



Rapport Projet d'Intergration

Déploiement d'une infrastructure réseau multiservice pour TechSolutions SARL

Submitted by :

Yassmin Selmi
Ines Mzoughi
Yassine Fray
Maha fares
Farah cherif
Aziz labidi

Academic Year : 2025-2026

Table des matières

Table des figures	2
Liste des tableaux	3
Introduction générale	4
1 Cadre général et conception du projet	5
1.1 Contexte général du projet	5
1.2 Problématique	6
1.3 Objectifs du projet	6
1.4 Présentation générale de la solution proposée	6
1.5 Conception du projet	7
1.5.1 Conception de l'architecture réseau	7
1.5.2 Outils et environnement de travail	9
2 Réalisation	12
2.1 Mise en place de l'infrastructure réseau	12
2.1.1 Configuration des routeurs du backbone	12
2.1.2 Configuration des routeurs des départements	15
2.1.3 Implémentation des services	16
2.2 Sécurité	20
2.3 Tests et résultats	22
2.3.1 Tests de connectivité réseau	22
2.3.2 Tests du routage dynamique OSPF	22
2.3.3 Tests d'accès aux services réseau	23
2.3.4 Tests d'accès à Internet (NAT)	24
2.3.5 Résultats et validation globale	25

Table des figures

1.1	Architecture du backbone en topologie maillée	7
1.2	Interface GNS3	10
1.3	Interface Ubuntu 22.04	10
1.4	Communication entre GNS3 et Ubuntu 22.04	11
2.1	Architecture du backbone en topologie maillée	13
2.2	Captures du fonctionnement du routage dynamique OSPF . .	14
2.3	Étapes de configuration des routeurs des départements	15
2.4	Mise en place du service Supervision / IT	16
2.5	Supervision des équipements via Prometheus et Grafana . .	17
2.6	Mise en œuvre du service Web – Département Web / Marketing	17
2.7	Mise en œuvre du service Base de données – Département Gestion	19
2.8	Mise en œuvre du service de partage NFS – Département Partage / Collaboration	20
2.9	ACL	21
2.10	Tests de connectivité réseau	22
2.11	Tests du routage dynamique OSPF	23
2.12	Tests d'accès aux services réseau	24
2.13	Tests d'accès à Internet (NAT)	24

Liste des tableaux

1.1	Plan d'adressage VLSM par département	9
-----	---	---

Introduction générale

Dans le cadre de la formation d'ingénieur en informatique à ESPRIT, le Projet Intégré (PI) de troisième année permet aux étudiants de mettre en pratique leurs connaissances théoriques à travers un travail de groupe simulant un contexte professionnel réel. Il vise à développer à la fois des compétences techniques, organisationnelles et collaboratives.

Le projet porte sur la conception et le déploiement d'une infrastructure réseau d'entreprise multiservice pour une société fictive, TechSolutions SARL, organisée en plusieurs départements aux besoins réseau spécifiques. L'objectif est de proposer une architecture fiable, sécurisée et évolutive, garantissant une communication efficace et un accès maîtrisé aux ressources internes et externes.

L'infrastructure repose sur un backbone utilisant le protocole OSPF, assurant un routage dynamique et une bonne tolérance aux pannes. Une segmentation du réseau via le VLSM est mise en œuvre pour optimiser l'adressage IP, tandis que l'accès Internet est assuré par un routeur central configuré en NAT. Le projet intègre également plusieurs services réseau essentiels (Web, base de données, partage de fichiers, supervision) ainsi que des mécanismes de sécurité, notamment des tunnels VPN.

Ce projet a permis aux membres de l'équipe d'appliquer concrètement les notions de routage, d'adressage IP, de services réseau et de sécurité, tout en renforçant le travail d'équipe et la préparation aux exigences du milieu professionnel.

Chapitre 1

Cadre général et conception du projet

Introduction

Ce chapitre présente le cadre général du projet ainsi que les choix de conception de l'infrastructure réseau de TechSolutions SARL. Il décrit le contexte, la problématique et les objectifs du projet, avant de détailler la solution proposée et l'architecture réseau retenue. Ce chapitre constitue la base conceptuelle nécessaire à la phase de réalisation.

1.1 Contexte général du projet

TechSolutions SARL est une entreprise spécialisée dans le développement de solutions numériques. Elle est organisée en plusieurs départements fonctionnels qui collaborent afin d'assurer le bon déroulement des activités et la fourniture de services efficaces aux clients.

Le département **Web / Marketing** est responsable de la gestion du site Internet de l'entreprise ainsi que des interactions avec les clients externes. Le département **Supervision / IT** assure la surveillance des serveurs et des équipements réseau. Le département **Base de données / Gestion** est chargé de la centralisation et de la sécurisation des données. Enfin, le département **Partage / Collaboration** permet le partage interne des fichiers et documents.

Avec l'augmentation du nombre d'utilisateurs et de services, l'infrastructure réseau actuelle devient insuffisante, ce qui nécessite sa modernisation.

1.2 Problématique

L'infrastructure réseau actuelle de TechSolutions SARL n'est plus adaptée aux besoins actuels de l'entreprise. L'augmentation du nombre d'utilisateurs, de services et de données a mis en évidence plusieurs limites au niveau des performances et de la disponibilité des services critiques.

De plus, le réseau présente un manque de sécurité et ne permet pas une supervision efficace des équipements et des services. L'absence d'une architecture bien structurée rend également difficile l'évolution du réseau pour intégrer de nouveaux services ou départements.

1.3 Objectifs du projet

L'objectif principal de ce projet est de concevoir et de déployer une infrastructure réseau moderne et professionnelle pour TechSolutions SARL. Cette infrastructure vise à garantir la disponibilité des services critiques, à assurer la sécurité du réseau et une bonne hiérarchisation des flux, ainsi qu'à mettre en place une supervision proactive permettant de détecter et de corriger rapidement les problèmes.

1.4 Présentation générale de la solution proposée

La solution proposée dans ce projet consiste à concevoir et à simuler une infrastructure réseau représentant un environnement d'entreprise réel. Cette infrastructure est basée sur une architecture structurée permettant une communication efficace entre les différents départements de l'entreprise.

Le réseau repose sur un **backbone** organisé selon une **topologie maillée**, assurant une interconnexion directe entre les routeurs des départements et une meilleure disponibilité des services. Chaque département est connecté au backbone à travers un routeur local, ce qui permet une gestion claire et hiérarchisée du trafic réseau.

L'accès à Internet est assuré par un **routeur principal configuré en NAT**, permettant aux utilisateurs internes d'accéder aux ressources externes de manière sécurisée. La **sécurisation du réseau est assurée par un firewall**, chargé de filtrer le trafic entrant et sortant selon des règles de sécurité définies, afin de protéger l'infrastructure contre les accès non autorisés.

La segmentation du réseau est réalisée à l'aide de la technique **VLSM**, permettant une allocation optimale des adresses IP en fonction des besoins de chaque département. Cette approche facilite la gestion du réseau et garantit une architecture évolutive et adaptée aux exigences de l'entreprise.

1.5 Conception du projet

1.5.1 Conception de l'architecture réseau

Backbone OSPF et choix de la topologie maillée

L'architecture réseau proposée repose sur un backbone utilisant le protocole de routage dynamique OSPF. Ce backbone est composé de **N + 1 routeurs**, où N représente le nombre de départements de l'entreprise. Chaque routeur du backbone est interconnecté avec les autres afin d'assurer une communication fiable entre tous les départements.

Le choix d'une **topologie maillée** pour le backbone est justifié par le besoin de haute disponibilité. Cette topologie permet de disposer de plusieurs chemins pour l'acheminement du trafic réseau. Ainsi, en cas de panne d'un lien ou d'un routeur, le trafic peut être redirigé automatiquement vers un autre chemin, ce qui garantit la continuité des services et améliore la fiabilité globale du réseau.

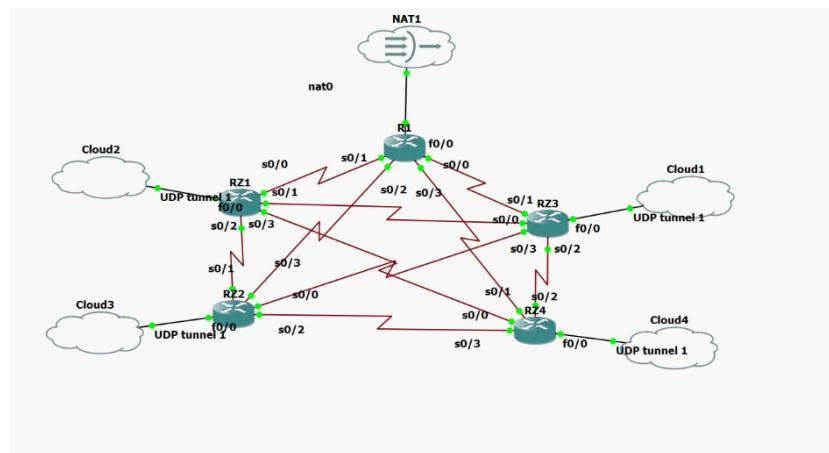


FIGURE 1.1 – Architecture du backbone en topologie maillée

Adressage IP public du backbone

Le backbone du réseau utilise un plan d'adressage IP public pour les liaisons entre les routeurs. Dans ce projet, le réseau **55.0.0.0/30** est utilisé pour les connexions du backbone.

Le choix du masque **/30** est justifié par le fait que les liaisons du backbone sont des liaisons **point à point** entre routeurs. Ce type de liaison ne nécessite que deux adresses IP utilisables, une pour chaque extrémité du lien. Le masque /30 permet de fournir exactement deux adresses utilisables, tout en minimisant le gaspillage d'adresses IP.

L'utilisation d'un adressage public au niveau du backbone permet de simuler un environnement réel d'entreprise connecté à un fournisseur d'accès Internet. Cette approche facilite la gestion du routage, améliore la lisibilité de l'architecture réseau et respecte les bonnes pratiques de conception des réseaux professionnels.

Description logique des départements

L'architecture réseau de TechSolutions SARL est organisée de manière logique en plusieurs départements, chacun représentant une zone fonctionnelle distincte du réseau. Cette séparation permet une meilleure organisation, une gestion plus efficace du trafic et un renforcement de la sécurité.

- **Web / Marketing** : dédié à la gestion du site Internet et des services accessibles aux clients externes.
- **Supervision / IT** : chargé de surveiller les équipements réseau et les serveurs afin d'assurer leur disponibilité et leurs performances.
- **Base de données / Gestion** : centralise et sécurise les données internes et les données clients de l'entreprise.
- **Partage / Collaboration** : permet aux employés de partager des fichiers et de collaborer efficacement au sein de l'entreprise.

Chaque département dispose de son propre routeur local, de postes clients et d'un serveur offrant un service spécifique, ce qui facilite l'administration et l'isolation logique du réseau.

Plan d'adressage IP global

Après l'intégration du service Internet, un plan d'adressage IP global basé sur le réseau **172.24.0.0/14** a été attribué à l'entreprise. Cette plage d'adresses offre un espace suffisant pour couvrir les besoins du backbone et des différents

départements, tout en permettant une évolution future de l'infrastructure réseau.

Ce choix garantit une organisation claire du réseau, facilite le routage entre les différentes zones et évite toute contrainte liée à l'extension du nombre d'utilisateurs ou de services.

Présentation des sous-réseaux par département (VLSM)

La segmentation du réseau est réalisée à l'aide de la technique **VLSM** (**V**ariable **L**ength **S**ubnet **M**ask). Cette méthode permet d'attribuer à chaque département un sous-réseau adapté à son nombre réel d'hôtes, tout en optimisant l'utilisation de l'espace d'adressage IP.

La répartition des sous-réseaux est effectuée en commençant par le département ayant le plus grand nombre d'hôtes, puis en allouant les sous-réseaux de manière progressive afin d'éviter tout chevauchement. Le tableau suivant présente le plan d'adressage VLSM final.

Département	Sous-réseau	Masque	Nombre d'hôtes
Web / Marketing	172.24.0.0/18	255.255.192.0	16382
Supervision / IT	172.24.64.0/21	255.255.248.0	2046
Base de données / Gestion	172.24.72.0/23	255.255.254.0	510
Partage / Collaboration	172.24.74.0/24	255.255.255.0	254

TABLE 1.1 – Plan d'adressage VLSM par département

Cette répartition permet une utilisation optimale des adresses IP et garantit une architecture réseau structurée, évolutive et conforme aux bonnes pratiques professionnelles.

1.5.2 Outils et environnement de travail

L'outil principal de simulation réseau utilisé est **GNS3**. Cet outil permet de concevoir et de simuler des architectures réseau complexes en intégrant des

routeurs, des commutateurs et des machines virtuelles. Grâce à GNS3, il a été possible de mettre en place le backbone OSPF, d'interconnecter les différents départements, de configurer le routage, le NAT ainsi que les mécanismes de sécurité, et de réaliser des tests de connectivité dans un environnement proche du réel.

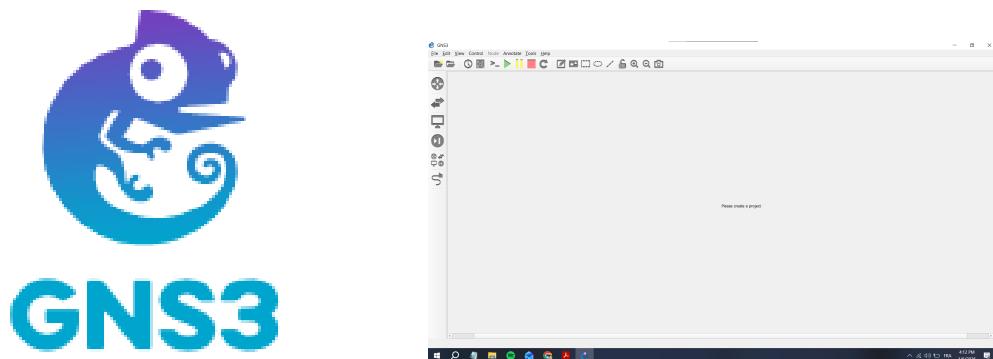


FIGURE 1.2 – Interface GNS3

Pour l'implémentation des services réseau, le système d'exploitation **Ubuntu 22.04**, basé sur **Linux (Unix)**, a été utilisé. Ce choix est justifié par sa stabilité, son niveau de sécurité élevé et sa large utilisation dans les environnements professionnels.

Ubuntu 22.04 a permis de déployer les différents serveurs du projet, notamment le serveur Web, le serveur de base de données, le serveur de supervision et le serveur de partage de fichiers.



FIGURE 1.3 – Interface Ubuntu 22.04



FIGURE 1.4 – Communication entre GNS3 et Ubuntu 22.04

Conclusion

Ce chapitre a permis de définir les besoins de TechSolutions SARL et de proposer une architecture réseau adaptée, basée sur un backbone OSPF, une segmentation VLSM et une organisation par départements. Les choix de conception retenus garantissent une infrastructure fiable, sécurisée et évolutive, servant de fondement à la phase de mise en oeuvre.

Chapitre 2

Réalisation

Introduction

Ce chapitre présente la mise en œuvre de l'infrastructure réseau conçue précédemment. Il détaille la configuration des équipements, l'implémentation du routage dynamique, le déploiement des services réseau ainsi que les mécanismes de sécurité adoptés. Des tests ont été réalisés afin de valider le bon fonctionnement de l'ensemble.

2.1 Mise en place de l'infrastructure réseau

2.1.1 Configuration des routeurs du backbone

La figure ci-dessus illustre l'architecture réseau globale déployée dans le cadre de ce projet. Cette architecture repose sur un backbone central interconnectant plusieurs routeurs représentant les différents départements de l'entreprise.

- **RZ-1 – Web / Marketing** : dédié à l'hébergement et à l'accès aux services Web.
- **RZ-2 – Supervision / IT** : chargé de la surveillance des équipements et des services réseau.
- **RZ-3 – Base de données / Gestion** : assure la centralisation et la sécurisation des données.
- **RZ-4 – Partage / Collaboration** : fournit les services de partage de fichiers via **NFS**.

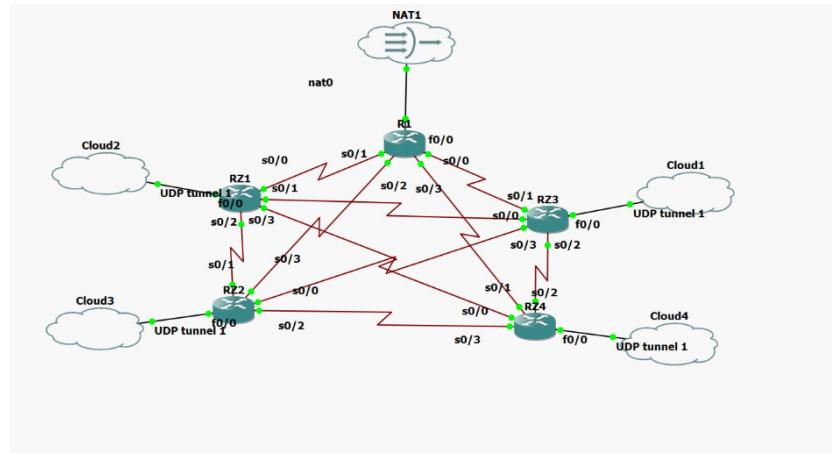


FIGURE 2.1 – Architecture du backbone en topologie maillée

L’ensemble de ces routeurs est interconnecté à travers le **backbone**, garantissant une communication fiable et redondante entre les départements. Le routeur **R-Internet** joue le rôle de passerelle vers Internet et permet aux différents départements d’accéder au réseau externe. Grâce à cette configuration, les postes des départements peuvent effectuer des tests de connectivité, tels que le **ping** vers Internet, en transitant par le backbone, ce qui garantit une architecture cohérente et proche d’un environnement réel d’entreprise.

```

RZ-3#show ip ospf neighbor

```

Neighbor ID	Pri	State	Dead Time	Address	Interface
3.3.3.4	1	FULL/DR	00:00:31	55.55.22.2	FastEthernet0/0
6.6.6.6	0	FULL/ -	00:00:36	55.55.15.2	Serial1/1
4.4.4.4	0	FULL/ -	00:00:33	55.55.13.1	Serial1/0
2.2.2.2	0	FULL/ -	00:00:39	55.55.11.1	Serial1/2
3.3.3.3	0	FULL/ -	00:00:38	55.55.5.2	Serial1/3

```

RZ-3#show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
      D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
      N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
      E1 - OSPF external type 1, E2 - OSPF external type 2
      i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
      ia - IS-IS inter area, * - candidate default, U - per-user static route
      o - ODR, P - periodic downloaded static route

Gateway of last resort is 55.55.5.2 to network 0.0.0.0

      55.0.0.0/30 is subnetted, 14 subnets
0      55.55.1.0 [110/74] via 55.55.11.1, 00:10:06, Serial1/2
0      55.55.2.0 [110/128] via 55.55.11.1, 00:10:06, Serial1/2
          [110/128] via 55.55.5.2, 00:09:56, Serial1/3
0      55.55.3.0 [110/128] via 55.55.15.2, 00:10:06, Serial1/1
          [110/128] via 55.55.5.2, 00:09:56, Serial1/3
0      55.55.4.0 [110/128] via 55.55.13.1, 00:10:06, Serial1/0
          [110/128] via 55.55.5.2, 00:09:56, Serial1/3
C      55.55.5.0 is directly connected, Serial1/3
0      55.55.10.0 [110/128] via 55.55.13.1, 00:10:08, Serial1/0
          [110/128] via 55.55.11.1, 00:10:08, Serial1/2
C      55.55.11.0 is directly connected, Serial1/2
0      55.55.12.0 [110/128] via 55.55.15.2, 00:10:08, Serial1/1
          [110/128] via 55.55.11.1, 00:10:08, Serial1/2
C      55.55.13.0 is directly connected, Serial1/0
0      55.55.14.0 [110/128] via 55.55.15.2, 00:10:09, Serial1/1
          [110/128] via 55.55.13.1, 00:10:09, Serial1/0
C      55.55.15.0 is directly connected, Serial1/1
0      55.55.21.0 [110/74] via 55.55.13.1, 00:10:12, Serial1/0
C      55.55.22.0 is directly connected, FastEthernet0/0
--More-- 

```

FIGURE 2.2 – Captures du fonctionnement du routage dynamique OSPF

La figure suivante présente une capture du routage dynamique **OSPF** mis en place sur les routeurs du backbone. Cette capture montre l'échange des informations de routage entre les routeurs, permettant à chacun de connaître les réseaux accessibles dans l'architecture.

Grâce au protocole OSPF, les routes sont apprises automatiquement et mises à jour de manière dynamique. En cas de modification de la topologie ou de défaillance d'un lien, OSPF permet de recalculer rapidement les chemins afin d'assurer la continuité de la communication entre les différents départements.

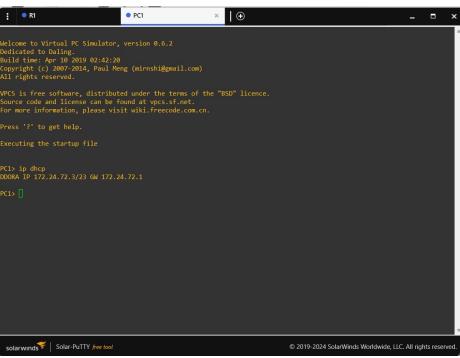
2.1.2 Configuration des routeurs des départements

Chaque département de l'entreprise dispose de son propre routeur local (RZ-1, RZ-2, RZ-3 et RZ-4), configuré pour assurer la connectivité interne du département et la communication avec le reste du réseau.

Les étapes suivantes ont été réalisées pour chaque routeur de département :

- Configuration des interfaces réseau reliant le routeur au backbone et au réseau local du département.
- Attribution des adresses IP selon le plan d'adressage défini.
- Mise en place du service **DHCP** pour l'attribution automatique des adresses IP aux postes clients.
- Définition des **adresses exclues** afin de réserver des adresses IP fixes aux serveurs du département.
- Configuration du **NAT** permettant aux équipements internes d'accéder au réseau Internet.
- Activation du **routage dynamique OSPF** afin d'échanger automatiquement les routes avec les autres départements via le backbone.
- Vérification de la connectivité inter-départements et de l'accès à Internet.

Grâce à cette configuration, chaque département peut communiquer avec les autres départements, accéder aux services partagés et se connecter à Internet de manière sécurisée.



```
PC1> ip dhcp
0008A IP 172.24.72.3/23 Gw 172.24.72.1
PC1> [green prompt]
PC1> show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
      D - EIGRP, E1 - OSPF external type 1, E2 - OSPF external type 2
      I1 - OSPF intra-area summary, I2 - OSPF inter-area summary, N1 - IS-IS level-1
      N2 - IS-IS level-2, * - candidate default, U - per-user static route
      o - OSPF, P - periodic downloaded static route, H - NHRP, 1 - LISP
      a - application route
      r - replicated route, S - next hop override
Gateway of last resort is 55.55.22.1 to network 0.0.0.0

S* 0.0.0.0/0 [1/0] via 55.55.22.1
  55.55.0.0/8 is verbally subnetted, 15 subnets, 2 masks
    55.55.0.0/24 [110/129] via 55.55.22.1, 00:30:50, FastEthernet1/0
    55.55.2.0/30 [110/129] via 55.55.22.1, 00:30:50, FastEthernet1/0
    55.55.3.0/30 [110/129] via 55.55.22.1, 00:30:50, FastEthernet1/0
    55.55.4.0/30 [110/129] via 55.55.22.1, 00:30:50, FastEthernet1/0
    55.55.5.0/30 [110/129] via 55.55.22.1, 00:30:50, FastEthernet1/0
    55.55.6.0/30 [110/129] via 55.55.22.1, 00:30:50, FastEthernet1/0
    55.55.7.0/30 [110/129] via 55.55.22.1, 00:30:50, FastEthernet1/0
    55.55.8.0/30 [110/129] via 55.55.22.1, 00:30:50, FastEthernet1/0
    55.55.9.0/30 [110/129] via 55.55.22.1, 00:30:50, FastEthernet1/0
    55.55.10.0/30 [110/129] via 55.55.22.1, 00:30:50, FastEthernet1/0
    55.55.11.0/30 [110/129] via 55.55.22.1, 00:30:50, FastEthernet1/0
    55.55.12.0/30 [110/129] via 55.55.22.1, 00:30:50, FastEthernet1/0
    55.55.13.0/30 [110/129] via 55.55.22.1, 00:30:50, FastEthernet1/0
    55.55.14.0/30 [110/129] via 55.55.22.1, 00:30:50, FastEthernet1/0
    55.55.15.0/30 [110/129] via 55.55.22.1, 00:30:50, FastEthernet1/0
    55.55.21.0/30 [110/129] via 55.55.22.1, 00:30:40, FastEthernet1/0
    55.55.22.0/32 [110/129] via 55.55.22.1, 00:30:40, FastEthernet1/0
    55.55.22.2/32 is directly connected, FastEthernet1/0
    55.55.23.0/30 [110/129] via 55.55.22.1, 00:30:40, FastEthernet1/0
    172.24.72.0/16 [110/76] via 55.55.22.1, 00:19:42, FastEthernet0/0
    172.24.72.0/24 [110/76] via 55.55.22.1, 00:19:42, FastEthernet0/0
    172.24.72.1/32 is directly connected, FastEthernet0/0
PC1>
```

FIGURE 2.3 – Étapes de configuration des routeurs des départements

Les routeurs de tous les départements ont été configurés de la même manière en suivant une approche standardisée. Chaque département dispose d'une configuration similaire incluant la mise en place des interfaces réseau, la

configuration du service DHCP avec des adresses exclues pour les serveurs, l'activation du NAT pour l'accès à Internet et l'activation du routage dynamique OSPF afin d'assurer la communication entre les différents départements via le backbone. Implémentation des services

2.1.3 Implémentation des services

Département Supervision / IT

Le département **Supervision / IT** est responsable de la surveillance et de la gestion de l'infrastructure informatique. Il utilise un **serveur de monitoring** pour contrôler la disponibilité, les performances et l'état des équipements réseau et des serveurs. Ce département joue un rôle essentiel dans la détection rapide des incidents et le maintien de la continuité des services.

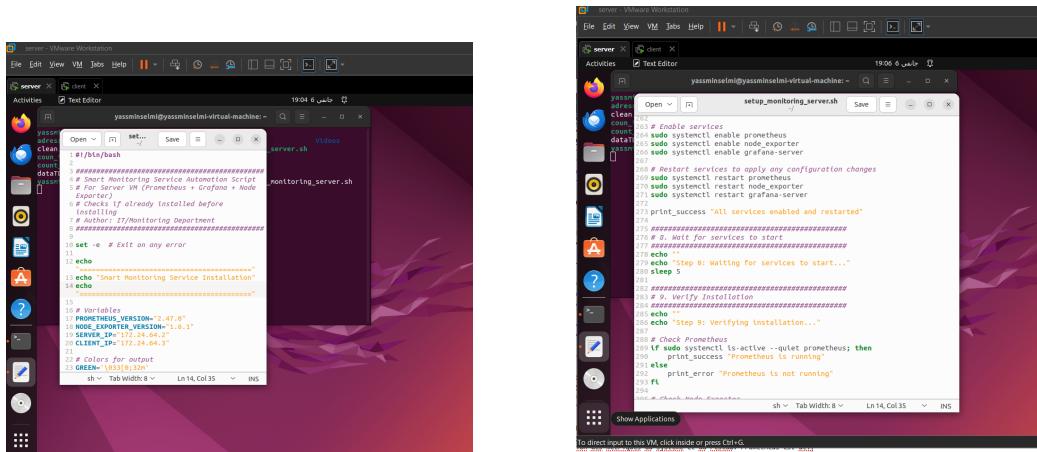


FIGURE 2.4 – Mise en place du service Supervision / IT

La figure ci-dessus illustre la mise en place du service de supervision au niveau du département **Supervision / IT**. Cette capture montre les différentes étapes d'installation et de configuration des outils de monitoring sur un serveur dédié sous **Ubuntu 22.04**.

Dans ce département, les outils **Prometheus** et **Grafana** ont été installés côté serveur afin d'assurer la collecte, le stockage et la visualisation des métriques du système et du réseau. Prometheus est utilisé pour la récupération des données de supervision, tandis que Grafana permet l'affichage des informations sous forme de tableaux de bord graphiques.

Le service **Node Exporter** a été déployé à la fois sur le serveur de supervision et sur les machines clientes. Côté serveur, il permet de surveiller l'état des

ressources système telles que le processeur, la mémoire et le disque. Côté clients, Node Exporter permet de remonter les métriques des différents équipements vers le serveur Prometheus.

Cette architecture de supervision permet un suivi en temps réel des performances, une détection rapide des anomalies et contribue au maintien de la disponibilité et de la continuité des services au sein de l'infrastructure réseau.

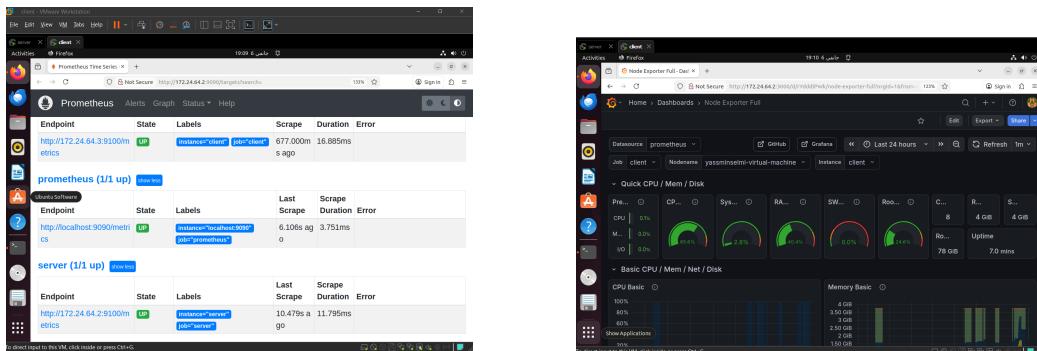


FIGURE 2.5 – Supervision des équipements via Prometheus et Grafana

Département Web / Marketing

Le département **Web / Marketing** est chargé de la gestion du site Internet de l'entreprise ainsi que des interactions avec les clients externes. Il héberge les services Web accessibles depuis l'extérieur et dispose d'un **serveur Web dédié**. Ce département comprend un grand nombre de postes clients représentant les employés travaillant sur les activités marketing et la présence en ligne de l'entreprise.

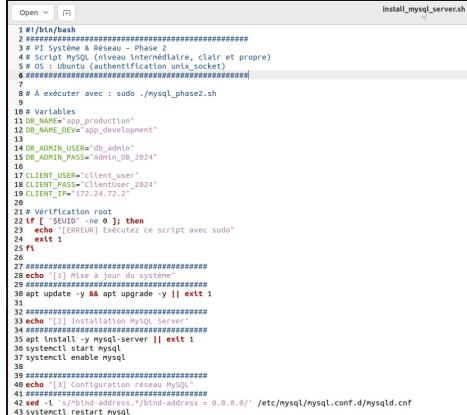


FIGURE 2.6 – Mise en œuvre du service Web – Département Web / Marketing

La figure ci-dessus illustre la mise en place du service Web à travers l'installation et la configuration du serveur **Apache**. Elle montre la création d'une page HTML, l'activation du service, la configuration des **VirtualHosts** et la vérification de l'accès à la page Web depuis un poste client.

Département Base de données / Gestion

Le département **Base de données / Gestion** assure la centralisation, le stockage et la sécurisation des données internes et des données clients. Il dispose d'un **serveur de base de données dédié** permettant de garantir l'intégrité, la confidentialité et la disponibilité des informations critiques pour l'entreprise.



```

1#!/bin/bash
2#####
3# TEST SYSTEM & MySQL - Phase 3 (FINAL)
4# Scénario MySQL Client Test
5# Machine : DB-Client [172.24.72.2]
6# Serveur : DB-Server (172.24.72.10)
7#####
8
9# Variables
10DB_SERVER=172.24.72.10
11CLIENT_USER="client_user"
12CLIENT_PASS="ClientUser_2024"
13DB_NAME="app_production"
14SHARED_DB="company_shared"
15
16echo "===== TEST CLIENT MySQL - Phase 3 (FINAL) ====="
17echo " Client: $(hostname) $(hostname -I | awk '{print $1}')"
18echo " Serveur: $DB_SERVER"
19echo "====="
20
21#####
22##### Vérification MySQL client
23echo "[1] Vérification MySQL client"
24#####
25if ! command -v mysql > /dev/null; then
26    echo "Installation de mysql-client..."
27    sudo apt update -y
28    sudo apt install -y mysql-client
29    echo "/ MySQL client installé"
30else
31    echo "/ MySQL client déjà installé"
32fi
33
34#####
35echo "[2] Test connexion vers DB-Server"
36#####
37echo "Ping vers $DB_SERVER."
38if ping -c 3 $DB_SERVER > /dev/null 2>&1; then
39    echo "/ Serveur accessible"
40else
41    echo "/> Serveur inaccessible - Vérifiez le réseau"
42    echo ""

```

```

Farah@00-Server: $ mysql -u root -p
Enter password:
ERROR 1045 (28000): Access denied for user 'root'@'localhost'
Farah@00-Server: $ 
Farah@00-Server: ~
Farah@00-Server: ~$ sudo mysql
[sudo] password for farah:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 28
Server version: 8.0.24-0ubuntu0.22.04.2 (Ubuntu)

Copyright (c) 2000, 2025, Oracle and/or its affiliates.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql> exit
Bye
Farah@00-Server: ~$ echo "## Vérification MySQL ##"
## Vérification MySQL ##
farah@00-Server: ~$ sudo systemctl status mysql | grep Active
    Active: active (running) since Tue 2025-12-10 19:33:36 CET; 3h 11min ago
farah@00-Server: ~$ echo -e "## Utilisateurs MySQL ##"

## Utilisateurs MySQL ##
farah@00-Server: ~$ sudo mysql -u root -p -e "SELECT user, host FROM mysql.user;" 
Enter password:
+-----+-----+
| user      | host     |
+-----+-----+
| db_admin   | %       |
| readonly_user | %       |
| webapp_user | %       |
| db_network  | 172.24.72.% |
| llm_user    | 172.24.72.% |
| debian-sys-maint | localhost |
| mysql.infoschema | localhost |
| mysql.session | localhost |
| mysql.sys    | localhost |
| root       | localhost |
+-----+-----+

```



```

Farah@00-Server: ~$ echo -e "\n## Bases de données ##"
## Bases de données ##
Farah@00-Server: ~$ sudo mysql -u root -p -e "SHOW DATABASES;" 
Enter password:
+-----+
| Database |
+-----+
| app_development |
| app_production |
| information_schema |
| mysql |
| performance_schema |
| sys |
+-----+
Farah@00-Server: ~$ echo -e "\n## Configuration réseau MySQL ##"
## Configuration réseau MySQL ##
Farah@00-Server: ~$ sudo grep bind-address /etc/mysql/mysql.conf.d/mysqld.cnf
bind-address          = 0.0.0.0
mysql-bind-address    = 0.0.0.1
Farah@00-Server: ~$ cd -
Farah@00-Server: ~$ gedit install_mysql_server.sh
`C
Farah@00-Server: ~$ chmod +x install_mysql_server.sh
Farah@00-Server: ~$ sudo ./install_mysql_server.sh
[sudo] password for farah:
[!] Mise à jour du système
HTTP://security.ubuntu.com/ubuntu jessie/InRelease
Get:2 http://in.archive.ubuntu.com/ubuntu jessy-updates InRelease [128 kB]
Get:3 http://in.archive.ubuntu.com/ubuntu jessy-backports InRelease [127 kB]
Get:4 http://security.ubuntu.com/ubuntu jessy-security InRelease [933 kB]
Get:5 http://security.ubuntu.com/ubuntu jessy-security/main Translation-en [417 kB]
Get:6 http://security.ubuntu.com/ubuntu jessy-security/restricted Translation-en [100 kB]
Get:7 http://security.ubuntu.com/ubuntu jessy-security/universe Translation-en [100 kB]
Get:8 http://security.ubuntu.com/ubuntu jessy-security/main amd64 DEP-11 Metadata [54.5 kB]
Get:9 http://security.ubuntu.com/ubuntu jessy-security/main amd64 c-n-f Metadata [14.0 kB]
Get:10 http://security.ubuntu.com/ubuntu jessy-security/restricted amd64 DEP-11 Metadata [208 B]
Get:11 http://security.ubuntu.com/ubuntu jessy-security/universe amd64 DEP-11 Metadata [125 kB]
Get:12 http://security.ubuntu.com/ubuntu jessy-security/universe amd64 DEP-11 Metadata [208 B]
Get:13 http://security.ubuntu.com/ubuntu jessy-security/main i386 DEP-11 Metadata [112 kB]
Get:14 http://in.archive.ubuntu.com/ubuntu jessy-updates/main amd64 DEP-11 Metadata [112 kB]
Get:15 http://in.archive.ubuntu.com/ubuntu jessy-updates/main amd64 c-n-f Metadata [19.0 kB]

```

FIGURE 2.7 – Mise en œuvre du service Base de données – Département Gestion

La figure ci-dessus illustre la mise en place du **service de base de données** à travers l’installation et la configuration du serveur **MySQL**. Elle montre la création des utilisateurs, l’attribution des droits d’accès, la vérification de l’accès depuis une machine cliente ainsi que l’automatisation du processus à l’aide d’un **script Shell**.

Département Partage / Collaboration

Le département **Partage / Collaboration** est dédié au partage interne des fichiers et des documents entre les employés. Il repose sur un **serveur NFS** permettant aux différents utilisateurs d'accéder aux ressources partagées. Ce département facilite la collaboration et le travail en équipe au sein de l'entreprise.

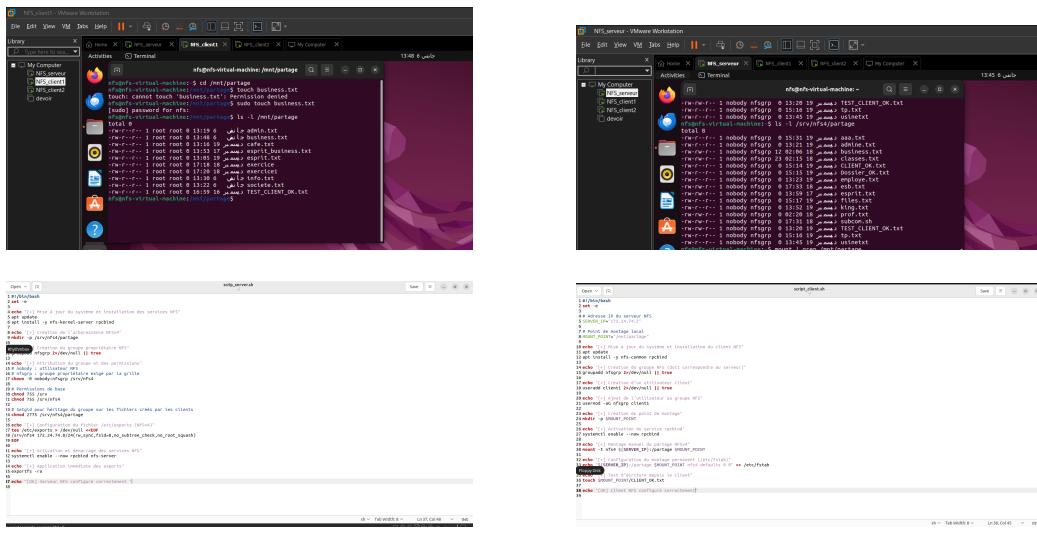


FIGURE 2.8 – Mise en œuvre du service de partage NFS – Département Partage / Collaboration

La figure ci-dessus illustre la mise en place du **service NFS** à travers l’installation des packages nécessaires et la configuration d’un répertoire partagé. Elle montre la création des utilisateurs et des groupes, la configuration des points de montage côté client, la vérification de l’accès aux ressources partagées ainsi que l’automatisation du processus à l’aide d’un **script Shell**.

2.2 Sécurité

La sécurité constitue un aspect essentiel de toute infrastructure réseau d’entreprise. Dans ce projet, plusieurs mécanismes ont été mis en place afin de garantir la confidentialité, l’intégrité et la disponibilité des données échangées entre les différents départements de TechSolutions SARL

Mise en place des tunnels VPN

Afin de sécuriser les communications entre les différents sites et départements, des tunnels VPN (Virtual Private Network) ont été mis en œuvre. Le VPN permet d’établir un canal de communication chiffré au-dessus d’un réseau non sécurisé, garantissant ainsi la protection des données échangées contre l’écoute et les attaques externes.

Les tunnels VPN assurent :

La confidentialité des données grâce au chiffrement,
L'authentification des équipements communicants,
La sécurisation des échanges inter-départements transitant par le backbone.
Cette solution permet de simuler un environnement professionnel où les sites distants d'une entreprise communiquent de manière sécurisée à travers Internet.

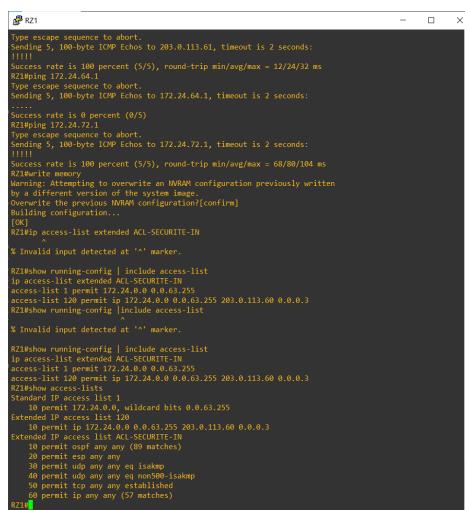
Listes de contrôle d'accès (ACL)

En complément du VPN, des listes de contrôle d'accès (ACL) ont été configurées sur les routeurs afin de filtrer le trafic réseau. Les ACL permettent de définir précisément quels flux sont autorisés ou refusés en fonction de critères tels que les adresses IP source et destination, les protocoles et les ports utilisés.

Les ACL mises en place permettent notamment :

- De limiter l'accès aux serveurs sensibles, comme le serveur de base de données,
- De restreindre les communications inter-départements aux seuls services nécessaires,
- De bloquer les accès non autorisés depuis l'extérieur du réseau.

Cette approche renforce la sécurité globale de l'infrastructure en appliquant le principe du moindre privilège, tout en conservant une communication fonctionnelle entre les différents services.



The screenshot shows a terminal window titled 'R21'. The user is configuring an Access Control List (ACL) named 'ACL-SECURITE-IN'. The configuration includes defining an extended IP access list with two rules: one permitting traffic from 172.24.0.0/255 to 203.0.113.0/255, and another permitting traffic from 172.24.0.0/255 to 172.24.0.0/255. The user also checks for existing configurations and overwrites them. The session ends with a successful configuration command.

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 203.0.113.61, timeout is 2 seconds:
Success rate is 100 percent (5/5), round-trip min/avg/max = 12/24/32 ms
R21#ping 172.24.64.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.24.64.1, timeout is 2 seconds:
Success rate is 0 percent (0/5)
R21#ping 172.24.72.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.24.72.1, timeout is 2 seconds:
Success rate is 100 percent (5/5), round-trip min/avg/max = 68/80/104 ms
R21#write memory
[confirm]
Overwriting the previous NVRAM configuration[confirm]
Overwriting configuration...
[OK]
R21#ip access-list extended ACL-SECURITE-IN
% Invalid input detected at `*' marker.
R21#show running-config | include access-list
access-list 1 permit 172.24.0.0 0.0.0.63.255
access-list 120 permit ip 172.24.0.0 0.0.63.255 203.0.113.0 0.0.0.3
R21#show running-config | include access-list
% Invalid input detected at `*' marker.
R21#show running-config | include access-list
ip access-list extended ACL-SECURITE-IN
access-list 1 permit 172.24.0.0 0.0.0.63.255
access-list 120 permit ip 172.24.0.0 0.0.63.255 203.0.113.0 0.0.0.3
R21#show access-lists
Standard IP access list Standard-IP-IN
 1 permit ip any 255.255.255.255 wildcard bits 0.0.63.255
Extended IP access list 10
 10 permit ip 172.24.0.0 0.0.63.255 203.0.113.0 0.0.0.3
Extended IP access list 100
 100 permit esp any any (89 matches)
 20 permit esp any any
 30 permit udp any any 514
 40 permit tcp any any eq 22
 50 permit tcp any any established
 50 permit permit any any (57 matches)
R21#
```

FIGURE 2.9 – ACL

2.3 Tests et résultats

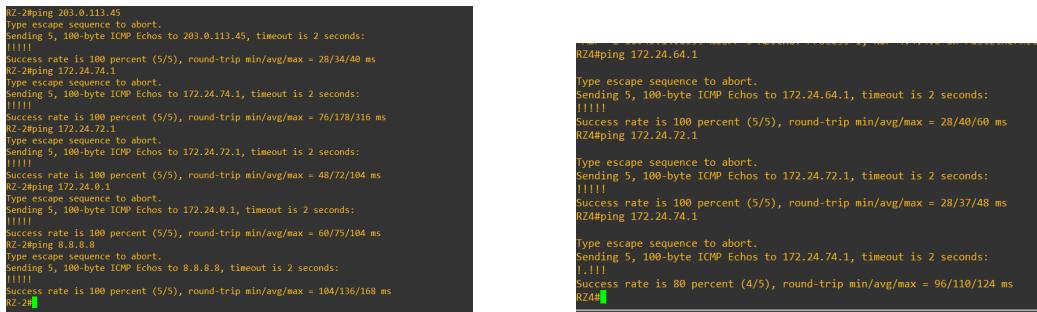
Afin de valider le bon fonctionnement de l'infrastructure réseau mise en place, une série de tests a été réalisée après la phase de configuration. Ces tests ont pour objectif de vérifier la connectivité entre les différents départements, le bon fonctionnement du routage dynamique, l'accès aux services réseau, ainsi que l'efficacité des mécanismes de sécurité implémentés.

Les résultats obtenus confirment la cohérence de l'architecture déployée et le respect des objectifs définis lors de la phase de conception .

2.3.1 Tests de connectivité réseau

Des tests de connectivité ont été effectués à l'aide de la commande ping entre les postes clients des différents départements et vers les serveurs internes. Ces tests ont permis de vérifier la communication inter-départements à travers le backbone OSPF.

Les résultats montrent que tous les départements peuvent communiquer entre eux sans perte de paquets, ce qui confirme le bon fonctionnement du routage dynamique et du plan d'adressage IP.



The figure consists of two side-by-side terminal windows. The left window, titled 'RZ-2#', shows a ping command to 203.0.113.45. It displays five successful echo replies (labeled '!!!!') and one failure ('Type escape sequence to abort...'). The right window, titled 'RZ4#', shows a ping command to 172.24.64.1. It displays five successful echo replies (labeled '!!!!') and one failure ('Type escape sequence to abort...'). Both windows show a success rate of 100% and round-trip times between 28ms and 40ms.

```
RZ-2#ping 203.0.113.45
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 203.0.113.45, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 28/34/40 ms
RZ-2#ping 172.24.74.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.24.74.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 76/178/316 ms
RZ-2#ping 172.24.72.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.24.72.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 48/72/104 ms
RZ-2#ping 172.24.0.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.24.0.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 60/75/104 ms
RZ-2#ping 8.8.8.8
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 8.8.8.8, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 104/136/168 ms
RZ-2#
```

```
RZ4#ping 172.24.64.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.24.64.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 28/40/60 ms
RZ4#ping 172.24.72.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.24.72.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 28/37/48 ms
RZ4#ping 172.24.74.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.24.74.1, timeout is 2 seconds:
!!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 96/110/124 ms
RZ4#
```

FIGURE 2.10 – Tests de connectivité réseau

2.3.2 Tests du routage dynamique OSPF

Le protocole OSPF a été testé afin de vérifier l'échange automatique des routes entre les routeurs du backbone. Les tables de routage ont été analysées pour confirmer la présence des réseaux de tous les départements.

Des tests de tolérance aux pannes ont également été réalisés en simulant l'arrêt d'un lien du backbone. Le trafic a été redirigé automatiquement via un autre chemin, démontrant la capacité d'OSPF à assurer la continuité des communications.

```

RZ-3#show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
      D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
      N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
      E1 - OSPF external type 1, E2 - OSPF external type 2
      i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
      ia - IS-IS inter area, * - candidate default, U - per-user static route
      o - ODR, P - periodic downloaded static route

Gateway of last resort is 55.55.5.2 to network 0.0.0.0

      55.0.0.0/30 is subnetted, 14 subnets
0      55.55.1.0 [110/74] via 55.55.11.1, 00:10:06, Serial1/2
0      55.55.2.0 [110/128] via 55.55.11.1, 00:10:06, Serial1/2
0          [110/128] via 55.55.5.2, 00:09:56, Serial1/3
0      55.55.3.0 [110/128] via 55.55.15.2, 00:10:06, Serial1/1
0          [110/128] via 55.55.5.2, 00:09:56, Serial1/3
0      55.55.4.0 [110/128] via 55.55.13.1, 00:10:06, Serial1/0
0          [110/128] via 55.55.5.2, 00:09:56, Serial1/3
0      55.55.5.0 [110/128] via 55.55.11.1, 00:10:08, Serial1/0
0      55.55.10.0 [110/128] via 55.55.11.1, 00:10:08, Serial1/2
C      55.55.11.0 is directly connected, Serial1/2
0      55.55.12.0 [110/128] via 55.55.15.2, 00:10:08, Serial1/1
0          [110/128] via 55.55.11.1, 00:10:08, Serial1/2
C      55.55.13.0 is directly connected, Serial1/0
0      55.55.14.0 [110/128] via 55.55.15.2, 00:10:00, Serial1/1
0          [110/128] via 55.55.13.1, 00:10:00, Serial1/0
C      55.55.15.0 is directly connected, Serial1/1
0      55.55.21.0 [110/74] via 55.55.13.1, 00:10:12, Serial0/0
0      55.55.22.0 is directly connected, FastEthernet0/0
--More-- 

```

Neighbor ID	Pri	State	Dead Time	Address	Interface
1.3.3.4	1	FULL/DR	00:00:31	55.55.22.2	FastEthernet0/0
6.6.6.6	0	FULL/ -	00:00:36	55.55.15.2	Serial1/1
4.4.4.4	0	FULL/ -	00:00:33	55.55.13.1	Serial1/0
2.2.2.2	0	FULL/ -	00:00:39	55.55.11.1	Serial1/2
3.3.3.3	0	FULL/ -	00:00:38	55.55.5.2	Serial1/3

FIGURE 2.11 – Tests du routage dynamique OSPF

2.3.3 Tests d'accès aux services réseau

Des tests ont été réalisés pour vérifier l'accessibilité et la disponibilité des services déployés dans chaque département.

- **Le service Web** a été testé via un navigateur depuis plusieurs postes clients.
- **Le service de base de données** a été testé à partir d'un client autorisé.
- **Le service de partage NFS** a été testé par l'accès et la modification de fichiers partagés.
- **Le service de supervision** a été vérifié par l'affichage des métriques dans Grafana.

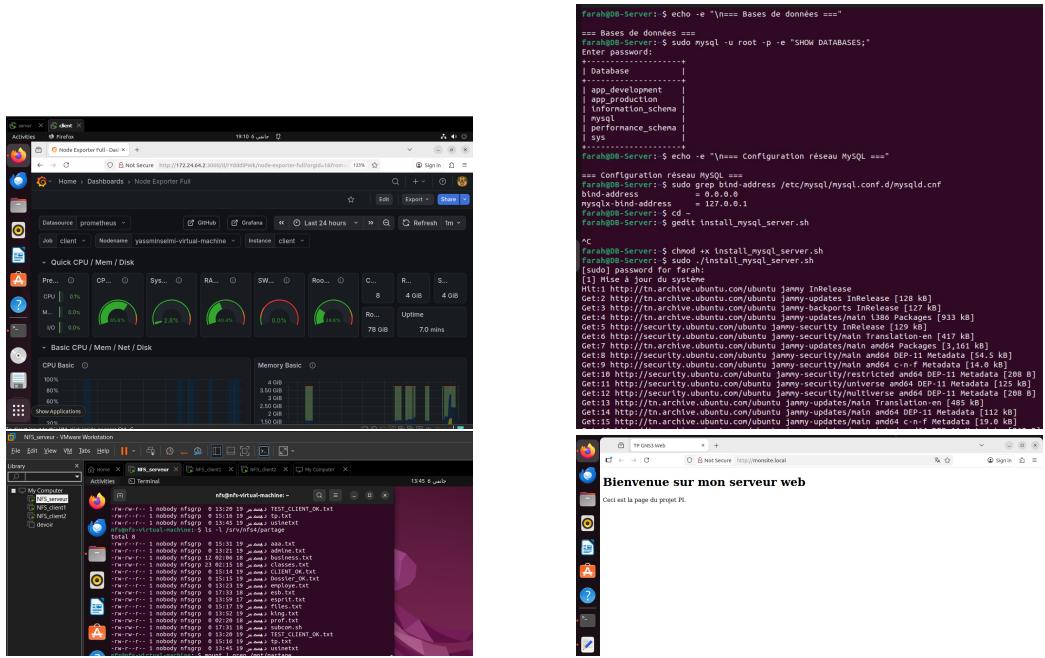


FIGURE 2.12 – Tests d'accès aux services réseau

Les résultats confirment que tous les services sont opérationnels et accessibles selon les règles définies.

2.3.4 Tests d'accès à Internet (NAT)

Des tests de connectivité vers Internet ont été réalisés depuis les postes clients des différents départements. Les résultats montrent que l'accès aux ressources externes est fonctionnel grâce à la configuration du NAT sur le routeur principal.

```
RZ-2#ping 8.8.8.8
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 8.8.8.8, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 104/136/168 ms
RZ-2#ping 172.24.0.2
```

FIGURE 2.13 – Tests d'accès à Internet (NAT)

2.3.5 Résultats et validation globale

L'ensemble des tests réalisés démontre que l'infrastructure réseau fonctionne conformément aux attentes. Le routage dynamique, la segmentation du réseau, l'accès aux services et les mécanismes de sécurité sont opérationnels.

Ces résultats valident les choix de conception effectués et confirment que l'architecture déployée répond aux besoins de TechSolutions SARL.

Conclusion

La phase de réalisation a permis de déployer avec succès l'infrastructure réseau et les services associés. Les tests effectués ont confirmé la connectivité, la disponibilité des services et l'efficacité des mécanismes de sécurité mis en place, notamment le VPN et les ACL. Cette étape valide la conformité de la solution aux objectifs définis.

Conclusion et perspectives

Ce projet intégré a permis de concevoir et de déployer une infrastructure réseau multiservice répondant aux besoins d'une entreprise fictive, TechSolutions SARL, dans un contexte académique simulant un environnement professionnel réel. À travers ce travail collaboratif, les objectifs fixés en début de projet ont été atteints, notamment la mise en place d'une architecture réseau fiable, sécurisée et évolutive.

L'infrastructure réalisée repose sur un backbone utilisant le protocole de routage dynamique OSPF, garantissant une communication efficace et une bonne tolérance aux pannes. L'adressage IP basé sur la technique VLSM a permis une utilisation optimisée de l'espace d'adressage, tandis que le déploiement des services réseau essentiels (Web, base de données, partage de fichiers et supervision) a assuré le bon fonctionnement des différents départements de l'entreprise.

Par ailleurs, des mécanismes de sécurité tels que les tunnels VPN et les listes de contrôle d'accès ont été intégrés afin de protéger les échanges de données et de restreindre l'accès aux ressources sensibles. Les tests réalisés ont confirmé la cohérence de l'architecture, la disponibilité des services et la conformité de la solution aux exigences définies.

Ce projet a également permis aux membres de l'équipe de renforcer leurs compétences techniques en réseaux informatiques, tout en développant des capacités essentielles en travail d'équipe, en organisation et en résolution de problèmes. Il constitue ainsi une expérience pédagogique enrichissante et une préparation concrète aux projets d'ingénierie rencontrés dans le cadre professionnel.