Université Hassan 1er

Faculté des Sciences et Techniques Settat

LICENCE SCIENCES ET TECHNIQUES EN GENIE INFORMATIQUE

Rapport sur le Projet de Conception d'un Centre de Données Sécurisé

Encadré par :

Mme Azroumahli Chaimae

Réalisé par :

MOHAMMED ABIDOU

SOMMAIRE

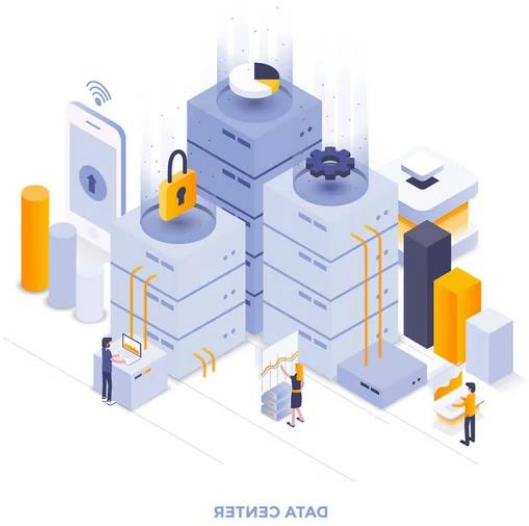
I. Introduction

1. Contexte général du projet

Dans le cadre de l'évolution des infrastructures réseau, ce projet vise à concevoir un centre de données performant et sécurisé pour une entreprise. Le réseau doit répondre aux exigences actuelles en matière de segmentation, de gestion des flux de données et de sécurité.

Pour ce faire, une infrastructure basée sur des VLAN sera mise en place afin d'assurer une séparation logique des différents départements de l'entreprise (**Informatique**, **Administratif**, **Commercial**, **RH, GUESTs**) tout en offrant un accès contrôlé aux **clients externes**. Cette configuration garantit une meilleure gestion des ressources et renforce la sécurité du réseau.

Le centre de données prendra également en charge les besoins suivants :



- **Stockage de Données** : Hébergement sécurisé et accès rapide aux données.
- **Hébergement de Sites et Applications** : Infrastructure pour sites web et services en ligne.
- **Calcul Haute Performance** : Exécution d'applications nécessitant une grande puissance de calcul.
- **Services Cloud** : Ressources informatiques à la demande via des plateformes cloud.
- **Sauvegarde et Récupération** : Protection et récupération des données en cas de panne.
- **Virtualisation** : Optimisation des ressources pour un déploiement flexible des applications.
- **Collaboration** : Outils pour faciliter le travail à distance et la communication en équipe.

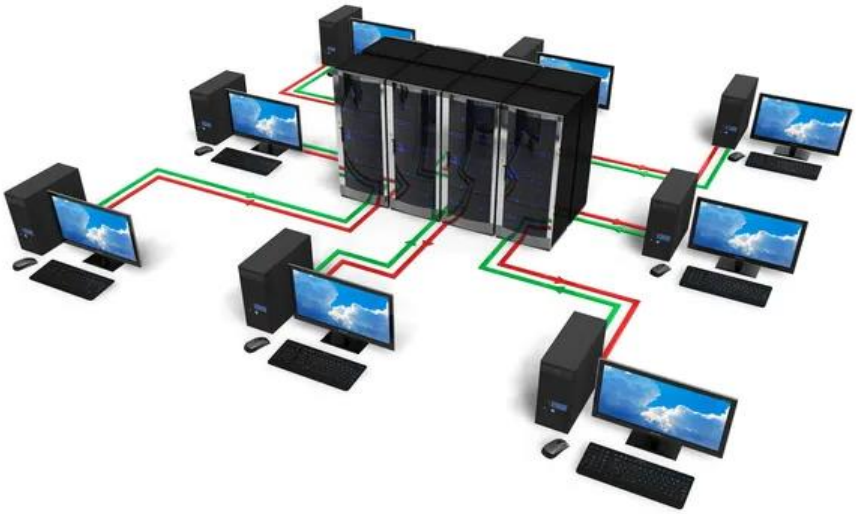
La conception du réseau intégrera les meilleures pratiques en matière de configuration des VLAN, des protocoles de routage et des listes de contrôle d'accès (ACL), pour offrir une solution évolutive, performante et adaptée aux besoins de l'entreprise.

2. Objectifs du projet

Le projet vise à concevoir et mettre en place une infrastructure réseau performante, segmentée et sécurisée pour répondre aux besoins d'une entreprise souhaitant déployer un **centre de données moderne**.

Les objectifs spécifiques sont :

1. **Concevoir une architecture réseau segmentée** :
    - Implémenter des VLANs pour séparer les différents départements (Informatique, Administratif, Commercial, RH, etc.) et les clients externes.
    - Garantir une connectivité efficace tout en assurant une gestion simplifiée du trafic.
2. **Assurer la sécurité et la fiabilité des données** :
    - Protéger l'accès aux ressources critiques via des ACLs et FIRE WALL.
    - Sécuriser les données sensibles hébergées sur les serveurs du centre de données.
3. **Fournir des services adaptés aux besoins de l'entreprise** :
    - Hébergement sécurisé pour le stockage des données et les applications.
    - Sauvegarde et récupération des données en cas de **panne.**
    - Collaboration à distance grâce à des outils modernes.
4. **Optimiser l'utilisation des ressources** :
    - Intégrer des mécanismes de virtualisation pour une gestion flexible des applications.
    - Réduire les coûts d'exploitation en utilisant des technologies avancées et adaptées.
5. **Faciliter l'accès pour les utilisateurs internes et externes** :
    - Mettre en place des protocoles d'accès différenciés pour les clients externes et les différents départements internes.
    - Améliorer l'expérience utilisateur grâce à des connexions rapides et fiables.



II. Analyse des Besoins et Conception de l'Architecture Réseau

1. Identification des utilisateurs et des services

L'entreprise souhaite construire un **centre de données** avec des sous-réseaux segmentés pour différents types de clients et des VLANs pour la sécurité. Voici une répartition des utilisateurs et des services nécessaires :

- **Informatique (IT)** : 15 utilisateurs (administrateurs systèmes, techniciens réseau).
  - **Services nécessaires** : Gestion des serveurs, accès SSH, FTP, monitoring, administration réseau.
  - **Équipements** : Serveurs, switches, équipements de stockage, contrôleurs de domaine.
- **Administratif** : 20 utilisateurs (gestionnaires, comptables).
  - **Services nécessaires** : Accès sécurisé aux bases de données, outils de gestion financière, intranet.
  - **Équipements** : Postes de travail, serveurs de base de données.
- **Marketing** : 10 utilisateurs (analystes, responsables publicitaires).
  - **Services nécessaires** : Accès à Internet, gestion des outils CRM et de stockage collaboratif.
  - **Équipements** : Ordinateurs de bureau, systèmes de gestion de la relation client, serveurs de sauvegarde.
- **Ressources Humaines (RH)** : 8 utilisateurs (gestionnaires RH, assistants).
  - **Services nécessaires** : Accès aux fichiers sensibles (contrats, paies), stockage et gestion de documents internes.
  - **Équipements** : Postes de travail, serveurs sécurisés pour données RH.
- **Clients externes** : 10 000 utilisateurs potentiels (accès limité à des ressources spécifiques comme FTP, stockage partagé).
  - **Services nécessaires** : Accès sécurisé à des ressources partagées via FTP, stockage cloud.
  - **Équipements** : Serveurs FTP, solutions de stockage cloud.

- **Invités** : Nombre variable, connectés via des points d'accès Wi-Fi dédiés.
    - **Services nécessaires** : Accès Internet isolé.
    - **Équipements** : Points d'accès Wi-Fi, routeurs dédiés.

2. Schéma d'architecture réseau

La segmentation du réseau permettra d'isoler les différents types de trafic pour améliorer les performances et la sécurité. Voici une répartition proposée :

- **VLAN 10 : Informatique (IT)** – Gestion des serveurs et de l'infrastructure réseau.
- **VLAN 20 : Administratif** – Accès aux bases de données internes et à des outils de gestion.
- **VLAN 30 : Marketing** – Accès aux services CRM, Internet et stockage collaboratif.
- **VLAN 40 : Ressources Humaines (RH)** – Accès sécurisé aux fichiers sensibles et gestion des documents internes.
- **VLAN 50 : Clients externes** – Connexion sécurisée aux serveurs FTP et stockage partagé.
- **VLAN 60 : Invités** – Accès Wi-Fi isolé avec restrictions de bande passante et de durée d'accès.
- **VLAN 70 : Serveurs de stockage** – Dédicacé aux serveurs de stockage pour une gestion optimisée des ressources de stockage.

La segmentation permet de limiter l'accès aux données sensibles, améliore la gestion du trafic et optimise les performances du réseau.

Topologies du Réseau :

- **Topologie en Étoile** : Idéale pour la gestion des VLANs et la connexion des équipements principaux. Elle associe les départements suivants : Informatique (IT) pour les serveurs et équipements réseau, Administratif pour les postes de travail et serveurs de base de données, Marketing pour les stations de travail et serveurs de sauvegarde, et Ressources Humaines (RH) pour les postes de travail et serveurs sécurisés pour les données RH.
- **Topologie Mallie** : Adaptée à la redondance et à la haute disponibilité des liens entre équipements critiques. Elle est utilisée pour relier les équipements de stockage (Serveurs de stockage) et assurer une connectivité fiable pour les Clients externes, notamment pour les accès FTP et stockage partagé.

Connexions réseau :

- Câble Console pour la configuration initiale.

- Câbles Ethernet (Copper) : Connectent les équipements critiques (serveurs, switches, routeurs).
- Câbles Fibre Optique : Pour des connexions longue distance et à haute bande passante entre switches.

3. Justification des Choix Technologiques :

- **Ethernet :**
  Ethernet est utilisé pour la communication interne rapide entre les équipements, essentiel pour les départements Informatique (IT) (serveurs, stockage), Administratif (bases de données), Marketing (outils collaboratifs) et RH (données sensibles). Les serveurs de stockage sont aussi connectés via Ethernet pour des performances optimales.
- **Wi-Fi :**
  Le Wi-Fi permet l'accès sans fil pour les Invités, avec des VLANs dédiés pour assurer la sécurité. Il offre également de la flexibilité pour les départements Informatique (IT), Administratif, Marketing, et RH.
- **Fibre optique :**
  Utilisée pour connecter les segments du réseau à haute vitesse, la fibre relie les équipements Informatique (IT) (serveurs, stockage) et les Serveurs de stockage pour garantir des transferts rapides et fiables.
- **Firewall :**
  Le pare-feu protège les échanges entre VLANs et sécurise l'accès aux données sensibles, essentiel pour les départements Informatique (IT), Administratif et RH, et les Serveurs de stockage.
- **ACL (Listes de Contrôle d'Accès) :**
  Les ACL contrôlent le trafic entre les VLANs, garantissant que chaque département accède uniquement aux ressources nécessaires. Elles assurent la sécurité pour Informatique (IT), Administratif, Marketing, RH, et les Serveurs de stockage.
- **NAT (Network Address Translation) :**
  Le NAT permet aux hôtes internes d'accéder à Internet tout en masquant les adresses IP internes, utilisé pour tous les départements et serveurs de stockage.
- **Routeur et Commutateurs :**
  Les routeurs assurent la connectivité entre les différents VLANs et l'Internet. Les commutateurs gèrent les connexions internes et les VLANs, permettant une gestion efficace du réseau et la segmentation des différents départements.

III. Plan d'Adressage IP et Segmentation Réseau

1. Création d'un plan d'adressage IP avec CIDR/VLSM

Le réseau utilise la plage d'adresses **192.168.0.0/22**, appartenant à la **classe C** d'adresses IPv4, offrant un total de **1024 adresses IP** (de **192.168.0.0** à **192.168.7.255**). Cette plage est subdivisée en sous-réseaux plus petits en fonction des besoins des différents départements, en utilisant les techniques de **CIDR** et **VLSM** pour optimiser l'utilisation des adresses.

Répartition des sous-réseaux avec CIDR/VLSM :

- **VLAN 10 : Informatique (IT)** : Besoin : **15 adresses IP**

- Le masque **/28** signifie que les 28 premiers bits sont réservés pour le masque de sous-réseau.
    - Masque : **255.255.255.240**.
    - Bits disponibles pour hôtes : 32−28=432 - 28 = 432−28=4.
- Plage d'adresses utilisables :
    - Début : **192.168.0.1**
    - Fin : **192.168.0.14**
    - Diffusion : **192.168.0.15**.

- **VLAN 20 : Administratif** : Besoin : **20 adresses IP**

- Le masque **/27** signifie que les 27 premiers bits sont réservés pour le masque de sous-réseau.
    - Masque : **255.255.255.224**.
    - Bits disponibles pour hôtes : 32−27=532 - 27 = 532−27=5.
- Plage d'adresses utilisables :
    - Début : **192.168.1.1**
    - Fin : **192.168.1.30**
    - Diffusion : **192.168.1.31**.

- **VLAN 30 : Marketing**: Besoin : **10 adresses IP**

1. Le masque **/28** est suffisant, identique au VLAN IT.

2. Nombre total d'adresses IP : 16.
3. Plage d'adresses utilisables :
    - Début : **192.168.2.1**
    - Fin : **192.168.2.14**
    - Diffusion : **192.168.2.15**.

➢ **VLAN 40 : Ressources Humaines (RH)** : Besoin : **8 adresses IP**

- Le masque **/29** signifie que les 29 premiers bits sont réservés pour le masque de sous-réseau.
    - Masque : **255.255.255.248**.
    - Bits disponibles pour hôtes : 32−29=332 - 29 = 332−29=3.
- Plage d'adresses utilisables :
    - Début : **192.168.3.1**
    - Fin : **192.168.3.6**
    - Diffusion : **192.168.3.7**.

➢ **VLAN 50 : Clients externes** : Besoin : **10 000 adresses IP**

- Le masque **/16** permet d'attribuer un grand nombre d'adresses.
    - Masque : **255.255.0.0**.
    - Bits disponibles pour hôtes : 32−16=1632 - 16 = 1632−16=16.
- Plage d'adresses utilisables :
    - Début : **192.168.4.1**
    - Fin : **192.168.255.254**
    - Diffusion : **192.168.255.255**.

➢ **VLAN 60 : Invités (Wi-Fi)** : Besoin : **100 adresses IP**

- Le masque **/25** signifie que les 25 premiers bits sont réservés pour le masque de sous-réseau.
    - Masque : **255.255.255.128**.

- Bits disponibles pour hôtes : 32−25=732 - 25 = 732−25=7.

- Plage d'adresses utilisables :
  - Début : **192.168.5.1**
  - Fin : **192.168.5.126**
  - Diffusion : **192.168.5.127**.

➢ **VLAN 70 : Serveurs de stockage** : Besoin : **10 adresses IP**

- Le masque **/28** est suffisant, identique aux VLAN IT et Marketing.

  Masque : 255.255.255.240

- Plage d'adresses utilisables :
  - Début : **192.168.6.1**
  - Fin : **192.168.6.14**
  - Diffusion : **192.168.6.15**.

Résumé du Plan d'Adressage IP et de la Segmentation Réseau

VLAN	Département	Utilisateurs + Équipements	Plage d'Adresses	Masque Sous-Réseau	Diffusion	Nombre d'IP
VLAN 10	Informatique (IT)	15	192.168.0.0/28	255.255.255.240	192.168.0.15	16
VLAN 20	Administratif	20	192.168.1.0/27	255.255.255.224	192.168.1.30	32
VLAN 30	Marketing	10	192.168.2.0/28	255.255.255.240	192.168.2.14	16
VLAN 40	RH	8	192.168.3.0/29	255.255.255.248	192.168.3.6	8
VLAN 50	Clients externes	10000	192.168.4.0/16	255.255.0.0	192.168.255.255	65534
VLAN 60	Invités	100	192.168.5.0/25	255.255.255.128	192.168.5.127	128
VLAN 70	Serveurs de stockage	10	192.168.6.0/28	255.255.255.240	192.168.6.15	16

2.Justification des Sous-Réseaux Attribués à Chaque Département

- **VLAN 10 : Informatique (IT)**
  Le sous-réseau **192.168.1.0/28** est attribué au département Informatique, qui nécessite peu d'hôtes (environ 15). Ce sous-réseau permet de gérer les équipements réseau essentiels et d'assurer une gestion sécurisée des serveurs et des outils de monitoring.
- **VLAN 20 : Administratif**
  Le sous-réseau **192.168.2.0/27** est attribué au département Administratif, avec un besoin de 20 adresses IP pour les postes de travail et les serveurs de bases de données. Ce sous-réseau permet de sécuriser l'accès aux informations financières et autres données sensibles.
- **VLAN 30 : Marketing**
  Le sous-réseau **192.168.3.0/28** est attribué au département Marketing. Avec un nombre d'hôtes plus réduit, ce sous-réseau assure une bonne performance pour l'accès aux outils de collaboration tout en isolant le trafic marketing des autres départements.
- **VLAN 40 : Ressources Humaines (RH)**
  Le sous-réseau **192.168.4.0/29** est attribué au département RH, où seuls 8 hôtes sont nécessaires pour accéder aux documents et informations sensibles. Cette taille de sous-réseau permet d'assurer la sécurité des données et de contrôler l'accès aux fichiers internes.
- **VLAN 50 : Clients externes**
  Le sous-réseau **192.168.5.0/20** est attribué aux Clients externes. Ce VLAN nécessite un nombre élevé d'adresses IP (jusqu'à 10 000 et plus), permettant une extension future en fonction de l'évolution du réseau. Cette taille de sous-réseau garantit également une isolation complète du trafic externe des systèmes internes.
- **VLAN 60 : Invités (Wi-Fi)**
  Le sous-réseau **192.168.6.0/25** est utilisé pour les invités. Ce sous-réseau permet de gérer un nombre limité d'utilisateurs tout en leur fournissant un accès sécurisé à Internet, en maintenant l'isolement par rapport aux autres départements internes.
- **VLAN 70 : Serveurs de stockage**
  Le sous-réseau **192.168.7.0/28** est dédié aux serveurs de stockage. Il permet une gestion optimisée des ressources de stockage et des sauvegardes, tout en garantissant des performances élevées pour l'accès aux données critiques.

IV. Configuration des Équipements Réseau

1.Configuration des routeurs et protocoles de routage

a. Description de la Configuration

- Configuration des sous-interfaces pour chaque VLAN avec la méthode **dot1Q**.
- Mise en place du DHCP pour chaque VLAN sur le routeur principal.
- Protocole de routage pour la connectivité inter-sous-réseaux.

b. Commandes Utilisées

```
Router> enable

Router# configure terminal

Router(config)# interface GigabitEthernet0/0.10

Router(config-if)# encapsulation dot1Q 10

Router(config-if)# ip address 192.168.0.1 255.255.255.240

Router(config-if)# no shutdown
```

c. Captures d'Écran

```
Router>enable
Router#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#interface gig0/0.10
Router(config-subif)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0.10, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0.10, changed state to up

Router(config-subif)#encapsulation dot1Q 10
Router(config-subif)#ip address 192.168.0.1 255.255.255.224
% 192.168.0.0 overlaps with GigabitEthernet0/0
Router(config-subif)#exit
Router(config)#int gig0/0.20
Router(config-subif)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0.20, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0.20, changed state to up

Router(config-subif)#encapsulation dot1Q 20
Router(config-subif)#ip address 192.168.1.1 255.255.255.224
Router(config-subif)#exit
Router(config)#int gig0/0.30
Router(config-subif)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0.30, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0.30, changed state to up

Router(config-subif)#encapsulation dot1Q 30
Router(config-subif)#ip address 192.168.2.1 255.255.255.248
Router(config-subif)#exit
Router(config)#int gig0/0.40
Router(config-subif)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0.40, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0.40, changed state to up

Router(config-subif)#encapsulation dot1Q 40
Router(config-subif)#ip address 192.168.3.1 255.255.255.248
Router(config-subif)#exit
```

d. Extrait de la Validation :

Commandes utilisées

```
Router# show ip interface brief
```

```
Router#show ip interface brief
Interface              IP-Address      OK? Method Status                Protoc
GigabitEthernet0/0     192.168.0.1     YES manual up                    up
GigabitEthernet0/0.10  unassigned      YES unset  up                    up
GigabitEthernet0/0.20  192.168.1.1     YES manual up                    up
GigabitEthernet0/0.30  192.168.2.1     YES manual up                    up
GigabitEthernet0/0.40  192.168.3.1     YES manual up                    up
GigabitEthernet0/0.60  192.168.5.1     YES manual up                    up
GigabitEthernet0/0.70  192.168.6.1     YES manual up                    up
GigabitEthernet0/1     unassigned      YES unset  administratively down down
Serial0/0/0            unassigned      YES unset  down                  down
Serial0/0/1            unassigned      YES unset  administratively down down
Vlan1                  unassigned      YES unset  administratively down down
```

1. Configuration des VLANs sur les commutateurs

a. Description de la Configuration

Création des VLANs et attribution des ports correspondants en mode access ou trunk.
Exemple :

- VLAN 10 : Informatique sur le port fa0/2.
- VLAN 20 : Administratif sur le port fa0/3

b. Commandes Utilisées

```
Switch> enable Switch# configure terminal
Switch(config)# vlan 10

Switch(config-vlan)# name Informatique

Switch(config)# interface fa0/2

Switch(config-if)# switchport mode access

Switch(config-if)# switchport access vlan 10
Switch(config-if)# no shutdown
```

c. Captures d'Écran

```
Switch>enable
Switch#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#vlan 10
Switch(config-vlan)#name IT
Switch(config-vlan)#exit
Switch(config)#vlan 20
Switch(config-vlan)#name Administratif
Switch(config-vlan)#exit
Switch(config)#vlan 30
Switch(config-vlan)#name Marketing
Switch(config-vlan)#exit
Switch(config)#vlan 40
Switch(config-vlan)#name RH
Switch(config-vlan)#exit
Switch(config)#vlan 60
Switch(config-vlan)#name Invites
Switch(config-vlan)#exit
Switch(config)#vlan 7
Switch(config-vlan)#exit
Switch(config)#vlan 70
Switch(config-vlan)#name Serveurstockage
Switch(config-vlan)#exit
```

pour chaque VLAN

```
Switch#
Switch#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#inter fa0/1
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 10
Switch(config-if)#exit
```

d. Extrait de la Validation :

Commandes utilisées

```
Switch# show vlan brief
```

```
Switch>enable
Switch#show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    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, Fa0/24, Gig0/1, Gig0/2
7    VLAN0007                         active
10   IT                               active
20   Administratif                    active    Fa0/2
30   Marketing                        active    Fa0/3
40   RH                               active    Fa0/4
60   Invites                          active    Fa0/5
70   Serveurstockage                  active    Fa0/6
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
```

V. Implémentation et Configuration des Services Réseau

1. Mise en place d'un serveur DHCP pour l'attribution des adresses IP

a. Description de la Configuration

- Le routeur principal agit comme un serveur DHCP pour attribuer des adresses IP dynamiques à chaque VLAN.
- Chaque VLAN dispose d'un pool DHCP configuré avec une plage d'adresses spécifique, un masque, une passerelle par défaut et une adresse DNS.

b. Commandes Utilisées

```
Router> enable
Router# configure terminal
Router(config)#VLAN 10
Router(config)# ip dhcp pool VLAN10
Router(dhcp-config)# network 192.168.0.0 255.255.255.240
Router(dhcp-config)# default-router 192.168.0.1
Router(dhcp-config)# dns-server 8.8.8.8
```

c. Captures d'Écran

```
Router>enable
Router#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#ip dhcp excluded-address 192.168.0.1 192.168.0.2
Router(config)#ip dhcp pool VLAN10
Router(dhcp-config)#network 192.168.0.0 255.255.255.240
Router(dhcp-config)#default-router 192.168.0.1
Router(dhcp-config)#exit
Router(config)#ip dhcp excluded-address 192.168.1.1 192.168.1.2
Router(config)#ip dhcp pool VLAN20
Router(dhcp-config)#network 192.168.1.0 255.255.255.224
Router(dhcp-config)#default-router 192.168.1.1
Router(dhcp-config)#dns-server 8.8.8.8
Router(dhcp-config)#exit
Router(config)#ip dhcp excluded-address 192.168.2.1 192.168.2.2
Router(config)#ip dhcp pool VLAN30
Router(dhcp-config)#network 192.168.2.0 255.255.255.240
Router(dhcp-config)#default-router 192.168.2.1
Router(dhcp-config)#dns-server 8.8.8.8
Router(dhcp-config)#exit
Router(config)#ip dhcp excluded-address 192.168.3.1 192.168.3.2
Router(config)#ip dhcp pool VLAN40
Router(dhcp-config)#network 192.168.3.0 255.255.255.248
Router(dhcp-config)#default-router 192.168.3.1
Router(dhcp-config)#dns-server 8.8.8.8
Router(dhcp-config)#exit
Router(config)#ip dhcp excluded-address 192.168.5.1 192.168.5.2
Router(config)#ip dhcp pool VLAN60
Router(dhcp-config)#network 192.168.5.0 255.255.255.128
Router(dhcp-config)#default-router 192.168.5.1
Router(dhcp-config)#dns-server 8.8.8.8
Router(dhcp-config)#exit
Router(config)#ip dhcp excluded-address 192.168.6.1 192.168.6.2
Router(config)#ip dhcp pool VLAN70
Router(dhcp-config)#network 192.168.6.0 255.255.255.240
Router(dhcp-config)#default-router 192.168.6.1
Router(dhcp-config)#dns-server 8.8.8.8
Router(dhcp-config)#exit
```

d. Extrait de la Validation :

Commandes utilisées :

```
Router# show ip dhcp pool

Router# show ip dhcp binding
```

```
Router>enable
Router#show ip dhcp pool

Pool VLAN10 :
 Utilization mark (high/low)    : 100 / 0
 Subnet size (first/next)       : 0 / 0
 Total addresses                : 14
 Leased addresses               : 0
 Excluded addresses             : 6
 Pending event                  : none

 1 subnet is currently in the pool
 Current index        IP address range                    Leased/Excluded/Total
 192.168.0.1          192.168.0.1      - 192.168.0.14      0    / 6     / 14

Pool VLAN20 :
 Utilization mark (high/low)    : 100 / 0
 Subnet size (first/next)       : 0 / 0
 Total addresses                : 30
 Leased addresses               : 0
 Excluded addresses             : 6
 Pending event                  : none

 1 subnet is currently in the pool
 Current index        IP address range                    Leased/Excluded/Total
 192.168.1.1          192.168.1.1      - 192.168.1.30      0    / 6     / 30

Pool VLAN30 :
 Utilization mark (high/low)    : 100 / 0
 Subnet size (first/next)       : 0 / 0
 Total addresses                : 14
 Leased addresses               : 0
 Excluded addresses             : 6
 Pending event                  : none

 1 subnet is currently in the pool
 Current index        IP address range                    Leased/Excluded/Total
 192.168.2.1          192.168.2.1      - 192.168.2.14      0    / 6     / 14
```

2.Configuration du NAT pour l'accès Internet

a. Description de la Configuration

Configurer les interfaces réseau : Le Routeur Principal (R1) a deux interfaces :

- Interface LAN (serial 0/0/0) avec adresse IP 10.10.0.1/24.
- Interface WAN (serial 0/0/1) avec adresse IP 172.16.0.1/30.

b. Commandes Utilisées

```
RouterPrincipal# configure terminal RouterPrincipal(config)# interface serial 0/0/0
RouterPrincipal(config-if)# ip address 10.0.0.1 255.255.255.0
RouterPrincipal(config-if)# ip nat inside

RouterPrincipal(config-if)# no shutdown RouterPrincipal(config-if)# exit
RouterPrincipal(config)# interface serial 0/0/1 RouterPrincipal(config-if)# ip address
172.16.0.1 255.255.255.252 RouterPrincipal(config-if)# ip nat outside

RouterPrincipal(config-if)# no shutdown

RouterPrincipal(config-if)# exit
```

c. Captures d'Écran

```
Router>enable
Router#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#interface serial 0/0/0
Router(config-if)#ip address 10.10.0.1 255.255.255.0
Router(config-if)#no shutdown
Router(config-if)#ip nat inside
Router(config-if)#exit
Router(config)#interface serial 0/0/1
Router(config-if)#ip address 172.16.0.1 255.255.255.252
Router(config-if)#ip nat outside
Router(config-if)#no shutdown
```

d. Extrait de la Validation :

Commandes utilisées :

```
RouterPrincipal# show ip nat translations
```

VI. Conclusion et Perspectives

1. Synthèse des réalisations techniques

Dans le cadre de ce projet, nous avons réalisé plusieurs étapes techniques essentielles pour garantir la connectivité et le bon fonctionnement d'un réseau d'entreprise comportant plusieurs VLANs et une connexion Internet sécurisée via NAT. Voici un aperçu des principales réalisations :

- **Configuration des VLANs :** Nous avons créé et configuré plusieurs VLANs pour segmenter le réseau en différentes zones fonctionnelles, y compris des VLANs pour l'Informatique, l'Administratif, le Marketing, les Ressources Humaines, les Invités et les Clients Externes. Chaque VLAN a été associé à un sous-réseau spécifique, avec une répartition adéquate des adresses IP grâce au mécanisme CIDR/VLSM.
- **Mise en place du routage entre les VLANs :** Nous avons configuré des interfaces de routage sur le routeur principal et mis en œuvre un protocole de routage dynamique (RIP/OSPF) pour assurer la communication entre les sous-réseaux, permettant ainsi une interaction fluide entre les différentes zones du réseau.
- **Configuration du DHCP :** Un serveur DHCP a été mis en place pour chaque VLAN afin d'attribuer dynamiquement les adresses IP aux périphériques clients, facilitant ainsi la gestion des adresses IP au sein de chaque sous-réseau.
- **Configuration de la traduction d'adresses réseau (NAT) :** Pour permettre aux périphériques internes d'accéder à Internet, une configuration de NAT a été établie sur le routeur principal. Cela permet de masquer les adresses privées internes en utilisant une adresse publique lors des communications avec l'extérieur.
- **Test de la connectivité :** Nous avons réalisé plusieurs tests pour valider la connectivité entre les sous-réseaux. Tous les tests ont confirmé que les configurations étaient opérationnelles et que la communication entre les VLANs ainsi qu'avec Internet était réussie.

2. Suggestions pour des améliorations et extensions futures

Bien que le réseau fonctionne correctement dans son état actuel, plusieurs améliorations et extensions pourraient être envisagées pour répondre à des besoins futurs et renforcer la performance ainsi que la sécurité du réseau :

- **Amélioration de la sécurité du réseau :**

- **Filtrage des adresses IP et des ports via ACLs :**
  Il serait judicieux de mettre en place des listes de contrôle d'accès (ACL) supplémentaires pour limiter l'accès aux VLANs sensibles (comme ceux des serveurs ou des invités) en fonction des besoins spécifiques.

- **Sécurisation des connexions distantes :**
  L'adoption de VPN ou de technologies similaires pourrait renforcer la sécurité des accès des utilisateurs distants aux ressources internes de l'entreprise.

➢ Optimisation du routage :

- **Mise en place de routage redondant :**
  Pour assurer une haute disponibilité, un routage redondant utilisant des protocoles tels que HSRP, VRRP ou GLBP pourrait être déployé sur les routeurs principaux et les commutateurs.
- **Mise à jour du protocole de routage :**
  L'implémentation d'OSPF ou EIGRP pourrait être envisagée pour remplacer RIP et offrir une gestion plus efficace du routage dynamique dans des réseaux de plus grande envergure.

➢ Extension de l'infrastructure de réseau :

- **Ajout de nouveaux VLANs :**
  À mesure que l'entreprise se développe, il serait pertinent de créer de nouveaux VLANs pour de nouveaux départements ou pour des zones spécialisées comme les serveurs de stockage, la sécurité, etc.
- **Mise en place d'un réseau sans fil (Wi-Fi) :**
  Un réseau sans fil sécurisé pourrait être instauré pour les employés et les invités, en intégrant des contrôles d'accès stricts pour les VLANs Wi-Fi.

➢ Surveillance et gestion du réseau :

- **Implémentation d'un système de surveillance réseau :**
  Des outils tels que SNMP, NetFlow, ou des systèmes de gestion centralisés comme Cisco Prime Infrastructure pourraient être déployés pour surveiller la performance et la santé du réseau en temps réel.