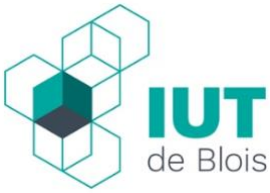
SAE 2.01 – Construire un réseau informatique pour une petite structure



Rapport détaillé – SAE 2.01

IUT de Blois

HEURTEBISE Johan

2024-2025

université de TOURS | Institut universitaire de technologie de Blois

Table des matières

1 Introduction

1.1 Présentation du contexte

1.1.1 Mise en situation

Dans le cadre de la SAE 2.01, nous avons dû concevoir une architecture réseau complète pour une entreprise. Cette architecture devait être aussi réaliste que possible, répondant à des besoins concrets tels que la gestion de différents services et la communication avec des FAI. Notre entreprise (Ciscorporation) est organisée en différentes salles, chacune ayant une fonction spécifique. Dans chaque salle, nous retrouvons différents équipements finaux, mais aussi des commutateurs.

1.1.2 Objectifs du projet

Ce projet a pour but de nous faire progresser et de consolider les compétences réseaux que nous avons acquises pendant l'année. On y retrouve des protocoles très utilisés en entreprise comme DHCP, DNS, IPv4 et IPv6.

Il nous permet aussi de mieux maîtriser la configuration des équipements Cisco, notamment les switches et les routeurs. Grâce à cette SAE, on a un aperçu concret de l'architecture réseau en entreprise, et on apprend à réfléchir de manière logique pour concevoir un réseau ou résoudre des problèmes.

1.2 Démarche de réalisation du projet

1.2.1 Méthodologie

Pour bien avancer dans notre projet, nous avons choisi de suivre une méthode de travail claire et structurée. On va réaliser les différentes étapes de façon logique et organisée.

D'abord, on commencera par créer les différentes salles et les associer à leurs VLAN respectifs. Ensuite, on configurera tous les équipements du réseau de l'entreprise, avant de passer à la mise en place des FAI.

Cette approche nous permettra de travailler dans de bonnes conditions et d'avoir une vue d'ensemble sur notre architecture. Une fois tout en place, on fera une série de tests pour vérifier que le réseau fonctionne correctement.

1.2.2 Outils utilisés

Pour réussir ce projet, nous allons utiliser plusieurs outils et ressources. Tout d'abord, on travaillera sur Cisco Packet Tracer, qui nous servira à concevoir et tester notre réseau.

En parallèle, on s'appuiera sur différentes connaissances acquises au cours de l'année. Par exemple, on a accès à pas mal de ressources via les formations Cisco sur Netacad, comme le CCNA ou l'initiation à Cisco Packet Tracer, qui vont bien nous aider tout au long du projet.

2 Conception globale du réseau LAN d'entreprise, et DMZ

Pour assurer une communication fluide, un minimum de sécurité et une adaptation aux besoins de chaque service de l'entreprise, nous avons conçu notre réseau local (LAN) en nous appuyant sur une organisation claire, à la fois physique et logique.

Dans cette partie, nous allons présenter les choix techniques que nous avons faits pour mettre en place une infrastructure à la fois performante, flexible et fiable.

On parlera de l'agencement des différentes salles, des équipements qu'on a installés, de la segmentation du réseau avec les VLANs, du plan d'adressage en IPv4 et IPv6, des services internes comme le serveur intranet ou le DHCP, et enfin des mécanismes de redondance qu'on a mis en place pour assurer la continuité du service.

2.1 Organisation Physique et Logique des salles

En premier lieu, nous avons créé différents espaces dédiés à chaque fonction de l'entreprise, tels que des bureaux d'ingénieurs, des espaces de travail collaboratifs, une salle des serveurs, etc.

2.1.1 Organisation des différentes salles de l'entreprise

Nous avons procédé à l'installation d'équipements adaptés à la nature des services offerts dans chaque espace. Par exemple, nous avons installé des imprimantes dans les salles où le métier en nécessite. Cette démarche a été appliquée à chaque salle de notre entreprise.

Nous pouvons dresser le tableau suivant, avec les différentes salles, ainsi que leurs équipements, pour les 2 étages de l'entreprise.

Salle	Ordinateur Fixe / Portable	Imprimante	Équipements sans fils (Tél, tablette)
Bureau n°1	4	1	Non
Bureau n°2	5	1	Non
Ingénieur 1	5	1	Non
Open Space 1	4	1	Non
Accueil n°1	2	Non	Non
Accueil n°2	2	Non	Non
Salle des Serveurs	4	Non	Non
SAV	3	1	Non
RH	4	1	Non
Cadre	4	1	Non
Salle d'attente	2	Non	3

2.1.2 Organisation des équipements dans la DMZ de l'entreprise

Ensuite, nous pouvons dresser une liste avec les différents serveurs / machines présentes dans la DMZ de notre entreprise :

Voici les différents appareils de notre DMZ :

- Serveur Web
- Serveur DNS

Ainsi, dans le cadre de la configuration de notre entreprise, nous avons cherché à équilibrer, alterner et adapter le type d'équipement en fonction de la salle.

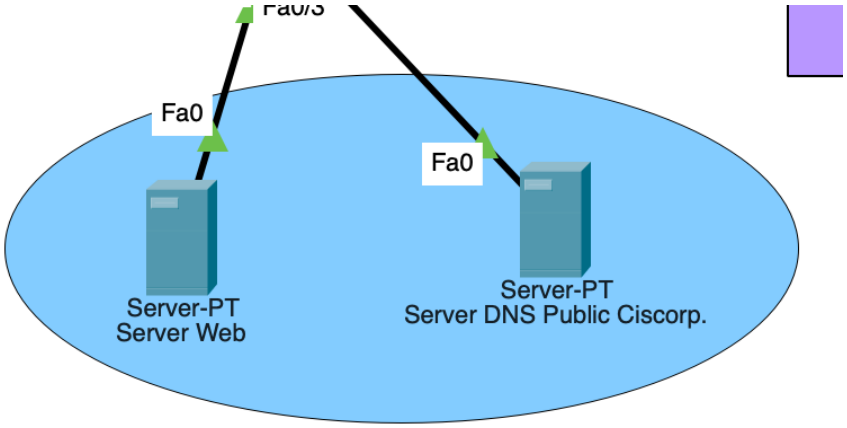


Figure 1 Schéma illustrant la DMZ.

2.2 Choix et justification des Équipements

Ensuite, nous allons nous intéresser aux différents équipements réseau utilisés dans notre architecture LAN. Les choix ont été réalisés en tenant compte des besoins de l'entreprise en matière de performance, de sécurité, de segmentation logique et d'évolutivité.

2.2.1 Choix des Switchs utilisés

Pour la partie commutation, nous avons opté pour des switchs *Cisco Catalyst 2960*, reconnus pour leur fiabilité et leur compatibilité. Ils permettent la configuration de VLAN et la gestion des boucles réseau grâce au Spanning Tree Protocol. Ces équipements sont déployés dans chaque salle pour relier les ordinateurs, imprimantes et téléphones IP.

Figure 2 Image représentant un switch Cisco Catalyst 2960.

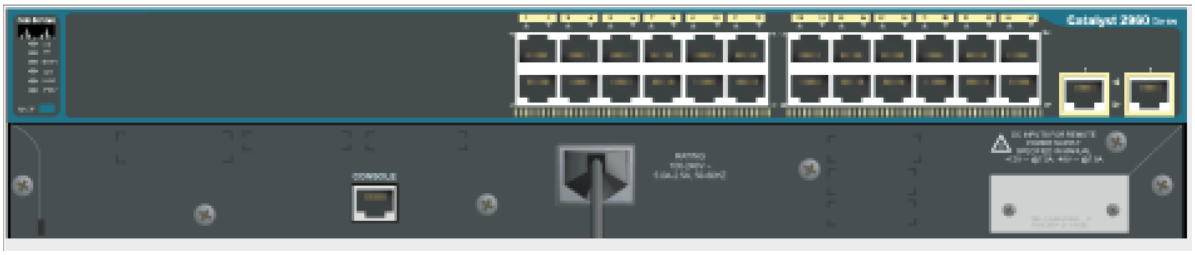


Figure 3 Capture du modèle physique du switch présent sur Cisco Packet Tracer.

Ainsi, grâce au modèle physique du switch présent dans Cisco Packet Tracer, nous pouvons clairement observer les différents ports de ce commutateur. Ce nombre de ports nous permet de connecter un nombre important d'équipements, ce qui est important pour notre réseau d'entreprise.

2.2.2 Choix des Routeurs utilisés

Le cœur du réseau est assuré par un routeur Cisco 4331, qui prend en charge le routage inter-VLAN, la gestion de la passerelle vers Internet et les listes de contrôle d'accès (ACL) pour renforcer la sécurité du trafic.

Figure 4 Photo d'un routeur Cisco 4331.

Figure 5 Module physique du routeur Cisco 4331.

Ce routeur ne dispose pas d'un nombre suffisant de ports utilisables pour un réseau. Nous pouvons donc ajouter une extension, NIM-ES2-4, qui permettra d'ajouter un commutateur à notre routeur et, par conséquent, d'augmenter le nombre de ports disponibles.

De plus, un routeur Cisco 2911 est utilisé pour notre réseau local d'entreprise. À l'instar du routeur 4331, il permet d'effectuer du routage inter-VLAN, de la traduction d'adresses de réseau (NAT), du routage par vecteur de liens (OSPF), etc.

Figure 6 Photo d'un routeur Cisco 2911.

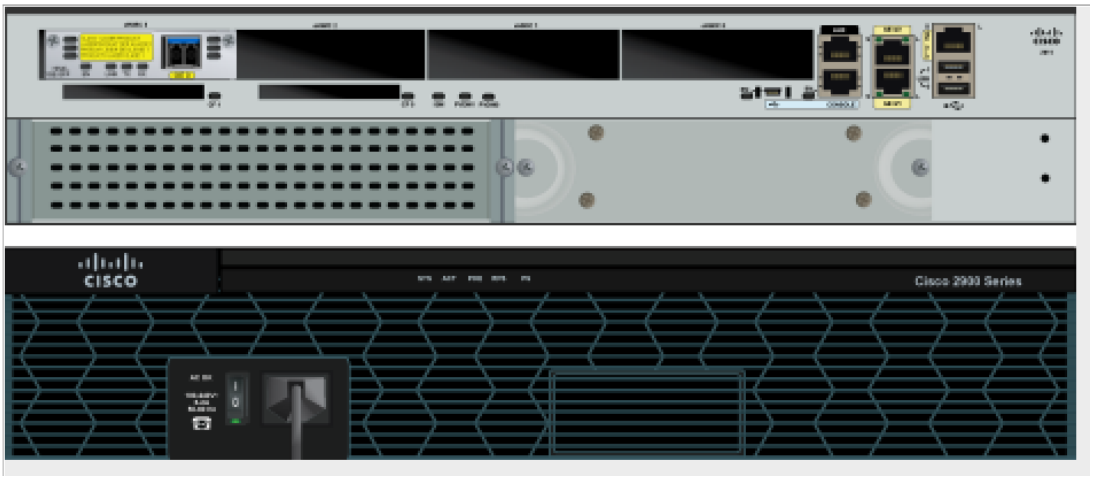


Figure 7 Module physique de notre routeur 2911.

Ce routeur ne dispose pas d'un nombre important d'interfaces. Cependant, cela ne pose pas de problème, car nous n'avons besoin que d'un nombre limité d'interfaces (trois maximums par routeur).

2.2.3 Choix d'équipements secondaires, et systèmes de communications

Afin d'assurer la connectivité sans fil, un point d'accès (Access Point PT) est déployé dans certaines zones, notamment dans la salle d'attente. Ce point d'accès permet aux utilisateurs mobiles de se connecter au réseau, tout en étant isolé dans un VLAN dédié (VLAN 240), distinct des autres VLANs, afin de garantir une certaine sécurité. Ce point d'accès est également utilisé dans notre réseau au niveau de la salle d'attente, permettant ainsi aux clients en attente d'accéder à Internet.

Figure 8 Image illustrant un Access-point.

Figure 9 Module physique de l'Access Point.

Dans cette représentation, on observe un port RJ45, permettant de connecter l'équipement à un commutateur.

Concernant la connectique, le réseau est câblé en Ethernet avec des câbles droits pour relier les équipements réseau entre eux, mais surtout des câbles croisés entre switchs et routeurs.

Tous ces appareils forment le cœur de notre réseau LAN, assurant une connexion stable, segmentée et sécurisée pour les besoins quotidiens de tous les services de l'entreprise.

2.3 Segmentation du Réseau : Mise en Place des VLANs

Pour optimiser la gestion du réseau local et renforcer sa sécurité, la segmentation en VLAN est une étape essentielle. Cette technique permet de découper le réseau physique en plusieurs réseaux logiques indépendants, chacun correspondant à un service ou une fonction précise de l'entreprise.

2.3.1 Justification des VLANs et plan d'adressage IP

Chaque VLAN regroupe ainsi des postes et équipements qui partagent des besoins similaires en termes de sécurité et de communication, tout en limitant la diffusion inutile des données à l'ensemble du réseau. Cette segmentation réduit également les risques d'intrusion et facilite l'administration du réseau.

Voici la répartition envisagée des VLAN au sein de notre réseau :

Nom du VLAN et N°	Nom de la salle	Adresse réseau IPv4
VLAN 10 – bureau1	Bureau 1	10.1.0.0/28
VLAN 20 – bureau2	Bureau 2	10.1.0.16/28
VLAN 30 – ingenieur1	Ingénieur 1	10.1.0.32/28
VLAN 40 – openspace1	Open Space 1	10.1.0.48/29
VLAN 50 – accueil1	Accueil 1	10.1.0.56/29
VLAN 60 – accueil2	Accueil 2	10.1.0.64/29
VLAN 100 – serveur	Serveur	10.1.0.72/29
VLAN 210 - rh	RH	10.2.0.16/29
VLAN 220 - SAV	SAV	10.2.0.32/29
VLAN 230 - cadre	Cadre	10.2.0.24/29
VLAN 240 – attente	Salle d'attente	10.2.0.64/26

D'après le tableau ci-dessus, nous pouvons constater que nous avons opté pour une répartition des réseaux IP en VLSM[1]. Nous verrons cela plus en détail dans une autre partie.

2.3.2 Configuration des équipements pour l'implémentation des VLANs

Pour pouvoir créer les différents VLANs de notre réseau, nous avons utilisé la commande suivante dans nos commutateurs.

```
Switch#int vlan 10
```

Figure 10 Commande permettant d'accéder au vlan 10.

Ensuite, nous accédons à l'interface souhaiter, et nous l'associons avec le vlan 10 créer précédemment.

```
Switch(config)#interface FastEthernet0/1
Switch(config-if)#
Switch(config-if)#
Switch(config-if)#switchport access vlan 10
```

Figure 11 Commandes permettant d'associé un port à un commutateur.

Ensuite, nous procédons de la même manière pour les autres commutateurs et VLANs du LAN d'entreprise.

2.3.3 Liaisons TRUNK sur les commutateurs

Nous allons maintenant nous intéresser aux liaisons entre les différents switchs. En effet, ces liaisons sont associées à tous les VLANs, ce qui permet la communication entre eux. Elles sont configurées en mode TRUNK, ce qui autorise le transport de données issues de plusieurs VLANs sur un même lien.

[1] VLSM : Variable Length Subnet Masking

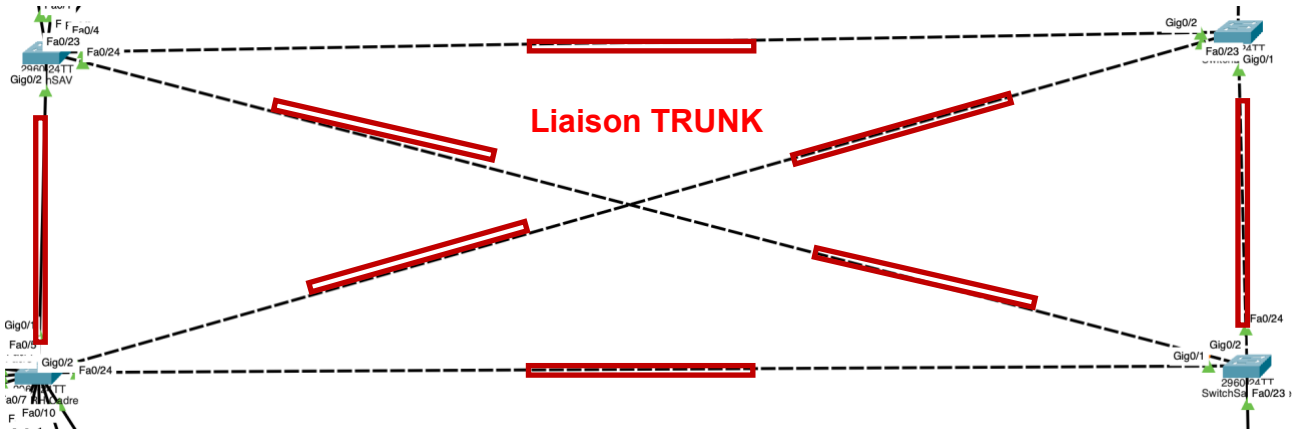


Figure 12 Schéma illustrant des liaisons entre les switchs.

Voici la commande permettant de mettre une liaison en mode TRUNK :

```
Switch(config-if)#switchport mode trunk
```

Figure 13 Commande permettant de mettre une liaison en mode TRUNK.

Nous configurons des liaisons TRUNK pour l'ensemble des connexions entre les différents commutateurs et routeurs. Cette configuration permet à toutes les trames provenant de tous les VLAN de pouvoir communiquer de manière optimale.

Ainsi, après avoir configurer tous les VLANs de notre LAN d'entreprise, nous pouvons vérifier la configuration avec les commandes suivantes :

```
Switch#show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                                Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                                Fa0/21, Fa0/22, Fa0/23
10   VLAN0010                         active
20   VLAN0020                         active
30   VLAN0030                         active
40   VLAN0040                         active
50   VLAN0050                         active
60   VLAN0060                         active
100  VLAN0100                         active
210  VLAN0210                         active
220  VLAN0220                         active
230  VLAN0230                         active
240  VLAN0240                         active
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
```

Figure 14 Commande permettant d'avoir une liste de tous les VLANs crées.

Et voici une commande permettant d'avoir la liste des interfaces en mode TRUNK :

```
Switch#show interface trunk
Port        Mode         Encapsulation  Status        Native vlan
Fa0/24      on           802.1q         trunking      1
Gig0/1      on           802.1q         trunking      1
Gig0/2      auto         n-802.1q       trunking      1

Port        Vlans allowed on trunk
Fa0/24      1-1005
Gig0/1      1-1005
Gig0/2      1-1005

Port        Vlans allowed and active in management domain
Fa0/24      1,10,20,30,40,50,60,100,210,220,230,240
Gig0/1      1,10,20,30,40,50,60,100,210,220,230,240
Gig0/2      1,10,20,30,40,50,60,100,210,220,230,240

Port        Vlans in spanning tree forwarding state and not pruned
Fa0/24      1,10,20,30,40,50,60,100,210,220,230,240
Gig0/1      1,10,20,30,40,50,60,100,210,220,230,240
Gig0/2      1,10,20,30,40,50,60,100,210,220,230,240
```

Figure 15 Commande permettant d'avoir la liste des interfaces en mode trunk.

Cette liste comprend effectivement les liaisons inter-commutateurs et inter-routeurs, permettant le routage inter-VLAN.

2.4 Adressage IPv4 avec VLSM

Le plan d'adressage repose sur une logique d'allocation efficace des sous-réseaux avec VLSM, ce qui permet d'adapter la taille des sous-réseaux aux besoins spécifiques de chaque VLAN (nombre de machines, équipements, etc.).

2.4.1 Attribution des adresses IP selon les salles

Chaque VLAN reçoit une plage d'adresses adaptée à sa taille via un découpage précis du réseau global, tout en évitant le gaspillage d'adresses IP. Le choix des masques se fait en fonction du nombre d'hôtes présents dans le VLAN.

Nous pouvons dresser le tableau suivant :

VLAN	Salle	Adresse réseau	Masque	Gateway (1re IP)	Dernière IP utilisable	Broadcast
10	Bureau 1	10.1.0.0	255.255.255.240 (/28)	10.1.0.1	10.1.0.14	10.1.0.15
20	Bureau 2	10.1.0.16	255.255.255.240 (/28)	10.1.0.17	10.1.0.30	10.1.0.31
30	Ingénieur 1	10.1.0.32	255.255.255.240 (/28)	10.1.0.33	10.1.0.46	10.1.0.47
40	Open Space 1	10.1.0.48	255.255.255.248 (/29)	10.1.0.49	10.1.0.54	10.1.0.55
50	Accueil 1	10.1.0.56	255.255.255.248 (/29)	10.1.0.57	10.1.0.62	10.1.0.63
60	Accueil 2	10.1.0.64	255.255.255.248 (/29)	10.1.0.65	10.1.0.70	10.1.0.71

100	Serveur	10.1.0.72	255.255.255.248 (/29)	10.1.0.73	10.1.0.78	10.1.0.79
210	RH	10.2.0.16	255.255.255.248 (/29)	10.2.0.17	10.2.0.22	10.2.0.23
220	SAV	10.2.0.32	255.255.255.248 (/29)	10.2.0.33	10.2.0.38	10.2.0.39
230	Cadre	10.2.0.24	255.255.255.248 (/29)	10.2.0.25	10.2.0.30	10.2.0.31
240	Salle d'attente	10.2.0.64	255.255.255.192 (/26)	10.2.0.65	10.2.0.126	10.2.0.127

Nous pouvons voir que l'utilisation du VLSM permet d'adapter précisément chaque sous-réseau au nombre réel d'hôtes nécessaires, évitant ainsi tout gaspillage d'adresses IP. Par exemple, les bureaux correspondant aux VLAN 10, 20 et 30 sont chacun configurés avec un masque /28, suffisant pour une quinzaine de machines au maximum. Les accueils ou petits espaces (VLAN 40, 50 et 60) utilisent un masque /29, qui offre six adresses utilisables, ce qui est adapté à leur faible besoin. Le VLAN 100, dédié au serveur, est isolé également sur un /29 pour des raisons de sécurité et d'organisation. Quant à la salle d'attente (VLAN 240), elle est configurée en /26 afin de pouvoir accueillir un grand nombre d'équipements comme des ordinateurs et des téléphones.

2.4.2 Configuration des sous-interfaces du routeur d'entreprise

Ainsi, sur le routeur de l'entreprise, nous avons ajouté une IP sur chaque sous-interface de l'interface Gig0/0. Cette adresse IP correspond à la passerelle par défaut des différents postes. Veuillez trouver ci-dessous la configuration de notre routeur d'entreprise. Afin d'ajouter ces adresses IP, nous avons exécuté les commandes suivantes :

```
interface GigabitEthernet0/0.10
 encapsulation dot1Q 10
 ip address 10.1.0.1 255.255.255.240
```

Figure 16 Exemple de commande effectué sur une sous interface du routeur.

Nous avons donc exécuté la commande « encapsulation dot1Q 10 », ce qui permet de configurer l'interface en mode TRUNK pour le VLAN 10. En effet, cette configuration permet aux routeurs d'identifier les trames provenant du VLAN 10.

```
Router#show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
GigabitEthernet0/0     unassigned      YES unset  up                    up
GigabitEthernet0/0.10  10.1.0.1        YES manual up                    up
GigabitEthernet0/0.20  10.1.0.17       YES manual up                    up
GigabitEthernet0/0.30  10.1.0.33       YES manual up                    up
GigabitEthernet0/0.40  10.1.0.49       YES manual up                    up
GigabitEthernet0/0.50  10.1.0.57       YES manual up                    up
GigabitEthernet0/0.60  10.1.0.65       YES manual up                    up
GigabitEthernet0/0.99  192.168.99.1    YES manual up                    up
GigabitEthernet0/0.100 10.1.0.73       YES manual up                    up
GigabitEthernet0/0.210 10.2.0.17       YES manual up                    up
GigabitEthernet0/0.220 10.2.0.33       YES manual up                    up
GigabitEthernet0/0.230 10.2.0.25       YES manual up                    up
GigabitEthernet0/0.240 10.2.0.65       YES manual up                    up
GigabitEthernet0/1     192.168.1.254   YES manual up                    up
GigabitEthernet0/2     205.0.113.1     YES manual up                    up
Vlan1                  unassigned      YES unset  administratively down down
```

Figure 17 Extrait de la configuration de notre routeur d'entreprise.

On observe que l'interface du routeur d'entreprise est divisée en plusieurs sous-interfaces, chaque sous-interface étant associée à un VLAN spécifique. Cette configuration permet aux équipements (PC, imprimante) issus de VLAN différents de communiquer entre eux.

2.4.3 Configuration IPv4 des ordinateurs de l'entreprise

Après avoir correctement configuré les interfaces et sous-interfaces du routeur d'entreprise, nous pouvons procéder à la configuration des ordinateurs de l'entreprise. Voici différents exemples de configuration réseau présents sur les ordinateurs de l'entreprise, issus de différents VLAN.

```
C:\>ipconfig /all

FastEthernet0 Connection:(default port)

   Connection-specific DNS Suffix..:
   Physical Address................: 0006.2A8C.7790
   Link-local IPv6 Address.........: FE80::206:2AFF:FE8C:7790
   IPv6 Address....................: ::
   IPv4 Address....................: 10.1.0.5
   Subnet Mask.....................: 255.255.255.240
   Default Gateway.................: ::
                                     10.1.0.1
   DHCP Servers....................: 0.0.0.0
   DHCPv6 IAID.....................:
   DHCPv6 Client DUID..............: 00-01-00-01-D6-83-DD-8C-00-06-2A-8C-77-90
   DNS Servers.....................: ::
                                     10.1.0.76

Bluetooth Connection:

   Connection-specific DNS Suffix..:
   Physical Address................: 0001.9757.2715
   Link-local IPv6 Address.........: ::
   IPv6 Address....................: ::
   IPv4 Address....................: 0.0.0.0
   Subnet Mask.....................: 0.0.0.0
   Default Gateway.................: ::
                                     0.0.0.0
   DHCP Servers....................: 0.0.0.0
   DHCPv6 IAID.....................:
   DHCPv6 Client DUID..............: 00-01-00-01-D6-83-DD-8C-00-06-2A-8C-77-90
   DNS Servers.....................: ::
                                     10.1.0.76
```

Figure 18 Capture d'écran de la configuration réseau d'un poste présent sur le VLAN 10.

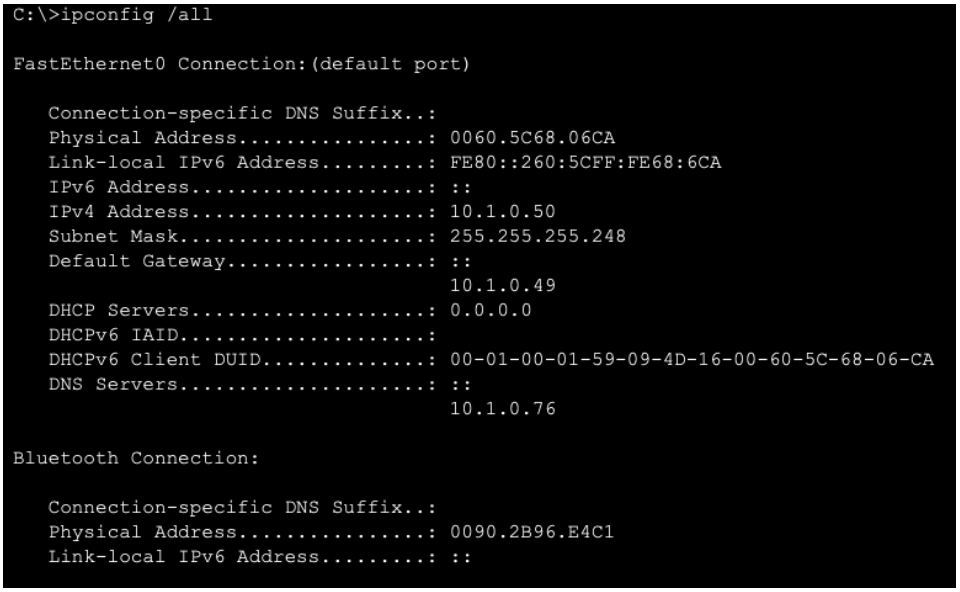


Figure 19 Capture d'écran de la configuration réseau d'un pc présent sur le VLAN 40.

Pour vérifier le bon fonctionnement de notre configuration, nous pouvons effectuer un ping entre des équipements de différents VLANs. Voici un exemple entre un PC du VLAN 10 et un autre du VLAN 220.

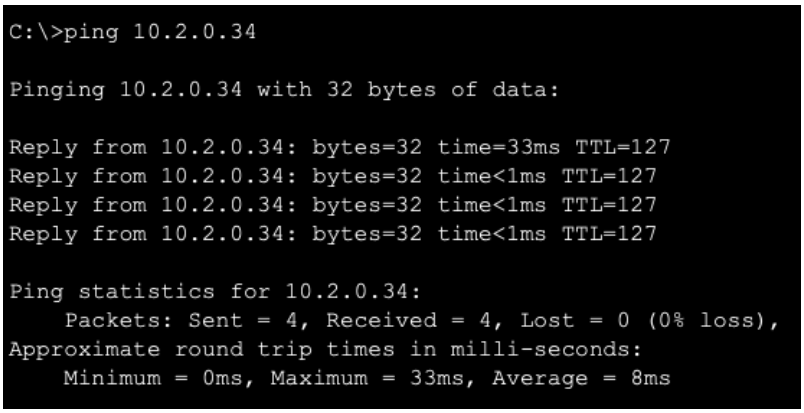


Figure 20 Extrait d'un ping entre 2 équipements issues de VLAN différents.

Notre configuration est donc fonctionnelle sur le réseau local de l'entreprise.

2.5 Implémentation de l'IPv6 dans le LAN

2.5.1 Plan d'adressage IPv6 du réseau d'entreprise

Suite à l'adressage IPv4 des équipements de notre réseau local, nous allons maintenant procéder de la même manière pour l'IPv6. Veuillez consulter le tableau ci-dessous :

VLAN	Salle	Adresse réseau IPv6	Gateway IPv6	Plage d'adresses utilisables
10	Bureau 1	2001:db8:1:10::/64	2001:db8:1:10::1	2001:db8:1:10::2 à 2001:db8:1:10::14
20	Bureau 2	2001:db8:1:20::/64	2001:db8:1:20::1	2001:db8:1:20::2 à 2001:db8:1:20::1e
30	Ingénieur 1	2001:db8:1:30::/64	2001:db8:1:30::1	2001:db8:1:30::2 à 2001:db8:1:30::2e
40	Open Space 1	2001:db8:1:40::/64	2001:db8:1:40::1	2001:db8:1:40::2 à 2001:db8:1:40::36
50	Accueil 1	2001:db8:1:50::/64	2001:db8:1:50::1	2001:db8:1:50::2 à 2001:db8:1:50::3e
60	Accueil 2	2001:db8:1:60::/64	2001:db8:1:60::1	2001:db8:1:60::2 à 2001:db8:1:60::46
100	Serveur	2001:db8:1:100::/64	2001:db8:1:100::1	2001:db8:1:100::2 à 2001:db8:1:100::4e
210	RH	2001:db8:1:210::/64	2001:db8:1:210::1	2001:db8:1:210::2 à 2001:db8:1:210::16
220	SAV	2001:db8:1:220::/64	2001:db8:1:220::1	2001:db8:1:220::2 à 2001:db8:1:220::26
230	Cadre	2001:db8:1:230::/64	2001:db8:1:230::1	2001:db8:1:230::2 à 2001:db8:1:230::1e
240	Salle d'attente	2001:db8:1:240::/64	2001:db8:1:240::1	2001:db8:1:240::2 à 2001:db8:1:240::7e

Nous avons procédé à un adressage en IPv6, avec un préfixe permettant d'identifier le sous-réseau de l'équipement. Par exemple, l'ordinateur dont l'adresse IPv6 est « 2001:db8:1:10::2 » appartient au VLAN 10. Et nous avons fait de même avec les autres VLAN.

2.5.2 Configuration du routeur d'entreprise IPv6

Ensuite, nous passons à la configuration de notre routeur d'entreprise. La démarche reste similaire à celle utilisée pour le protocole IPv4. Les commandes suivantes seront saisies sur les sous-interfaces du routeur :

```
interface GigabitEthernet0/0.10
 encapsulation dot1Q 10
 ip address 10.1.0.1 255.255.255.240
 ipv6 address 2001:DB8:1:10::1/64
```

Figure 21 Commande IPv6 effectué sur le routeur d'entreprise.

Nous avons donc ajouté une adresse IPv6 à la sous-interface du VLAN 10. Nous procédons de la même manière pour les autres sous-interfaces.

Voici la configuration de toutes nos interfaces du routeur, en IPv6.

```
Router#show ipv6 int b
GigabitEthernet0/0         [up/up]
    unassigned
GigabitEthernet0/0.10      [up/up]
    FE80::260:70FF:FE73:6A01
    2001:DB8:1:10::1
GigabitEthernet0/0.20      [up/up]
    FE80::260:70FF:FE73:6A01
    2001:DB8:1:20::1
GigabitEthernet0/0.30      [up/up]
    FE80::260:70FF:FE73:6A01
    2001:DB8:1:30::1
GigabitEthernet0/0.40      [up/up]
    FE80::260:70FF:FE73:6A01
    2001:DB8:1:40::1
GigabitEthernet0/0.50      [up/up]
    FE80::260:70FF:FE73:6A01
    2001:DB8:1:50::1
GigabitEthernet0/0.60      [up/up]
    FE80::260:70FF:FE73:6A01
    2001:DB8:1:60::1
GigabitEthernet0/0.99      [up/up]
    unassigned
GigabitEthernet0/0.100     [up/up]
    FE80::260:70FF:FE73:6A01
    2001:DB8:1:100::1
GigabitEthernet0/0.210     [up/up]
    FE80::260:70FF:FE73:6A01
    2001:DB8:1:210::1
GigabitEthernet0/0.220     [up/up]
    FE80::260:70FF:FE73:6A01
    2001:DB8:1:220::1
GigabitEthernet0/0.230     [up/up]
    unassigned
GigabitEthernet0/0.240     [up/up]
    FE80::260:70FF:FE73:6A01
    2001:DB8:1:230::1
    2001:DB8:1:240::1
GigabitEthernet0/1         [up/up]
    FE80::260:70FF:FE73:6A02
    2001:1234:ABCD:1::1
GigabitEthernet0/2         [up/up]
    FE80::260:70FF:FE73:6A03
    2001:1A2B:85A3::1
GigabitEthernet0/3/0       [down/down]
    unassigned
Vlan1                      [administratively down/down]
    unassigned
```

Figure 22 Configuration du routeur, après l'implémentation de l'IPv6.

2.5.3 Configuration IPv6 des équipements de l'entreprise

Après avoir organiser notre adressage de manière structuré, nous pouvons affecter chaque équipement à son IP. Pour cela, nous avons fait :

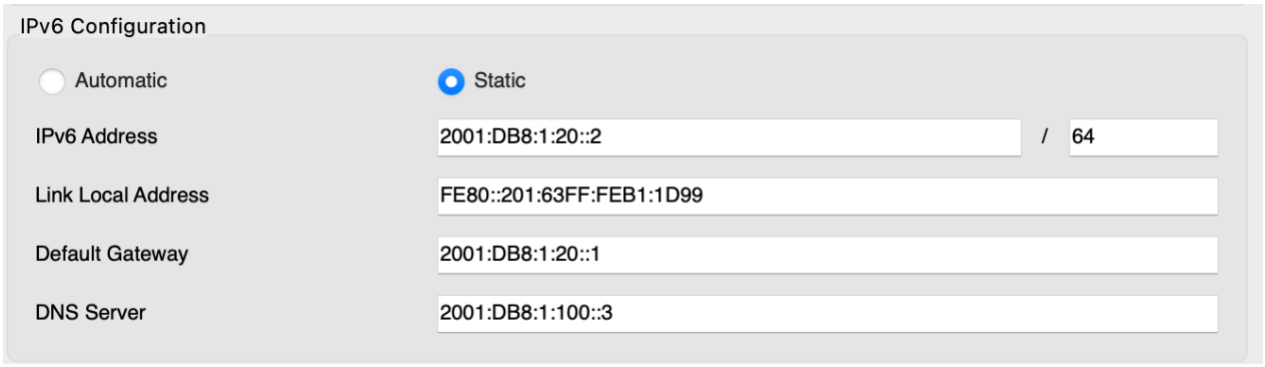


Figure 23 Configuration IPv6 d'un PC du VLAN 20.

Nous avons procédé de la même manière pour tous les ordinateurs du réseau local de l'entreprise.

Ainsi, nous pouvons relever la configuration de 2 équipements issues de VLAN différents.

```
C:\>ipconfig /all

FastEthernet0 Connection:(default port)

   Connection-specific DNS Suffix..:
   Physical Address.................: 0000.0CC1.B209
   Link-local IPv6 Address.........: FE80::200:CFF:FEC1:B209
   IPv6 Address....................: 2001:DB8:1:10::2
   IPv4 Address....................: 10.1.0.2
   Subnet Mask.....................: 255.255.255.240
   Default Gateway.................: 2001:DB8:1:10::1
                                     10.1.0.1
   DHCP Servers....................: 0.0.0.0
   DHCPv6 IAID.....................:
   DHCPv6 Client DUID..............: 00-01-00-01-79-91-BD-CA-00-00-0C-C1-B2-09
   DNS Servers.....................: 2001:DB8:1:100::3
                                     10.1.0.76
```

Figure 24 Configuration réseau d'une machine du VLAN 10.

```
C:\>ipconfig /all

FastEthernet0 Connection:(default port)

   Connection-specific DNS Suffix..:
   Physical Address.................: 0001.63B1.1D99
   Link-local IPv6 Address.........: FE80::201:63FF:FEB1:1D99
   IPv6 Address....................: 2001:DB8:1:20::2
   IPv4 Address....................: 10.1.0.18
   Subnet Mask.....................: 255.255.255.240
   Default Gateway.................: 2001:DB8:1:20::1
                                     10.1.0.17
   DHCP Servers....................: 0.0.0.0
   DHCPv6 IAID.....................:
   DHCPv6 Client DUID..............: 00-01-00-01-93-C9-A5-73-00-01-63-B1-1D-99
   DNS Servers.....................: 2001:DB8:1:100::3
                                     10.1.0.76
```

Figure 25 Configuration réseau d'une machine du VLAN 20.

2.6 Serveurs Internes et Services Réseaux de l'entreprise

L'entreprise dispose de plusieurs serveurs internes centralisés dans le VLAN 100 (Salle des Serveurs), situé dans le sous-réseau 10.1.0.72/29. Ces serveurs assurent des fonctions essentielles pour le bon fonctionnement du réseau, la communication entre les employés, et la gestion des ressources internes.

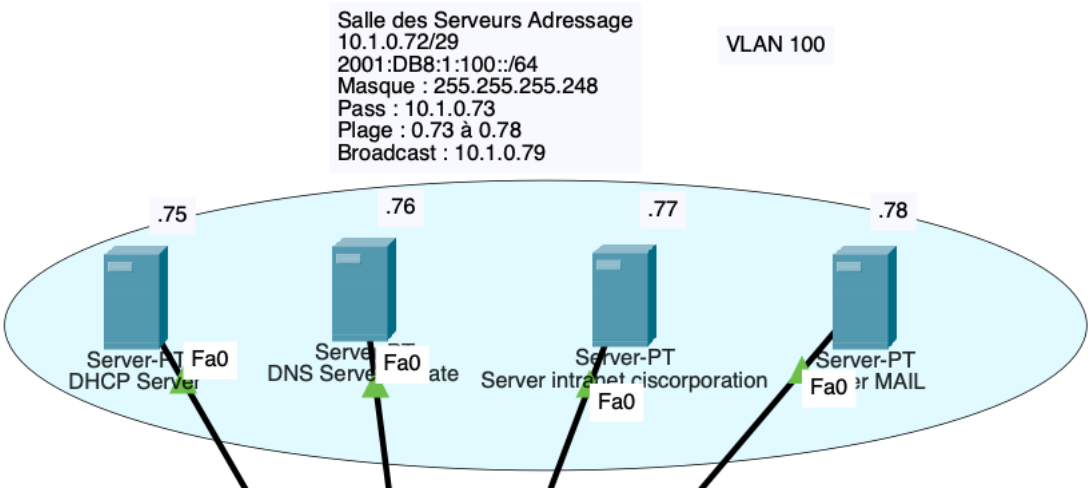


Figure 26 Capture d'écran du VLAN 100, le VLAN contenant les serveurs interne à l'entreprise.

2.6.1 Serveur WEB Intranet

Un serveur web interne a été mis en place afin d'héberger un site intranet réservé aux salariés de l'entreprise. Ce site regroupe diverses ressources utiles comme des documents internes, des actualités de l'entreprise, les informations RH, les procédures de sécurité.

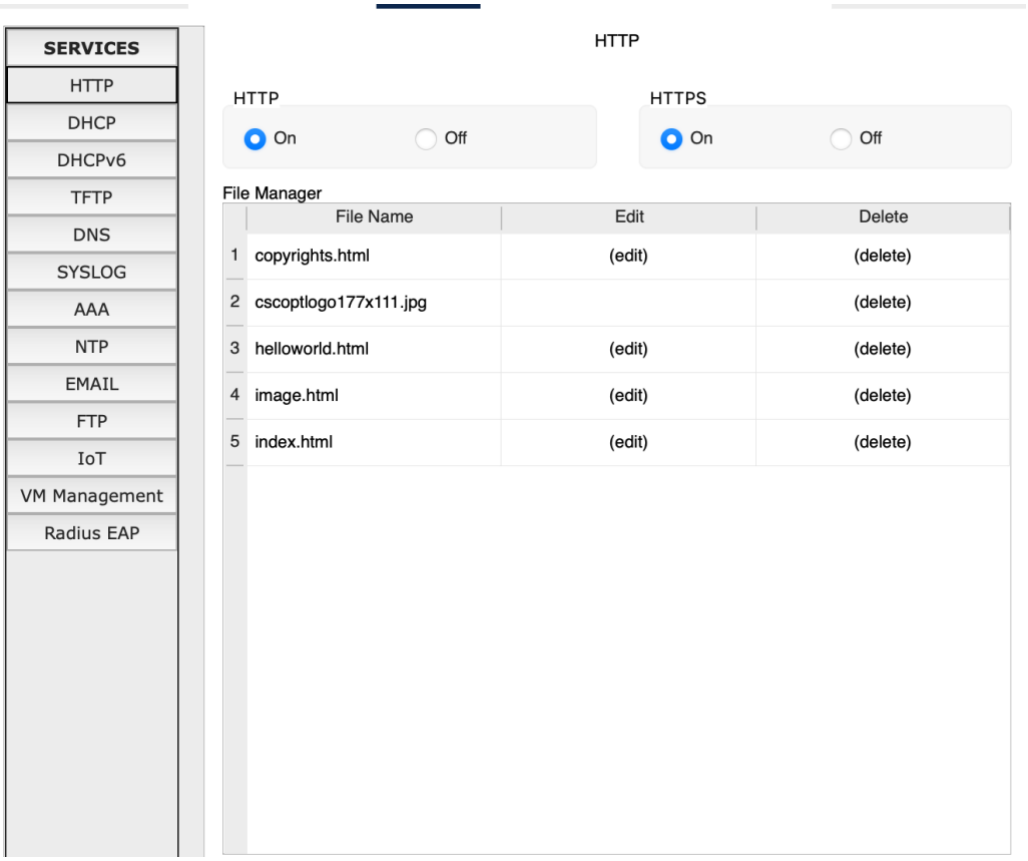


Figure 27 Capture d'écran du service HTTP sur le serveur web intranet de l'entreprise.

Dans notre serveur Web, la première page correspond au fichier « index.html ». Voici le contenu de ce fichier :

File Name: index.html

```
<!DOCTYPE html>
<html lang="fr">
<head>
  <meta charset="UTF-8">
  <title>Intranet Ciscoporation</title>
  <style>
    body {
      font-family: Arial, sans-serif;
      background-color: #f4f6f8;
      margin: 0;
      padding: 0;
      text-align: center;
    }

    header {
      background-color: #003366;
      color: white;
      padding: 30px 20px;
    }

    h1 {
      margin: 0;
      font-size: 2.5em;
    }

    p {
      font-size: 1.2em;
      margin-top: 10px;
    }

    nav {
      margin: 30px auto;
    }

    ul {
      list-style-type: none;
      padding: 0;
    }

    li {
      margin: 15px 0;
    }

    a {
      text-decoration: none;
```

File Manager Save

Figure 28 Extrait du fichier index.html.

Et voici notre site web intranet de l'entreprise CisCorporation, accessible seulement par le LAN de l'entreprise (intranet.ciscorporation.com).

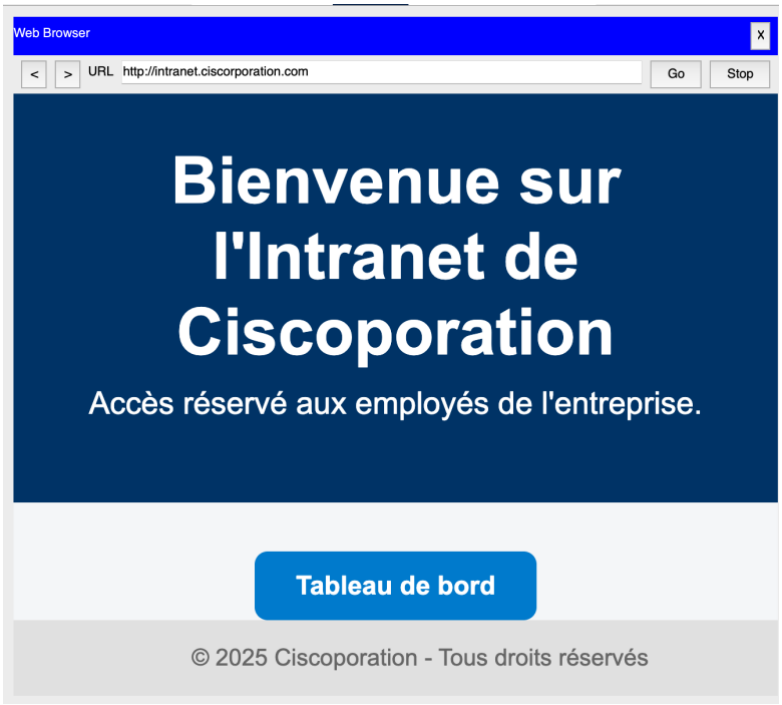


Figure 29 Aperçu du site web intranet de l'entreprise

```
C:\>ping intranet.ciscorporation.com

Pinging 10.1.0.77 with 32 bytes of data:

Reply from 10.1.0.77: bytes=32 time<1ms TTL=127
Reply from 10.1.0.77: bytes=32 time<1ms TTL=127
Reply from 10.1.0.77: bytes=32 time<1ms TTL=127
Reply from 10.1.0.77: bytes=32 time<1ms TTL=127

Ping statistics for 10.1.0.77:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Figure 30 Extrait d'un ping depuis un PC du LAN d'entreprise, vers le serveur Intranet.

Le site web Intranet de l'entreprise est donc accessible pour tous les équipements du LAN d'entreprise.

2.6.2 Serveur DNS Intranet

Le serveur intranet est accessible via le nom DNS intranet.ciscorporatoion.com, résolu grâce au DNS interne de l'entreprise. Il fonctionne sur le protocole HTTP et n'est pas accessible depuis l'extérieur ni depuis le VLAN des visiteurs. Il est hébergé dans le VLAN 100 et utilise l'adresse IP 10.1.0.74.

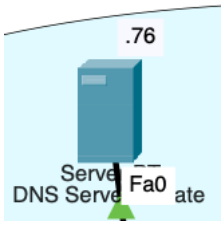


Figure 31 Emplacement du serveur DNS Intranet.

Voici la configuration réseau de notre serveur DNS Intranet.

```
C:\>ipconfig /all

FastEthernet0 Connection:(default port)

   Connection-specific DNS Suffix..:
   Physical Address.................: 0010.11B5.DE98
   Link-local IPv6 Address.........: FE80::210:11FF:FEB5:DE98
   IPv6 Address....................: 2001:DB8:1:100::3
   IPv4 Address....................: 10.1.0.76
   Subnet Mask.....................: 255.255.255.248
   Default Gateway.................: 2001:DB8:1:100::1
                                     10.1.0.73
   DHCP Servers....................: 0.0.0.0
   DHCPv6 IAID.....................:
   DHCPv6 Client DUID..............: 00-01-00-01-4D-E5-5E-97-00-10-11-B5-DE-98
   DNS Servers.....................: 2001:DB8:1:100::3
                                     10.1.0.76
```

Figure 32 Configuration réseau de notre serveur DNS Intranet.

Ensuite, nous pouvons relever les différents enregistrements présents dans ce serveur.

			Retry :10 MinTTL :10
1	ciscorporation.com	NS	dns.ciscorporation.com
2	com	NS	dns.com
3	dns.ciscorporation.com	A Record	10.1.0.76
4	dns.ciscorporation.com	AAAA Record	2001:1234:ABCD:1::3
5	dns.com	A Record	170.0.0.53
6	dns.com	AAAA Record	2001:1111:85A3::2
7	intranet.ciscorporation.com	A Record	10.1.0.77
8	intranet.ciscorporation.com	AAAA Record	2001:DB8:1:100::4
9	www.ciscorporation.com	A Record	192.168.1.100
10	www.ciscorporation.com	AAAA Record	2001:1234:ABCD:1::2

Figure 33 Capture d'écran des enregistrements du serveur DNS intranet de l'entreprise.

Dans les enregistrements DNS présentés, on retrouve tout d'abord un enregistrement SOA, qui contient des informations telles que le minTTL et le nom du serveur.

Ensuite, des enregistrements de type A et AAAA sont utilisés pour associer des noms de domaine à des adresses IPv4 ou IPv6. On y trouve l'adresse IP publique du serveur DNS de l'entreprise, celle du serveur DNS intranet, ainsi que celles des serveurs web intranet et web public.

Enfin, des enregistrements NS sont présents pour indiquer les serveurs DNS responsables du domaine. Ces enregistrements permettent de rediriger les requêtes vers le serveur DNS public de l'entreprise, ainsi que vers un serveur racine de type .com, permettant notamment d'accéder au serveur web des FAI.

2.6.3 Serveur DHCP privé

Suite à cela, nous avons dans notre salle des serveurs, un serveur DHCP permettant de donner une configuration réseau pour les équipements présents dans la salle d'attente de l'entreprise.

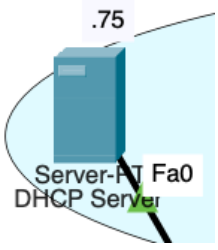


Figure 34 Emplacement du serveur DHCP interne

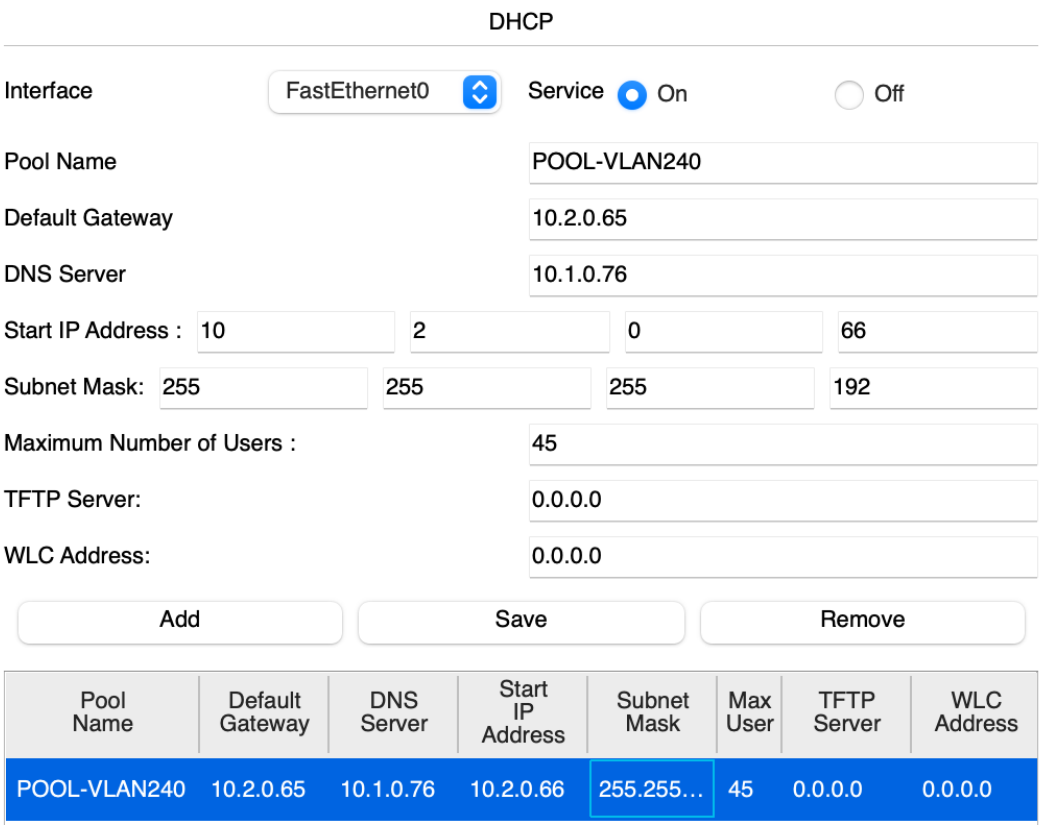


Figure 35 Capture d'écran de la configuration de notre serveur DHCP de l'entreprise.

Dans cette configuration, nous disposons de différents champs, notamment la plage d'adresses IP disponibles, la passerelle par défaut, le serveur DNS attribué au client DHCP, ainsi que le nombre maximal d'utilisateurs.

Ainsi, les équipements du VLAN 240, correspondant à la salle d'attente de l'entreprise, peuvent recevoir une configuration réseau, permettant d'accéder au site web privée de l'entreprise (Intranet).

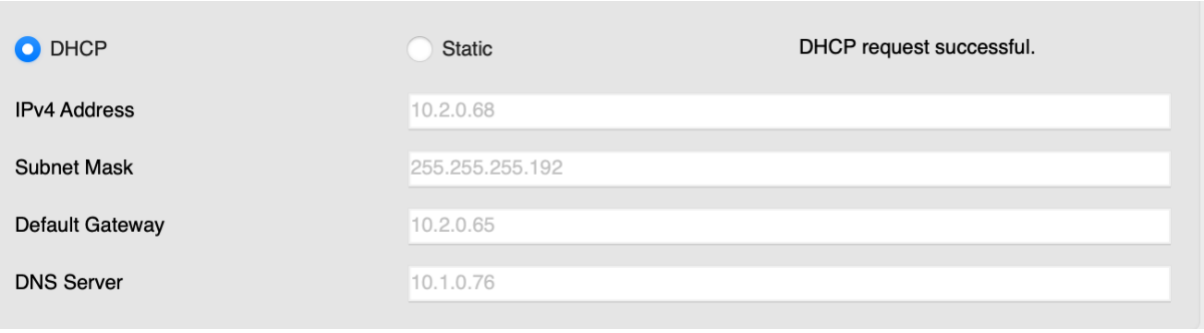


Figure 36 Capture d'écran de la configuration réseau reçu par le client DHCP, grâce au serveur DHCP

Suite à cela, nous avons aussi créer un POOL permettant de donner une configuration IPv6 aux équipements du VLAN 240.

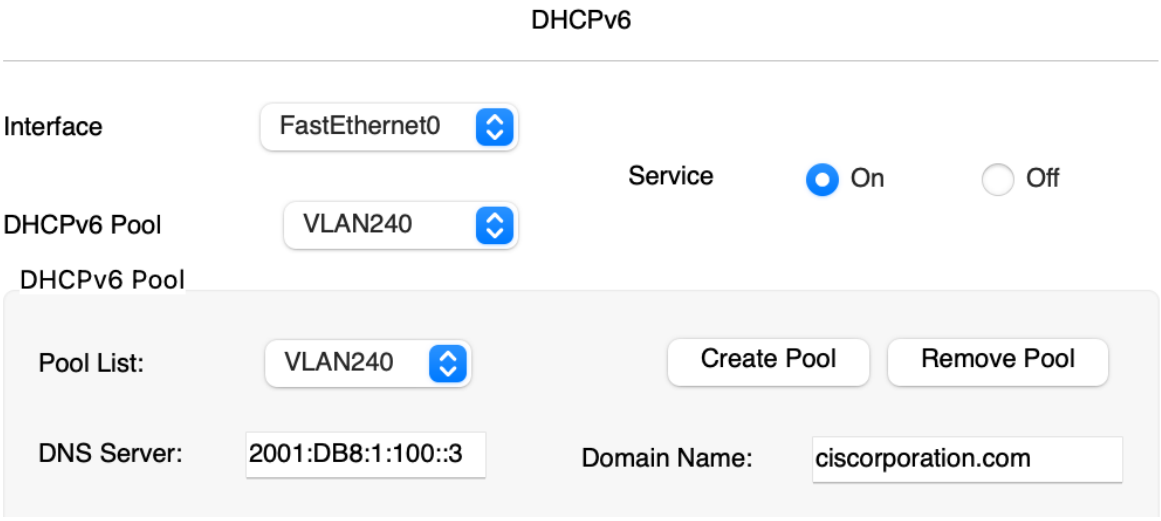


Figure 37 Extrait du POOL DHCPv6.

Ainsi, les équipements issus du VLAN 240 pourrons recevoir une configuration IPv4, mais aussi une configuration IPv6.

Voici un exemple d'une configuration IPv6 reçu par un client :

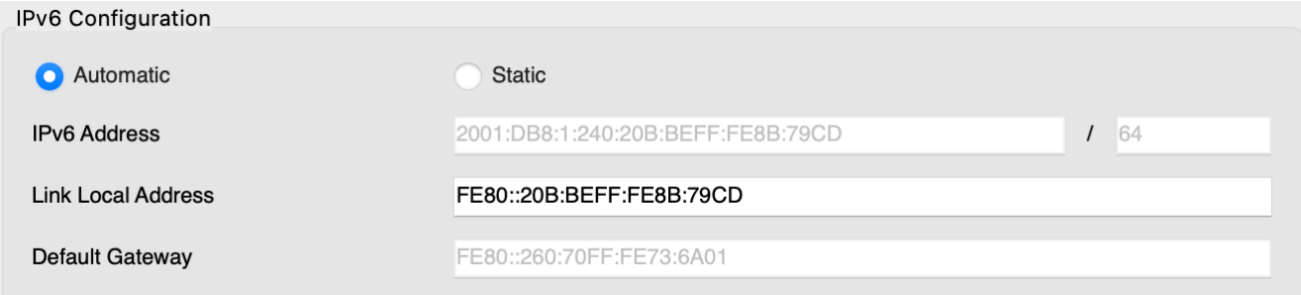


Figure 38 Configuration IPv6 reçu par le client.

2.6.4 Serveur MAIL privé

Finalement, après la configuration des serveurs privés essentiels à l'entreprise, nous avons pu déployer un serveur de messagerie. Ce serveur va permettre aux différents employés de l'entreprise de pouvoir communiquer par mail au sein de l'entreprise. Pour cela, nous avons créer un serveur de mail dans la zone Intranet de notre entreprise.

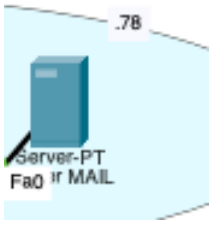


Figure 39 Emplacement du serveur mail de l'entreprise.

Ensuite, nous pouvons relever la configuration réseau de l'équipement.

```
C:\>ipconfig /all

FastEthernet0 Connection:(default port)

   Connection-specific DNS Suffix..:
   Physical Address................: 0040.0BE7.3C92
   Link-local IPv6 Address.........: FE80::240:BFF:FEE7:3C92
   IPv6 Address....................: 2001:DB8:1:100::5
   IPv4 Address....................: 10.1.0.78
   Subnet Mask.....................: 255.255.255.248
   Default Gateway.................: 2001:DB8:1:100::1
                                     10.1.0.73
   DHCP Servers....................: 0.0.0.0
   DHCPv6 IAID.....................:
   DHCPv6 Client DUID..............: 00-01-00-01-A3-09-65-53-00-40-0B-E7-3C-92
   DNS Servers.....................: 2001:DB8:1:100::3
                                     10.1.0.76
```

Figure 40 Configuration réseau du serveur de mail.

Suite à la validation de la configuration de notre serveur, nous pouvons procéder à la mise en place du serveur de messagerie. Cette étape nous permettra de créer plusieurs utilisateurs, chacun associé à un ordinateur du réseau.

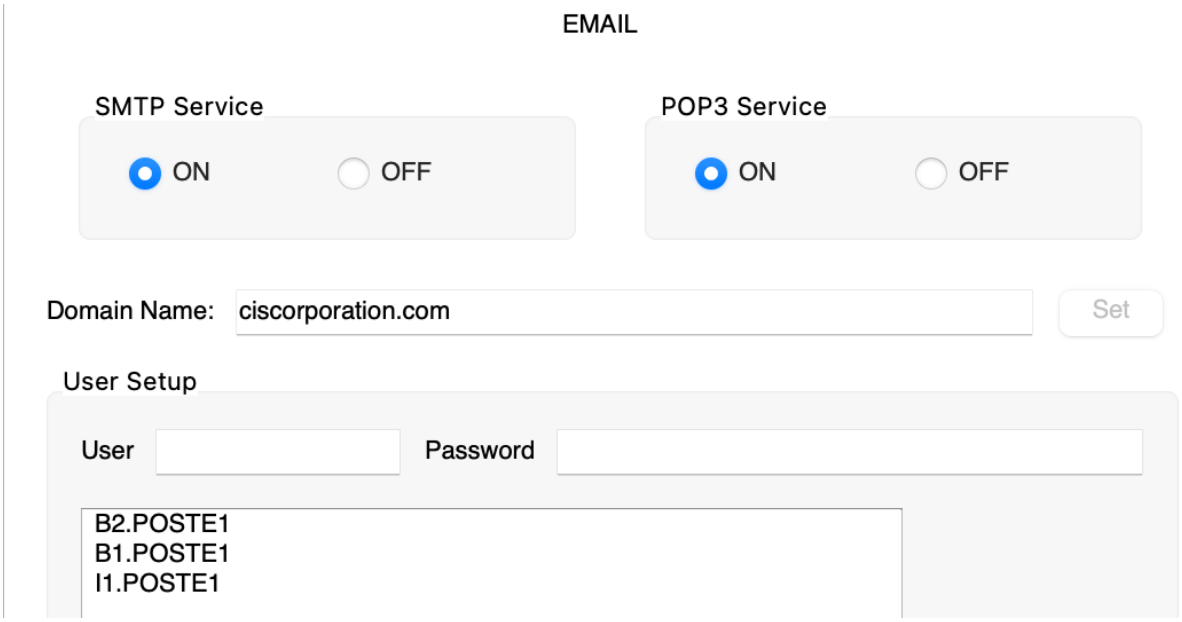


Figure 41 Extrait de la configuration de notre serveur de mail, avec les utilisateurs.

Ainsi, nous pouvons nous connecter sur un des PC de l'entreprise, avec l'application mail présente sur ces derniers. Cela nous donne :

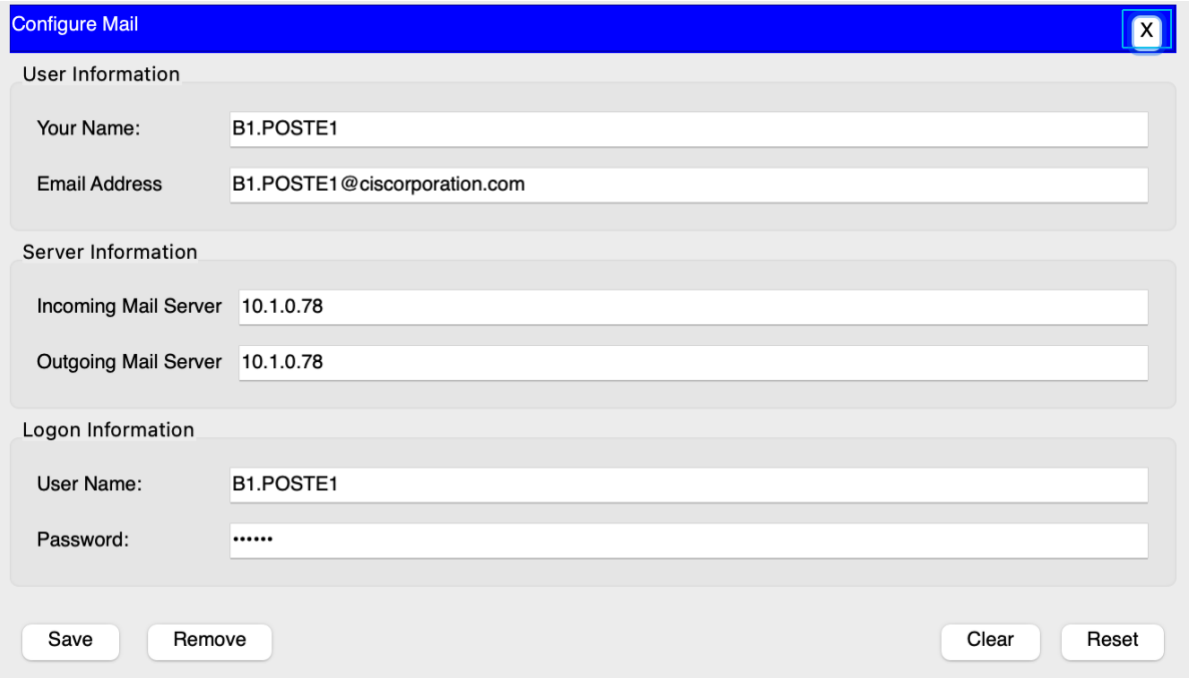


Figure 42 Connexion d'un utilisateur du serveur mail de l'entreprise.

Pour finir, l'utilisateur peut envoyer et recevoir des mails issus de l'entreprise.

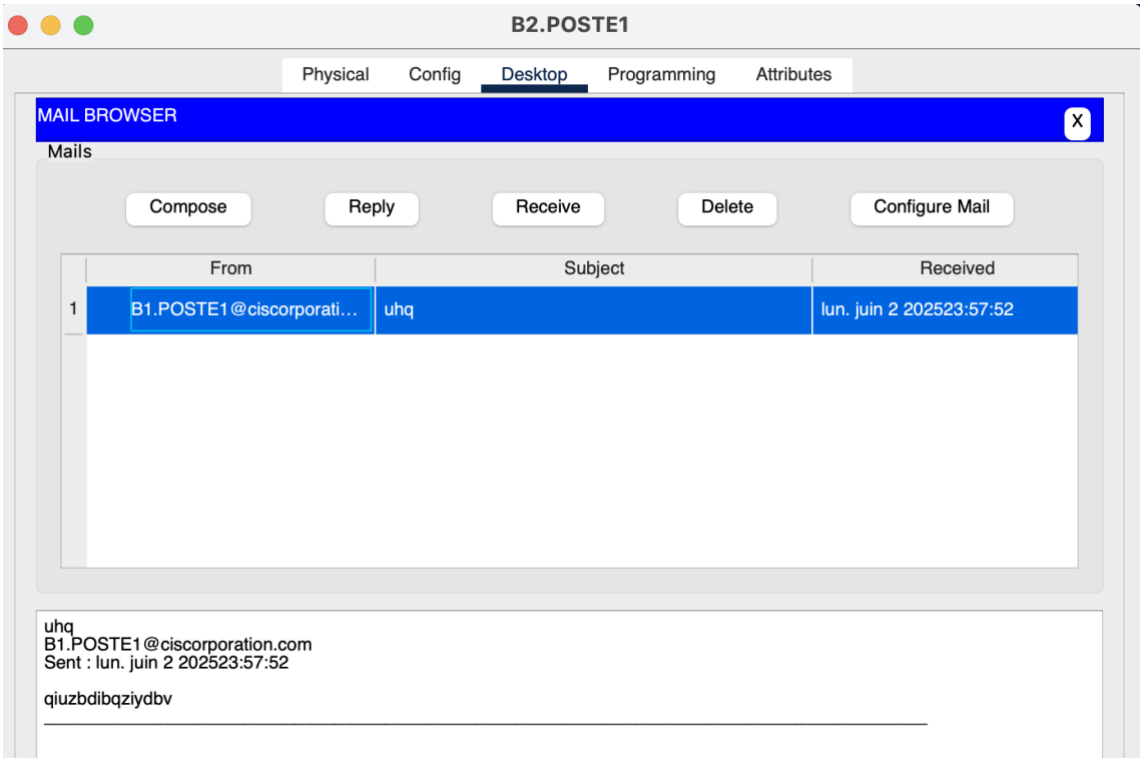


Figure 43 Extrait d'un mail envoyé de l'utilisateur B1.POSTE1 vers B2.POSTE1.

Ce serveur de messagerie est essentiel pour les employés de l'entreprise. En effet, son emplacement sur le réseau interne garantit une certaine sécurité des communications, qui restent ainsi exclusivement sur le réseau local de l'entreprise.

Remarques :

Nous avons seulement créé 3 utilisateurs pour le service de mail de l'entreprise, mais nous aurions très bien pu le faire pour tous les employés.

2.7 Zone démilitarisée (DMZ) et services associés

Premièrement, la présence d'un site web est essentielle pour toute entreprise, lui permettant de diffuser ses offres et services. Au sein de notre entreprise (CisCorporation), ce site web sera hébergé dans une zone externe au réseau local (LAN), appelée DMZ. Cette zone accueillera le serveur web, hébergeant le site web, ainsi qu'un serveur DNS public. Ce dernier assurera la résolution des noms et redirigera vers son serveur DNS racine (un point que nous aborderons ultérieurement). Nous allons donc examiner la configuration de ces équipements.

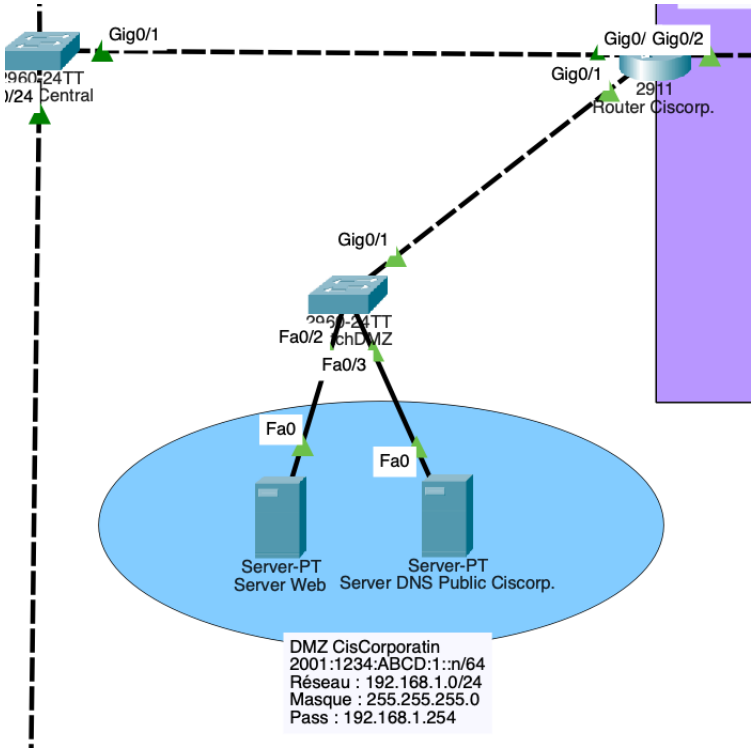


Figure 44 Capture d'écran illustrant l'emplacement de notre DMZ.

Ainsi, la DMZ est connectée à une interface différente de celle du réseau local de l'entreprise, mais sur le même routeur.

2.7.1 Adressage IP de la DMZ

Premièrement, notre DMZ est déployée sur un réseau privé. Il s'agit du réseau 192.168.1.0/24, étant donné que nous n'avons besoin que d'un nombre restreint d'équipements. Nous pouvons donc trouver ci-dessous un tableau récapitulatif du plan d'adressage de cette zone.

Nom de l'équipement	Adresse IPv4 et masque	Adresse IPv6 et masque
Serveur WEB	192.168.1.100/24	2001:1234:ABCD:1::2/64
Serveur DNS	192.168.1.53/24	2001:1234:ABCD:1::3/64

2.7.2 Serveur DNS public

Par la suite, nous configurons le serveur DNS de notre DMZ. Ce serveur contient des enregistrements A et AAAA, permettant de rediriger des noms tels que www.ciscorporation.com vers des machines avec leur adresse IPv4 ou IPv6. Il contiendra également un enregistrement SOA, permettant de renseigner le nom de domaine du serveur. Enfin, nous aurons des enregistrements NS permettant de rediriger les requêtes vers le serveur racine (.com).

Mais Tout d'abord, nous pouvons relever la configuration IP de notre serveur DNS.

```
C:\>ipconfig /all

FastEthernet0 Connection:(default port)

   Connection-specific DNS Suffix..:
   Physical Address.................: 00E0.F783.AE01
   Link-local IPv6 Address.........: FE80::2E0:F7FF:FE83:AE01
   IPv6 Address....................: 2001:1234:ABCD:1::3
   IPv4 Address....................: 192.168.1.53
   Subnet Mask.....................: 255.255.255.0
   Default Gateway.................: 2001:1234:ABCD:1::1
                                     192.168.1.254
   DHCP Servers....................: 0.0.0.0
   DHCPv6 IAID.....................:
   DHCPv6 Client DUID..............: 00-01-00-01-AE-20-7A-BA-00-E0-F7-83-AE-01
   DNS Servers.....................: 2001:1234:ABCD:1::3
                                     192.168.1.53
```

Figure 45 Configuration réseau de notre serveur DNS.

No.	Name	Type	Detail
0	ciscorporation.com	NS	dns.ciscorporation.com
1	ciscorporation.com	SOA	ServerName:dns.cis… MailBox :admin@ciscorporati… Expiry :10 Refresh :10 Retry :10 MinTTL :10
2	com	NS	dns.com
3	dns.ciscorporation.com	A Record	205.0.113.1
4	dns.com	A Record	170.0.0.53
5	www.ciscorporation.com	A Record	205.0.113.1

Figure 46 Enregistrement présent dans le serveur DNS public.

Remarques :

Suite à plusieurs tests, nous avons retiré les enregistrements AAAA, car cela engendrait de multiples crashs du logiciel.

2.7.3 Serveur WEB public

Suite à la configuration réussie de notre serveur DNS public, nous pouvons procéder à la configuration de notre serveur web. Ce dernier héberge le site web de notre entreprise, accessible depuis le réseau local de l'entreprise, mais également depuis les clients du FAI.

Tout d'abord, voici la configuration IP de notre serveur web public :

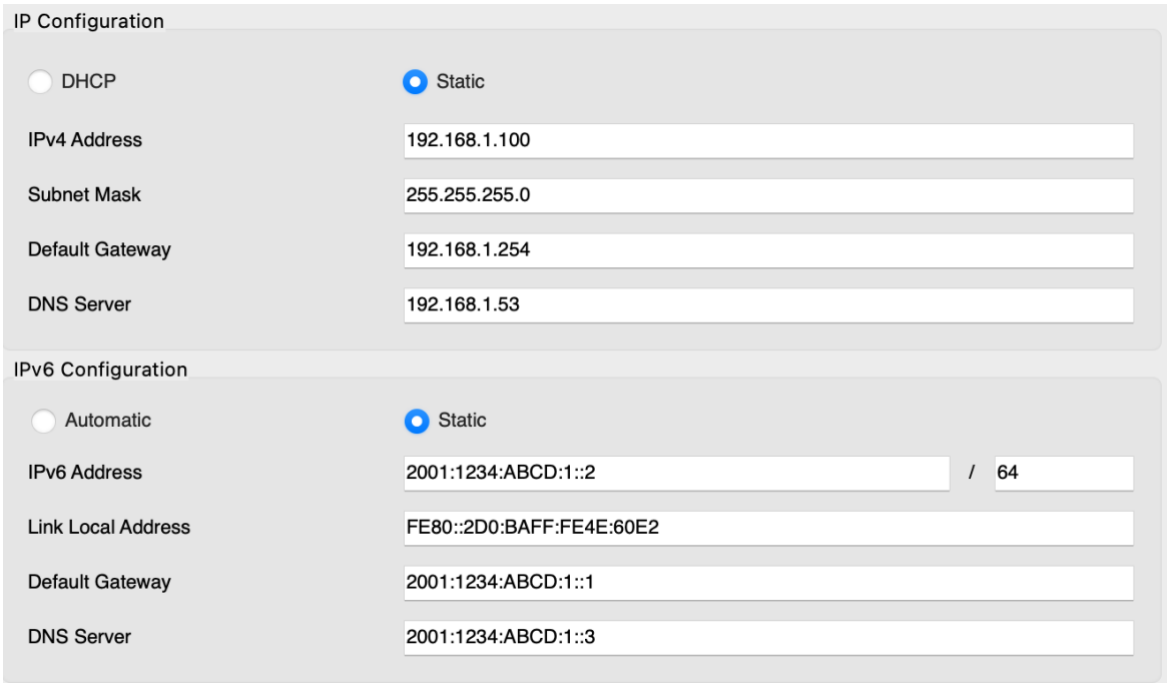


Figure 47 Configuration réseau du serveur WEB public.

2.8 Disponibilité et Sécurité de nos équipements

Dans notre LAN d'entreprise, nous avons mis en place un réseau qui reste disponible même en cas de panne, tout en assurant un minimum de sécurité. Pour garantir la disponibilité, nous avons utilisé des mécanismes de redondance comme le protocole Spanning Tree sur les switches. Côté sécurité, même si elle reste assez simple, elle est tout de même présente, nous utilisons des connexions chiffrées en SSH pour l'accès aux équipements, et des ACLs basiques sur le routeur permettent de filtrer certains flux réseau (Vers la DMZ).

2.8.1 Redondance des Switchs et Spanning-tree

Pour cela, nous avons organisé l'implantation des salles et la répartition des switchs de manière à créer une topologie redondante. Chaque poste utilisateur est connecté à au moins deux chemins réseau différents, ce qui permet de maintenir la connectivité même si un élément tombe en panne.

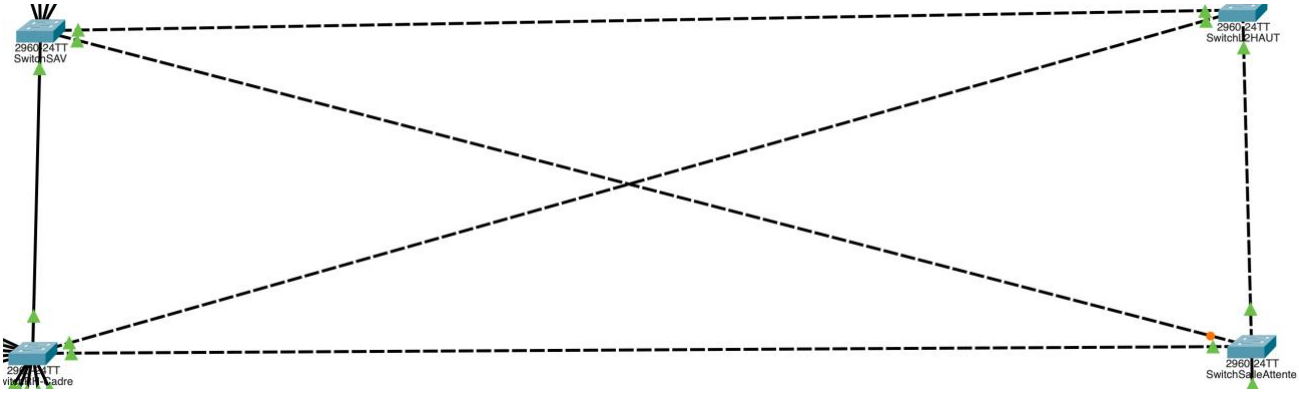


Figure 48 Capture d'écran représentant la redondance de switch.

Par conséquent, l'activation du protocole Spanning-tree est nécessaire afin d'éviter la création de boucles réseau sur le LAN. Ce protocole est implémenté par défaut sur les switchs utilisés dans le LAN. De plus, en cas de panne, il permet d'activer des interfaces garantissant l'accessibilité aux équipements.

Afin de déterminer si le protocole Spanning-tree est activé sur les différents commutateurs, il est possible de consulter le fichier de configuration de chaque appareil.

```
spanning-tree mode pvst
spanning-tree extend system-id
!
```

Figure 49 Commande permettant d'activer le protocole Spanning-tree.

Par conséquent, le protocole Spanning-tree est correctement configuré sur l'ensemble des commutateurs.

2.8.2 Sécurisation des accès aux équipements

Par la suite, nous allons aborder la sécurité des différents équipements de notre réseau local d'entreprise. Premièrement, nous allons sécuriser l'accès à nos commutateurs et à notre routeur, ce qui permettra d'établir une première ligne de défense contre les attaques externes. À cet effet, nous avons exécuté les commandes suivantes sur nos équipements (mot de passe : Admin. sur tous les équipements) :

```
SwitchAccueil#username admin secret Admin.
```

Figure 50 Commande permettant d'ajouter un mode de passe pour accéder au mode privilégié.

De plus, le mot de passe n'est pas visible en clair directement dans le fichier de configuration de l'équipement, comme en témoigne la capture d'écran ci-dessous.

```
username admin secret 5 $1$mERr$yvk.vvD0wkxM2stTa36ra1
!
```

Figure 51 Extrait du fichier de configuration de notre équipement.

Ainsi, en essayant d'accéder à la console privilégié, l'utilisateur devra entrer le mot de passe. Cela permet de créer une première barrière, en ne laissant pas une personne lambda le pouvoir de modifier les équipements de notre LAN.

```
SwitchL1Ingenieur-OpenSpace>enable
Password:
SwitchL1Ingenieur-OpenSpace#
```

Figure 52 Capture d'écran illustrant la demande de mot de passe sur l'équipement.

Par la suite, nous procéderons à la configuration de notre équipement afin de nous permettre d'y accéder via SSH, un protocole sécurisé équivalent à Telnet.

Nous avons exécuté les commandes suivantes, sur tous les switchs du LAN :

```
ip ssh version 2

line vty 0 4
 exec-timeout 5 0
 login local
 transport input ssh
```

```
Vlan99                 192.168.99.4    YES manual up                    up
```

En résumé, les commandes précédentes ont permis la création d'un VLAN de gestion (VLAN 99), facilitant l'accès aux équipements à distance via SSH. Une adresse IP et une passerelle par défaut ont été ajoutées à ce VLAN. Cette passerelle correspond à l'adresse IP du VLAN 99 sur le routeur de l'entreprise (sous interface Gig0/0.99).

```
GigabitEthernet0/0.99  192.168.99.1    YES manual up                    up
```

Figure 53 Capture d'écran de la configuration du routeur, avec l'interface correspondant au VLAN 99.

Après avoir effectué toutes les commandes précédentes, nous pouvons nous connecter aux équipements depuis le PC de Gestion, présent dans le VLAN 99 de Gestion.

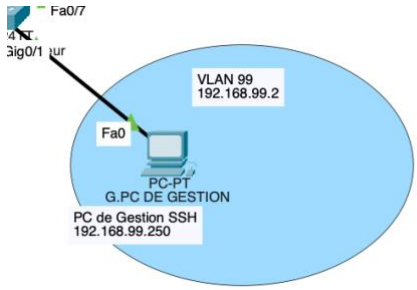


Figure 54 Capture d'écran du VLAN 99, avec le PC de Gestion.

Ainsi, nous renseignons l'adresse IP du l'équipement souhaité, ainsi que le nom d'utilisateur.

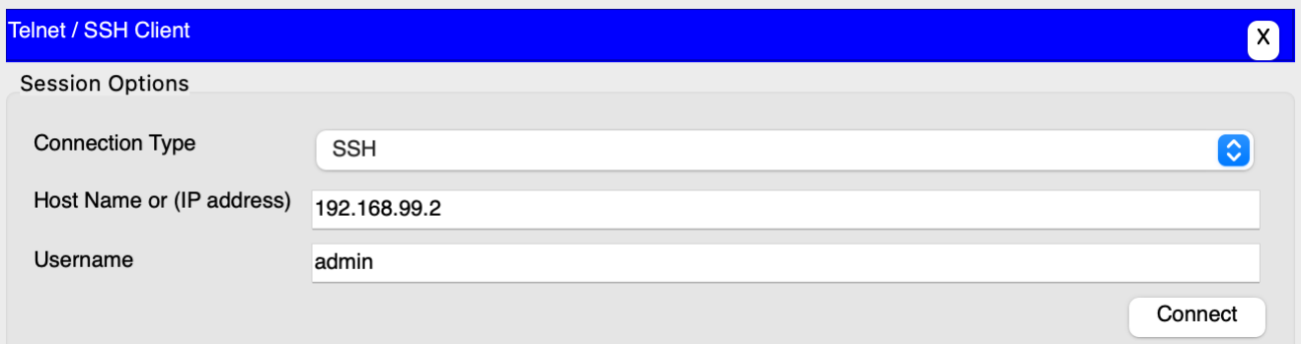


Figure 55 Interface permettant de se connecter aux équipements.

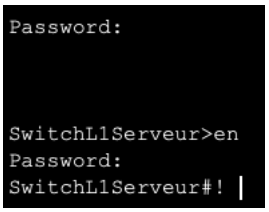


Figure 56 Capture d'écran représentant l'accès via SSH aux équipements.

On constate donc que cette méthode permet d'accéder de manière sécurisée à des équipements. Afin d'accéder à un équipement par son nom, plutôt que par son adresse IP, nous allons créer un serveur DNS dans le VLAN 99. Cela nous donne :

No.	Name	Type	Detail
0	switchaccueil	A Record	192.168.99.5
1	switchcentral	A Record	192.168.99.6
2	switchl1bureau	A Record	192.168.99.3
3	switchl1ingenieur-openspace	A Record	192.168.99.4
4	switchl1serveur	A Record	192.168.99.2
5	switchl2haut	A Record	192.168.99.7
6	switchrh-cadre	A Record	192.168.99.9
7	switchsalleattente	A Record	192.168.99.10
8	switchsav	A Record	192.168.99.8

Figure 57 Enregistrement présent dans le DNS du VLAN 99.

Ainsi, nous pouvons accéder directement aux équipements via SSH, en utilisant leur nom d'hôte au lieu de leur adresse IP.

2.8.3 Contrôle des flux avec les ACL

Par la suite, nous procéderons au contrôle des flux de trafic à l'aide de listes de contrôle d'accès (ACL). Ces ACL seront configurées sur le routeur et permettront uniquement l'accès au serveur web et au serveur DNS situés dans la DMZ. Ainsi, sur notre routeur d'entreprise, nous aurons :

```
access-list 110 permit tcp any host 192.168.1.100 eq www
access-list 110 permit tcp any host 192.168.1.100 eq 443
access-list 110 permit udp any host 192.168.1.53 eq domain
access-list 110 deny ip any 192.168.1.0 0.0.0.255
access-list 110 permit ip any any
```

Figure 58 Extrait des ACL présentent sur le routeur.

Ainsi, nous associons l'interface menant à la DMZ en « in », avec la commande suivante :

```
interface GigabitEthernet0/1
 ip address 192.168.1.254 255.255.255.0
 ip access-group 110 in
 duplex auto
 speed auto
 ipv6 address 2001:1234:ABCD:1::1/64
 ipv6 enable
 ipv6 ospf 1 area 10
```

Figure 59 Extrait de l'interface menant à la DMZ.

Ainsi, avec les listes de contrôle d'accès présentes sur le routeur, nous ne pouvons contacter que le serveur Web et le serveur DNS de la DMZ.

Nous pouvons vérifier le bon fonctionnement de cette ACL, avec un ping depuis un PC du LAN vers

2.9 Traduction d'adresses (NAT)

Dans notre réseau d'entreprise, nous avons mis en place le NAT pour permettre aux équipements internes, qui utilisent des adresses IPv4 privées, de se connecter à Internet via le réseau de l'opérateur. Cette traduction d'adresses est indispensable, et elle est gérée par le routeur principal, qui fait le lien entre notre LAN et le backbone.

2.9.1 NAT en mode PAT, et configuration de liste d'accès

Le NAT est ici configuré en mode PAT. Cette méthode permet à tous les postes internes de partager une seule adresse IPv4 publique pour accéder à Internet, tout en différenciant les connexions par des ports dynamiques. Cela répond à la problématique de pénurie d'adresses IPv4 tout en assurant une forme de cloisonnement du réseau interne.

Sur notre routeur, la liste d'accès est :

```
access-list 1 permit any
```

Figure 60 Capture d'écran de la liste d'accès.

2.9.2 Configuration des Interfaces du routeur d'entreprise

Ensuite, nous avons associé les interfaces en les mettant soit Inside, soit Outside, cela nous donne :

```
interface GigabitEthernet0/0
 no ip address
 ip helper-address 10.1.0.75
 ip nat inside
 duplex auto
 speed auto
```

Figure 61 Capture d'écran de la configuration sur l'interface du routeur (coté entreprise).

```
interface GigabitEthernet0/2
 ip address 205.0.113.1 255.255.255.0
 ip access-group 100 in
 ip nat outside
 duplex auto
 speed auto
```

Figure 62 Capture d'écran de la configuration sue l'interface du routeur (coté Backbone).

Suite à cela, les différents équipements de l'entreprise peuvent communiquer avec Internet.

2.9.3 Redirection de port pour serveur Web et DNS de la DMZ

Après avoir configuré les listes d'accès et les interfaces nécessaires pour le NAT, nous passons maintenant à la redirection de port.

La redirection de port permet de rendre accessibles, depuis l'extérieur, les services hébergés dans la DMZ (comme un serveur web, DNS, etc.). Elle consiste à rediriger les connexions entrantes sur un certain port de l'adresse publique du routeur vers une machine précise dans le réseau privé.

Par exemple, une connexion entrante sur le port 80 (HTTP) de l'adresse publique peut être redirigée vers le serveur web situé dans la DMZ. Pour cela, nous avons utilisé les commandes suivantes :

```
ip nat inside source static tcp 192.168.1.100 80 205.0.113.1 80
ip nat inside source static udp 192.168.1.53 80 205.0.113.1 53
```

Figure 63 Commande permettant de faire une redirection de port.

Ainsi, lorsque nous établissons une connexion depuis l'extérieur, nous recevons une réponse provenant de l'adresse IP publique du routeur de l'entreprise. Voici un exemple ci-dessous :

```
C:\>ping www.ciscorporation.com

Pinging 205.0.113.1 with 32 bytes of data:

Reply from 205.0.113.1: bytes=32 time<1ms TTL=252
Reply from 205.0.113.1: bytes=32 time<1ms TTL=252
Reply from 205.0.113.1: bytes=32 time<1ms TTL=252
Reply from 205.0.113.1: bytes=32 time<1ms TTL=252

Ping statistics for 205.0.113.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Figure 64 Connexion initié depuis l'extérieur, vers le serveur web de l'entreprise.

Nous avons donc une réponse depuis l'adresse IPv4 publique du routeur (schéma ci-dessous).

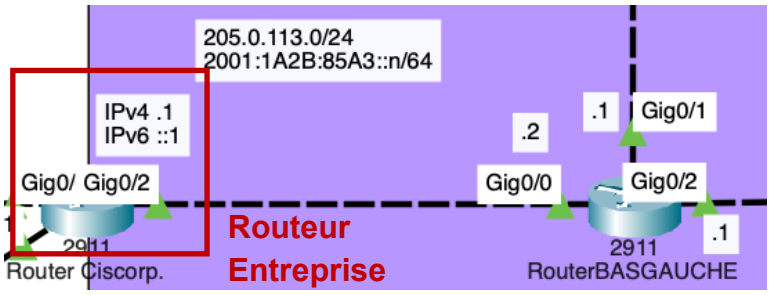


Figure 65 Schéma illustrant notre routeur d'entreprise, avec une IP publique.

2.10 Routage dynamique avec OSPF

Pour permettre à nos équipements de communiquer avec Internet et avec les clients des FAI, nous allons configurer le routage sur notre routeur d'entreprise. Pour que ce soit plus simple à gérer et adaptable en cas de changement, nous avons choisi d'utiliser un protocole de routage dynamique, OSPF.

Ce protocole, basé sur l'état des liens, est couramment utilisé dans les réseaux d'entreprise. Les routeurs OSPF échangent entre eux les informations sur les réseaux qu'ils connaissent, ce qui leur permet de remplir automatiquement leurs tables de routage.

2.10.1 Attribution des différentes aires

Pour commencer, nous allons attribuer un numéro d'aire à chaque partie du réseau afin de faire fonctionner correctement le protocole OSPF.

Pour notre entreprise, nous avons choisi d'utiliser l'aire 10 pour le LAN et la DMZ. Le backbone, lui, sera placé dans l'aire 0. La configuration de cette partie sera détaillée un peu plus loin.

Cette séparation permet d'isoler le trafic entre le réseau local de l'entreprise et le backbone, ce qui rend l'ensemble plus clair et mieux organisé.

2.10.2 Configuration du protocole OSPF pour IPv4, sur le routeur d'entreprise.

Afin de configurer le protocole OSPF sur notre routeur, nous allons d'abord activer le protocole à l'aide de la commande suivante.

```
router ospf 1
 router-id 10.10.10.10
```

Figure 66 Commande permettant d'activer OSPF sur notre routeur.

Comme illustré précédemment, nous attribuons un identifiant à notre routeur. Cet identifiant permettra d'identifier le routeur qui fournit les informations sur les réseaux connus.

Ensuite, nous renseignons les réseaux connus par le routeur. Pour l'instant, nous avons juste le LAN d'entreprise, ainsi que la DMZ.

```
network 10.0.0.0 0.255.255.255 area 10
network 192.168.1.0 0.0.0.255 area 10
```

Figure 67 Commande permettant de renseigner les réseaux connus par le routeur.

Ainsi, OSPF est maintenant configuré pour la partie entreprise.

2.10.3 Configuration du protocole OPSFv3 pour IPv6, sur le routeur d'entreprise

Suite à la configuration du routeur d'entreprise, afin d'effectuer des tâches de routage via un protocole de routage dynamique, nous allons procéder de la même manière pour l'IPv6. À cet effet, nous allons utiliser le protocole OSPFv3.

Tout d'abord, nous allons effectuer les commandes suivantes :

```
ipv6 router ospf 1
 router-id 10.10.10.10
```

Figure 68 Commande permettant de configurer le protocole OSPFv3.

Ainsi, nous activons le protocole OPSFv3, et nous attribuons un ID à notre routeur, comme cela a été fait pour l'IPv4.

Par la suite, nous configurons chaque interface, sur une aire définie. Pour l'instant, nous allons uniquement nous occuper des interfaces reliant le réseau local et la DMZ, sur l'aire 10.

```
interface GigabitEthernet0/0.10
 encapsulation dot1Q 10
 ip address 10.1.0.1 255.255.255.240
 ipv6 address 2001:DB8:1:10::1/64
 ipv6 ospf 1 area 10
```

Figure 69 Commande renseignant l'interface Gig0/0.10, sur l'area 10.

Nous faisons cela pour chaque VLAN de notre LAN, ainsi qu'avec la DMZ.

```
interface GigabitEthernet0/1
 ip address 192.168.1.254 255.255.255.0
 duplex auto
 speed auto
 ipv6 address 2001:1234:ABCD:1::1/64
 ipv6 enable
 ipv6 ospf 1 area 10
```

Figure 70 Commande similaire pour la DMZ.

Nous avons donc mis en place la première partie du routage dynamique sur notre routeur. Nous continuerons cette configuration dans la partie suivante, dédiée à la connexion Internet.

3 Création et configuration du backbone

Le backbone est la partie centrale du réseau qui relie le routeur principal de l'entreprise à plusieurs fournisseurs d'accès à Internet (FAI). Il permet également la connexion à un réseau externe simulant l'Internet, avec un serveur DNS racine (.com). Dans cette partie, on configure les adresses IP et le protocole OSPF pour permettre une communication fluide et dynamique entre l'entreprise, les FAI et les services DNS externes.

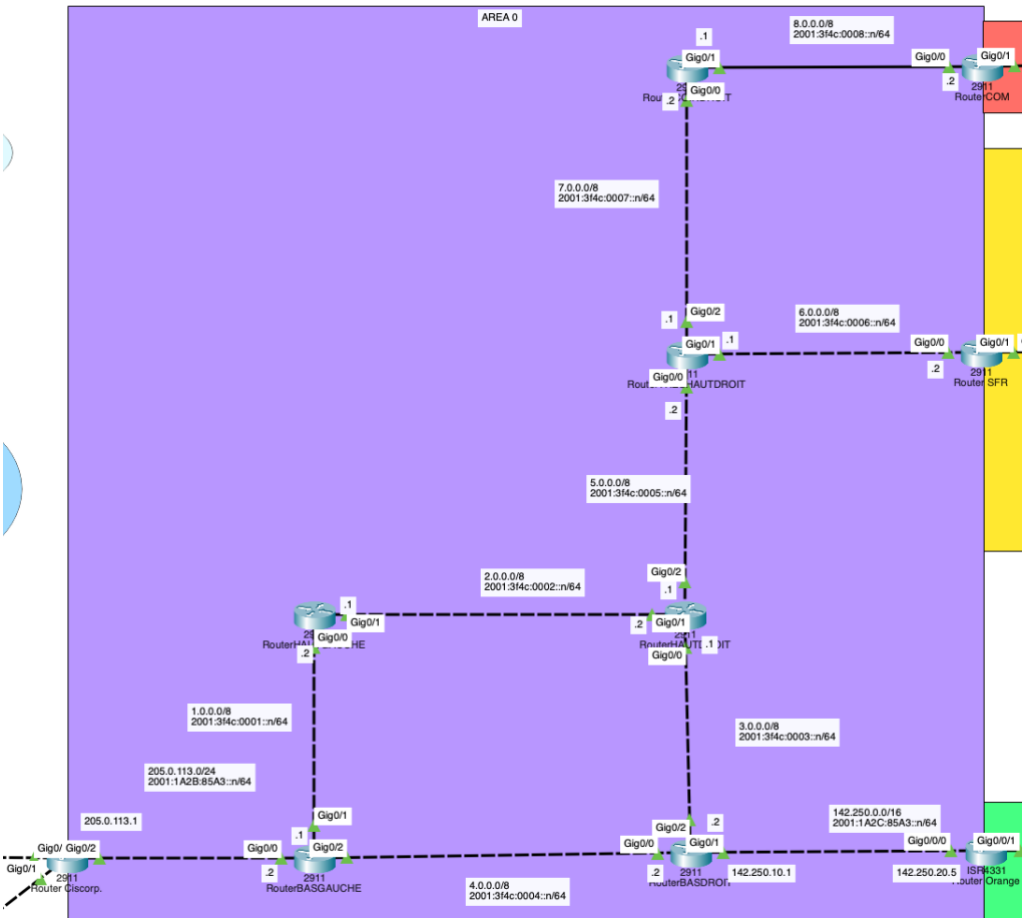


Figure 71 Capture d'écran du Backbone (violet).

3.1 Choix des équipements et des supports de communications

3.1.1 Choix des équipements réseaux

Pour la réalisation du backbone, nous avons choisi d'utiliser principalement des routeurs Cisco 2911 et Cisco 4331, qui offrent des performances adaptées au routage IPv4 et IPv6 ainsi qu'à la gestion des protocoles dynamiques comme OSPF.

Figure 72 Image d'un routeur 2911.

3.1.2 Choix des supports de communications

Concernant les supports de communication, les connexions entre les équipements sont majoritairement établies à l'aide de câbles croisés, afin d'assurer une bonne compatibilité entre interfaces routeurs. Pour certaines liaisons spécifiques, notamment entre un PC et un switch, nous avons utilisé des câbles droits. Ces choix garantissent une infrastructure réseau fiable et conforme aux standards des réseaux d'entreprise.

Figure 73 Image illustrant un câble croisé

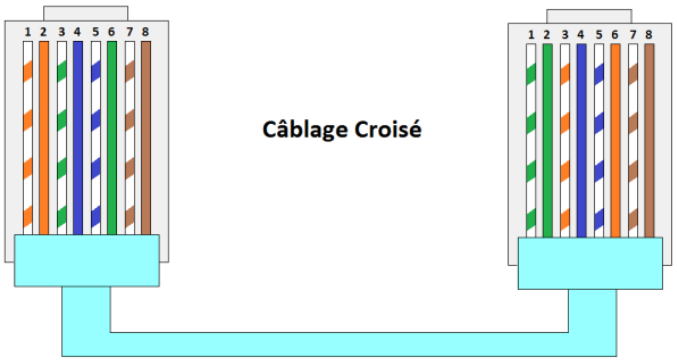


Figure 74 Schéma illustrant un câble croisé.

3.2 Adressage IPv4 et IPv6 sur équipement du Backbone

3.2.1 Plan d'adressage IPv4 et IPv6

Pour le plan d'adressage IPv4, nous avons choisi d'utiliser plusieurs plages d'adresses publiques simulées, allant de 1.0.0.0/8 à 8.0.0.0/8, ainsi que des blocs plus spécifiques comme 205.0.113.0/24 et 142.250.0.0/16. Voici le schéma avec les différents réseaux, appliqués aux routeurs.

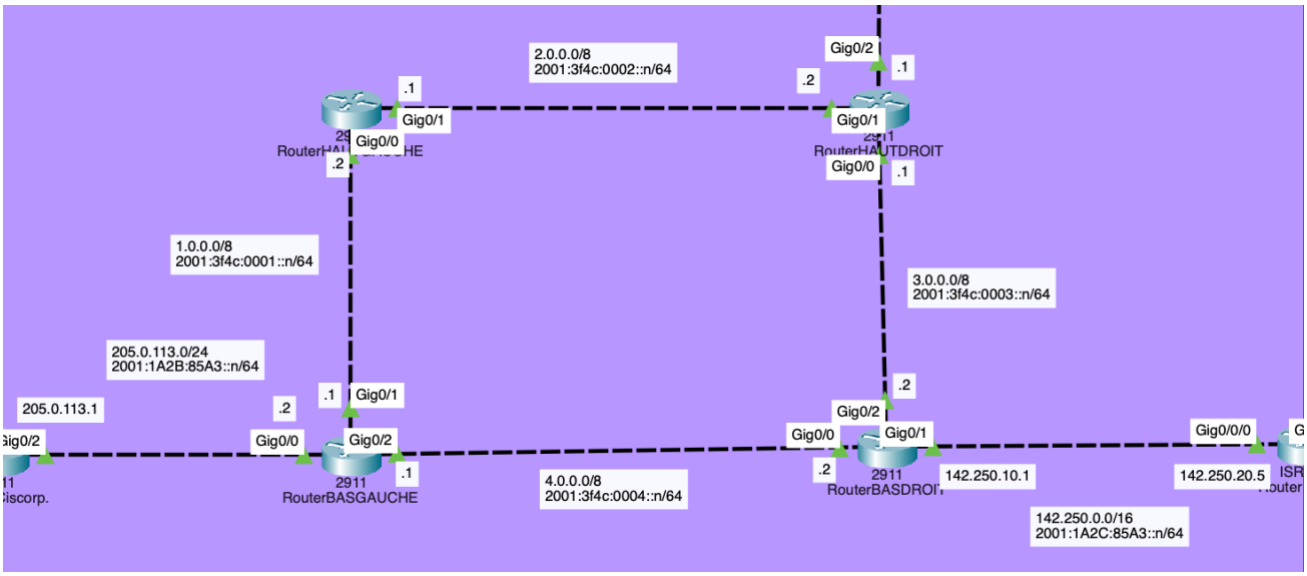


Figure 75 Capture d'écran illustrant le bas du Backbone.

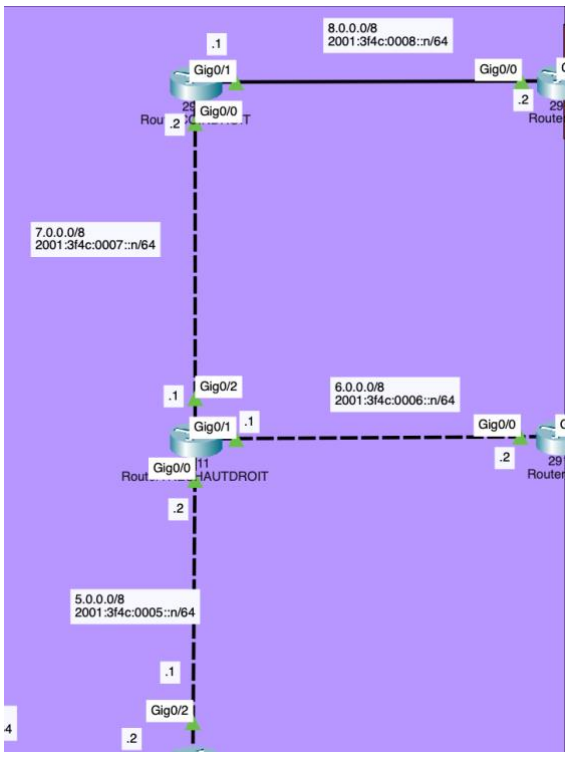


Figure 76 Capture d'écran illustrant le haut du Backbone.

Nous pouvons relever le tableau ci-dessous, illustrant toutes les interfaces des routeurs du backbone (area 0).

Nom du routeur	Interfaces	Adresse IPv4	Adresse IPv6
Routeur d'entreprise	Gig0/2	205.0.113.1/24	2001:1A2B:85A3::1/64
Routeur BASGAUCHE	Gig0/0	205.0.113.2/24	2001:1A2B:85A3::2/64
-	Gig0/1	1.0.0.1/8	2001:3f4c:0001::1/8
-	Gig0/2	4.0.0.1/8	2001:3F4C:4:0001:1/64
Routeur BASDROIT	Gig0/0	4.0.0.2/8	2001:3f4c:0004::2/64
-	Gig0/1	142.250.10.1/16	2001:1A2C:85A3::1/64
-	Gig0/2	3.0.0.2/8	2001:3f4c:0003::2/64
Routeur HAUTGAUCHE	Gig0/1	1.0.0.2/8	2001:3f4c:0001::2/64
-	Gig0/2	2.0.0.1/8	2001:3f4c:0002::1/64
Routeur HAUDROIT	Gig0/0	3.0.0.1/8	2001:3f4c:0003::1/64
-	Gig0/1	2.0.0.2/8	2001:3f4c:0002::2/64
-	Gig0/2	5.0.0.1/8	2001:3f4c:0005::1/64
Routeur TRES HAUTDROIT	Gig0/0	5.0.0.2/8	2001:3f4c:0005::2/64
-	Gig0/1	6.0.0.1/8	2001:3f4c:0006::1/64
-	Gig0/2	7.0.0.1/8	2001:3f4c:0007::1/64
Routeur COINDROIT	Gig0/0	7.0.0.2/8	2001:3f4c:0007::2/64
-	Gig0/1	8.0.0.1/8	2001:3f4c:0008::1/64
Routeur ORANGE	Gig0/0/0	142.250.20.5/16	2001:1A2C:85A3::2/64
Routeur SFR	Gig0/0	6.0.0.2/8	2001:3f4c:0006::2/64
Routeur COM	Gig0/0	8.0.0.2/8	2001:3f4c:0008::2/64

Ainsi, nous pouvons constater que notre Backbone ne comprend que des réseaux IPv4 publics. Ces derniers donnent accès aux différents fournisseurs d'accès Internet de l'entreprise, ainsi qu'au serveur DNS racine.

3.2.2 Configuration des interfaces des routeurs

Après avoir établi un plan détaillé de notre adressage IPv4 et IPv6 pour le backbone, nous procédons à la configuration de nos équipements Cisco afin de mettre en œuvre cet adressage.

Tout d'abord, nous attribuons une adresse IPv4 pour une interface de nos routeurs, voici un exemple :

```
interface GigabitEthernet0/0
 ip address 4.0.0.2 255.0.0.0
```

Figure 77 Commande permettant d'ajouter une IPv4 sur une interface.

Et nous faisons de même avec l'IPv6 :

```
ipv6 address 2001:3F4C:4::2/64
ipv6 enable
```

Figure 78 Commande permettant d'ajouter une IPv6 sur une interface.

Ainsi, nous avons configuré une interface d'un de nos routeurs, avec une adresse IPv4 et une IPv6. Nous procédons de la même manière pour toutes les interfaces des routeurs du backbone.

3.3 Configuration du routage dynamique sur routeurs du Backbone

3.3.1 Configuration d'OPSF pour IPv4, sur routeur du Backbone

Après avoir configurer toutes les interfaces des routeurs du Backbone, nous allons maintenant nous intéresser au protocole de routage OSPF. Ce protocole de routage est un protocole dynamique, déjà configurer pour la partie LAN et DMZ de l'entreprise. Nous allons maintenant le configurer pour le Backbone. Pour chaque routeur, nous rentrons les commandes suivantes :

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

Figure 79 Démarrage du protocole OPSF, et attribution d'ID.

Tout d'abord, nous démarrons le protocole OSPF, avec la commande ci-dessus. Et nous attribuons un ID (unique), sur chacun de nos routeurs.

Ensuite, nous renseignons sur tous les routeurs, les réseaux que connaissent ces derniers. Nous pouvons faire cela avec la commande suivante :

```
network 205.0.113.0 0.0.0.255 area 0
network 10.0.0.0 0.255.255.255 area 10
network 192.168.1.0 0.0.0.255 area 10
network 10.1.0.0 0.0.0.15 area 10
```

Figure 80 Commande permettant de renseigner, pour le protocole OSPF, les réseaux que connait un routeur (routeur d'entreprise).

Ainsi, nous pouvons faire cela pour tous routeurs du Backbone. Voici toutes les configurations.

Pour le routeur BASGAUCHE :

```
router ospf 1
 router-id 1.1.1.1
 log-adjacency-changes
 network 205.0.113.0 0.0.0.255 area 0
 network 1.0.0.0 0.255.255.255 area 0
 network 4.0.0.0 0.255.255.255 area 0
```

Figure 81 Commande OSPF pour le routeur BASGAUCHE.

Pour le routeur BASDROIT :

```
router ospf 1
 router-id 4.4.4.4
 log-adjacency-changes
 network 3.0.0.0 0.255.255.255 area 0
 network 4.0.0.0 0.255.255.255 area 0
 network 142.250.0.0 0.0.255.255 area 0
```

Figure 82 Commande OSPF pour le routeur BASDROIT.

Pour le routeur HAUTGAUCHE :

```
router ospf 1
 router-id 2.2.2.2
 log-adjacency-changes
 network 1.0.0.0 0.255.255.255 area 0
 network 2.0.0.0 0.255.255.255 area 0
```

Figure 83 Commande OSPF pour le routeur HAUTGAUCHE.

Pour le routeur HAUTDROIT :

```
router ospf 1
 router-id 3.3.3.3
 log-adjacency-changes
 network 2.0.0.0 0.255.255.255 area 0
 network 3.0.0.0 0.255.255.255 area 0
 network 5.0.0.0 0.255.255.255 area 0
```

Figure 84Commande OSPF pour le routeur BASGAUCHE.HAUDROIT.

Pour le routeur THAUTDROIT :

```
router ospf 1
 router-id 6.6.6.6
 log-adjacency-changes
 network 5.0.0.0 0.255.255.255 area 0
 network 6.0.0.0 0.255.255.255 area 0
 network 7.0.0.0 0.255.255.255 area 0
```

Figure 85 Commande OSPF pour le routeur BASGAUCHE.THAUDROIT.

Pour le routeur COINDROIT :

```
router ospf 1
 router-id 8.8.8.8
 log-adjacency-changes
 network 7.0.0.0 0.255.255.255 area 0
 network 8.0.0.0 0.255.255.255 area 0
```

Figure 86 Commande OSPF pour le routeur COINDROIT.

Pour le routeur ORANGE :

```
router ospf 1
 router-id 20.20.20.20
 log-adjacency-changes
 network 150.0.0.0 0.0.255.255 area 5
 network 142.250.0.0 0.0.255.255 area 0
```

Figure 87 Commande OSPF pour le routeur ORANGE.

Pour le routeur SFR :

```
router ospf 1
 router-id 7.7.7.7
 log-adjacency-changes
 network 6.0.0.0 0.255.255.255 area 0
 network 160.0.0.0 0.0.255.255 area 15
```

Figure 88 Commande OSPF pour le routeur SFR.

Et pour le routeur COM :

```
router ospf 1
 router-id 9.9.9.9
 log-adjacency-changes
 network 8.0.0.0 0.255.255.255 area 0
 network 170.0.0.0 0.0.255.255 area 100
```

Figure 89 Commande OSPF pour le routeur COM.

Pour vérifier la bonne configuration d'OSPF, nous pouvons effectuer un ping entre 2 routeurs éloignés. Cela nous donne :

```
RouterCOM#ping 1.0.0.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 1.0.0.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/0 ms
```

Figure 90 Ping depuis le routeur COM vers le réseau 1.0.0.0/8.

3.3.2 Configuration d'OSPFv3 pour IPv6, sur routeur du Backbone

Nous allons maintenant configurer le protocole OSPFv3, qui permet d'effectuer un routage dynamique avec l'IPv6. Pour ce faire, nous allons démarrer le protocole et attribuer un identifiant unique à chaque routeur.

```
ipv6 router ospf 1
 router-id 10.10.10.10
```

Figure 91 Commande permettant d'activer l'OSPFv3, et attribue un ID pour le routeur.

Après avoir procédé ainsi pour tous les routeurs du Backbone, nous allons maintenant associer, pour chaque interface, l'aire à laquelle elle appartient. Cela nous donne :

```
interface GigabitEthernet0/2
 ip address 205.0.113.1 255.255.255.0
 ip access-group 100 in
 ip nat outside
 duplex auto
 speed auto
 ipv6 address 2001:1A2B:85A3::1/64
 ipv6 enable
 ipv6 ospf 1 area 0
```

Figure 92 Commande associant une interface a une aire.

Nous procédons de la même manière, pour toutes les interfaces des routeurs.

Après avoir fait cela, nous pouvons vérifier notre configuration avec un ping entre 2 routeurs distants.

```
RouterCOM#ping 2001:1A2B:85A3::1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:1A2B:85A3::1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/0 ms
```

Figure 93 Ping entre le routeur COM et le routeur BASGAUCHE.

Ainsi, nous pouvons confirmer le bon fonctionnement de notre configuration OSPFv3.

4 Création et configuration des FAI de l'entreprise

Dans notre simulation, l'entreprise est connectée à deux fournisseurs d'accès à Internet, Orange et SFR, pour garantir la redondance et une bonne disponibilité de l'accès Internet. Chaque FAI a sa propre infrastructure, avec un client, un serveur web et un serveur DNS. Ces FAI sont reliés au backbone de l'entreprise via un routeur spécifique.

4.1 Configuration du premier FAI : Orange

Pour notre premier fournisseur d'accès Internet, nous avons opté pour Orange, un opérateur de télécommunications reconnu en Europe et en Afrique.

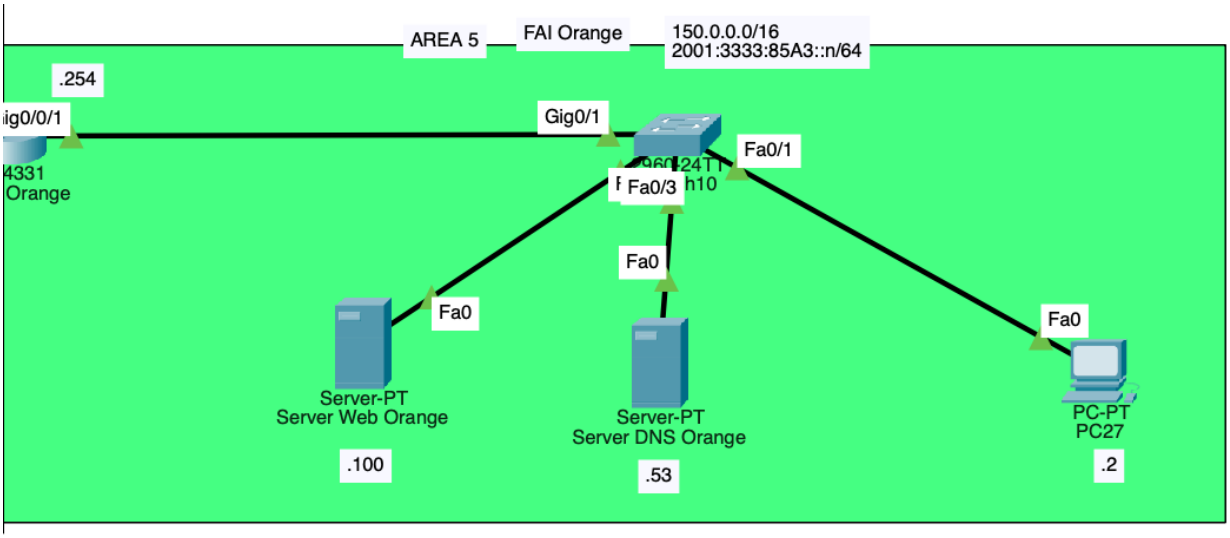


Figure 94 Topologie de notre FAI Orange.

4.1.1 Choix des équipements du FAI Orange

Pour la configuration de notre fournisseur d'accès à Internet (FAI), nous avons sélectionné un routeur Cisco 4331, capable de gérer le routage dynamique en IPv4 et IPv6. Concernant la partie commutateur, nous avons opté pour des commutateurs Cisco 2960, permettant de connecter un grand nombre d'équipements (non nécessaire dans notre cas compte tenu du faible nombre de machines). Enfin, notre FAI dispose d'un serveur DNS et d'un serveur web publics, accessibles depuis le réseau local de l'entreprise.

4.1.2 Plan d'adressage IPv4 et IPv6

Tout d'abord, nous allons nous intéresser à l'IPv4. Pour notre fournisseur d'accès à Internet (Orange), composé de deux serveurs et d'un client, nous allons utiliser un réseau IPv4 public. Nous allons affecter le réseau 150.0.0.0/16.

Ensuite, nous allons affecter le réseau IPv6 suivant : 2001:3333:85A3::/64.

Nous pouvons dresser ci-dessous le plan d'adressage IPv4 et IPv6.

Nom de l'équipement	Adresse IPv4	Adresse IPv6
Routeur Orange – Gig0/0/1	150.0.0.254/16	2001:3333:85A3::1/64
Client FAI	150.0.0.2/16	2001:3333:85A3::2/64
Serveur DNS	150.0.0.53/16	2001:3333:85A3::3/64
Serveur Web	150.0.0.100/16	2001:3333:85A3::4/64

Ainsi, nous pouvons relever les configurations réseaux des différents équipements.

Tout d'abord, voici la configuration sur le routeur Orange :

```
interface GigabitEthernet0/0/1
 ip address 150.0.0.254 255.255.0.0
 duplex auto
 speed auto
 ipv6 address 2001:3333:85A3::1/64
 ipv6 enable
 ipv6 ospf 1 area 5
```

Figure 95 Configuration du routeur Orange.

Ensuite, voici la configuration réseau du client FAI :

```
C:\>ipconfig

FastEthernet0 Connection:(default port)

   Connection-specific DNS Suffix..:
   Link-local IPv6 Address.....: FE80::230:A3FF:FECD:E62D
   IPv6 Address.....: 2001:3333:85A3::2
   IPv4 Address.....: 150.0.0.2
   Subnet Mask.....: 255.255.0.0
   Default Gateway.....: 2001:3333:85A3::1
                         150.0.0.254
```

Figure 96 Configuration du client FAI.

Enfin, voici les configurations des serveurs :

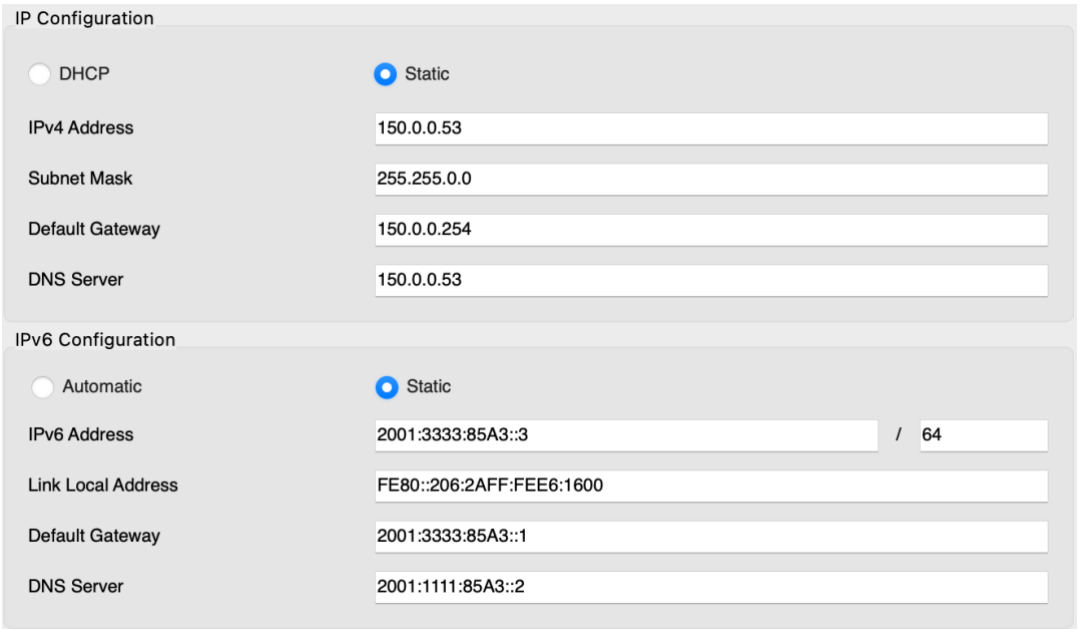


Figure 97 Configuration réseau du serveur DNS

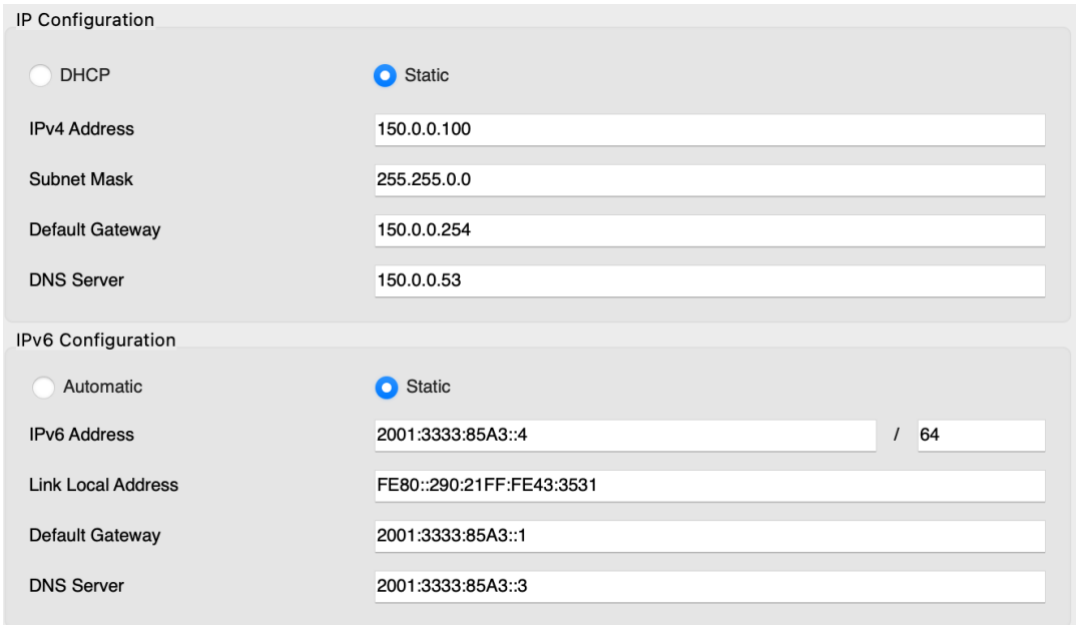


Figure 98 Configuration réseau du serveur Web.

Ainsi, nous pouvons désormais établir des connexions en provenance du réseau local de l'entreprise vers le client du fournisseur d'accès à Internet. En revanche, l'inverse n'est pas possible, tant en IPv4 qu'en IPv6, car nous avons configuré des listes de contrôle d'accès permettant de bloquer le trafic initié depuis l'extérieur du réseau d'entreprise vers ce dernier.

```
C:\>ping 150.0.0.2

Pinging 150.0.0.2 with 32 bytes of data:

Reply from 150.0.0.2: bytes=32 time<1ms TTL=124
Reply from 150.0.0.2: bytes=32 time<1ms TTL=124
Reply from 150.0.0.2: bytes=32 time<1ms TTL=124
Reply from 150.0.0.2: bytes=32 time<1ms TTL=124

Ping statistics for 150.0.0.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Figure 99 Extrait d'un ping depuis le LAN d'entreprise vers le client FAI.

Il ne nous reste plus qu'à configurer le serveur DNS et le serveur Web du FAI afin de permettre l'accès au site Web du FAI depuis l'entreprise.

4.1.3 Configuration d'OPSF et OPSFv3 sur le routeur Orange

Suite à la configuration de nos adresses IPv4 et IPv6 sur nos équipements, nous procéderons à la configuration du protocole de routage dynamique OSPF et OSPFv3 sur notre routeur. Nous commencerons par la configuration du réseau du fournisseur d'accès Internet.

```
router ospf 1
 router-id 20.20.20.20
 log-adjacency-changes
 network 150.0.0.0 0.0.255.255 area 5
```

Figure 100 Commande permettant de renseigner le réseau 150.0.0.0/16, dans l'area 5.

Ainsi, le client du FAI Orange peut communiquer avec les réseaux du Backbone, via le protocole IPv4.

Nous allons maintenant configurer le protocole OSPFv3, qui permet d'effectuer la même opération, mais pour l'IPv6. Contrairement à OSPF, nous allons cette fois-ci associer une interface à une aire. Cela nous donne, pour le routeur Orange :

```
interface GigabitEthernet0/0/1
 ip address 150.0.0.254 255.255.0.0
 duplex auto
 speed auto
 ipv6 address 2001:3333:85A3::1/64
 ipv6 enable
 ipv6 ospf 1 area 5
```

Figure 101 Configuration de l'interface Gig0/0/1 pour OSPFv3.

Ainsi, le client du FAI peut communiquer avec les autres réseaux du backbone, en IPv4 et en IPv6.

4.1.4 Configuration des serveurs Web et DNS du FAI d'Orange

Pour mettre en place une configuration correcte côté fournisseur d'accès, nous allons maintenant configurer un serveur web qui hébergera le site d'Orange, ainsi qu'un serveur DNS chargé de gérer les résolutions de noms et les redirections.

Nous avons donc pour le serveur Web :

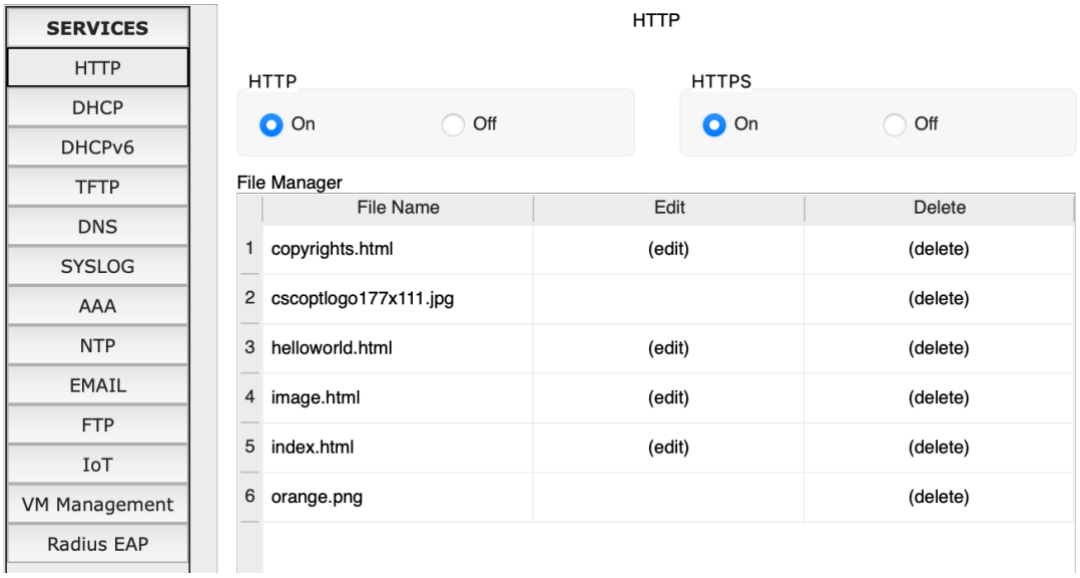


Figure 102 Extrait de la configuration HTTP du serveur Web.

Ensuite, nous pouvons relever la configuration du serveur DNS d'Orange. Cela nous donne :

No.	Name	Type	Detail
0	com	NS	dns.com
1	dns.com	A Record	170.0.0.53
2	dns.orange.com	A Record	150.0.0.53
3	orange.com	SOA	ServerName:dns.ora... MailBox :admin@orange.com Expiry :10 Refresh :10 Retry :10 MinTTL :10
4	orange.com	NS	dns.orange.com
5	www.ciscorporation.com	A Record	205.0.113.1
6	www.orange.com	A Record	150.0.0.100

Figure 103 Enregistrement présent dans le DNS d'Orange.

Dans les enregistrements ci-dessus, nous retrouvons tout d'abord un enregistrement SOA, qui indique les informations principales sur la zone DNS : le nom de domaine, le nom du serveur DNS principal, l'adresse email de l'administrateur, ainsi que plusieurs paramètres comme le refresh, le retry, l'expire et le minimum TTL.

Ensuite, nous avons différents enregistrements A et AAAA, qui associent respectivement des noms d'hôtes à leurs adresses IPv4 et IPv6. Ces enregistrements permettent d'indiquer les adresses IP des serveurs Web, des serveurs DNS ou d'autres machines du domaine.

Enfin, nous avons les enregistrements NS, qui désignent les serveurs faisant autorité pour le domaine. Ces enregistrements permettent de déléguer la gestion DNS du domaine à un ou plusieurs serveurs spécifiques. L'un de ces enregistrements peut pointer vers un serveur DNS situé dans le domaine supérieur (.com), ce qui permet une redirection ou délégation vers le serveur racine.

Ainsi, l'ensemble de ces enregistrements permet le bon fonctionnement de la résolution de noms vers le domaine orange.com.

Toutefois, il nous est impossible d'effectuer des tests de résolution de noms depuis le réseau local de l'entreprise, le serveur DNS racine n'étant pas configuré. Mais nous pouvons tester la résolution de nom depuis le client FAI. Cela nous donne :

```
C:\>ping www.orange.com

Pinging 2001:3333:85A3::4 with 32 bytes of data:

Reply from 2001:3333:85A3::4: bytes=32 time<1ms TTL=128
Reply from 2001:3333:85A3::4: bytes=32 time<1ms TTL=128
Reply from 2001:3333:85A3::4: bytes=32 time<1ms TTL=128
Reply from 2001:3333:85A3::4: bytes=32 time<1ms TTL=128

Ping statistics for 2001:3333:85A3::4:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Figure 104 Ping depuis le client FAI, vers la machine www.orange.com.

Ceci nous permet donc de constater que la résolution de nom est fonctionnelle, depuis le client FAI.

La configuration du fournisseur d'accès à Internet Orange est maintenant en place et fonctionne correctement. L'architecture réseau s'appuie sur un routeur Cisco 4331, des switches Cisco 2960, et un plan d'adressage structuré en IPv4 et IPv6. Les services DNS et Web sont opérationnels, et les tests de connectivité depuis le client FAI montrent que la résolution des noms de domaine se fait sans problème. Cette infrastructure permet à l'entreprise d'accéder aux services d'Orange, tout en maintenant un certain niveau de sécurité grâce aux ACL configurées sur le routeur de l'entreprise.

4.2 Configuration du seconde FAI : SFR

Pour notre deuxième fournisseur d'accès à Internet, nous avons opté pour SFR, un opérateur français majeur dans le secteur des télécommunications, reconnu pour ses services en métropole. Le choix de plusieurs FAI pour notre entreprise vise à assurer une plus grande flexibilité, notamment en cas de panne.

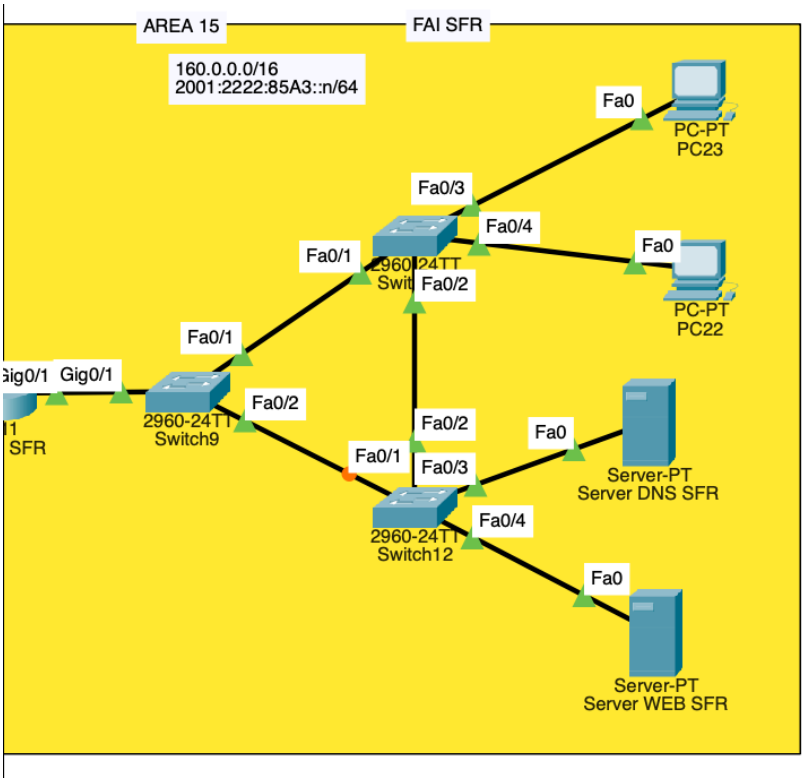


Figure 105 Topologie du FAI SFR, deuxième FAI de l'entreprise.

4.2.1 Choix des équipements pour le FAI SFR

Pour la configuration de notre second fournisseur d'accès à Internet, SFR, nous avons opté pour un routeur Cisco 2911. Celui-ci assure les fonctions essentielles de routage, notamment en IPv4 et IPv6. L'architecture interne du FAI est construite autour d'une topologie en arbre, constituée de plusieurs commutateurs interconnectés pour une meilleure répartition du trafic et une facilité d'évolution. Cette structure permet également une redondance minimale pour éviter tout point de défaillance unique. Sur ce réseau, nous avons intégré deux clients qui simulent des utilisateurs finaux du FAI, ainsi que deux serveurs : un serveur DNS, chargé de la résolution des noms de domaine dans la zone sfr.com, et un serveur Web hébergeant un site.

4.2.2 Plan d'adressage IPv4 et IPv6

Tout d'abord, nous allons nous intéresser à l'IPv4. Pour notre fournisseur d'accès à Internet (Orange), composé de deux serveurs et d'un client, nous allons utiliser un réseau IPv4 public. Nous allons affecter le réseau 160.0.0.0/16.

Ensuite, nous allons affecter le réseau IPv6 suivant : 2001:2222:85A3::/64.

Nous pouvons dresser ci-dessous le plan d'adressage IPv4 et IPv6.

Nom de l'équipement	Adresse IPv4	Adresse IPv6
Routeur Orange – Gig0/0/1	160.0.0.254/16	2001:2222:85A3::1/64
Client FAI n°1	160.0.0.2/16	2001:2222:85A3::2/64
Client FAI n°2	160.0.0.3/16	2001:2222:85A3:32/64
Serveur DNS	160.0.0.53/16	2001:2222:85A3::3/64
Serveur Web	160.0.0.100/16	2001:2222:85A3::4/64

Ainsi, nous pouvons relever les configurations réseaux des différents équipements.

Tout d'abord, voici la configuration sur le routeur SFR :

```
interface GigabitEthernet0/1
 ip address 160.0.0.254 255.255.0.0
 duplex auto
 speed auto
 ipv6 address 2001:2222:85A3::1/64
 ipv6 enable
 ipv6 ospf 1 area 15
```

Figure 106 Configuration de l'interface Gig0/1 du routeur SFR.

Suite à cela, nous pouvons relever la configuration réseau sur un des clients FAI :

```
C:\>ipconfig

FastEthernet0 Connection:(default port)

   Connection-specific DNS Suffix..:
   Link-local IPv6 Address.....: FE80::260:3EFF:FE0A:1017
   IPv6 Address.....: 2001:2222:85A3::3
   IPv4 Address.....: 160.0.0.3
   Subnet Mask.....: 255.255.0.0
   Default Gateway.....: 2001:2222:85A3::1
                         160.0.0.254
```

Figure 107 Configuration réseau du client n°2.

4.2.3 Configuration d'OSPF et OSPFv3, sur le routeur SFR

Suite à la configuration des adresses IP sur nos équipements, nous procéderons à la configuration des protocoles OSPF et OSPFv3. En ce qui concerne OSPF, nous commencerons par configurer le réseau du fournisseur d'accès à Internet. Cela nous permettra d'obtenir :

```
network 160.0.0.0 0.0.255.255 area 15
```

Figure 108 Commande permettant de renseigner un réseau pour le protocole OSPF.

Ainsi, le client SFR peut communiquer avec les différents réseaux IPv4 du Backbone. Nous allons donc faire de même pour OSPFv3, en associant une interface à une aire :

```
interface GigabitEthernet0/1
 ip address 160.0.0.254 255.255.0.0
 duplex auto
 speed auto
 ipv6 address 2001:2222:85A3::1/64
 ipv6 enable
 ipv6 ospf 1 area 15
```

Figure 109 Configuration de l'interface du routeur SFR avec OSPFv3.

Ainsi, le client FAI peut communiquer avec les réseaux IPv4 et IPv6 du Backbone.

4.2.4 Configuration des serveurs DNS et Web

Tout d'abord, nous pouvons relever les différentes configurations des serveurs.

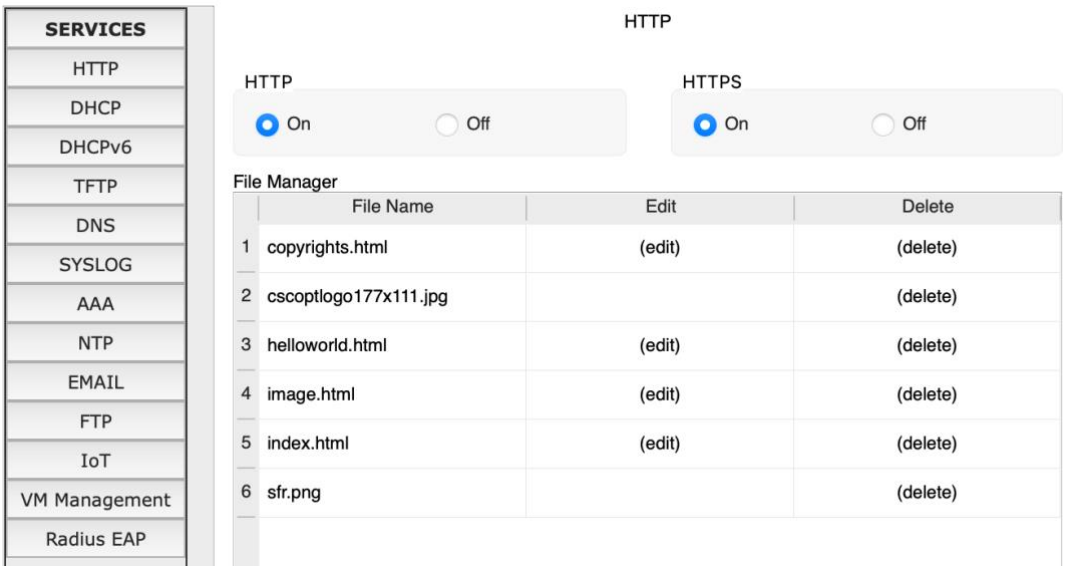


Figure 110 Extrait de la configuration du serveur Web.

Dans ce serveur web, nous avons la page principale (index.html), et un logo présent dans cette page (sfr.png).

No.	Name	Type	Detail
0	com	NS	dns.com
1	dns.com	A Record	170.0.0.53
2	dns.sfr.com	A Record	160.0.0.53
3	sfr.com	SOA	ServerName:dns.sfr.... MailBox :admin@sfr.com Expiry :10 Refresh :10 Retry :10 MinTTL :10
4	sfr.com	NS	dns.sfr.com
5	www.ciscorporation.com	A Record	205.0.113.1
6	www.sfr.com	A Record	160.0.0.100

Figure 111 Enregistrement présent dans le serveur DNS du FAI SFR.

Les enregistrements SOA contiennent les informations principales sur la zone DNS, telles que le nom de domaine, le serveur DNS principal, l'adresse email de l'administrateur et les paramètres. Les enregistrements A et AAAA associent des noms d'hôtes à leurs adresses IPv4 et IPv6, indiquant les adresses IP des serveurs Web, des serveurs DNS ou d'autres machines du domaine. Les enregistrements NS désignent les serveurs faisant autorité pour le domaine, déléguant la gestion DNS à des serveurs spécifiques. L'un de ces enregistrements peut pointer vers un serveur DNS dans le domaine supérieur (.com), permettant une redirection ou une délégation vers le serveur racine. Ces enregistrements permettent la résolution de noms pour le domaine sfr.com.

Comme mentionné précédemment avec le FAI Orange, nous ne pouvons pas tester la résolution de noms depuis le réseau local de l'entreprise, car le serveur DNS racine n'est pas configuré.

Cependant, nous allons tester cette résolution de nom depuis le client SFR, mais aussi Orange.

Tout d'abord, depuis le client SFR :

```
C:\>ping www.sfr.com

Pinging 2001:2222:85A3::5 with 32 bytes of data:

Reply from 2001:2222:85A3::5: bytes=32 time=1ms TTL=128
Reply from 2001:2222:85A3::5: bytes=32 time<1ms TTL=128
Reply from 2001:2222:85A3::5: bytes=32 time<1ms TTL=128
Reply from 2001:2222:85A3::5: bytes=32 time<1ms TTL=128

Ping statistics for 2001:2222:85A3::5:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

Figure 112 Extrait d'une résolution de nom (www.sfr.com), depuis le client SFR.

Ensuite, nous pouvons effectuer la même résolution de nom, mais depuis le client Orange :

```
C:\>ping www.sfr.com

Pinging 2001:2222:85A3::5 with 32 bytes of data:

Reply from 2001:2222:85A3::5: bytes=32 time<1ms TTL=123
Reply from 2001:2222:85A3::5: bytes=32 time<1ms TTL=123
Reply from 2001:2222:85A3::5: bytes=32 time<1ms TTL=123
Reply from 2001:2222:85A3::5: bytes=32 time<1ms TTL=123

Ping statistics for 2001:2222:85A3::5:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Figure 113 Extrait d'une résolution de nom (www.sfr.com), depuis le client Orange.

Ainsi, ces tests confirment la bonne configuration de nos équipements, que ce soit pour l'adressage en IPv4 et IPv6, ou encore pour la configuration de serveurs tels que le serveur Web et le serveur DNS.

La configuration du fournisseur d'accès à Internet SFR est opérationnelle. L'architecture réseau utilise un routeur Cisco 2911, des commutateurs Cisco 2960, et un plan d'adressage IPv4 et IPv6 bien structuré. Les services DNS et Web fonctionnent, et les tests de connectivité depuis les clients FAI confirment la bonne résolution des noms de domaine. Cette infrastructure permet l'accès aux services du FAI tout en assurant la sécurité réseau grâce aux ACL sur le routeur de l'entreprise.

5 Configuration du réseau et test du serveur DNS racine

Suite à la configuration réussie de notre réseau local d'entreprise, du backbone assurant la liaison entre l'entreprise et les fournisseurs d'accès à Internet (FAI) tels qu'Orange et SFR, nous allons désormais concevoir un réseau dédié à l'hébergement du serveur DNS racine de l'entreprise et des FAI. Ce réseau hébergera le serveur DNS .com, responsable de la résolution des noms de domaine.

Ainsi, nous allons d'abord aborder l'aspect matériel de notre réseau. Ensuite, nous procéderons à l'élaboration d'un plan d'adressage en IPv4 et IPv6. Puis, nous configurerons le routage dynamique OSPF et OSPFv3. Enfin, nous procéderons à la configuration de notre serveur DNS .com.

5.1 Conception du réseau

Pour commencer, voici un schéma illustrant notre réseau :

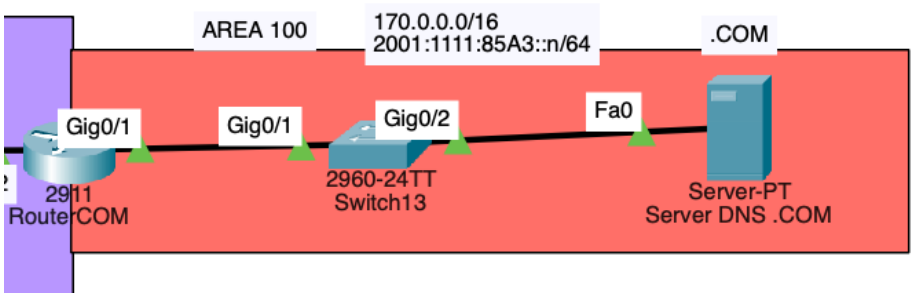


Figure 114 Configuration de notre réseau.

5.1.1 Choix des équipements réseaux

Pour notre petit réseau hébergeant le serveur DNS racine, nous avons opté pour un routeur Cisco 2911, permettant d'effectuer des fonctionnalités de base telles que le routage dynamique. Ce routeur est connecté par un câble droit à l'un des routeurs du Backbone, permettant ainsi de communiquer avec le LAN d'entreprise, mais également avec les FAI. Après notre routeur COM, nous avons un commutateur Cisco 2960, permettant ensuite d'établir le lien avec le serveur DNS .com.

5.1.2 Plan d'adressage IPv4 et IPv6

Suite à la sélection de nos différents équipements, nous allons nous intéresser au plan d'adressage IPv4 et IPv6 de notre réseau. Concernant la partie IPv4, notre réseau sera sur un réseau public, 170.0.0.0/16. Pour la partie IPv6, notre réseau sera : 2001:1111:85A3::/64.

Nous pouvons dresser le tableau de notre configuration ci-dessous.

Nom de l'équipement	Adresse IPv4	Adresse IPv6
Routeur COM – Gig0/1	170.0.0.254/16	2001:1111:85A3::1/64
Serveur DNS .COM	170.0.0.53/16	2001:1111:85A3::2/64

Ensuite, nous avons configuré notre routeur, et plus précisément l'interface Gig0/1 du routeur. Cela nous donne :

```
interface GigabitEthernet0/1
 ip address 170.0.0.254 255.255.0.0
 duplex auto
 speed auto
 ipv6 address 2001:1111:85A3::1/64
 ipv6 enable
 ipv6 ospf 1 area 100
```

Figure 115 Configuration de l'interface Gig0/1 du routeur COM.

Par la suite, nous pouvons relever la configuration réseau du serveur DNS :

```
C:\>ipconfig /all

FastEthernet0 Connection:(default port)

   Connection-specific DNS Suffix..:
   Physical Address.................: 00E0.F780.D2ED
   Link-local IPv6 Address.........: FE80::2E0:F7FF:FE80:D2ED
   IPv6 Address....................: 2001:1111:85A3::2
   IPv4 Address....................: 170.0.0.53
   Subnet Mask.....................: 255.255.0.0
   Default Gateway.................: 2001:1111:85A3::1
                                     170.0.0.254
   DHCP Servers....................: 0.0.0.0
   DHCPv6 IAID.....................:
   DHCPv6 Client DUID..............: 00-01-00-01-1D-03-7A-55-00-E0-F7-80-D2-ED
   DNS Servers.....................: 2001:1111:85A3::2
                                     170.0.0.53
```

Figure 116 Configuration réseau de notre serveur DNS .COM.

Ainsi, le serveur DNS peut communiquer avec sa passerelle par défaut, et par conséquent avec les autres réseaux.

5.1.3 Configuration d'OSPF et OSPFv3 sur le routeur COM

Suite à la configuration des différents équipements de notre réseau, nous procéderons à la configuration du protocole OSPF afin de permettre à notre réseau de communiquer avec d'autres réseaux. Cela sera particulièrement utile pour les futures résolutions de noms.

Dans un premier temps, nous allons configurer le protocole OSPF afin d'établir des routes dynamiques entre les réseaux IPv4. À cet effet, nous allons définir le réseau 170.0.0.0/16, avec une area de 100.

```
network 170.0.0.0 0.0.255.255 area 100
```

Figure 117 Commande permettant de renseigner le réseau 170.0.0.0/16, dans l'area 100.

Après cela, notre serveur DNS peut communiquer avec les réseaux du Backbone, mais aussi avec les différents FAI. Voici un ping initié depuis le serveur DNS COM, en destination du client du FAI Orange :

```
C:\>ping 150.0.0.2

Pinging 150.0.0.2 with 32 bytes of data:

Reply from 150.0.0.2: bytes=32 time<1ms TTL=122
Reply from 150.0.0.2: bytes=32 time<1ms TTL=122
Reply from 150.0.0.2: bytes=32 time<1ms TTL=122
Reply from 150.0.0.2: bytes=32 time<1ms TTL=122

Ping statistics for 150.0.0.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Figure 118 Ping initié par le serveur DNS COM, en destination du client Orange.

Ainsi, nous pouvons en déduire le bon fonctionnement d'OSPF sur le routeur COM.

Suite à la configuration du protocole OSPF pour l'IPv4, nous allons procéder de la même manière pour l'IPv6 avec le protocole OSPFv3. Contrairement à OSPF, il est nécessaire d'associer une interface à une aire pour OSPFv3. Ainsi, pour l'interface Gig0/1 du routeur COM :

```
interface GigabitEthernet0/1
 ip address 170.0.0.254 255.255.0.0
 duplex auto
 speed auto
 ipv6 address 2001:1111:85A3::1/64
 ipv6 enable
 ipv6 ospf 1 area 100
```

Figure 119 Commande permettant d'associer l'interface Gig0/1 à l'aire 100.

Ainsi, l'interface Gig0/1 est associé à l'aire 100. Nous pouvons donc maintenant communiquer avec les différents réseaux IPv6 du Backbone, et des FAI. Voici un test de connexion entre le serveur DNS COM et un client SFR :

```
C:\>ping 2001:2222:85A3::2

Pinging 2001:2222:85A3::2 with 32 bytes of data:

Reply from 2001:2222:85A3::2: bytes=32 time<1ms TTL=124
Reply from 2001:2222:85A3::2: bytes=32 time<1ms TTL=124
Reply from 2001:2222:85A3::2: bytes=32 time=1ms TTL=124
Reply from 2001:2222:85A3::2: bytes=32 time<1ms TTL=124

Ping statistics for 2001:2222:85A3::2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

Figure 120 Ping initié depuis le serveur DNS COM, en direction du client SFR.

En conclusion, nous sommes désormais en mesure d'établir une communication sur les réseaux IPv4 et IPv6, incluant le backbone, les clients des FAI et les entreprises (uniquement si l'entreprise est à l'origine de la connexion).

5.1.4 Configuration du serveur DNS racine

Suite à la configuration d'un adressage clair et d'un protocole de routage tel qu'OSPF et OSPFv3, nous allons maintenant configurer notre serveur DNS COM. Ce serveur constitue un point central pour nos réseaux, car il permet de rediriger les résolutions de noms dans les domaines inférieurs tels que Ciscorporation.com et Orange.com.

Voici la configuration de notre serveur DNS racine, avec les différents enregistrements :

No.	Name	Type	Detail
0	ciscorporation.com	NS	dns.ciscorporation.com
1	com	SOA	ServerName:dns.com MailBox :admin@com.com Expiry :10 Refresh :10 Retry :10 MinTTL :10
2	com	NS	dns.com
3	dns.ciscorporation.com	A Record	205.0.113.1
4	dns.com	A Record	170.0.0.53
5	dns.orange.com	A Record	150.0.0.53
6	dns.sfr.com	A Record	160.0.0.53
7	orange.com	NS	dns.orange.com
8	sfr.com	NS	dns.sfr.com

Figure 121 Configuration du serveur DNS racine, avec les différents enregistrements.

Dans la configuration ci-dessus, nous retrouvons divers enregistrements. Les enregistrements NS présents sur le serveur DNS racine désignent les serveurs faisant autorité pour différents domaines comme ciscorporation.com, orange.com, sfr.com et même le domaine supérieur com. Cela permet au serveur racine de rediriger les requêtes DNS vers les serveurs spécialisés dans chaque domaine. L'enregistrement SOA définit les paramètres principaux de la zone com, incluant le serveur DNS principal (dns.com), l'adresse email de l'administrateur et les durées liées à la mise à jour de la zone. Les enregistrements A et AAAA associent les noms d'hôtes des serveurs DNS à leurs adresses IPv4 et IPv6 respectives. Grâce à cette configuration, le serveur DNS racine peut orienter les requêtes DNS vers les serveurs autoritaires des différents domaines, jouant un rôle central dans la résolution des noms au sein du réseau simulé.

En conclusion, la configuration réussie du serveur DNS racine permet désormais la résolution de noms depuis l'entreprise et les fournisseurs d'accès à Internet. Ce point sera vérifié dans la section suivante.

5.2 Test sur le serveur DNS racine COM

Suite à la configuration réussie du serveur DNS COM, la résolution des noms devient beaucoup plus complexe. Par exemple, un client d'un fournisseur d'accès à Internet peut désormais résoudre un nom de domaine permettant d'accéder au site web de l'entreprise (www.Ciscorporation.com). Nous allons procéder à un test dès maintenant.

5.2.1 Test initié par un équipement du LAN d'entreprise

Tout d'abord, nous allons tester les différentes résolutions possibles depuis le LAN de l'entreprise. Nous allons prendre un PC issue du VLAN 10, et tester toutes les résolutions de nom possible.

Tout d'abord, nous testons avec le serveur web Intranet de l'entreprise.

```
C:\>ping intranet.ciscorporation.com

Pinging 2001:DB8:1:100::4 with 32 bytes of data:

Reply from 2001:DB8:1:100::4: bytes=32 time<1ms TTL=127
Reply from 2001:DB8:1:100::4: bytes=32 time<1ms TTL=127
Reply from 2001:DB8:1:100::4: bytes=32 time<1ms TTL=127
Reply from 2001:DB8:1:100::4: bytes=32 time<1ms TTL=127

Ping statistics for 2001:DB8:1:100::4:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Figure 122 Ping depuis un PC du VLAN 10, en direction de la machine intranet.ciscorporation.com.

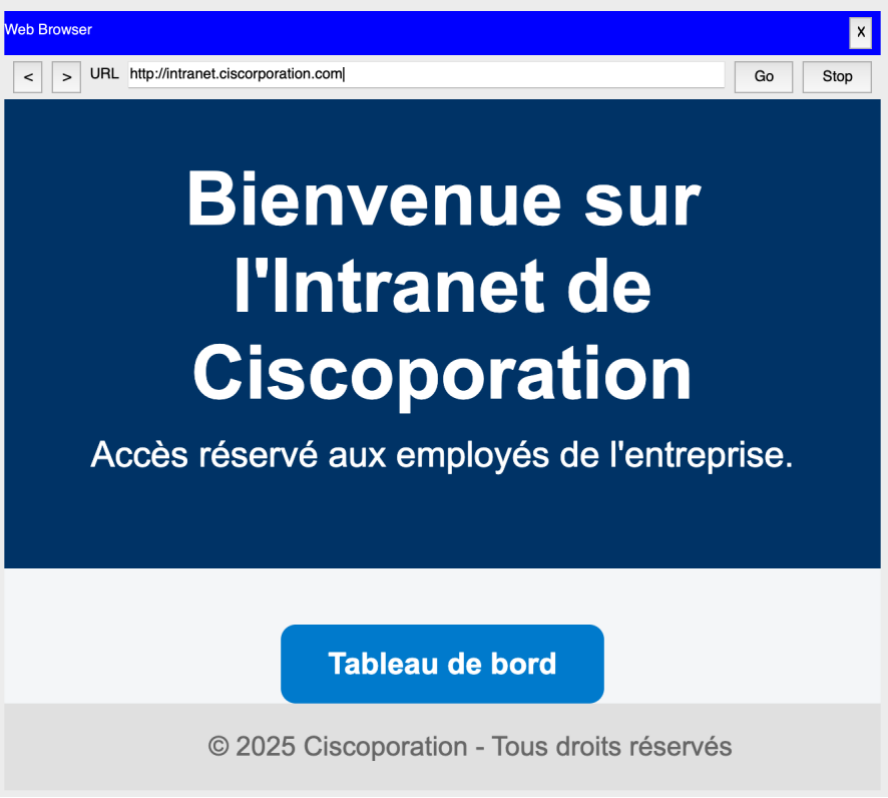


Figure 123 Test permettant d'afficher la page web interne à l'entreprise, en procédant avec une résolution de nom.

Nous pouvons donc voir que la résolution marche depuis le LAN d'entreprise, en direction du serveur Internet (présent dans le VLAN 100).

Nous allons maintenant tester la résolution de nom pour 1 FAI (www.orange.com).

```
C:\>ping www.orange.com

Pinging 2001:3333:85A3::4 with 32 bytes of data:

Reply from 2001:3333:85A3::4: bytes=32 time<1ms TTL=124
Reply from 2001:3333:85A3::4: bytes=32 time<1ms TTL=124
Reply from 2001:3333:85A3::4: bytes=32 time<1ms TTL=124
Reply from 2001:3333:85A3::4: bytes=32 time<1ms TTL=124

Ping statistics for 2001:3333:85A3::4:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Figure 124 Ping initié par le LAN de l'entreprise, en direction de www.orange.com.

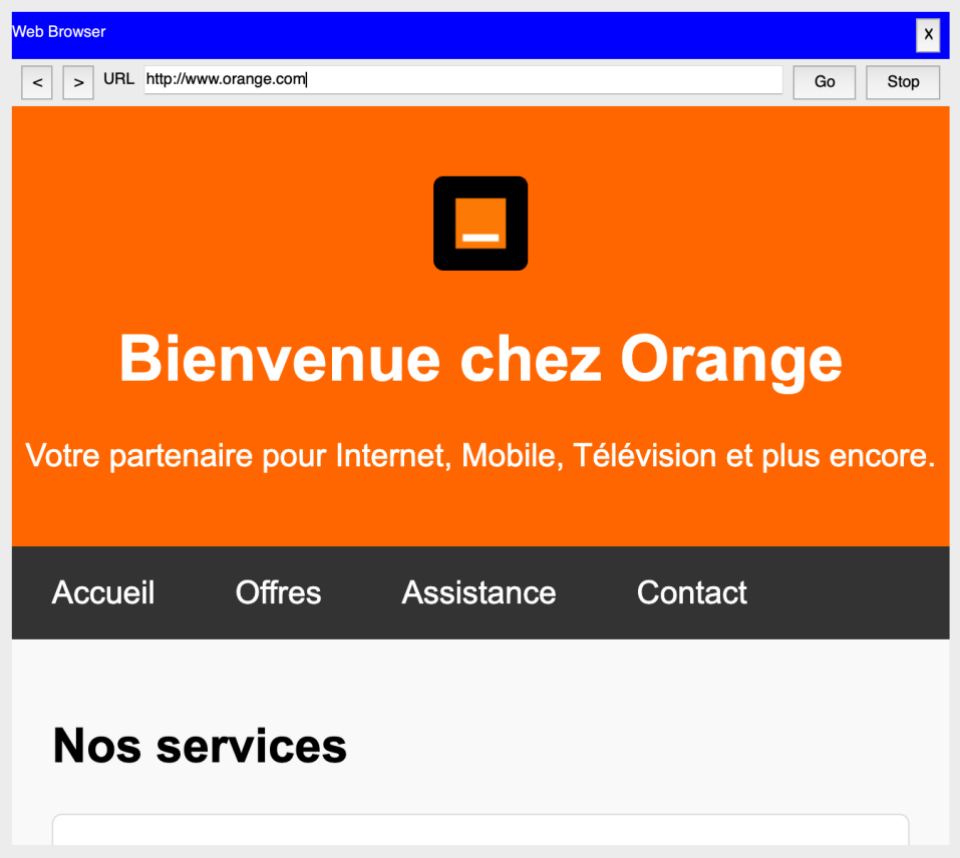


Figure 125 Test permettant d'afficher la page web d'orange, en procédant avec une résolution de nom.

La résolution de nom fonctionne donc correctement pour les FAI. Nous allons maintenant tester cette résolution pour le site Web public de l'entreprise.

```
C:\>ping www.ciscorporation.com

Pinging 2001:1234:ABCD:1::2 with 32 bytes of data:

Reply from 2001:1234:ABCD:1::2: bytes=32 time=1ms TTL=127
Reply from 2001:1234:ABCD:1::2: bytes=32 time<1ms TTL=127
Reply from 2001:1234:ABCD:1::2: bytes=32 time<1ms TTL=127
Reply from 2001:1234:ABCD:1::2: bytes=32 time<1ms TTL=127

Ping statistics for 2001:1234:ABCD:1::2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

Figure 126 Ping effectué depuis le LAN de l'entreprise, en direction du serveur web de l'entreprise (DMZ).

Figure 127 Page web de l'entreprise Ciscorporation.

On peut conclure que la résolution est opérationnelle depuis le réseau local de l'entreprise, et ce, pour le site Web Internet, le site Web public et les sites Web des FAI. Nous allons maintenant procéder de la même manière pour les deux FAI.

5.2.2 Test initié par un client du FAI Orange

Pour commencer, nous allons tester la résolution de nom depuis le client Orange, en direction du serveur web Intranet de l'entreprise.

```
C:\>ping intranet.ciscorporation.com
Ping request could not find host intranet.ciscorporation.com. Please check the name and try again.
```

Figure 128 Résultat du ping en direction du serveur web interne à l'entreprise.

Figure 129 Résultat de la résolution de nom.

On constate que la résolution de nom n'a pas fonctionné dans ce cas, ce qui est normal. En effet, nous avons tenté de communiquer avec le serveur Web interne à l'entreprise, lequel doit être accessible uniquement à partir du réseau local de l'entreprise. De plus, aucun enregistrement A, AAAA ni NS n'a été renseigné dans le serveur DNS racine pour la machine intranet.ciscorporation.com.

Maintenant, nous allons essayer d'aller sur le site web public de l'entreprise.

```
C:\>ping www.ciscorporation.com

Pinging 2001:1234:ABCD:1::2 with 32 bytes of data:

Reply from 2001:1234:ABCD:1::2: bytes=32 time=10ms TTL=124
Reply from 2001:1234:ABCD:1::2: bytes=32 time<1ms TTL=124
Reply from 2001:1234:ABCD:1::2: bytes=32 time<1ms TTL=124
Reply from 2001:1234:ABCD:1::2: bytes=32 time<1ms TTL=124

Ping statistics for 2001:1234:ABCD:1::2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 10ms, Average = 2ms
```

Figure 130 Ping en direction de la machine hébergeant le site web.

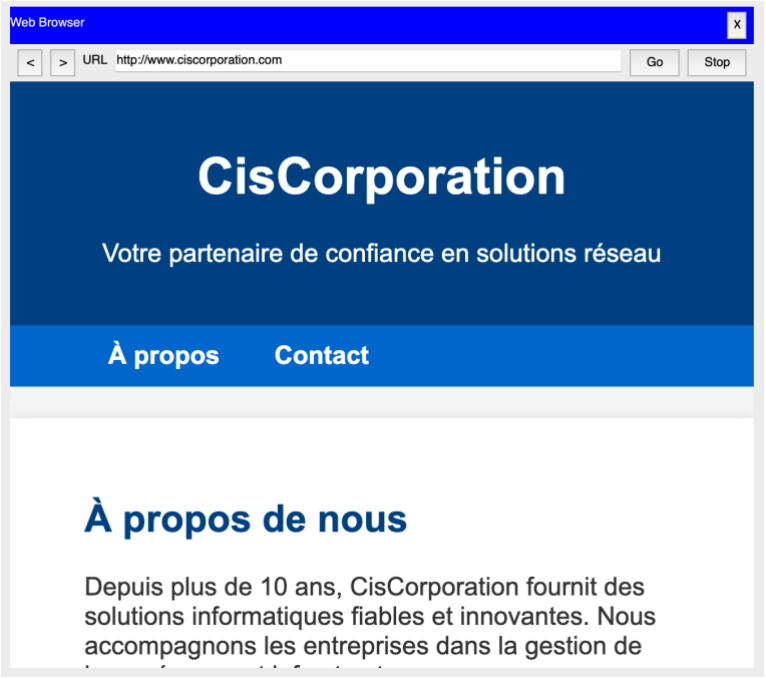


Figure 131 Page web affiché, grâce à une résolution de nom.

```
C:\>ping www.orange.com

Pinging 2001:3333:85A3::4 with 32 bytes of data:

Reply from 2001:3333:85A3::4: bytes=32 time<1ms TTL=128
Reply from 2001:3333:85A3::4: bytes=32 time<1ms TTL=128
Reply from 2001:3333:85A3::4: bytes=32 time<1ms TTL=128
Reply from 2001:3333:85A3::4: bytes=32 time<1ms TTL=128

Ping statistics for 2001:3333:85A3::4:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Figure 132 Ping en direction du serveur web d'Orange.

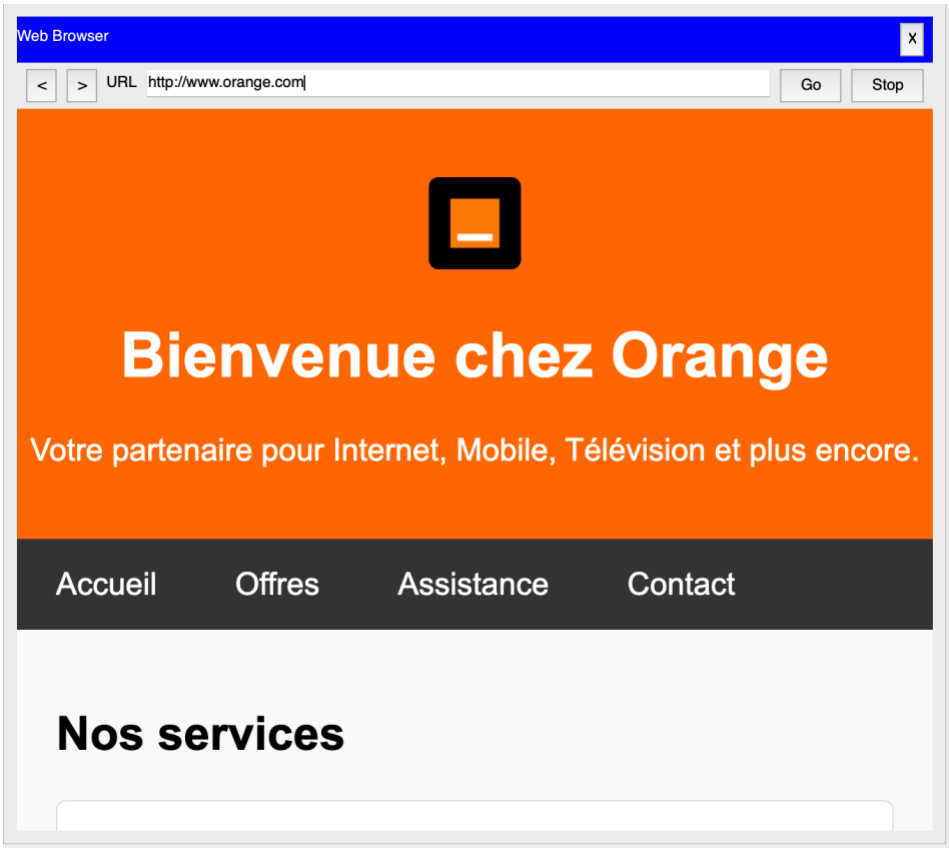


Figure 133 Page web du FAI.

Ainsi, hormis le serveur Web interne à l'entreprise, le client du fournisseur d'accès Internet d'Orange peut communiquer avec tous les serveurs. Après cela, nous allons tester pour l'autre client du FAI SFR.

5.2.3 Test initié par un client du FAI SFR

Pour commencer, nous allons tester la résolution de nom depuis le client SFR, en direction du serveur web Intranet de l'entreprise.

```
C:\>ping intranet.ciscorporation.com
Ping request could not find host intranet.ciscorporation.com. Please check the name and try again.
```

Figure 134 Résultat du ping en direction du serveur web interne à l'entreprise.

Figure 135 Résultat de la résolution de nom.

On constate que la résolution de nom n'a pas fonctionné dans ce cas, ce qui est normal. En effet, nous avons tenté de communiquer avec le serveur Web interne à l'entreprise, lequel doit être accessible uniquement à partir du réseau local de l'entreprise. De plus, aucun enregistrement A, AAAA ni NS n'a été renseigné dans le serveur DNS racine pour la machine intranet.ciscorporation.com.

Maintenant, nous allons essayer d'aller sur le site web public de l'entreprise.

```
C:\>ping www.ciscorporation.com

Pinging 2001:1234:ABCD:1::2 with 32 bytes of data:

Reply from 2001:1234:ABCD:1::2: bytes=32 time=10ms TTL=124
Reply from 2001:1234:ABCD:1::2: bytes=32 time<1ms TTL=124
Reply from 2001:1234:ABCD:1::2: bytes=32 time<1ms TTL=124
Reply from 2001:1234:ABCD:1::2: bytes=32 time<1ms TTL=124

Ping statistics for 2001:1234:ABCD:1::2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 10ms, Average = 2ms
```

Figure 136 Ping en direction de la machine hébergeant le site web.

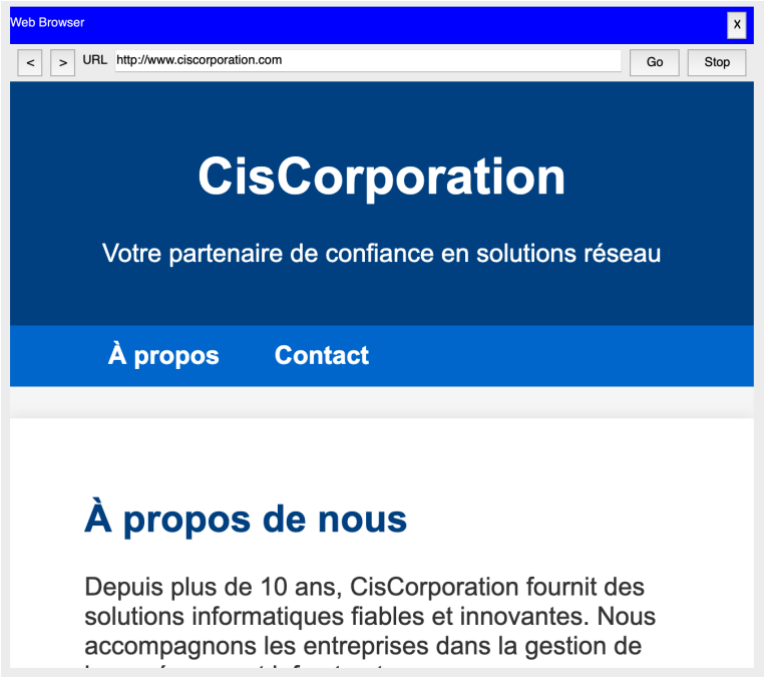


Figure 137 Page web affiché, grâce à une résolution de nom.

Ensuite, nous allons essayer d'accéder au site web du FAI SFR :

```
C:\>ping www.sfr.com

Pinging 2001:2222:85A3::5 with 32 bytes of data:

Reply from 2001:2222:85A3::5: bytes=32 time<1ms TTL=128
Reply from 2001:2222:85A3::5: bytes=32 time<1ms TTL=128
Reply from 2001:2222:85A3::5: bytes=32 time<1ms TTL=128
Reply from 2001:2222:85A3::5: bytes=32 time<1ms TTL=128

Ping statistics for 2001:2222:85A3::5:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Figure 138 Ping en direction du site web du FAI SFR

Figure 139 Site web du FAI SFR.

Ainsi, hormis le serveur Web interne à l'entreprise, le client du fournisseur d'accès Internet d'Orange peut communiquer avec tous les serveurs.

5.2.4 Tableau récapitulatif des tests effectués

Après tous les tests effectués précédemment, nous pouvons dresser le tableau suivant :

	Serveur Intranet entreprise	Serveur Web public entreprise	Serveur web Orange	Serveur Web SFR
LAN entreprise	Oui	Oui	Oui	Oui
Client Orange	Non	Oui	Oui	Oui
Client SFR	Non	Oui	Oui	Oui

6 Conclusion et perspectives

6.1 Résumé du projet

6.1.1 Objectifs du projet

Ce projet vise à mettre en pratique les compétences acquises au cours de l'année et à en développer de nouvelles. Nous avons mis en pratique une grande quantité de connaissances, notamment les différents protocoles du modèle OSI, tels que les protocoles IP, DHCP et DNS. Nous avons également renforcé nos compétences en matière de configuration d'équipements tels que les routeurs, les commutateurs et les différents serveurs (DNS, DHCP). De plus, le projet visait à nous familiariser avec les architectures de réseaux d'entreprise typiques et leurs conceptions.

6.1.2 Solutions mises en œuvre

Pour concevoir notre architecture réseau, nous avons commencé par créer des VLAN et les associer à des sous-réseaux. Ensuite, nous avons configuré le routage OSPF, ce qui nous a permis d'implémenter un protocole de routage dynamique. Enfin, nous avons configuré divers équipements, tels que les routeurs, en utilisant le NAT, la redirection de port et le filtrage simple.

6.1.3 Résultat global

Après avoir effectué toutes les manipulations citées dans le compte rendu, nous avons une configuration opérationnelle permettant de répondre à toutes les problématiques. En effet, notre LAN de l'entreprise arrive à accéder aux différents sites web, notamment le site Intranet, public de l'entreprise, mais aussi ceux des FAI. En revanche, les FAI arrivent à accéder à tous les sites, sauf le site web Intranet. Nous avons aussi configuré les équipements de l'entreprise pour permettre d'y accéder à distance avec SSH. Enfin, nous avons créé des simples règles de filtrage, permettant de créer un minimum de sécurité.