09/06/2025

SAE21

Concevoir le réseau informatique d'une petite entreprise

Esteban Fernandez
IUT DE BLOIS

Table des matières

Introduction 2
Cahier des charges 3
Présentation de l'entreprise 4
Première conception 4
Schéma du réseau informatique de l'entreprise 6
Adressage IPV4, IPV6 8
Configuration du réseau d'entreprise 9
1. Salle de réunion (DHCP, DHCPv6) 9
DHCPv4 10
DHCPv6 11
2. Bureau Administration Réseau, Serveur Intranet (LAN 1) 14
3. Serveur DNS public et Serveur Web Public (DMZ) 19
4. Bureau ingénieurs et bureau designers 24
5. VLAN 10 et VLAN 20 pour la Direction et le Secrétariat et l'accueil 25
Configuration du réseau de la FAI 28
1. Les serveurs 28
2. Backbone 33
Routage OSPF et OSPFv3 35
Traduction d'adresses NAT 39
Mis en place des ACL 43
Routeur Principal 43
ACL « VERS_DMZ » 43
ACL « VERS_DMZ6 » 44
Configuration SSH pour le réseau de l'entreprise 46
Conclusion 49
Liste des figures 50

Introduction

Dans ce compte rendu, nous allons analyser les étapes pour concevoir le réseau d'une petite entreprise. L'objectif de cette SAE est de créer et configurer le réseau informatique d'une entreprise avec un accès à internet. Nous allons utiliser le logiciel Cisco Packet Tracer pour mener à bien ce projet. J'ai choisi de créer une entreprise fictive nommé Technova. Il est nécessaire de répondre à certain besoin dans ce projet, telle que le routage, les services de bases réseaux (DHCP, DNS…) et de la sécurité (ACL). Nous allons donc voir dans un premier temps, l'analyse du cahier des charges et les premiers pas de l'architecture de mon réseau. Dans un deuxième temps, nous allons voir en détail la configuration du réseau dans la partie entreprise. Dans un troisième temps, nous allons nous intéresser à la configuration de la FAI et la jointure entre le réseau privé et publique. Et dans un dernier temps, nous analyserons les firewall mis en place pour la sécurité du réseau privé.

Cahier des charges

Afin de mener à bien notre projet, voici le cahier des charges que nous devons respecter :

- Plusieurs switchs en redondance,
- Plusieurs VLANs,
- Une architecture de sous-réseaux IPv4 privés en VLSM,
- Un serveur web 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 de l'administrateur de l'entreprise en SSH,
- Double adressage : IPv4 obligatoire, IPv6 fortement apprécié,
- D'autres services et fonctionnalités de votre choix peuvent être ajoutés, l'architecture et l'étendu de votre réseau d'entreprise ne dépend que de vous. Mais inutile d'élaborer un réseau complexe si les fonctionnalités de bases 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 : c'est votre entreprise à votre nom/prénom, pas de nom générique du style PC1, PC2, SRV1, SRV2, SW1, SW2, VLAN1, VLAN2, client1, client2, ...

Présentation de l'entreprise

Première conception

J'ai choisi de créer une entreprise du nom de Technova. Technova est une entreprise fictive spécialisée dans le domaine de la technologie et de l'innovation. Avec plusieurs bureaux.

Le siège social de Technova est équipé d'une infrastructure réseau robuste pour assurer la connectivité et la sécurité des données. Ce bureau central héberge les principales équipes administratives, les bureaux de développement ou encore la salle de conférence. Le réseau est divisé en plusieurs VLAN pour segmenter les différents départements et assurer une gestion efficace du trafic réseau.

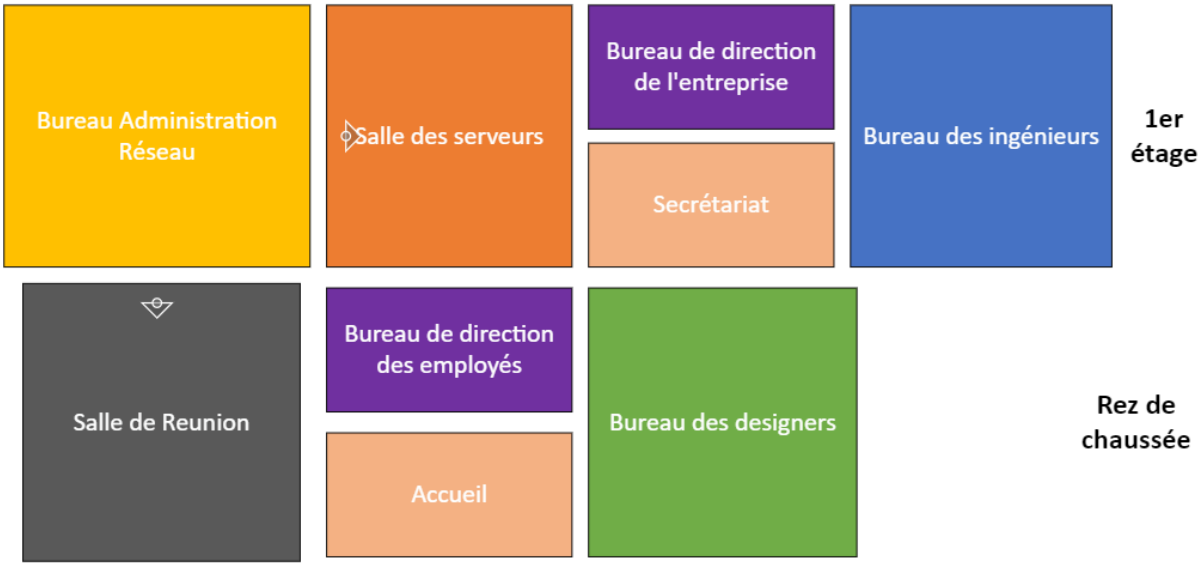


Figure 1 : Première conception de l'entreprise

Voici une liste du nombre d'employés dans l'entreprise :

<u>1er étage :</u>

Bureau Administration Réseau (1 employé)
Bureau de direction de l'entreprise (2 employés)
Secrétariat (2 employés)

Bureau des ingénieurs (10 employés)
Salle des serveurs (3 serveurs)

Rez-de-chaussée :

Salle de réunion (8 employés ou plus)
Bureau de direction des employés (2 employés)
Accueil (2 employés)
Bureau des designers (10 employés)

La salle des serveurs est constituée de deux parties, un serveur intranet qui lui est accessible par l'entreprise, et 2 serveurs dans la zone démilitarisés qui eux sont accessibles que sur internet.

Schéma du réseau informatique de l'entreprise

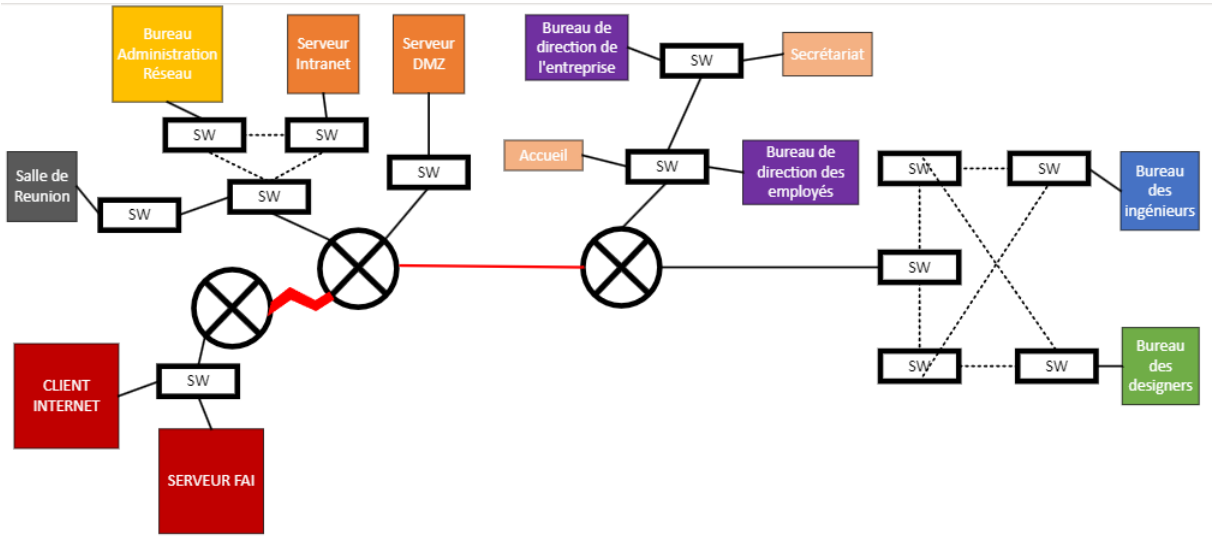


Figure 2 : Deuxième conception du réseau en schéma

On voit bien dans le schéma que conformément au cahier des charges, le réseau est relié au FAI qui se situe en bas à droite.

Voici une estimation des appareils que l'entreprise va utiliser :

SWITCH	12
ROUTEUR	2
ORDINATEUR PORTABLE	8
ORDINATEUR FIXE	29
SERVEURS	3

Suite à ces estimations, j'ai pu concevoir un dernier schéma représentatif de l'entreprise en y ajoutant une backbone entre le routeur du FAI et le routeur de l'entreprise.

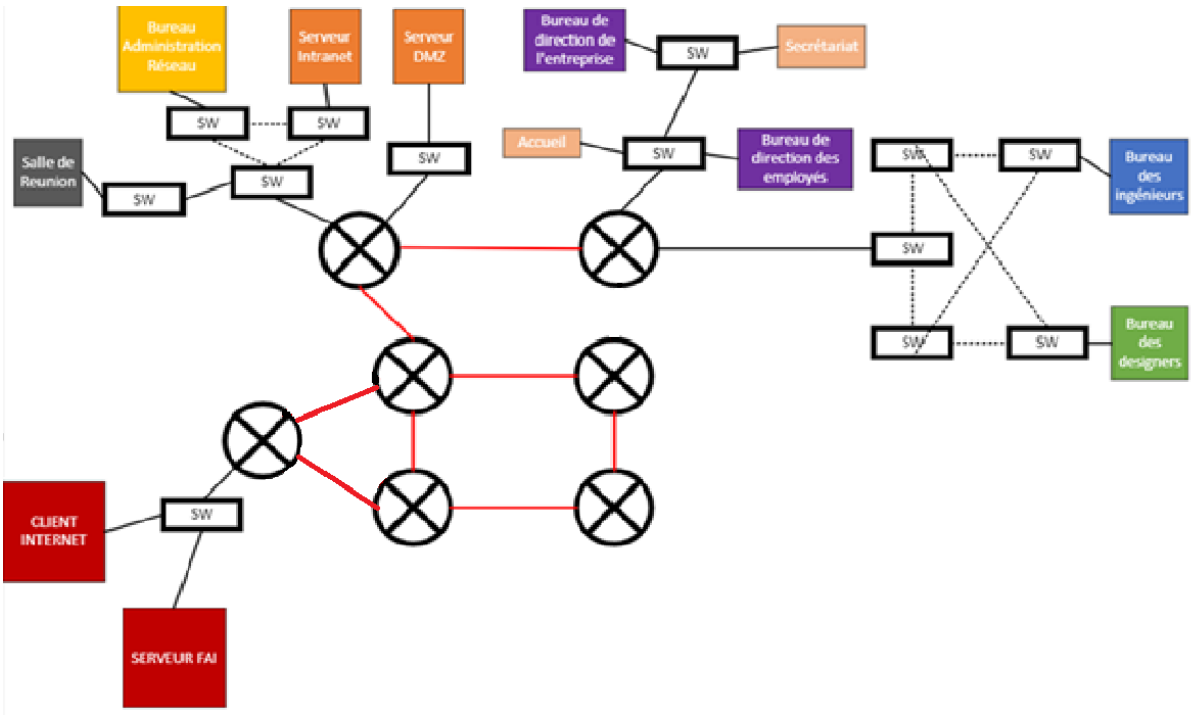


Figure 3 : Schéma final du réseau de l'entreprise Technova

J'ai ajouté un backbone relié au routeur principal de l'entreprise.

Le réseau informatique de l'entreprise va contenir deux routeurs. Le premier routeur que l'on appellera, « Routeur Principal ». Le second routeur que l'on appellera, « Routeur Secondaire » permet de faire le lien entre différents réseaux internes de l'entreprise. Le routeur principal permettra d'entrée et de sortir du réseau. Les noms des équipements seront changés sur le réseau final.

Adressage IPV4, IPV6

J'ai pu concevoir un double adressage IPV4 et IPV6, pour le réseau interne, voici la liste de ces différents réseaux interne :

Bureaux	Réseaux + masque
Salle de réunion, Serveur Intranet, Bureau Administration Réseau	192.168.1.0/24
Direction	192.168.10.0/24
Secrétariat et Accueil	192.168.20.0/24
Serveur DNS public, Serveur WEB public (DMZ)	192.168.200.0/24
Bureau ingénieurs, bureau designers	192.168.0.0/24
Lien entre Routeur Principal et Routeur Secondaire	192.168.60.0/24

Figure 4 : Différents réseaux interne IPV4

Bureaux	Réseau + masque
Salle de réunion, Serveur Intranet, Bureau Administrateur Réseau	2001:db8:1000:1::/64
Direction	2001:db8:1000:A::/64
Secrétariat et Accueil	2001:db8:1000:14::/64
Serveur DNS public, Serveur WEB public (DMZ)	2001:db8:1000:C8::/64
Bureau ingénieurs, bureau designers	2001:db8:1000::/64
Lien entre Routeur Principal et Routeur Secondaire	2001:db8:1000:3C::/64

Figure 5 : Différents réseaux interne IPV6

On peut donc commencer la configuration des différents équipements.

Configuration du réseau d'entreprise

Cette partie est consacrée à la configuration des équipements qui serviront à mettre en place le réseau informatique de l'entreprise. Les différentes captures seront faites sur Cisco Packet Tracer pour une meilleur visibilité. On va utiliser le système du modèle OSI ascendant en commençant par la couche physique et le câblage du réseau.

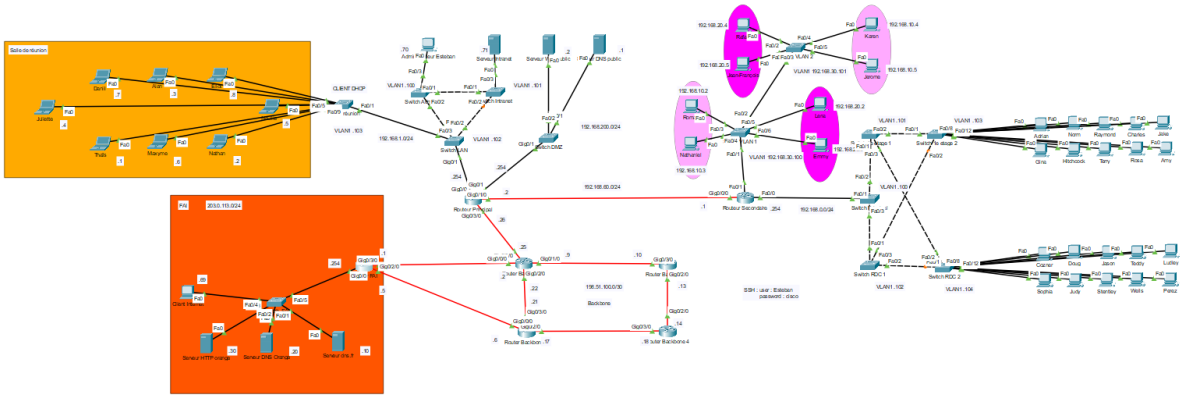


Figure 6 : Câblage du réseau en entier comme sur le schéma

1. Salle de réunion (DHCP, DHCPv6)

Nous allons donc dans un premier temps expliquer ce qu'est le service DHCP. Donc, le DHCP (Dynamic Host Configuration Protocol) est un protocole réseau utilisé pour attribuer automatiquement des adresses IP et d'autres paramètres de configuration réseau (comme les serveurs DNS, la passerelle par défaut) aux appareils sur un réseau. Il simplifie la gestion des adresses IP en évitant la configuration manuelle pour chaque appareil, en assurant qu'il n'y a pas de conflits d'adresses IP et en permettant une réutilisation efficace des adresses. Dans le contexte du réseau de cette entreprise, l'interface du routeur offrira une plage d'adresse pour la configuration de ces PC.

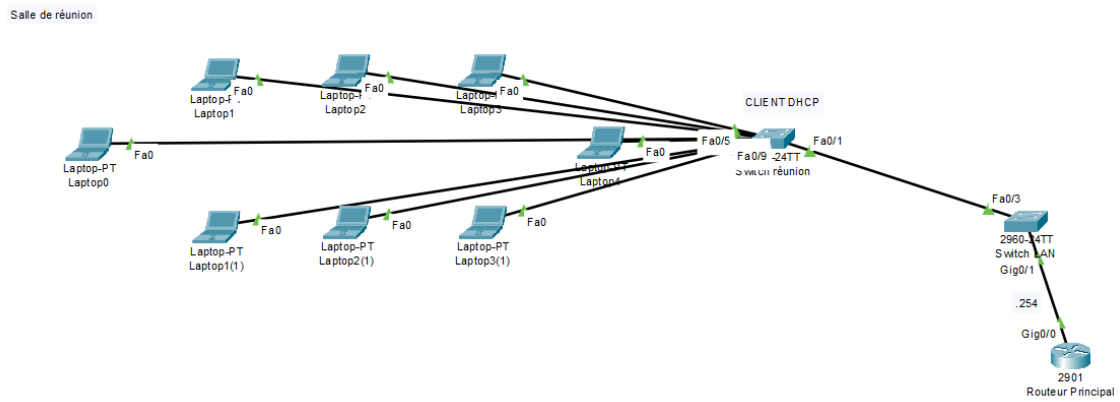


Figure 7 : Salle de réunion, client DHCP

DHCPv4

Nous allons passer en mode configuration sur le Routeur Principal pour offrir la configuration suivante :

```
rePrincipal>en
rePrincipal#conf t
rePrincipal(config)#ip dhcp pool REUNION
rePrincipal(dhcp-config)#network 192.168.1.0 255.255.255.0
rePrincipal(dhcp-config)#default-router 192.168.1.254
rePrincipal(dhcp-config)#dns-server 192.168.1.71
rePrincipal(config)#ip dhcp excluded-address 192.168.1.254
```

Ici, on crée un pool dhcp REUNION qui distribuera des adresses entre 192.168.1.1 et 192.168.1.253. On indique que la route par défaut de ces différents clients est l'interface du routeur et on indique également l'adresse IP du serveur Intranet. On exclut également, l'adresses 192.168.1.254 qui est celle de l'interface du routeur.

DHCPv6

Nous allons refaire la même chose mais pour les adresses IPV6 :

```
rePrincipal>en
rePrincipal#conf t
rePrincipal(config)#ipv6 dhcp pool REUNIONv6
rePrincipal(config-dhcpv6)#address prefix 2001:db8:1000:1::/64
lifetime 3600 1800
rePrincipal(config-dhcpv6)#dns-server 2001:DB8:1000:1::71
rePrincipal(config-dhcpv6)#ex
rePrincipal(config)#int Gig0/0
rePrincipal(config-if)#ipv6 dhcp server REUNIONv6
```

Le paramètre de lifetime (durée de vie) dans le contexte de DHCPv6 se réfère à la durée pendant laquelle une adresse IPv6 ou un préfixe est valide et utilisable.

Lorsque des ordinateurs se connecteront au réseau dans la salle de réunion, la configuration IP leur sera envoyée automatiquement.

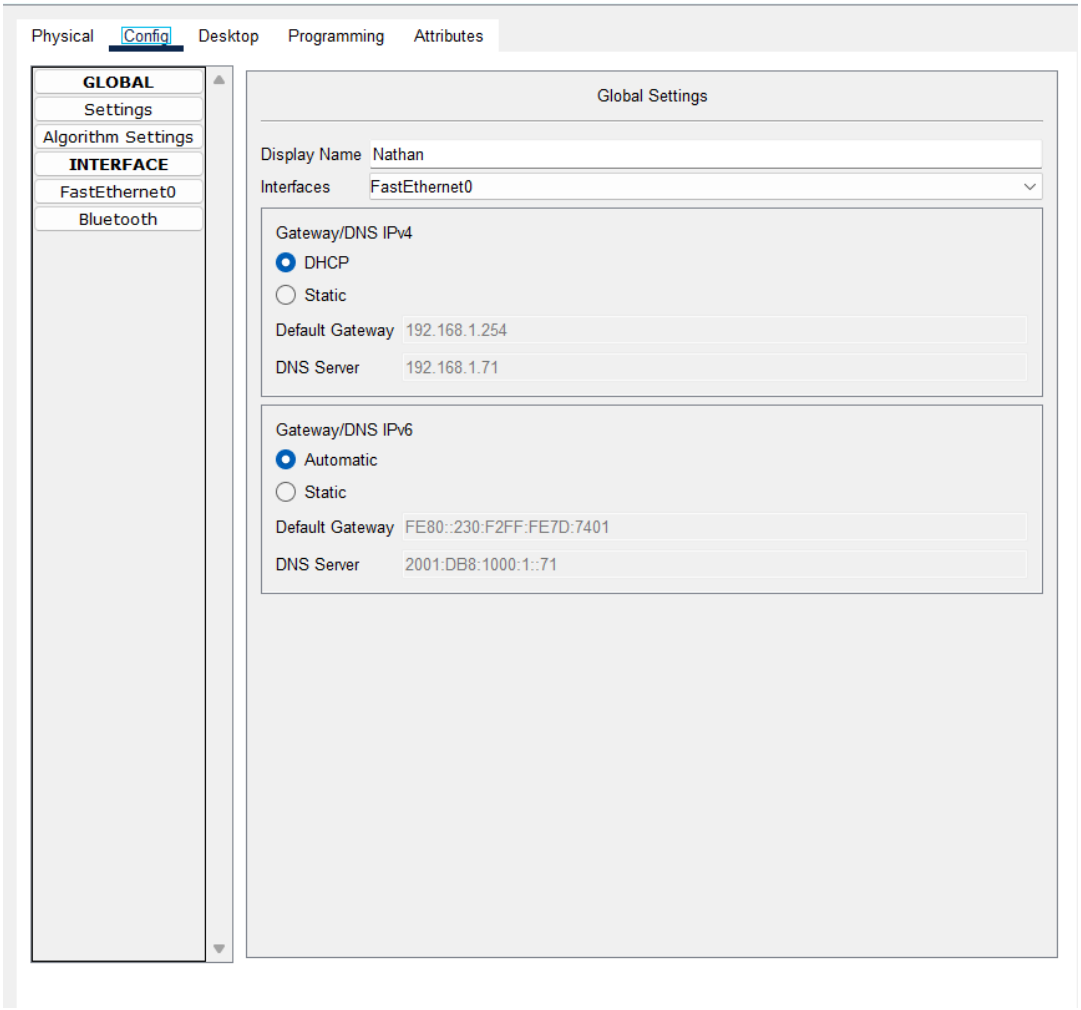


Figure 8 : Adressage automatique grâce au DHCP

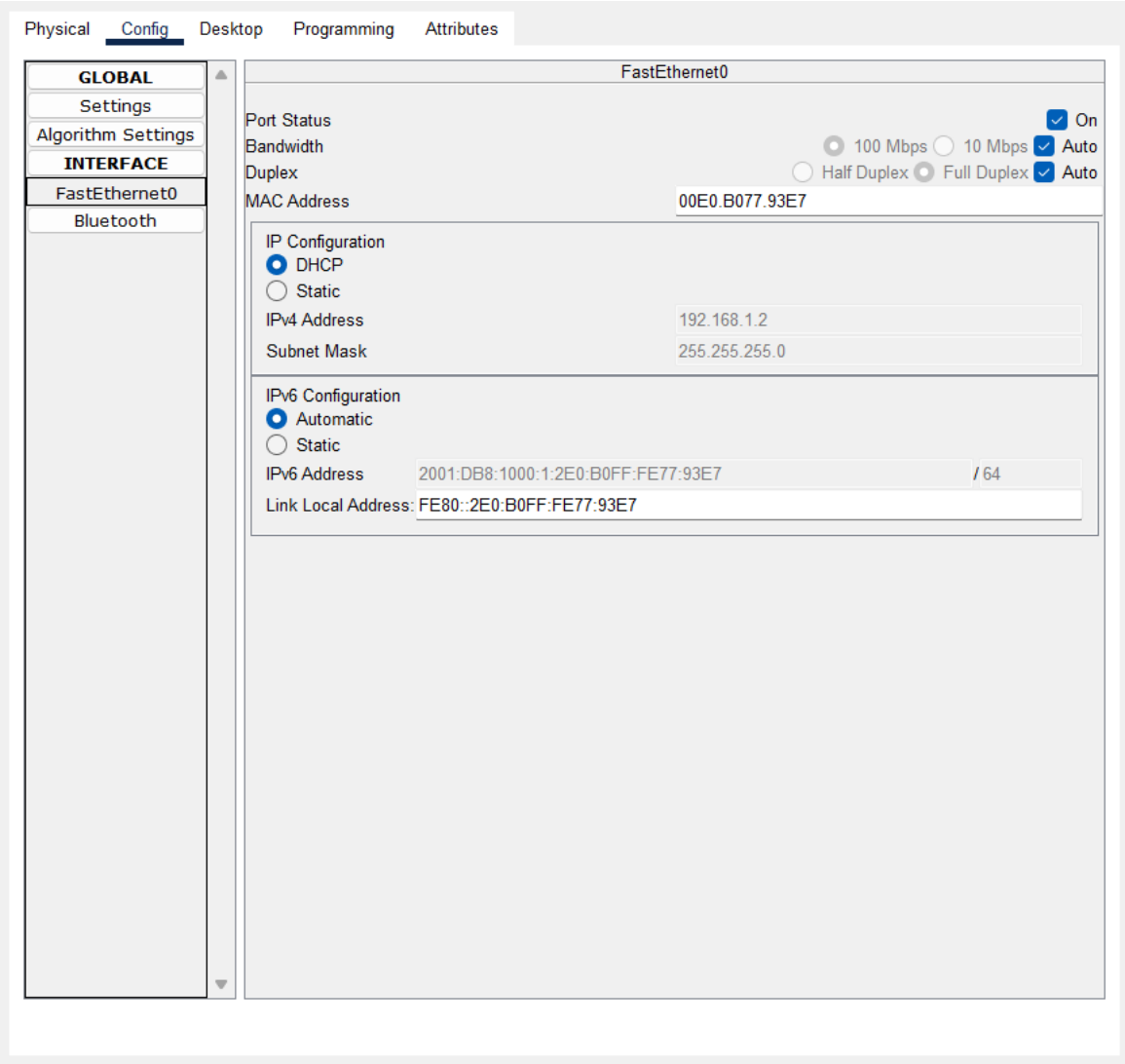


Figure 9 : Adressage automatique grâce au DHCP

2. Bureau Administration Réseau, Serveur Intranet (LAN 1)

Dans la continuité du réseau 192.168.1.0/24, nous allons nous intéresser au serveur intranet qui se situe sur le LAN et dans ce même réseau.

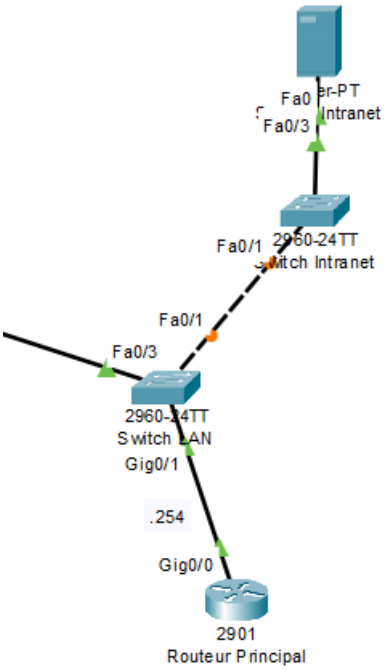


Figure 10 : Serveur Intranet

Le serveur intranet de l'entreprise comprend plusieurs services tels que HTTP et DNS. La configuration IP du serveur a été affectée manuellement au serveur. Son adresse IP est 192.168.1.71/24 en IPv4 et 2001:DB8:1000:1::71/64 en IPv6. Le service HTTP installé sur le serveur correspond au site web intranet de l'entreprise. Ce site web devrait être accessible que par les employés de l'entreprise cependant nous avons pas vus les ACL d'état cette année. Il est accessible via l'url « http://intranet.technova.fr ».

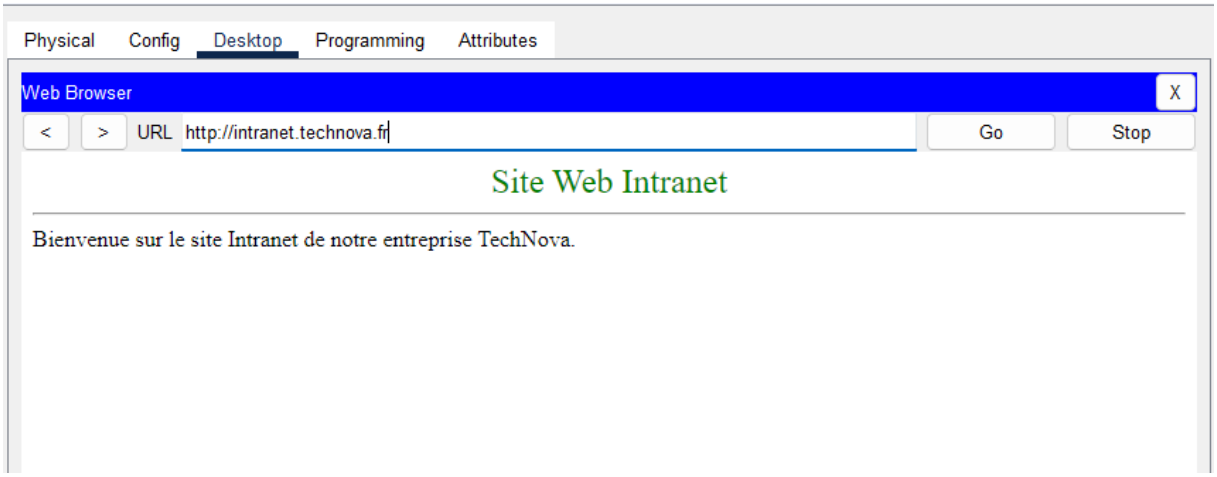


Figure 11 : Site web de l'entreprise accessible qu'aux employés

Le deuxième service présent sur le serveur est le service DNS. Ce service permet de gérer la résolution de noms dans l'entreprise et n'est accessible seulement par les employés de l'entreprise. Il faut donc le configurer en IPv4 et en IPv6. On fera une configuration manuelle. Voici la configuration :

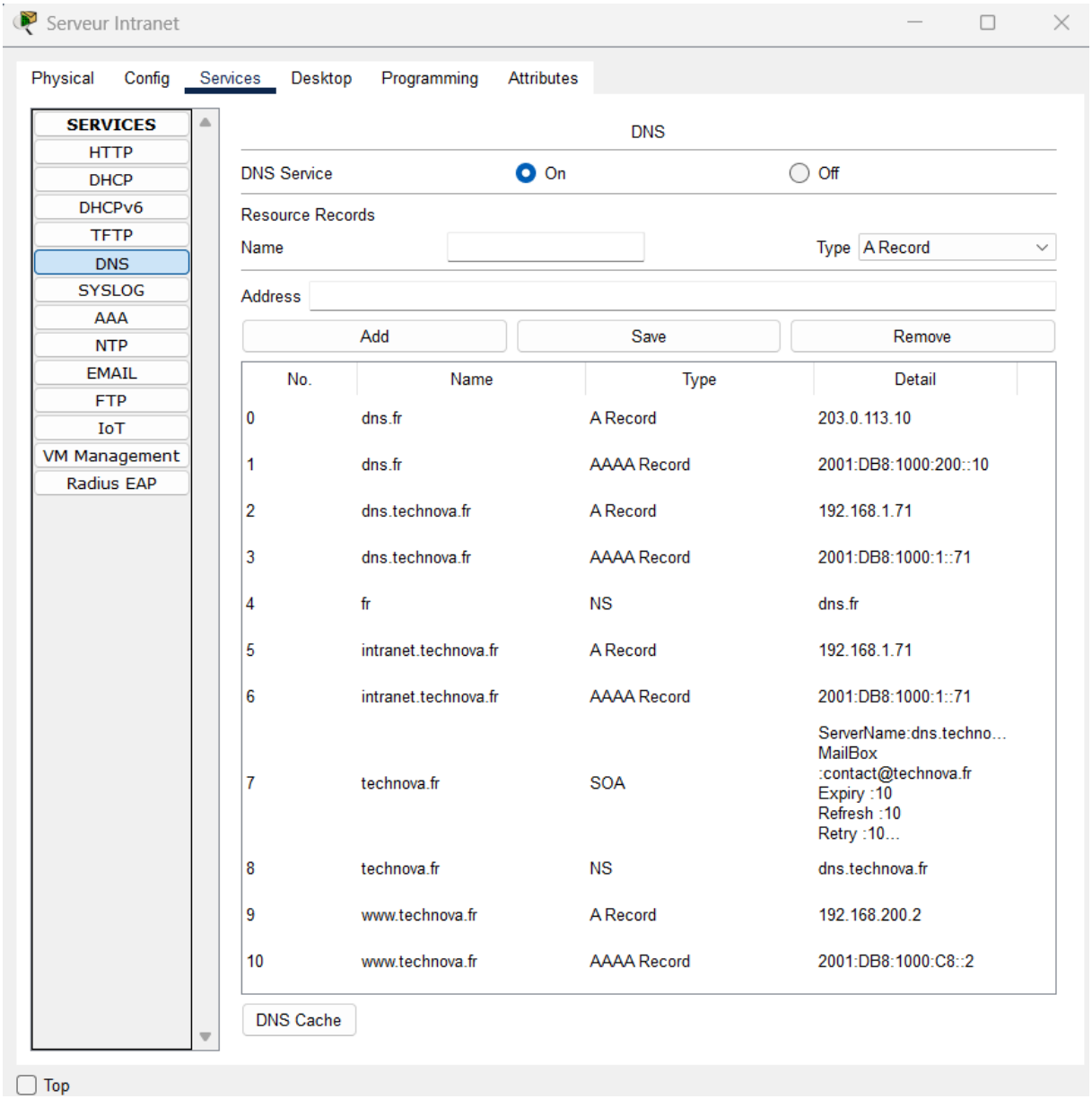


Figure 12 : Configuration DNS du serveur Intranet

dns.fr (A Record) :

Associe dns.fr à l'adresse IPv4 203.0.113.10.

dns.fr (AAAA Record) :

Associe dns.fr à l'adresse IPv6 2001:DB8:1000:200::10.

dns.technova.fr (A Record) :

Associe dns.technova.fr à l'adresse IPv4 192.168.1.71.

dns.technova.fr (AAAA Record) :

Associe dns.technova.fr à l'adresse IPv6 2001:DB8:1000:1::71.

fr (NS Record) :

Indique que dns.fr est le serveur de noms autoritaire pour la zone fr.

intranet.technova.fr (A Record) :

Associe intranet.technova.fr à l'adresse IPv4 192.168.1.71.

intranet.technova.fr (AAAA Record) :

Associe intranet.technova.fr à l'adresse IPv6 2001:DB8:1000:1::71.

technova.fr (SOA Record) :

Contient des informations sur le serveur de noms principal (dns.technova.fr) pour la zone technova.fr, l'adresse e-mail du responsable (contact@technova.fr), et les paramètres de mise à jour de la zone (Expiry, Refresh, Retry...).

technova.fr (NS Record) :

Indique que dns.technova.fr est le serveur de noms autoritaire pour la zone technova.fr.

www.technova.fr (A Record) :

Associe www.technova.fr à l'adresse IPv4 192.168.200.2.

www.technova.fr (AAAA Record) :

Associe www.technova.fr à l'adresse IPv6 2001:DB8:1000:C8::2.

Ensuite, on configure le PC de l'administrateur réseau avec des switchs en redondance comme sur le schéma. Le PC de l'administrateur sera configuré manuellement avec l'adresse IPv4 192.168.1.70/24 et l'adresse IPV6 FD00::46/64.

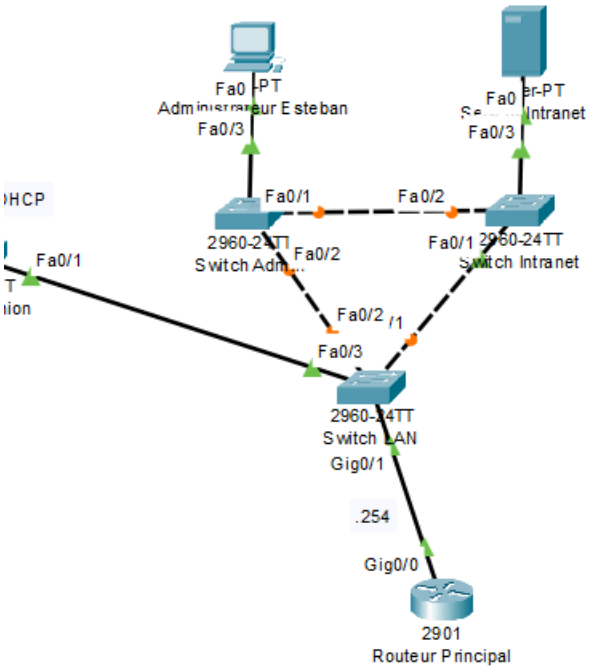


Figure 13 : Administrateur Réseau sur le LAN

Pour conclure cette partie adressage sur le LAN, nous allons configurer l'interface du routeur en 192.168.1.254/24 pour l'IPv4 et ensuite, sur cette même interface, configuré l'adresse IPv6 en FD00::FE/64. Voici la configuration :

```
rePrincipal>en
rePrincipal#conf t
rePrincipal(config)#int Gig0/0
rePrincipal(config-if)#ip address 192.168.1.254 255.255.255.0
rePrincipal(config-if)#no shutdown
rePrincipal(config-if)# ipv6 address 2001:DB8:1000:1::254/64
rePrincipal(config-if)#ipv6 enable
```

On fera le routage dans une autre partie quand toute la partie liaison de données et réseau du modèle OSI sera faite.

3. Serveur DNS public et Serveur Web Public (DMZ)

Une DMZ (Demilitarized Zone) est un sous-réseau séparé et isolé du réseau local et d'internet. La DMZ stocke différents services et des ressources externes d'un réseau et sert de barrière entre internet et le réseau local. La zone DMZ de l'entreprise fait partie du sous-réseau 192.168.200.0/24. Elle est composée d'un serveur Web et d'un serveur DNS.

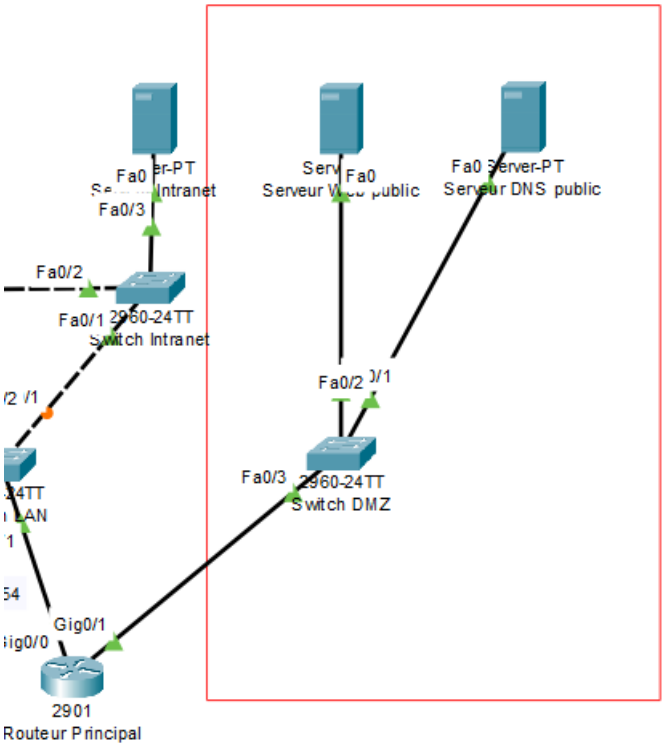


Figure 14 : Zone Démilitarisé DMZ

Le premier service installé sur le serveur de la DMZ est un serveur HTTP qui correspond au site web public. C'est le site web que les clients de l'entreprise verront. Il est accessible via l'url « http://www.technova.fr ».

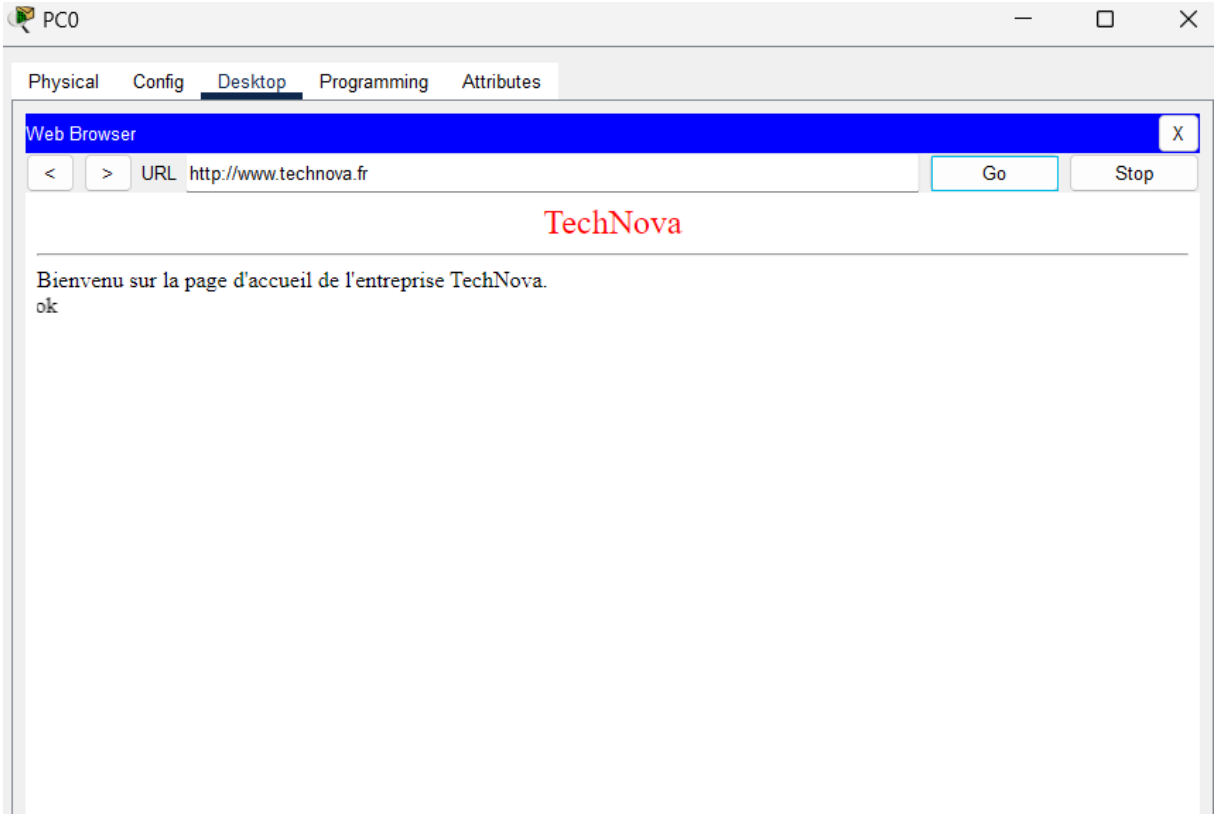


Figure 15 : Page web du site

Le deuxième service présent sur le serveur est le service DNS. Ce service permet de gérer la résolution de noms de l'entreprise. Il faut donc le configurer :

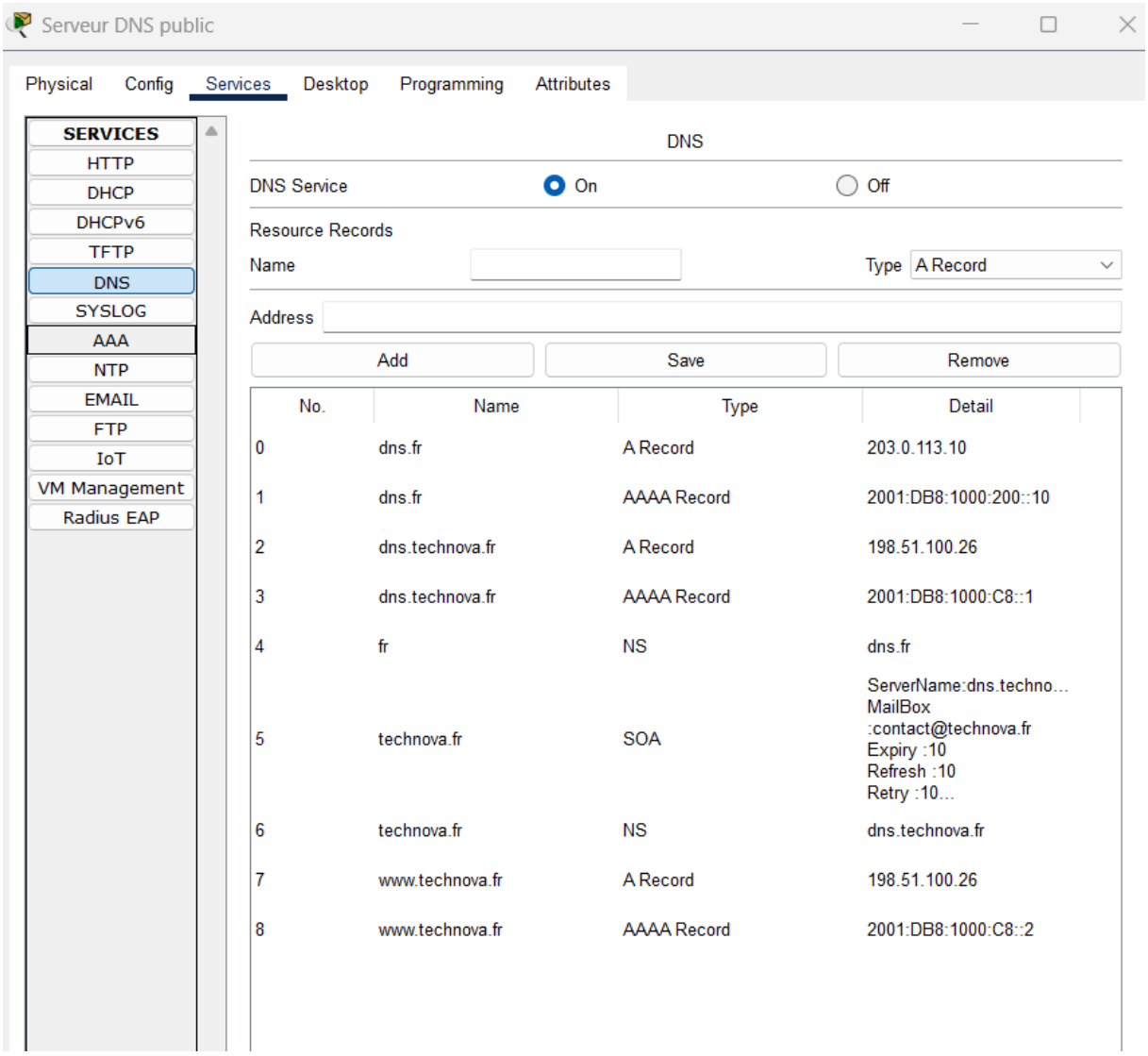


Figure 16 : Configuration DNS du serveur DNS public

dns.fr (A Record) :

Associe dns.fr à l'adresse IPv4 203.0.113.10.

dns.fr (AAAA Record) :

Associe dns.fr à l'adresse IPv6 2001:DB8:1000:200::10.

dns.technova.fr (A Record) :

Associe dns.technova.fr à l'adresse IPv4 198.51.100.26.

dns.technova.fr (AAAA Record) :

Associe dns.technova.fr à l'adresse IPv6 2001:DB8:1000:C8::1.

fr (NS Record) :

Indique que dns.fr est le serveur de noms autoritaire pour la zone fr.

technova.fr (SOA Record) :

Contient des informations sur le serveur de noms principal (dns.technova.fr) pour la zone technova.fr, l'adresse e-mail du responsable (contact@technova.fr), et les paramètres de mise à jour de la zone (Expiry, Refresh, Retry...).

technova.fr (NS Record) :

Indique que dns.technova.fr est le serveur de noms autoritaire pour la zone technova.fr.

www.technova.fr **(A Record)** :

Associe www.technova.fr à l'adresse IPv4 198.51.100.26.

www.technova.fr **(AAAA Record)** :

Associe www.technova.fr à l'adresse IPv6 2001:DB8:1000:C8::2.

On a aussi la configuration du routeur pour le réseau de la DMZ, voici sa configuration :

```
rePrincipal>en
rePrincipal#conf t
rePrincipal(config)#int Gig0/1
rePrincipal(config-if)#ip address 192.168.200.254 255.255.255.0
rePrincipal(config-if)#no shutdown
rePrincipal(config-if)# ipv6 address 2001:DB8:1000:C8::254/64
rePrincipal(config-if)#ipv6 enable
```

Nous allons passer à l'interface, qui relie le routeur Principal et le routeur Secondaire.

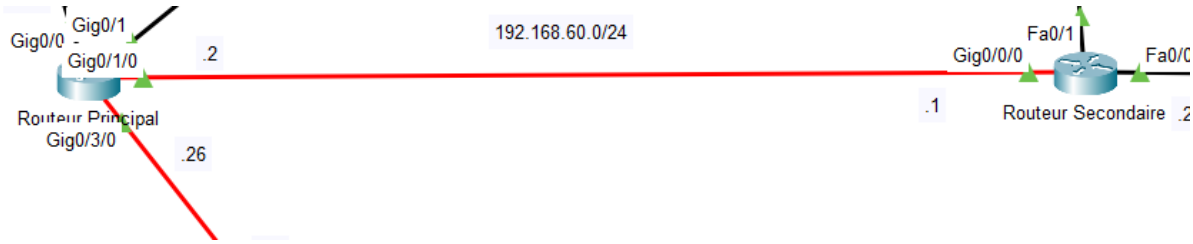


Figure 17 : Liaison entre le Routeur Principal et le Routeur Secondaire

Voici la configuration de l'interface Gig0/1/0 sur le routeur Principal :

```
rePrincipal>en
rePrincipal#conf t
rePrincipal(config)#int Gig0/1/0
rePrincipal(config-if)#ip address 192.168.60.2 255.255.255.0
rePrincipal(config-if)#no shutdown
rePrincipal(config-if)# ipv6 address 2001:DB8:1000:3C::2/64
rePrincipal(config-if)#ipv6 enable
```

Et voici la configuration de l'interface Gig0/0/0 du routeur Secondaire :

```
reSecondaire>en
reSecondaire#conf t
reSecondaire(config)#int Gig0/0/0
reSecondaire(config-if)#ip address 192.168.60.1 255.255.255.0
reSecondaire(config-if)#no shutdown
reSecondaire(config-if)# ipv6 address 2001:DB8:1000:3C::1/64
reSecondaire(config-if)#ipv6 enable
```

4. Bureau ingénieurs et bureau designers

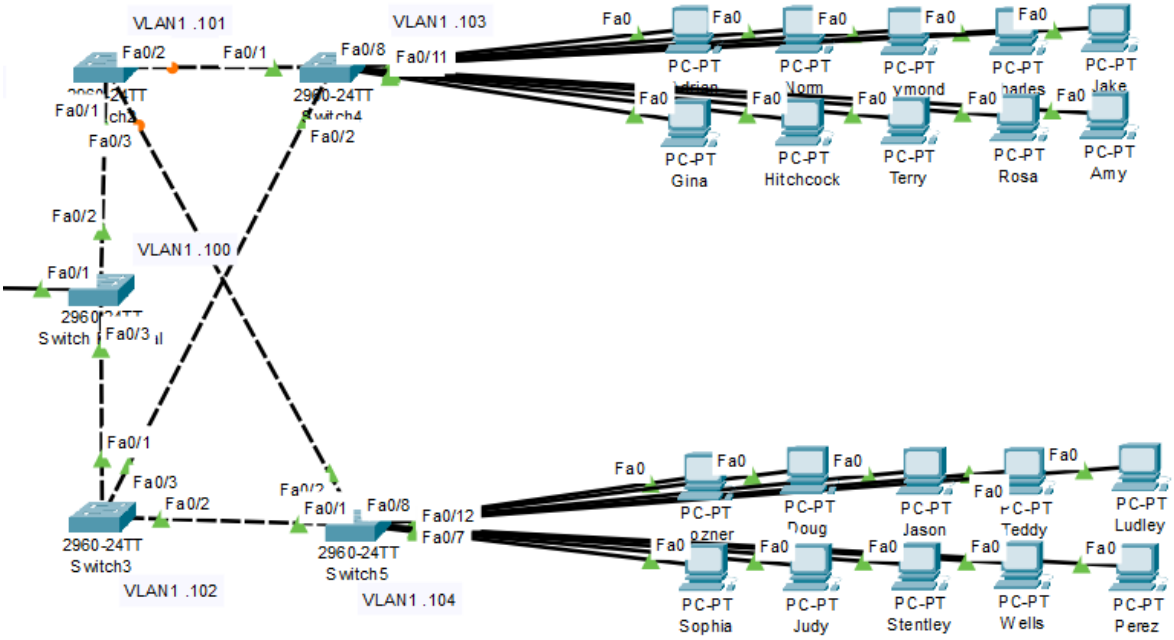


Figure 18 : Bureau ingénieurs et bureau designers

On peut voir ici, 5 routeurs en redondance, et les deux bureaux ingénieurs et designers. Ces différents bureaux sont sur le même réseau qui est 192.168.0.0/24 et tous ces employés sont configurer en méthode statique. Voici la plage d'adresse IPv4 et IPv6 de ces deux réseaux :

	Plages d'adresses IPv4	Plages d'adresses IPv6
Bureau Ingénieurs	192.168.0.1 à 192.168.0.10	2001:DB8:1000::10 à 2001:DB8:1000::19
Bureau Designers	192.168.0.33 à 192.168.0.42	2001:DB8:1000::20 à 2001:DB8:1000::29

Figure 19 : Plages d'adresses IPv4 et IPv6 pour les deux bureaux

Nous allons ensuite configurer l'interface du routeur Secondaire vers ces bureaux :

```
reSecondaire>en
reSecondaire#conf t
reSecondaire(config)#int Fa0/0
reSecondaire(config-if)#ip address 192.168.0.254 255.255.255.0
reSecondaire(config-if)#no shutdown
reSecondaire(config-if)#ipv6 address 2001:DB8:1000::1/64
reSecondaire(config-if)#ipv6 enable
```

5. VLAN 10 et VLAN 20 pour la Direction et le Secrétariat et l'accueil

Pour configurer les réseaux 192.168.10.0/24 et 192.168.20.0/24, je vais utiliser des VLANs. Un Virtual Local Area Network c'est-à-dire la création de plusieurs réseaux. Pour commencer, je vais configurer les 2 VLANs puis je vais affecter une liaison trunk sur les switchs et sur le routeur. Cette liaison particulière permet de faire transiter plusieurs VLANs dans un même lien physique.

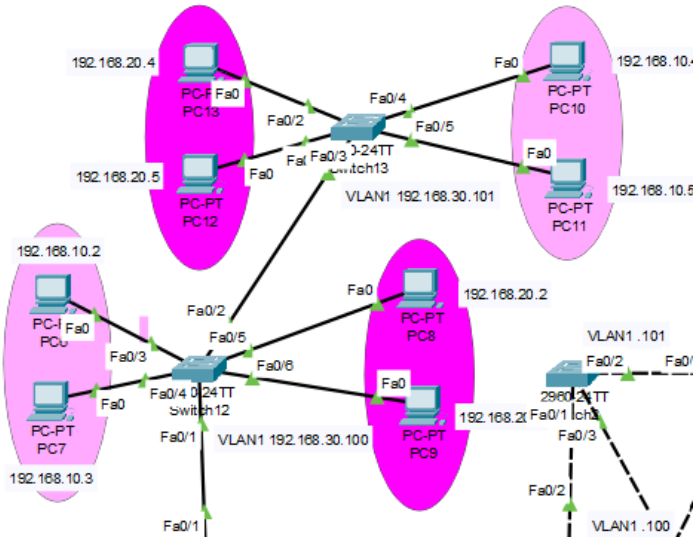


Figure 20 : VLAN 10 et 20

Donc voici la première configuration sur l'interface Fa0/1.10 du routeur Secondaire pour le VLAN 10 :

```
reSecondaire>en
reSecondaire#conf t
reSecondaire(config)#int Fa0/1.10
reSecondaire(config-subif)#encapsulation dot1Q 10
reSecondaire(config-subif)#ip address 192.168.10.1 255.255.255.0
reSecondaire(config-subif)#no shutdown
reSecondaire(config-subif)#ipv6 address 2001:DB8:1000:A::1/64
reSecondaire(config-subif)#ipv6 enable
```

Et la configuration sur l'interface Fa0/1.20 du routeur Secondaire pour le VLAN 20 :

```
reSecondaire>en
reSecondaire#conf t
reSecondaire(config)#int Fa0/1.20
reSecondaire(config-subif)#encapsulation dot1Q 10
reSecondaire(config-subif)#ip address 192.168.20.1 255.255.255.0
reSecondaire(config-subif)#no shutdown
reSecondaire(config-subif)#ipv6 address 2001:DB8:1000:14::1/64
reSecondaire(config-subif)#ipv6 enable
```

L'interface des switchs qui sont reliés entre eux et au routeur Secondaire sont reliés en mode Trunk.

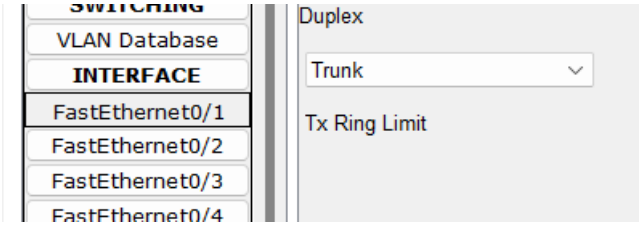


Figure 21 : Interface en mode trunk

On configure également en statique les pc du VLAN 10 et du VLAN 20 :

	Plages d'adresses IPv4	Plages d'adresses IPv6
Direction (VLAN 10)	192.168.10.2 à 192.168.10.5	2001:DB8:1000:A::2 à 2001:DB8:1000:A::5
Secrétariat et Accueil (VLAN 20)	192.168.20.2 à 192.168.20.5	2001:DB8:1000:14::2 à 2001:DB8:1000:14::5

Figure 22 : Plages des adresses IPv4 et IPv6 des VLAN 10 et VLAN 20

Pour finir cette première partie, chaque appareil du réseau est relié à sa passerelle par défaut (interface du routeur concerné) et aussi, chaque appareil est relié au serveur Intranet d'adresse IPv4 192.168.1.71/24 et en IPv6 2001:DB8:1000:1::71/64. Nous configurerons le SSH plus tard dans le compte rendu et le routage OSPF aussi pour respecter le modèle OSI ascendant.

Configuration du réseau de la FAI

Cette partie est dédiée à la configuration du réseau FAI (Fournisseur d'Accès à Internet) et à ses équipements. J'ai choisi Orange comme FAI. L'adresse réseau du FAI est 203.0.113.0/24 et 2001:DB8:1000:200::/64.

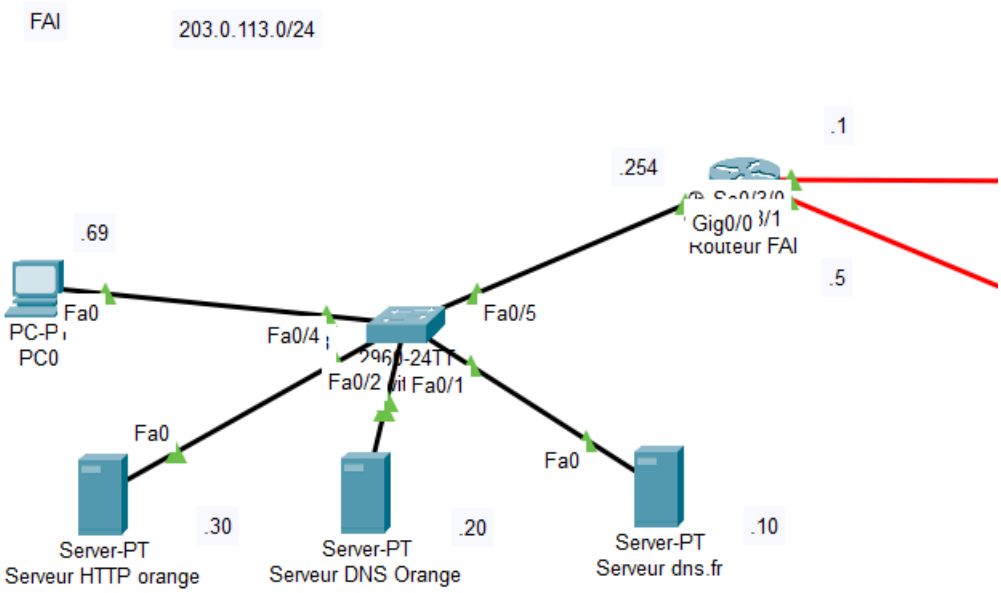


Figure 23 : Réseau de la FAI

1. Les serveurs

Dans cette partie de réseau, nous allons trouver 3 serveurs et 1 client internet. Les serveurs présents dans le FAI sont un serveur Web et deux serveurs DNS. Le serveur web contient la page internet du FAI. Elle est accessible via l'url « www.orange.fr » et elle contient une page « index.html » :

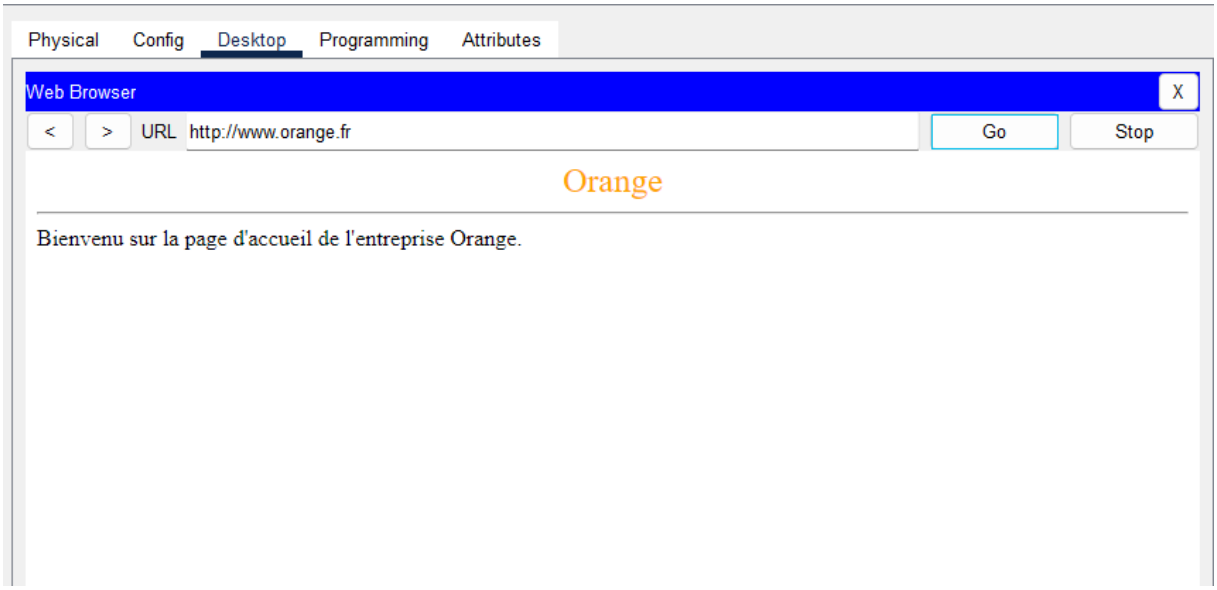


Figure 24 : Site web du FAI

Le premier serveur DNS (203.0.113.20, 2001:DB8:1000:200::20) est le serveur du FAI (orange.fr). Comme l'entreprise, il faut que le FAI fasse des résolutions de noms pour que les clients puissent accéder aux autres sites web. Voici le contenu de ce serveur DNS :

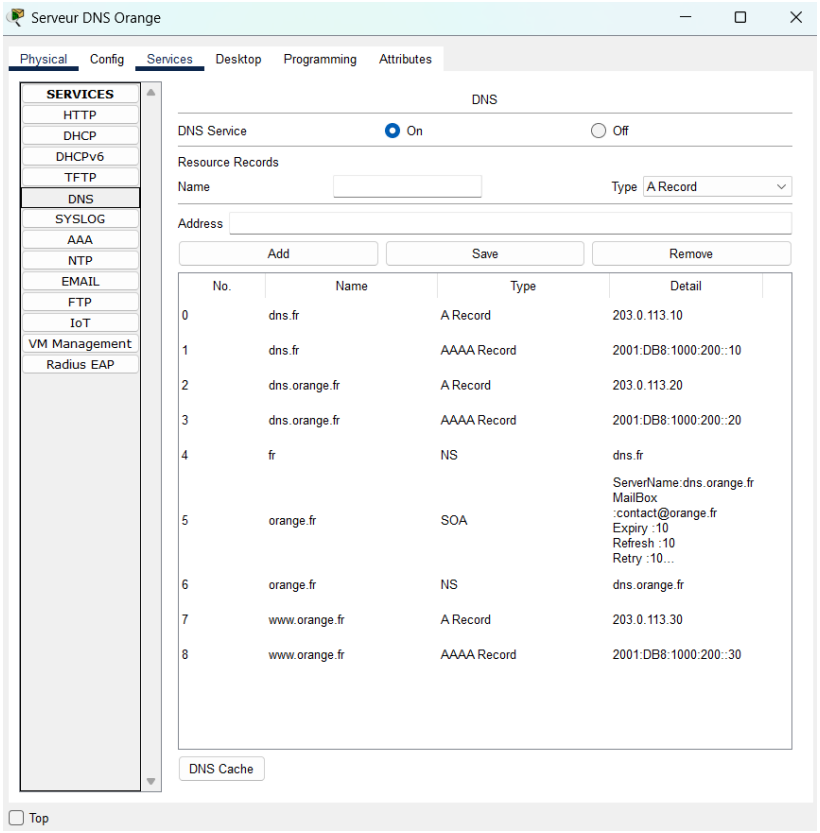


Figure 25 : Configuration du serveur DNS Orange

dns.fr (A Record) :

Associe dns.fr à l'adresse IPv4 203.0.113.10.

dns.fr (AAAA Record) :

Associe dns.fr à l'adresse IPv6 2001:DB8:1000:200::10.

dns.orange.fr (A Record) :

Associe dns.orange.fr à l'adresse IPv4 203.0.113.20.

dns.orange.fr (AAAA Record) :

Associe dns.orange.fr à l'adresse IPv6 2001:DB8:1000:200::20.

fr (NS Record) :

Indique que dns.fr est le serveur de noms autoritaire pour la zone fr.

orange.fr (SOA Record) :

Contient des informations sur le serveur de noms principal (dns.orange.fr) pour la zone orange.fr, l'adresse e-mail du responsable (contact@orange.fr), et les paramètres de mise à jour de la zone :

- ServerName : dns.orange.fr
- MailBox : contact@orange.fr
- Expiry : 10
- Refresh : 10
- Retry : 10
- ...

orange.fr (NS Record) :

Indique que dns.orange.fr est le serveur de noms autoritaire pour la zone orange.fr.

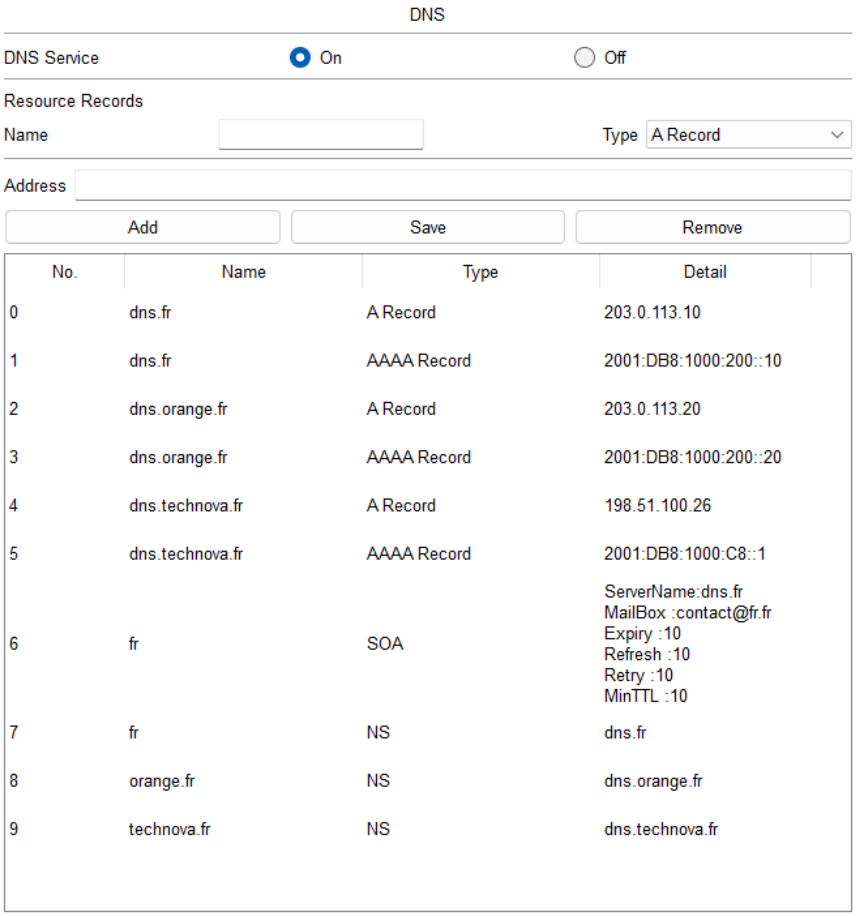
www.orange.fr **(A Record)** :

Associe www.orange.fr à l'adresse IPv4 203.0.113.30.

www.orange.fr **(AAAA Record)** :

Associe www.orange.fr à l'adresse IPv6 2001:DB8:1000:200::30.

Le deuxième serveur DNS (203.0.113.10, 2001:DB8:1000:200::10) est le serveur DNS.fr qui est le serveur racine. Voici sa configuration :



No.	Name	Type	Detail
0	dns.fr	A Record	203.0.113.10
1	dns.fr	AAAA Record	2001:DB8:1000:200::10
2	dns.orange.fr	A Record	203.0.113.20
3	dns.orange.fr	AAAA Record	2001:DB8:1000:200::20
4	dns.technova.fr	A Record	198.51.100.26
5	dns.technova.fr	AAAA Record	2001:DB8:1000:C8::1
6	fr	SOA	ServerName:dns.fr MailBox :contact@fr.fr Expiry :10 Refresh :10 Retry :10 MinTTL :10
7	fr	NS	dns.fr
8	orange.fr	NS	dns.orange.fr
9	technova.fr	NS	dns.technova.fr

Figure 26 : Configuration du serveur DNS.fr

dns.fr (A Record) :

Associe dns.fr à l'adresse IPv4 203.0.113.10.

dns.fr (AAAA Record) :

Associe dns.fr à l'adresse IPv6 2001:DB8:1000:200::10.

dns.orange.fr (A Record) :

Associe dns.orange.fr à l'adresse IPv4 203.0.113.20.

dns.orange.fr (AAAA Record) :

Associe dns.orange.fr à l'adresse IPv6 2001:DB8:1000:200::20.

dns.technova.fr (A Record) :

Associe dns.technova.fr à l'adresse IPv4 198.51.100.26.

dns.technova.fr (AAAA Record) :

Associe dns.technova.fr à l'adresse IPv6 2001:DB8:1000:C8::1.

fr (SOA Record) :

Contient des informations sur le serveur de noms principal (dns.fr) pour la zone fr, l'adresse e-mail du responsable (contact@fr.fr), et les paramètres de mise à jour de la zone :

- ServerName : dns.fr
- MailBox : contact@fr.fr
- Expiry : 10
- Refresh : 10
- Retry : 10
- ...

fr (NS Record) :

Indique que dns.fr est le serveur de noms autoritaire pour la zone fr.

orange.fr (NS Record) :

Indique que dns.orange.fr est le serveur de noms autoritaire pour la zone orange.fr.

technova.fr (NS Record) :

Indique que dns.technova.fr est le serveur de noms autoritaire pour la zone technova.fr.

Le Client Internet sera configuré en statique avec l'adresse IP 203.0.113.69/24, 2001:DB8:1000:200::69/64. Ce client aura comme serveur DNS le serveur du FAI.

Tout les membres du réseau on comme route par défaut l'interface du routeur FAI. Voici sa configuration :

```
reFAI>en
reFAI#conf t
reFAI(config)#int Gig0/0
reFAI(config-if)#ip address 203.0.113.254 255.255.255.0
reFAI(config-if)#no shutdown
reFAI(config-if)#ipv6 address 2001:DB8:1000:200::254/64
reFAI(config-if)#ipv6 enable
```

2. Backbone

Le backbone est la partie principale d'un réseau informatique, constituée de liaisons à haute capacité et de routeurs principaux, qui interconnecte différentes sections ou segments d'un réseau. Il permet le transfert rapide et efficace de données entre les sous-réseaux, assurant la communication entre divers sites, centres de données et utilisateurs.

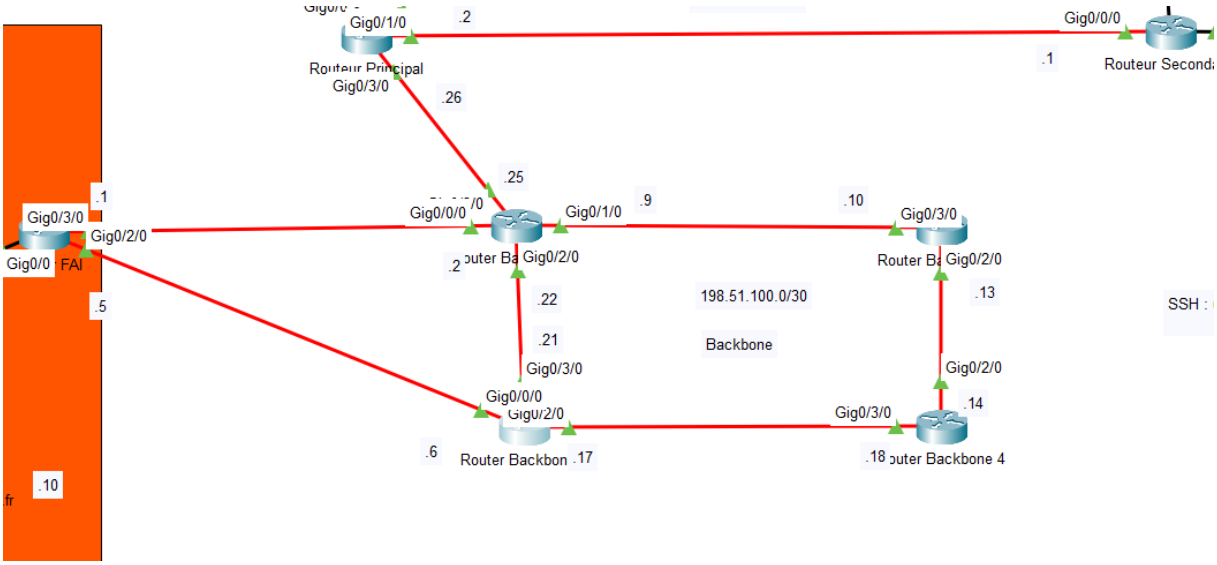


Figure 27 : Backbone

J'ai découpé cette backbone en sous réseaux avec comme adresse IPv4 198.51.100.0/30 comme on peu voir sur la figure 27. J'ai aussi configuré chaque interface en IPv6 global. Voici la plage que j'ai pu faire :

2001:DB8:1000:100::1/64 et 2001:DB8:1000:100::2/64,

2001:DB8:1000:101::5/64 et 2001:DB8:1000:101::6/64,

2001:DB8:1000:102::9/64 et 2001:DB8:1000:102::10/64,

2001:DB8:1000:103::13/64 et 2001:DB8:1000:103::14/64,

2001:DB8:1000:104::17/64 et 2001:DB8:1000:104::18/64,

2001:DB8:1000:105::21/64 et 2001:DB8:1000:105::22/64,

2001:DB8:1000:106::25/64 et 2001:DB8:1000:106::26/64.

Routage OSPF et OSPFv3

Le routage OSPF (Open Shortest Path First) est un protocole de routage à état de liens utilisé pour déterminer le meilleur chemin pour le trafic de données au sein d'un réseau IP. OSPF fonctionne en distribuant des informations sur l'état des liens entre les routeurs, qui construisent ensuite une vue de la topologie complète du réseau. Il utilise l'algorithme de Dijkstra pour calculer les chemins les plus courts, assurant une mise à jour rapide et efficace des routes en cas de changement de la topologie du réseau.

Nous allons commencer par le routage OSPF du Routeur Principal de l'entreprise :

```
router ospf 1
router-id 1.1.1.1
network 192.168.1.0 0.0.0.255 area 1
network 192.168.200.0 0.0.0.255 area 1
network 192.168.60.0 0.0.0.255 area 1
```

Et on active le routage :

```
ip routing
```

```
router ospf 1
 router-id 1.1.1.1
 log-adjacency-changes
 network 192.168.1.0 0.0.0.255 area 1
 network 192.168.200.0 0.0.0.255 area 1
 network 192.168.60.0 0.0.0.255 area 1
```

Figure 28 : Routage OSPF sur le Routeur Principal

On met une route par défaut vers le premier routeur de la backbone pour éviter de faire des ACL plus tard :

```
ip route 0.0.0.0 0.0.0.0 198.51.100.25
```

On va ensuite configurer le routage OSPF pour le routeur Secondaire :

```
router ospf 1
router-id 2.2.2.2
network 192.168.0.0 0.0.0.255 area 1
network 192.168.10.0 0.0.0.255 area 1
network 192.168.20.0 0.0.0.255 area 1
network 192.168.60.0 0.0.0.255 area 1
network 192.168.30.0 0.0.0.255 area 1
```

Et on active aussi le routage :

```
ip routing
```

```
router ospf 1
 router-id 2.2.2.2
 log-adjacency-changes
 network 192.168.0.0 0.0.0.255 area 1
 network 192.168.10.0 0.0.0.255 area 1
 network 192.168.20.0 0.0.0.255 area 1
 network 192.168.60.0 0.0.0.255 area 1
 network 192.168.30.0 0.0.0.255 area 1
```

Figure 29 : Routage OSPF pour le routeur Secondaire

Nous allons essayer un PING entre le pc Administrateur réseau et un des PC dans la VLAN 10 pour voir si le routage fonctionne bien.

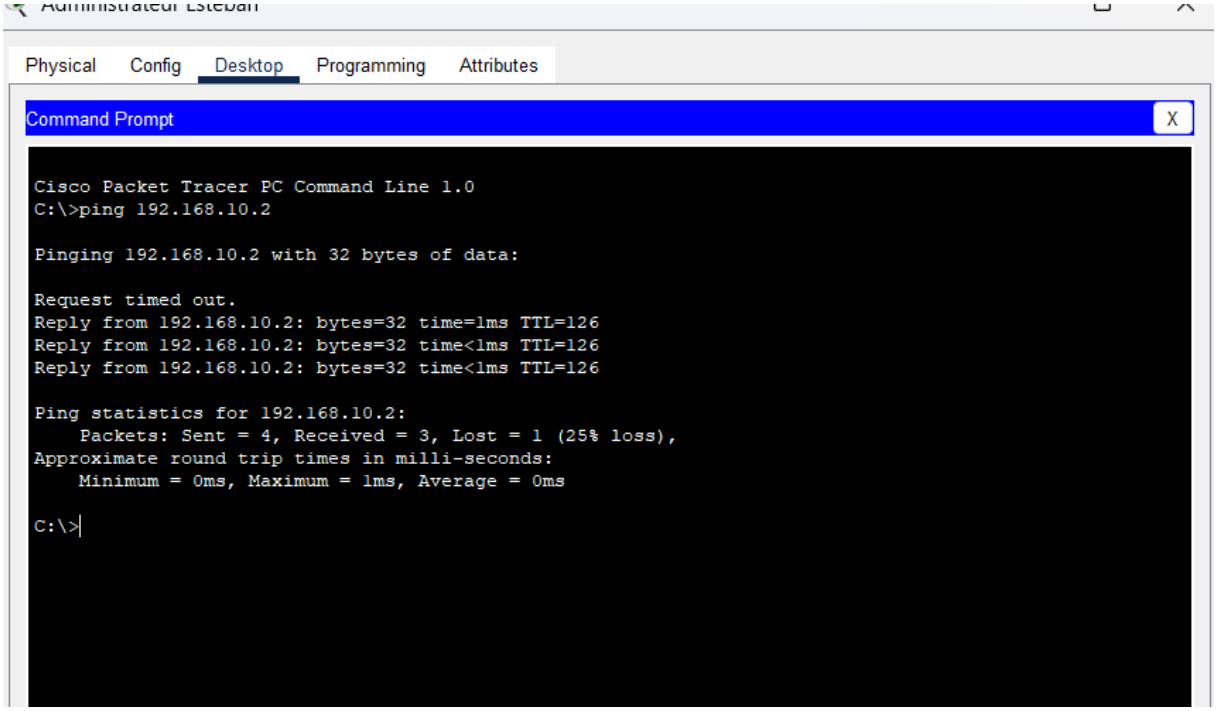


Figure 30 : PING entre Administrateur et la Direction

Le ping fonctionne donc le routage OSPF fonctionne bien aussi.

Nous allons donc passer au routage du Routeur du FAI voici sa configuration :

```
router ospf 1
router-id 3.3.3.3
log-adjacency-changes
network 203.0.113.0 0.0.0.255 area 0
network 198.51.100.0 0.0.0.3 area 0
network 198.51.100.4 0.0.0.3 area 0
```

Et on active le routage :

```
ip routing
```

```
router ospf 1
 router-id 3.3.3.3
 log-adjacency-changes
 network 203.0.113.0 0.0.0.255 area 0
 network 198.51.100.0 0.0.0.3 area 0
 network 198.51.100.4 0.0.0.3 area 0
```

Figure 31 : Routage OSPF du routeur FAI

Et nous allons aussi configurer le routage sur tous les routeurs de la backbone de la même manière en prenant chaque réseau directement connecté.

Pour faire du routage OSPF en IPv6, nous allons utiliser OSPv3, la différence avec l'OSPF classique c'est qu'on va directement activer le routage sur les interfaces des routeurs. Voici la syntaxe :

```
ipv6 router ospf 1
router-id 1.1.1.1
```

Et sur une interface on applique le routage :

```
ipv6 ospf 1 area 1
```

Et finalement on applique le routage IPv6 :

```
ipv6 unicast-routing
```

On répète cette étape pour chaque routeur du réseau, et on change le « area 1 » en « area 0 » quand c'est nécessaire comme en ipv4.

Nous allons maintenant essayer un PING entre le pc de l'Administrateur Réseau et le client Internet mais cela n'aboutira pas puisque que nous n'avons pas mis en place la traduction d'adresse NAT.

Traduction d'adresses NAT

Le NAT est une technique utilisée pour modifier les adresses IP dans les en-têtes des paquets IP en transit à travers un routeur ou un pare-feu. Il permet aux réseaux privés avec des adresses IP non routables globalement de communiquer avec des réseaux externes en utilisant une adresse IP publique unique ou un ensemble d'adresses IP publiques. NAT aide à conserver les adresses IPv4 et à renforcer la sécurité en masquant les adresses IP internes.

Sur mon réseau j'ai pu réaliser 1 NAT pour le routeur Principal :

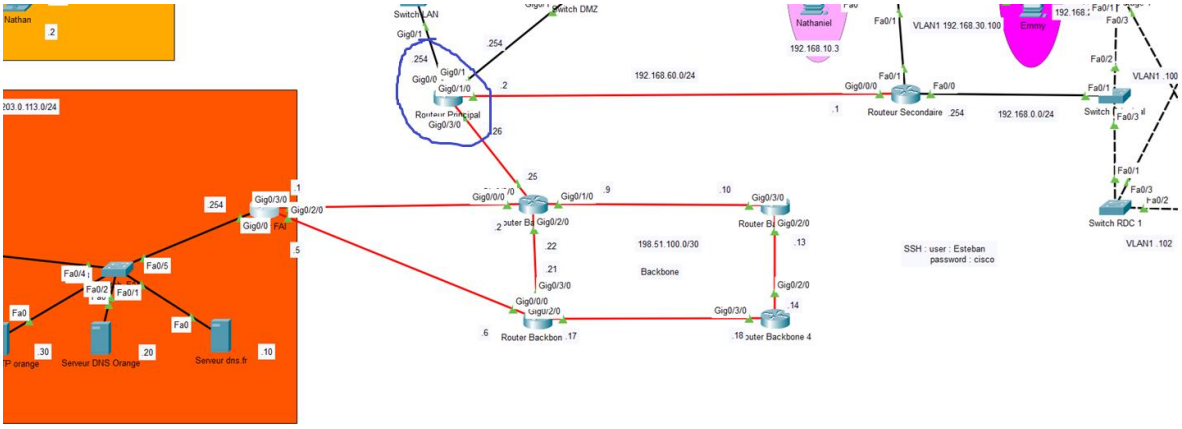


Figure 32 : Configuration NAT

Voici la configuration du NAT du routeur Principal :

```
access-list 99 permit 192.168.0.0 0.0.0.255
access-list 99 permit 192.168.1.0 0.0.0.255
access-list 99 permit 192.168.60.0 0.0.0.255
access-list 99 permit 192.168.200.0 0.0.0.255
access-list 99 permit 192.168.20.0 0.0.0.255
access-list 99 permit 192.168.10.0 0.0.0.255
```

On utilise ici des ACL (Access Control List) qui est un ensemble de règles utilisées pour contrôler le trafic réseau en spécifiant quels paquets de données sont autorisés ou refusés à travers un réseau. Les ACL sont appliquées sur les routeurs et les pares-feux pour filtrer le trafic basé sur des critères tels que les adresses IP source et destination, les numéros de port et les protocoles. Elles permettent d'améliorer la sécurité et la gestion du réseau en régulant l'accès aux ressources réseau. Ici on autorise l'accès à tous les réseaux directement connectés.

On va appliquer les ACL sur les interfaces du routeur en utilisant les mots clés inside pour dire que c'est le réseaux intérieur et outside pour le réseau extérieur.

```
int Gig0/0
ip nat inside
```

```
int Gig0/1
ip nat inside
```

```
int Gig0/1/0
ip nat inside
```

```
int Gig0/3/0
ip nat outside
```

```
ip nat inside source list 99 interface GigabitEthernet0/3/0
overload
```

Ici on autorise l'accès aux réseaux inside d'accéder au réseau outside.

Ensuite on va autoriser les ports pour permettre l'accès aux pages web et du coup aux requêtes http et DNS.

```
ip nat inside source static tcp 192.168.200.2 80 198.51.100.26 80
ip nat inside source static udp 192.168.200.1 53 198.51.100.26 53
```

On va maintenant essayer un ping de l'administrateur réseau vers le client internet :

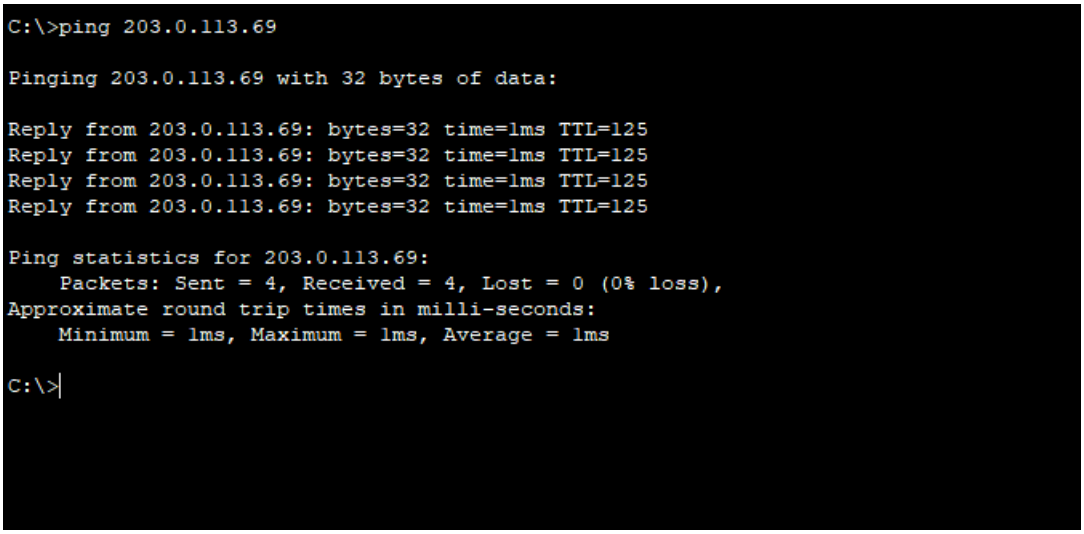


Figure 33 : Ping aboutit de l'administrateur réseau vers le client internet

Et on va essayer d'accéder au site web de l'entreprise depuis le client internet :

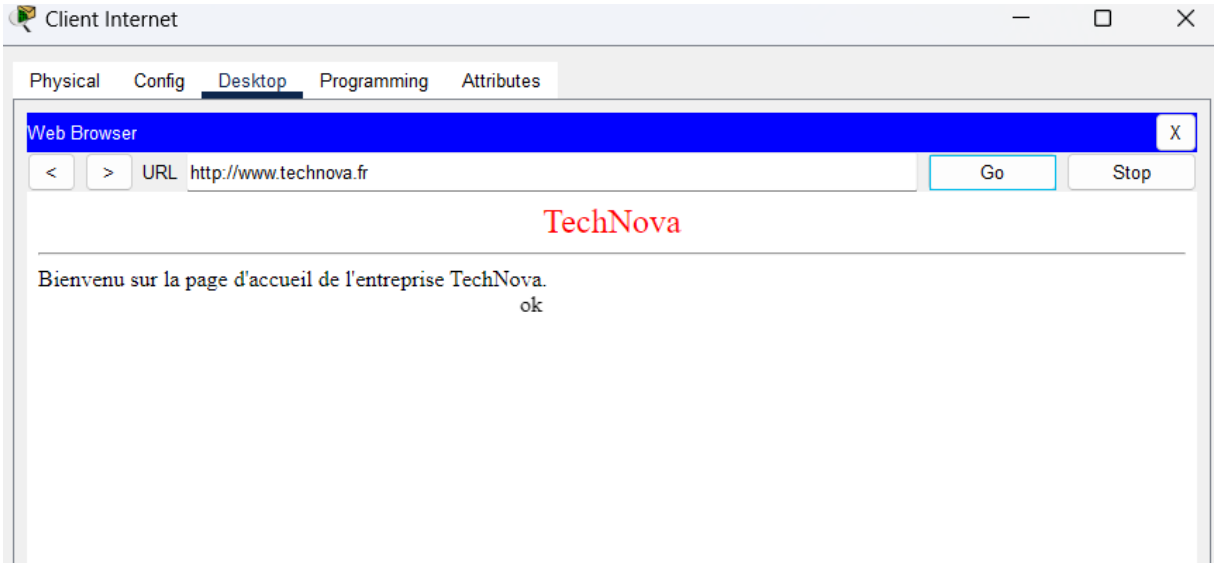


Figure 34 : Requête HTTP du client Internet vers entreprise

Nous n'avons pas besoin de configurer de NAT pour l'IPv6 car ils utilisent le système d'adresse unique local qui ne sont pas routable sur internet et des adresses globales qui sont routable sur internet.

Mis en place des ACL

Les Access Control Lists (ACL) sont essentielles pour sécuriser les réseaux en contrôlant le trafic autorisé et refusé. Elles permettent de définir des règles précises pour filtrer le trafic basé sur des critères spécifiques comme les adresses IP et les protocoles.

Pour sécuriser le réseau de Technova, il est crucial d'empêcher l'accès des réseaux privés à la DMZ et vice versa. La DMZ, qui héberge des services accessibles de l'extérieur comme les serveurs web et DNS, doit être isolée des réseaux internes pour minimiser les risques de sécurité.

En mettant en place des ACL spécifiques sur les interfaces des routeurs, nous pouvons bloquer le trafic entre les réseaux privés et la DMZ tout en permettant les autres communications nécessaires. Cela garantit que seules les connexions autorisées sont permises, protégeant ainsi les ressources internes de Technova contre les accès non autorisés et les menaces potentielles.

Nous allons donc configurer les ACL sur le routeur principal.

Routeur Principal

ACL « VERS_DMZ »

Cette ACL permet d'empêcher la DMZ d'accéder à tous les réseaux privés.

```
ip access-list extended VERS_DMZ
permit udp any host 192.168.200.1 eq domain
permit tcp any host 192.168.200.2 eq www
deny ip any any
```

On applique cette ACL sur l'interface Gig0/1 en out

```
ip access-group VERS_DMZ out
```

ACL « VERS_DMZ6 »

```
ipv6 access-list VERS_DMZ6
permit udp any host 2001:DB8:1000:C8::1 eq domain
permit tcp any host 2001:DB8:1000:C8::2 eq www
deny ipv6 any any
```

On applique cette ACL sur l'interface Gig0/1 en out

```
ipv6 traffic-filter VERS_DMZ6 out
```

On test donc un ping d'un employé de l'entreprise, vers la DMZ :

```
C:\>ping 192.168.200.2

Pinging 192.168.200.2 with 32 bytes of data:

Reply from 192.168.1.254: Destination host unreachable.
Reply from 192.168.1.254: Destination host unreachable.
Reply from 192.168.1.254: Destination host unreachable.
Reply from 192.168.1.254: Destination host unreachable.

Ping statistics for 192.168.200.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Figure 35 : Ping d'un pc de l'entreprise vers la DMZ

On voit ici que les serveurs de la DMZ sont inaccessibles, testons côté internet :

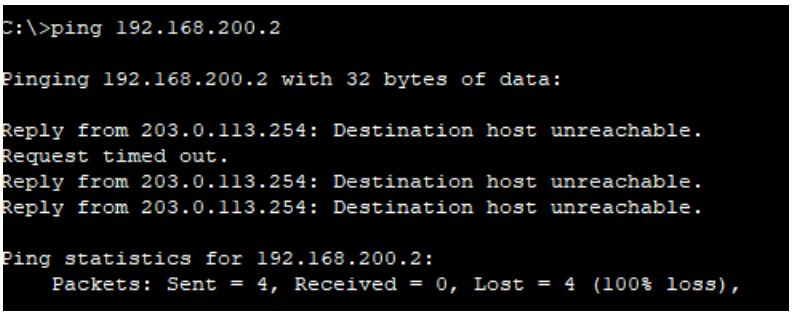


Figure 36 : Ping du client internet vers la DMZ

Personne ne peut accéder à la DMZ ce qui est cohérent. Testons d'accéder aux services de la DMZ maintenant :

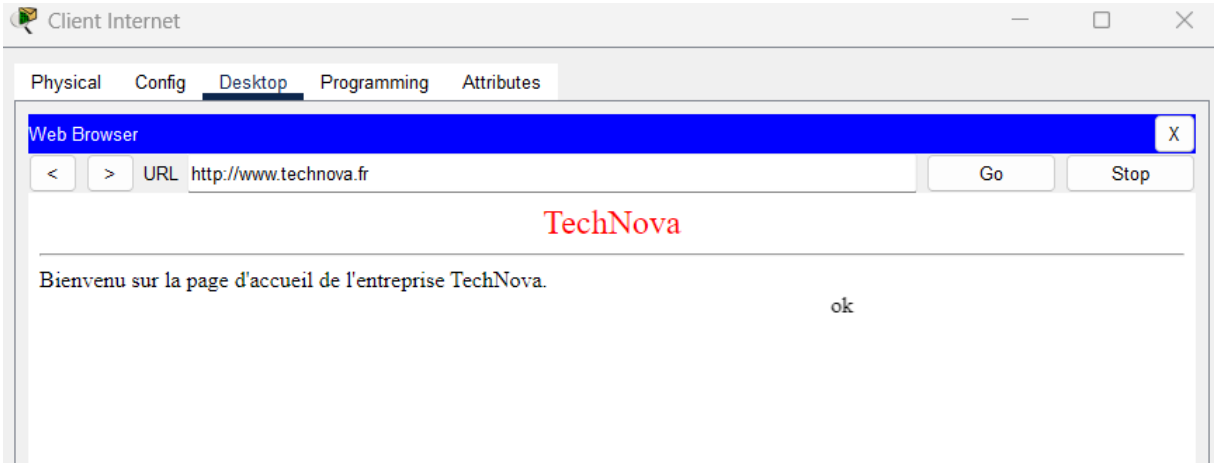


Figure 37 : Accès aux services de la DMZ grâce aux ACL

On voit bien ici qu'on accède au service de la DMZ depuis le client Internet ce qui valide nos ACL.

Configuration SSH pour le réseau de l'entreprise

Les équipements d'interconnexion tels que les switchs et les routeurs doivent être sécurisés. Afin de sécuriser les appareils, il faut configurer sur chaque équipement le service SSH qui permet de configurer, à distance, des appareils informatiques de manière cryptée. De plus, il faut sécuriser les switchs et les routeurs par des mots de passe pour que seul l'administrateur réseau puisse accéder aux privilèges d'administrateur.

Chaque switch contient un VLAN par défaut (VLAN 1). C'est grâce à ce VLAN que nous allons pouvoir nous connecter à distance sur les switchs. Pour les routeurs, ce sont les interfaces qui vont permettre de s'y connecter.

Voici la liste des appareils avec l'adresse IP à laquelle se connecter :

Routeur Principal	192.168.1.254
Routeur Secondaire	192.168.60.1
Switch Réunion	192.168.1.103
Switch LAN	192.168.1.102
Switch Admin	192.168.1.100
Switch Intranet	192.168.1.101
Switch VLAN1	192.168.30.100
Switch VLAN2	192.168.30.101
Switch Principal	192.168.0.100
Switch RDC 1	192.168.0.102
Switch RDC 2	192.168.0.104
Switch 1e etage 1	192.168.0.101
Switch 1e etage 2	192.168.0.103

Figure 38 : Liste des appareils pour se connecter en ssh

On partira du principe, que l'administrateur se connectera que en ipv4.

Voici un exemple de connexion de l'Administrateur Réseau sur le switch LAN par exemple :

On rentre les détails pour la configuration ssh :

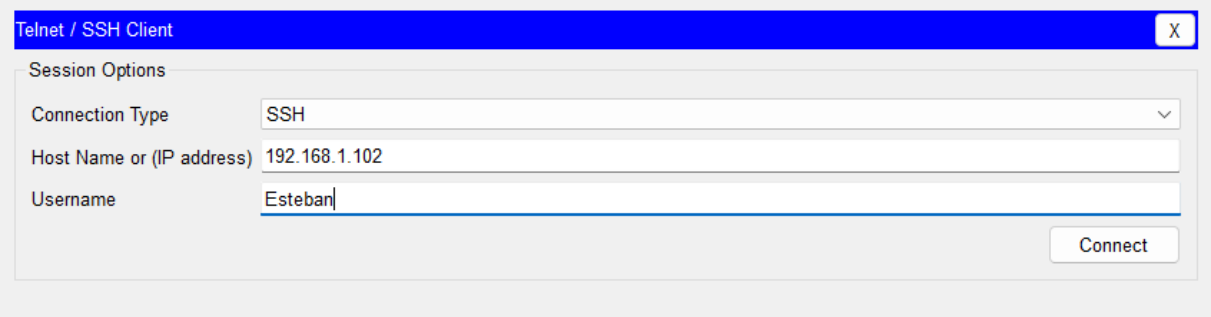


Figure 39 : Details de la connexion ssh

Ensuite, on se connecte avec le mot de passe « cisco » pour accéder directement à la configuration à distance du switch LAN :

Figure 40 : Mot de passe à rentrer pour accéder à distance au switch LAN

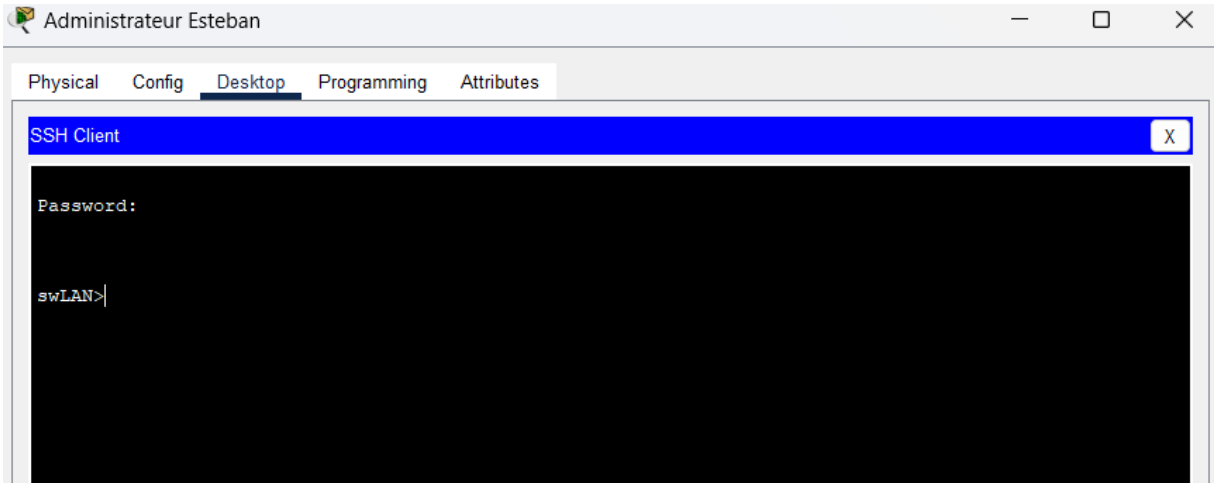


Figure 41 : Connexion au switch LAN à distance

Voici la configuration pour le switch réunion par exemple :

```
interface Vlan1
ip address 192.168.1.103 255.255.255.0

line vty 0 4
logging synchronous
login local
transport input ssh
line vty 5 15
logging synchronous
login local
transport input ssh
```

Conclusion

Au cours de ce projet, j'ai réalisé le réseau informatique d'une petite entreprise nommé Technova tout en respectant un cahier des charges bien précis dans le but de faire une synthèse de mes connaissances en réseau informatique que j'ai acquises lors des semestres 1 et 2 de cette première année de BUT R&T. Apprendre à réaliser la conception d'un réseau informatique en tant qu'étudiants est bénéfique pour la suite de nos études et de notre carrière car nous pourrons être sollicité pour construire divers réseaux informatiques.

Liste des figures

Figure 1 : Première conception de l'entreprise 4
Figure 2 : Deuxième conception du réseau en schéma 6
Figure 3 : Schéma final du réseau de l'entreprise Technova 7
Figure 4 : Différents réseaux interne IPV4 8
Figure 5 : Différents réseaux interne IPV6 8
Figure 6 : Câblage du réseau en entier comme sur le schéma 9
Figure 7 : Salle de réunion, client DHCP 10
Figure 8 : Adressage automatique grâce au DHCP 12
Figure 9 : Adressage automatique grâce au DHCP 13
Figure 10 : Serveur Intranet 14
Figure 11 : Site web de l'entreprise accessible qu'aux employés 15
Figure 12 : Configuration DNS du serveur Intranet 16
Figure 13 : Administrateur Réseau sur le LAN 18
Figure 14 : Zone Démilitarisé DMZ 19
Figure 15 : Page web du site 20
Figure 16 : Configuration DNS du serveur DNS public 21
Figure 17 : Liaison entre le Routeur Principal et le Routeur Secondaire 23
Figure 18 : Bureau ingénieurs et bureau designers 24
Figure 19 : Plages d'adresses IPv4 et IPv6 pour les deux bureaux 25
Figure 20 : VLAN 10 et 20 25
Figure 21 : Interface en mode trunk 26
Figure 22 : Plages des adresses IPv4 et IPv6 des VLAN 10 et VLAN 20 27
Figure 23 : Réseau de la FAI 28
Figure 24 : Site web du FAI 29
Figure 25 : Configuration du serveur DNS Orange 29
Figure 26 : Configuration du serveur DNS.fr 31
Figure 27 : Backbone 33
Figure 28 : Routage OSPF sur le Routeur Principal 35
Figure 29 : Routage OSPF pour le routeur Secondaire 36
Figure 30 : PING entre Administrateur et la Direction 37
Figure 31 : Routage OSPF du routeur FAI 38
Figure 32 : Configuration NAT 39
Figure 33 : Ping aboutit de l'administrateur réseau vers le client internet 41
Figure 34 : Requête HTTP du client Internet vers entreprise 42
Figure 35 : Ping d'un pc de l'entreprise vers la DMZ 44
Figure 36 : Ping du client internet vers la DMZ 45
Figure 37 : Accès aux services de la DMZ grâce aux ACL 45
Figure 38 : Liste des appareils pour se connecter en ssh 46
Figure 39 : Details de la connexion ssh 47
Figure 40 : Mot de passe à rentrer pour accéder à distance au switch LAN 47
Figure 41 : Connexion au switch LAN à distance 47