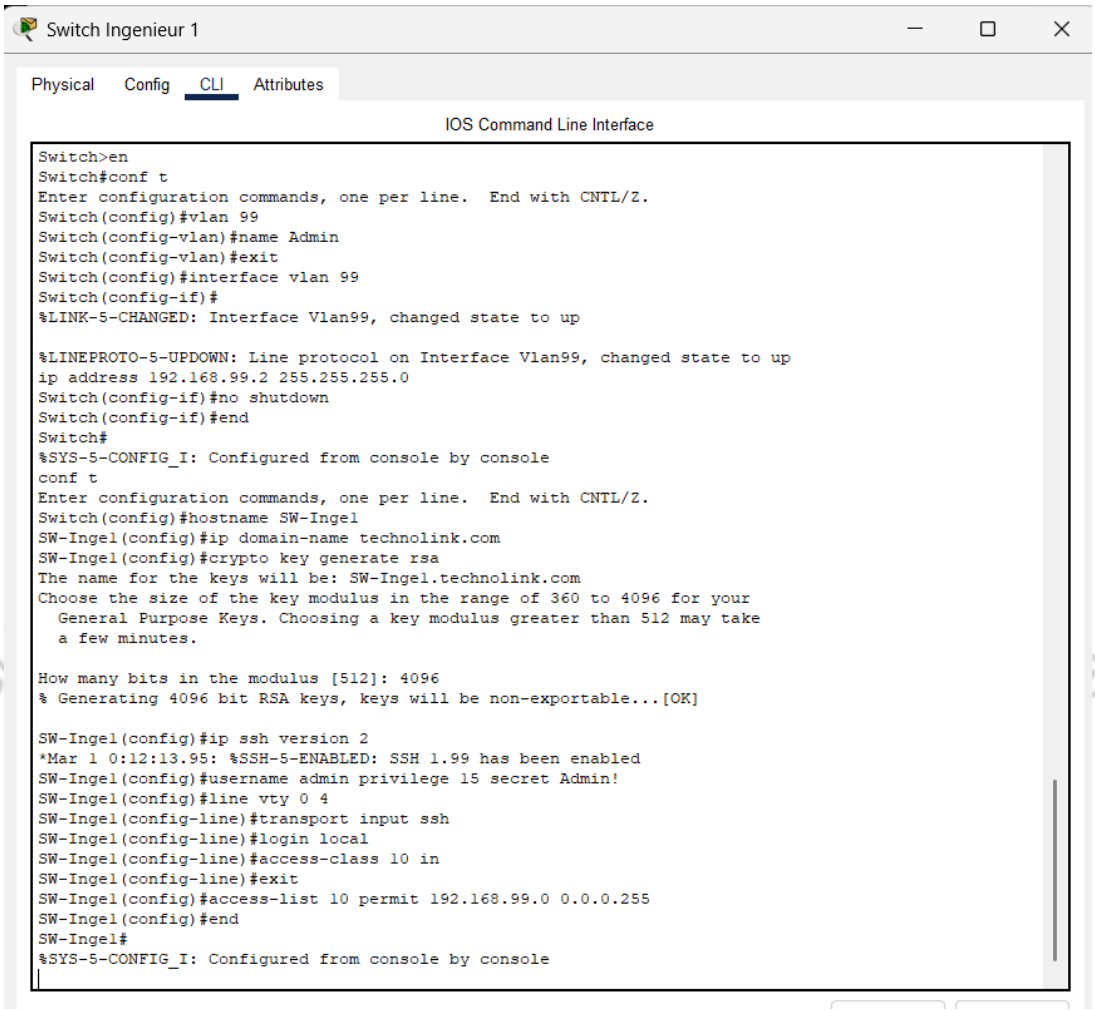

Figure 60 : Configuration SSH du Switch Ingénieur 1

On réitère les commandes en adaptant les adresses IP pour chaque Switchs tout en veillant à respecter la plage d'adresse du réseau 192.168.99.0/24. Le nom d'utilisateur sera donc « admin » et le mot de passe sera « Admin ! »

On aura donc par exemple la configuration du switch Serveur suivante :

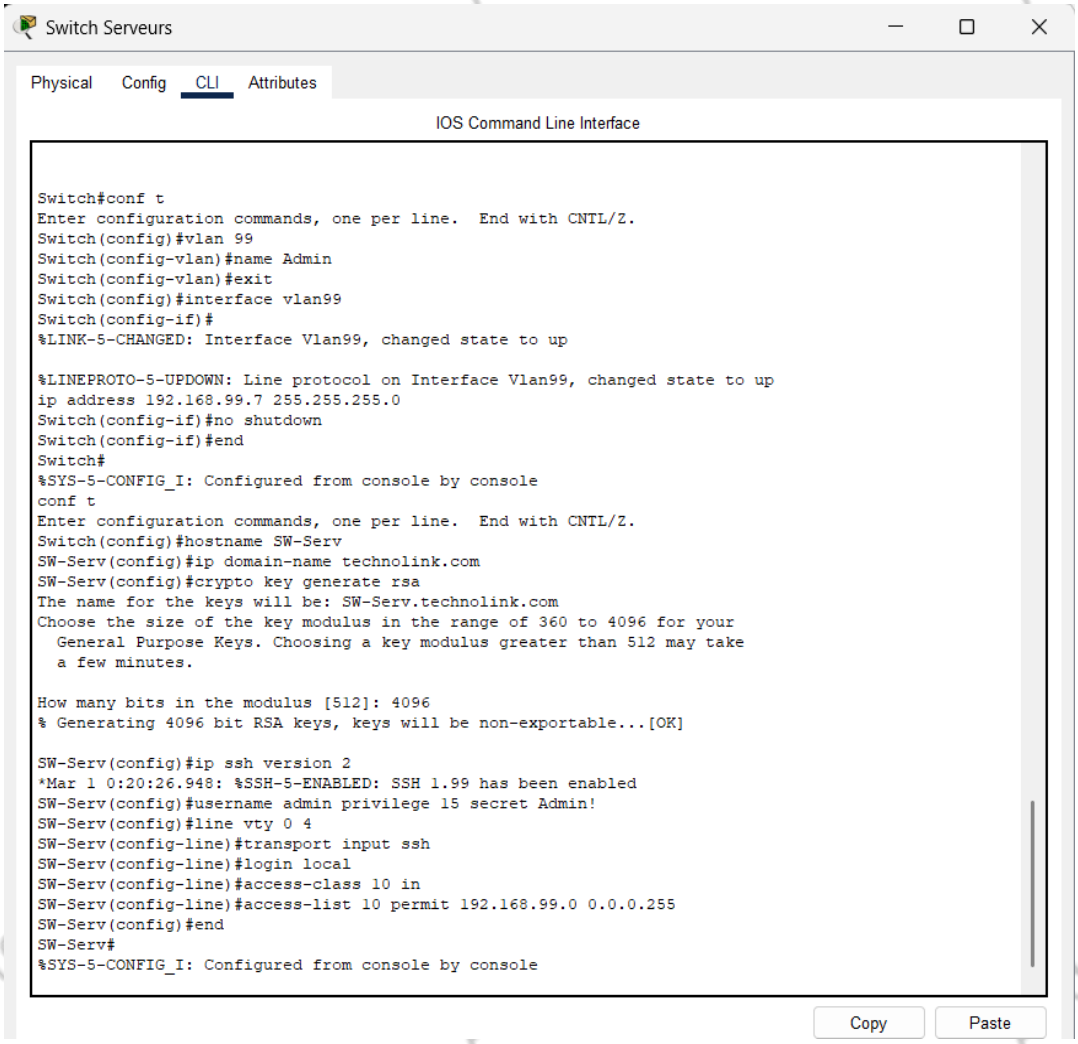

Figure 61 : Configuration SSH du Switch Serveur

Pour que les équipements puissent être accessibles depuis le PC de l'administrateur réseau présent dans la salle des serveurs, nous allons configurer l'adressage IP statique de cet hôte dans le réseau du VLAN 99. On aura donc le PC Admin avec la configuration IP suivante :

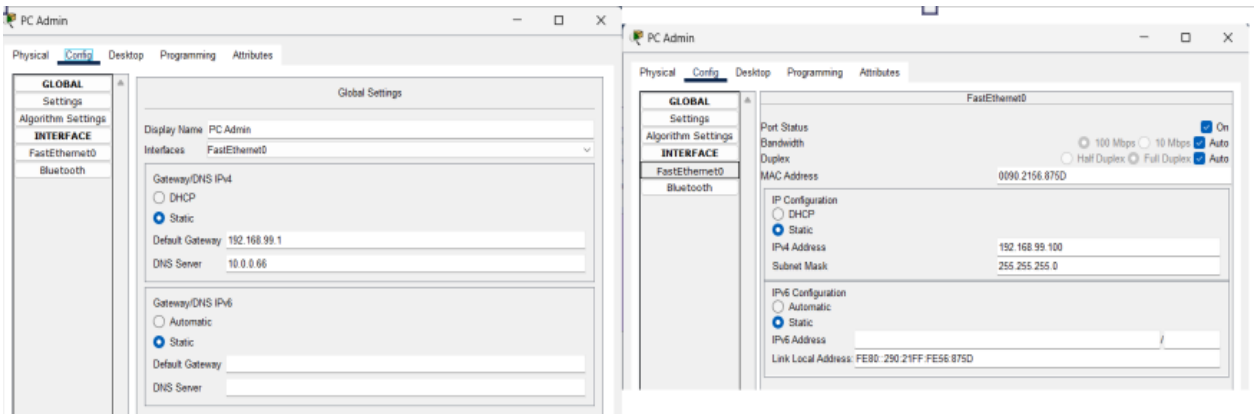

Figure 62 : Configuration IPv4 du PC Administrateur réseau

On continue ensuite par mettre le port du Switch Serveur connecté à ce PC en « mode Access » pour le VLAN 99.

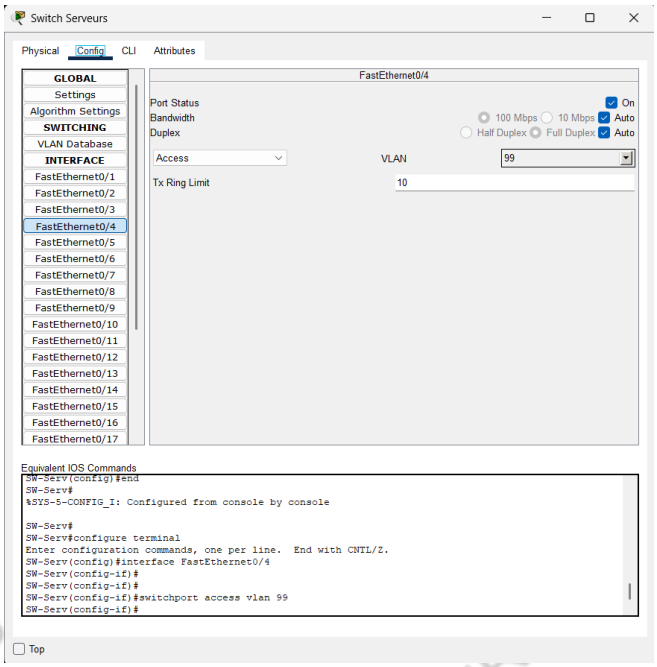

Figure 63 : Configuration en « mode Access » du port connecté au PC admin sur le Switch Serveur

Maintenant que tous nos équipements sont bien configurés, nous pouvons effectuer les tests pour vérifier le fonctionnement. Pour cela, nous allons nous connecter en SSH depuis le PC admin vers le Switch Inge1 et vers le Routeur.

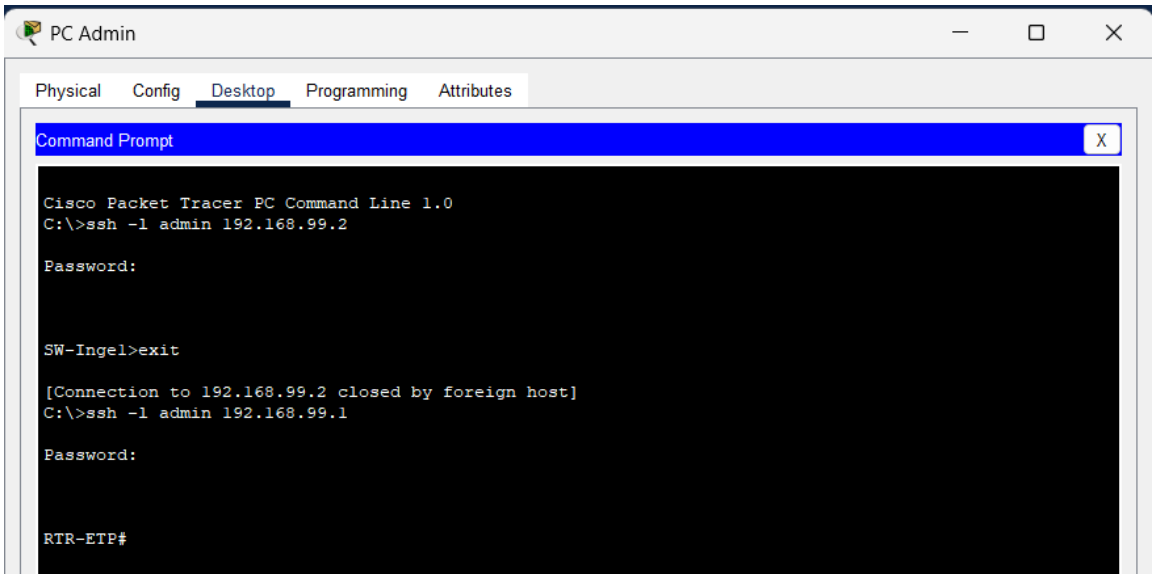

Figure 64 : Vérification du fonctionnement du SSH depuis le PC admin

On voit donc que pour chaque cas, la connexion s'établie, le SSH est donc bien configuré.

Conclusion

Ce projet SAE201 nous a permis de mobiliser l'ensemble des compétences acquises durant notre première année de BUT – Réseaux et Télécommunications. A travers la conception et la mise en œuvre d'une infrastructure réseau complète pour l'entreprise fictive « TechnoLink », nous avons pu appliquer concrètement des notions fondamentales à la création du réseau informatique d'une entreprise.

Chaque étape de ce projet nous a confrontés à des étapes techniques diverses, commençant par l'adressage IP et allant jusqu'à la sécurisation des équipements du réseau informatique. La mise en place de la DMZ, d'un accès FAI et des différents mécanismes tels que le NAT, le PAT ou la sécurité, ont consolidé notre compréhension des infrastructures réseaux.

Enfin, les tests réalisés ont démontré le fonctionnement de notre architecture. Ce travail nous a permis de développer nos capacités techniques, notre capacité à effectuer des dépannages pour que tout fonctionne et notre autonomie. Il nous est bénéfique pour la suite de nos études et de notre carrière car nous pourrions être sollicité pour construire d'autres réseaux informatiques pour des entreprises.

Table des illustrations

Figure 1 : Schéma de la disposition des salles composant les locaux de TechnoLink....5
Figure 2 : Schéma de la mise en place du réseau informatique de TechnoLink....6
Figure 3 : Tableau récapitulatif du nombre de PC et d'imprimantes en fonction des salles....6
Figure 4 : Tableau récapitulatif des équipements utilisé du coté entreprise..6
Figure 5 : Mise en place des Switchs et des Routeurs....7
Figure 6 : Tableau récapitulatif des VLAN du réseau de TechnoLink....8
Figure 7 : Ajout des VLANs sur les Switchs de l'entreprise TechnoLink....8
Figure 8 : Exemple de la configuration en mode access des ports des Switchs Ingénieurs....9
Figure 9 : Exemple de configuration en mode access des ports du Switch Comm' 9
Figure 10 : Exemple de configuration en mode Trunk du switch «Com-Admi » 10
Figure 11 : Tableau récapitulant l'adressage IP des VLANs 11
Figure 12 : Représentation du réseau de TechnoLink 12
Figure 13 : Exemple de configuration IP statique sur un PC d'ingénieur....13
Figure 14 : Configuration des sous-interfaces sur le routeur + encapsulation (photo 1) 14
Figure 15 : Configuration des sous-interfaces sur le routeur + encapsulation (photo 2) 14
Figure 16 : Test de ping inter-VLAN 15
Figure 17 : Adressage IPv4 statique du serveur DNS privé....16
Figure 18 : Adressage IPv4 du serveur Intranet de TechnoLink....16
Figure 19 : Adressage IPv4 du serveur DHCP 17
Figure 20 : Activation du service HTTP/HTTPS sur le serveur WEB privé de TechnoLink....17
Figure 21 : Saisie du code HTML de la page intranet de TechnoLink 17
Figure 22 : Vérification du serveur Intranet de TechnoLink depuis le PC du PDG....18
Figure 23 : Commande du routeur d'entreprise pour que le DHCP fonctionne dans le VLAN_Reu 19
Figure 24 : Configuration du Pool DHCP "Pool_Reu" donnant la configuration IPv4 des PC présents dans la salle de réunion....19

Figure 25 : Demande de configuration IPv4 via DHCP depuis un PC de la salle de réunion 20
Figure 26 : Ajout de la DMZ sur une interface (G0/1) de notre routeur d'entreprise 21
Figure 27 : Adressage IP du VLAN 80 de la DMZ 21
Figure 28 : Configuration de la sous-interface du VLAN_DMZ sur le routeur d'entreprise 22
Figure 29 : Ajout du VLAN_DMZ sur le Switch DMZ 22
Figure 30 : Adressage des serveurs présents dans la DMZ 22
Figure 31 : Extrait du code HTML/CSS du site internet public de TechnoLink 23
Figure 32 : Activation du service HTTP et HTTPs du serveur WEB public de TechnoLink 23
Figure 33 : Vérification du serveur WEB public de TechnoLink depuis le PC du PDG 23
Figure 34 : Configuration IPv4 de l'interface publique du routeur de l'entreprise 25
Figure 35 : Configuration IPv4 de l'interface publique du routeur FAI reliée au routeur de l'entreprise 25
Figure 36 : Zone du FAI avec l'adressage choisi 26
Figure 37 : Ping de la passerelle par défaut depuis le client FAI 27
Figure 38 : Activation du service HTTP et HTTPs sur le serveur WEB du FAI 27
Figure 39 : Extrait du code HTML/CSS du site web simulé d'orange (FAI) 27
Figure 40 : Vérification du fonctionnement du site WEB du FAI depuis le client FAI 28
Figure 41 : Exemple de 3 sous-interfaces ayant la mention "ip nat inside" 29
Figure 42 : Commande permettant l'activation de la traduction des adresses privées vers l'adresse publique du routeur de l'entreprise 30
Figure 43 : Lignes CLI permettant de créer l'ACL contenant les réseaux associés à nos sous interfaces 30
Figure 44 : Commandes permettant la redirection de ports sur le routeur de l'entreprise 30
Figure 45 : Configuration DNS du serveur privé de l'entreprise 31
Figure 46 : Configuration du DNS public de l'entreprise 32
Figure 47 : Configuration du DNS racine dans la zone du FAI 32
Figure 48 : Configuration du DNS FAI Orange 33

Figure 49 : Vérification du fonctionnement du site Intranet de TechnoLink depuis le PC du PDG ADJ 34
Figure 50 : Vérification du fonctionnement du site WEB de l'entreprise TechnoLink depuis le PC du PDG ADJ 34
Figure 51 : Vérification du fonctionnement du site du FAI (Orange) depuis le PC du PDG ADJ 35
Figure 52 : Vérification du serveur Intranet de l'entreprise depuis le client FAI 35
Figure 53 : Vérification du fonctionnement du Site du FAI (Orange) depuis le Client FAI 36
Figure 54 : Vérification du fonctionnement du site de l'entreprise depuis le client FAI 36
Figure 55 : Schéma illustrant le filtrage appliqué par des ACL avec états 37
Figure 56 : Création de l'access-list VERS_DMZ 37
Figure 57 : Attribution de l'ACL VERS_DMZ à la sous-interface de la DMZ... 38
Figure 58 : Création de la sous-interface Vlan Admin 99 39
Figure 59 : Configuration du SSH sur le routeur d'entreprise 39
Figure 60 : Configuration SSH du Switch Ingénieur 1 40
Figure 61 : Configuration SSH du Switch Serveur 41
Figure 62 : Configuration IPv4 du PC Administrateur réseau 41
Figure 63 : Configuration en « mode access » du port connecté au PC admin sur le Switch Serveur 42
Figure 64 : Vérification du fonctionnement du SSH depuis le PC admin 42