

# SAE 3.03 :

Mettre en place un  
réseau informatique  
multisites

FOUKA Anisse  
ABOUHNAIK Chadi  
KILIC Fatih  
BERRADA Mehdi

2023  
2024

V  
r  
o  
n

M. Bouillet  
M. Lecoq

## Table des matières

<b>I.</b>	<b><i>Introduction</i></b>	<b>2</b>
A.	Contexte du Projet .....	2
B.	Objectifs de la Restructuration du Réseau .....	2
C.	Inventaire.....	2
<b>II.</b>	<b><i>Présentation de l'Entreprise Beerok</i></b>	<b>3</b>
A.	Implantations et Organisation Territoriale.....	3
a)	Implantations de Beerok.....	3
b)	Schéma d'Implantation .....	4
B.	Objectifs de la SAE.....	4
<b>III.</b>	<b><i>Infrastructure Réseau Multisites</i></b>	<b>5</b>
A.	Serveurs et Services Hébergés .....	6
a)	Serveur d'Attribution d'Adresse Automatisée (Service DHCP) : .....	6
b)	Configuration Réseau .....	7
c)	Wi-Fi Sécurisé.....	7
B.	Interconnexion des Sites.....	7
a)	Services de VPN .....	7
b)	Différenciation des Flux .....	7
c)	Qualité de Service (QoS) .....	7
<b>IV.</b>	<b><i>Services Réseaux</i></b>	<b>10</b>
A.	Implantation des Services du siège .....	10
a)	Infrastructure Serveurs .....	11
b)	Gestion Centralisée.....	11
B.	Services pour les Magasins et le Showroom.....	11
a)	Magasin.....	11
b)	Showroom.....	11
C.	Schéma du Projet (Détailé) .....	11
<b>V.</b>	<b><i>Développement des Services</i></b>	<b>12</b>
A.	Services de Base .....	12
a)	Messagerie .....	12
b)	Téléphonie .....	17
c)	Stockage en Ligne/Applicatifs .....	17
B.	Services Avancés .....	19
a)	DAAS : Serveur de Terminaux .....	19
b)	Gestion Technique des Bâtiments .....	20
<b>VI.</b>	<b><i>Services Spécifiques aux Magasins et Showroom</i></b>	<b>20</b>
A.	Réseau Wi-Fi et Portail Captif .....	20
B.	Connexion Sécurisée au Showroom .....	21
<b>VII.</b>	<b><i>Déroulement du Projet</i></b>	<b>21</b>
A.	Planning et Méthode Kanban .....	21
B.	Répartition des Tâches .....	23

<b>VIII. Conclusion .....</b>	<b>24</b>
A. Réalisation des Objectifs .....	24
B. Retours d'Expérience.....	24

## I. Introduction

### A. Contexte du Projet

Ce projet s'inscrit dans le cadre d'une simulation pédagogique visant à développer et mettre en pratique nos compétences dans le domaine des réseaux informatiques. Notre groupe, composé de quatre membres, se divise en deux parcours complémentaires : deux personnes en parcours Cybersécurité, Fouka Anisse et Mehdi Berrada, et deux autres en Internet des Objets (IoM), Fatih Kilic et Chadi Abouhnaik.

### B. Objectifs de la Restructuration du Réseau

L'objectif central de cette simulation est de concevoir et déployer une infrastructure réseau multisites pour une entreprise fictive nommée Beerok, spécialisée dans la chaussure sportive. La restructuration vise à répondre aux besoins spécifiques de Beerok en matière de services informatiques, tout en intégrant des éléments de sécurité et de gestion des objets connectés (IoM). Cette démarche pédagogique nous permettra de mettre en œuvre des compétences variées, de la configuration réseau à la sécurisation des systèmes en passant par la mise en place d'un réseau d'objets connectés.

Le réseau Beerok est conçu comme une étude de cas réaliste, nous permettant de développer nos compétences de manière holistique, allant de la planification stratégique à la mise en œuvre technique. L'objectif ultime est d'acquérir une compréhension approfondie des défis liés à la gestion d'un réseau informatique complexe, tout en répondant de manière efficace aux besoins spécifiques d'une entreprise fictive.

### C. Inventaire

Pour assurer le bon fonctionnement du projet de restructuration du réseau Beerok, une variété d'appareils a été soigneusement sélectionnée pour répondre aux besoins spécifiques. Ces dispositifs comprennent :

- **2 serveurs DHCP** : Essentiels pour attribuer dynamiquement les adresses IP aux périphériques du réseau.
- **8 routeurs** : Ils assurent la connectivité entre les différents sites et contribuent à la gestion du trafic.
- **3 switches** : Facilitent la commutation des données au sein du réseau local, assurant une communication efficace entre les appareils connectés.
- **4 PCs** : Utilisés pour les besoins informatiques généraux et pour tester la connectivité.

- **3 téléphones** : Intégrés dans le réseau pour prendre en charge les services de téléphonie.
- **1 serveur de messagerie** : Responsable de la gestion des emails et de la communication interne.
- **1 serveur de bureau à distance** : Permet l'accès distant aux ressources du réseau.
- **1 serveur Active Directory** : Assure l'authentification des utilisateurs et la gestion des droits d'accès.
- **1 serveur RADIUS** : Garantit la sécurité de l'accès au réseau en authentifiant les utilisateurs.
- **2 bornes WiFi** : Assurent une connectivité sans fil dans les zones désignées.
- **3 ESP8266** : Utilisés pour les objets connectés, renforçant ainsi la connectivité IoT du réseau.
- **1 serveur de certificat** : Gère les certificats de sécurité pour assurer des communications chiffrées.
- **1 serveur de téléphonie** : Apporte des fonctionnalités de téléphonie au réseau.
- **1 serveur de stockage NextCloud** : Fournit des services de stockage en ligne pour les utilisateurs.
- **1 serveur MQTT** : Sert de broker pour les communications machine à machine dans l'IoT.
- **1 Portail Captif** : Assure un contrôle d'accès à Internet, notamment dans les zones publiques.
- **1 tablette** : Utilisée pour des démonstrations pratiques et des tests sur le terrain.

Cette liste exhaustive témoigne de la diversité des composants nécessaires à la mise en place d'une infrastructure réseau complète et fonctionnelle. Chacun de ces dispositifs a été intégré avec soin pour répondre aux exigences spécifiques du projet et contribuer de manière significative à la réussite globale de la restructuration du réseau Beerok.

## II. Présentation de l'Entreprise Beerok

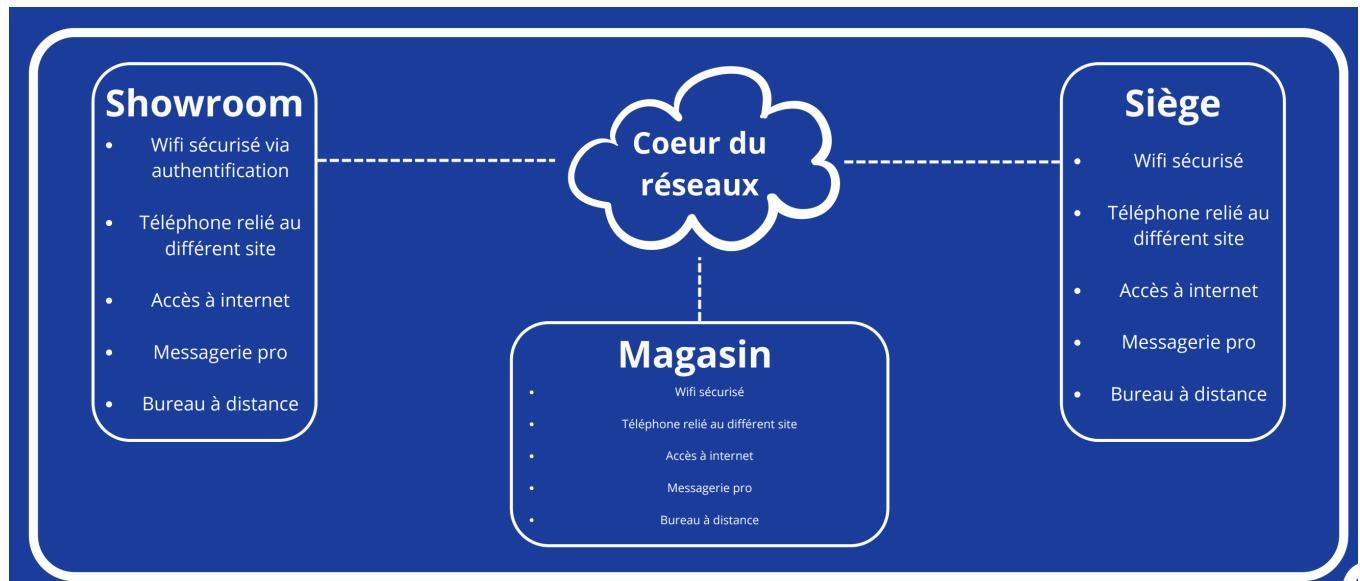
### A. Implantations et Organisation Territoriale

Beerok, entreprise fictive spécialisée dans la chaussure sportive, dispose d'une organisation territoriale comprenant plusieurs implantations stratégiques.

#### a) Implantations de Beerok

1. **Siège Social à Meaux (100 personnes) :**
  - Centralisation des opérations administratives et de direction.
2. **Magasins à travers la France (48 magasins, 10 personnes/magasin) :**
  - Répartition nationale pour la vente au détail.
3. **Showroom à Paris (10 personnes) :**
  - Espace dédié à la présentation des produits de manière élégante.

*b) Schéma d'Implantation*



Beerok a une présence nationale avec des magasins, un showroom à Paris et un siège à Meaux.

**B. Objectifs de la SAE**

La simulation pédagogique Beerok a pour objectif principal de déployer des services sur une infrastructure réseau multisites sécurisée. Ces services seront hébergés en partie localement (in premise) au siège de Meaux, et en partie dans un cloud privé basé sur des serveurs de virtualisation.

Pour garantir un fonctionnement optimal et répondre aux besoins spécifiques de chaque site, les services ont été stratégiquement répartis au sein du réseau Beerok. Voici une vue détaillée des services situés à différents emplacements :

**Siège de Meaux :**

- **Serveur Active Directory :** Responsable de l'authentification des utilisateurs et de la gestion des droits d'accès au sein du siège.
- **Serveur RADIUS :** Assure la sécurité de l'accès au réseau en authentifiant les utilisateurs de manière centralisée.

- **Serveur de messagerie** : Gère les communications internes par le biais des emails.
- **Serveur de certificats** : Fournit des certificats de sécurité pour garantir des communications chiffrées.
- **Serveur MQTT** : Fonctionne en tant que broker pour les communications machine à machine dans le domaine de l'IoT.
- **Serveur cloud NextCloud** : Offre des services de stockage en ligne pour les utilisateurs du siège.
- **Serveur de Bureau à Distance** : Permet un accès distant aux ressources du réseau.
- **1 switch, 1 routeur, 1 téléphone, 1 borne wifi** : Éléments essentiels pour assurer la connectivité et les communications au siège de Meaux.

#### Showroom de Paris :

- **Serveur DHCP** : Gère dynamiquement l'attribution des adresses IP aux périphériques du réseau au showroom.
- **2 PCs** : Utilisés à des fins d'affichage et de démonstration au showroom.
- **1 borne wifi, 1 routeur, 1 switch, 1 téléphone, 1 portail captif, 1 tablette** : Équipements nécessaires pour fournir des services réseau avancés au showroom de Paris.

#### Chaque Magasin :

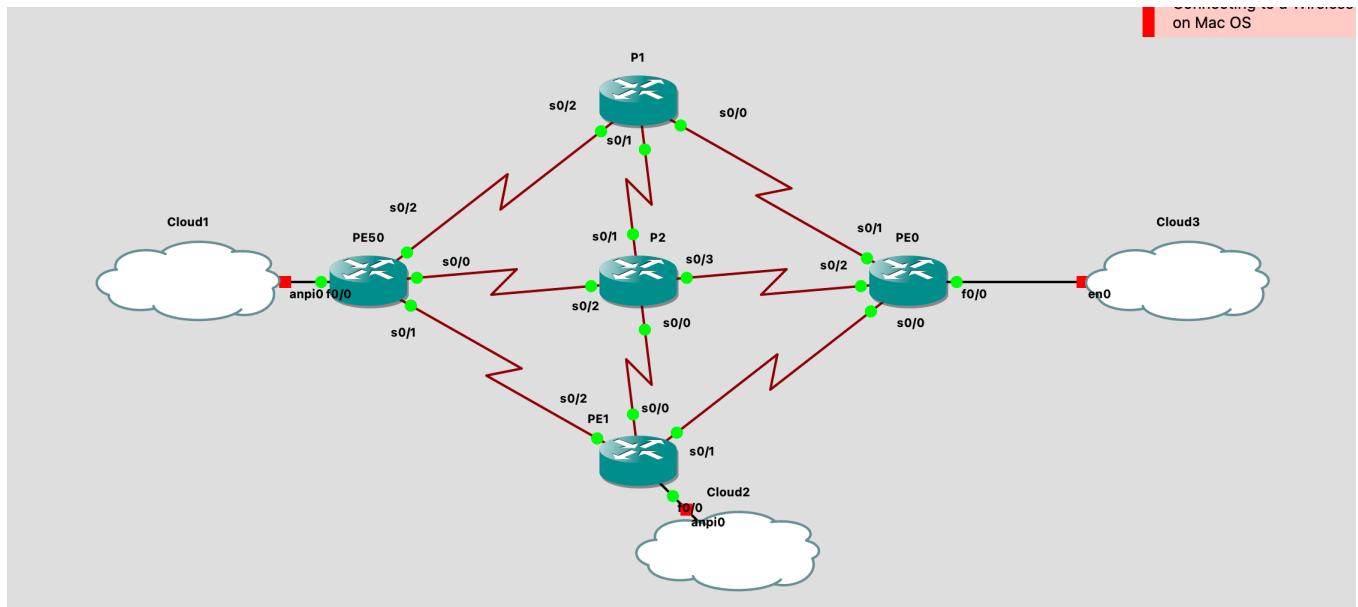
- **Serveur DHCP** : Assure la gestion dynamique des adresses IP dans chaque magasin.
- **2 PCs** : Utilisés pour les besoins informatiques généraux dans chaque magasin.
- **1 borne wifi, 1 routeur, 1 switch, 1 téléphone** : Éléments cruciaux pour établir une connectivité fiable et fournir des services de base dans chaque magasin.

Cette répartition stratégique des services garantit une offre adaptée à chaque site, répondant ainsi aux besoins spécifiques de chaque entité au sein du réseau Beerok. Chaque composant a été sélectionné et configuré en fonction des exigences particulières de son emplacement respectif, contribuant ainsi à l'efficacité et à la fonctionnalité globales du réseau.

L'objectif est de développer une infrastructure robuste capable de répondre aux besoins variés de Beerok, en intégrant des services adaptés à chaque site de l'entreprise simulée.

### III. Infrastructure Réseau Multisites

Dans le cadre du projet Beerok, l'ensemble du cœur du réseaux a été implémenté avec minutie, en utilisant GNS3 comme environnement de simulation. En raison de contraintes temporelles, certaines fonctionnalités, telles que la configuration VRRP au siège et la mise en place de STP, n'ont pas pu être intégrées dans le délai imparti de 3 jours.



Cette fois-ci, en accord avec le schéma, nous avons configuré le protocole BGP (Border Gateway Protocol) entre le cœur de réseau de notre opérateur et les trois sites, utilisant ainsi quatre AS (Autonomous Systems) distincts. Pour activer ce protocole sur les routeurs PE50, PE0, P2, CE50, CE1 et CE0, nous avons saisi les commandes suivantes sur le routeur PE0 :

```
PE0>conf t
PE0#router bgp 123
PE0#network 10.0.2.0 mask 255.255.255.0
PE0#network 10.0.2.4 mask 255.255.255.0
PE0#network 10.0.2.8 mask 255.255.255.0
PE0#network 10.0.2.12 mask 255.255.255.0
PE0#neighbor 10.0.2.1 remote-as 300
PE0#redistributed connected
PE0#redistributed ospf 10 internal external 1 external 2
```

La commande '**network 10.0.2.4 mask 255.255.255.0**' inscrit le réseau dans le protocole de routage BGP. Comme la commande habituelle '**redistribute ospf 10**' ne fonctionnait pas, nous avons effectué des recherches et constaté que chaque version IOS des routeurs et switchs peut différer. Ainsi, la commande '**redistributed ospf 10 internal external 1 external 2**' permet de redistribuer les routes apprises par le protocole BGP au protocole OSPF, similaire à la commande '**redistribute bgp 123**' dans la configuration OSPF. Cela permet la mise en commun des tables de routage et le partage des informations entre les différents protocoles présents sur les mêmes routeurs, facilitant le transit des informations et des communications entre les réseaux.

#### A. Serveurs et Services Hébergés

##### a) Serveur d'Attribution d'Adresse Automatisée (Service DHCP) :

Un service DHCP a été configuré sur les routeurs CE50 pour fournir des adresses IP dynamiques à l'ensemble des clients du réseau, simplifiant ainsi la gestion des adresses IP. Les serveurs essentiels ont été assignés des adresses IP statiques pour assurer une stabilité dans la résolution des noms.

Un serveur DNS a été mis en place pour permettre la résolution efficace des noms de domaine, assurant ainsi une communication fluide au sein de l'infrastructure. Le nom du serveur DNS est Beerok.com

*b) Configuration Réseau :*

La configuration réseau repose sur des protocoles avancés tels que OSPF, MP-BGP, MPLS et VRF, garantissant un routage optimal au cœur du réseau. Le protocole BGP a été utilisé sur les routeurs EDGE du siège, des magasins et du showroom, assurant ainsi une connectivité robuste et évolutive. La commutation a été organisée en VLAN multiples, attribués à des fonctions spécifiques telles que vente, administration, voix, gestion, et plus encore. Cette configuration assure une gestion efficace du trafic. Des mécanismes avancés, tels que VRRP au siège et STP, n'ont pas été intégrés en raison de contraintes temporelles.

*c) Wi-Fi Sécurisé*

Le Wi-Fi a été configuré en utilisant le protocole WPA2 pour assurer un niveau élevé de sécurité dans les communications sans fil. Un portail captif Pfsense a été mis en place pour l'authentification sécurisée des utilisateurs, garantissant ainsi un accès contrôlé au réseau Wi-Fi.

**B. Interconnexion des Sites**

Tous les sites distants sont interconnectés au site central via un cœur de réseau robuste, garantissant ainsi une accessibilité universelle, indépendamment de leur situation géographique.

*a) Services de VPN*

Des services VPN ont été déployés pour sécuriser les communications entre les sites distants et le site central, renforçant ainsi la confidentialité des données échangées.

*b) Différenciation des Flux*

Les flux réseau ont été catégorisés en fonction des VLAN, distinguant les flux direction, ventes, wifi, voix et gestion. Cette différenciation permet une gestion efficace du trafic, optimisant ainsi les performances du réseau.

*c) Qualité de Service (QoS)*

La mise en place de la QoS garantit une priorité optimale aux flux critiques, en particulier pour la téléphonie, assurant ainsi un fonctionnement fluide des services.

**IV. Configuration des Éléments Réseaux**

**A. Configuration du Switch**

*a) Configuration des VLANs et Interfaces*

Nous avons débuté la configuration en définissant les différents VLANs sur le switch et en leur attribuant des noms descriptifs. Les commandes exécutées sont les suivantes :

```
SWI>en
SWI#conf t
SWI(config)#vIan 10
SWI(config-vlan)#name direction
```

Ces commandes ont pour objectif de créer les VLANs nécessaires et de leur assigner des noms explicites.

Pour associer ces VLANs à des ports spécifiques, nous avons utilisé les commandes suivantes, en configurant les ports en mode access, étant donné que chaque port est destiné à un seul VLAN :

```
SWI#conf t
SWI(config)#interface GigabitEthernet1/0/1
SWI(config-if)#switchport mode access
SWI(config-if)#switchport access vlan 10
```

Cette configuration a été appliquée aux quatre premiers ports Gigabit Ethernet, affectant ainsi les VLANs Direction, Ventes, Voix et Wifi. Le VLAN Gestion, ne nécessitant pas de relais après le switch, n'a reçu aucune interface attribuée. Néanmoins, une adresse IP lui a été assignnée pour permettre une connexion distante via SSH, facilitant ainsi la gestion du switch. Les commandes suivantes ont été utilisées à cet effet :

```
SWI#conf t
SWI(config)#interface vlan 99
SWI(config-if)#ip addr 130.2.99.253 255.255.255.0
```

Une fois les VLANs créés et assignés aux ports du switch, nous les avons configurés en mode trunk sur le port Gigabit Ethernet 1/0/24, qui sera connecté à l'Edge Routeur. Le mode trunk autorise la communication de plusieurs VLANs différents à travers un seul lien physique, tandis que le mode access permet la communication d'un seul VLAN par lien physique. Les commandes suivantes illustrent cette configuration :

```
SWI#conf t
SWI#(config)#interface GigabitEthernet1/0/24
SWI(config-if)#switchport mode trunk
SWI(config-if)#switchport trunk allowed vlan 10,20,30,40,99
```

## B. Configuration des Edge Routeurs

Pour déployer la configuration "Router on a Stick" au sein du réseau actif, la première étape consistait à créer des sous-interfaces sur l'interface Gigabit Ethernet0/1 du routeur CE1. Les étapes détaillées sont les suivantes :

```
CE1#conf t
CE1(config)#interface GigabitEthernet0/1
CE1(config-if)#description CONNECTEE AU SWITCH
CE1(config-if)#no shutdown
```

Une fois cette étape accomplie, des sous-interfaces ont été instaurées et leurs adresses IP respectives attribuées pour chaque VLAN, tel qu'exemplifié ci-dessous pour le VLAN 10 :

```
CE1#conf t
CE1(config)#interface GigabitEthernet0/1.10
CE1(config-if)#ip addr 130.4.10.254 255.255.255.0
```

Cette opération a été répétée pour chaque VLAN, aboutissant à la configuration de cinq sous-interfaces distinctes. Par la suite, une encapsulation dot1Q a été appliquée à chaque sous-interface, autorisant l'attribution de balises aux trames conformément à la norme IEEE 802.1q. Ces balises facilitent l'identification des trames et leur transmission au VLAN correspondant, garantissant une segmentation efficace du réseau :

```
CE1#conf t
CE1(config)#interface GigabitEthernet0/1.10
CE1(config-if)#encapsulation dot1Q 10
```

Afin de permettre la communication entre les routeurs des sites (magasin, showroom, siège) via le cœur de réseau, la configuration de l'interface reliée au cœur de réseau a été effectuée conformément au plan d'adressage IP préétabli :

```
CE1#conf t
CE1(config)#interface GigabitEthernet0/0
CE1(config-if)#ip address 10.0.4.26 255.255.255.252
CE1(config-if)#no shutdown
```

Conformément aux exigences du cahier des charges initial, les sites du Showroom et du Magasin devaient disposer d'un serveur DHCP pour fournir des adresses IP et des informations réseau essentielles au bon fonctionnement des clients. Plutôt que d'utiliser une machine physique à l'intérieur du réseau, la configuration de ce service a été effectuée directement sur les routeurs. Pour chaque VLAN, un pool d'adresses IP a été défini avec les informations nécessaires, comme indiqué ci-dessous pour le VLAN 10 :

```
CE1#conf t
CE1(config)#ip dhcp pool vlan 10
CE1(dhcp-config)#network 130.4.10.0 255.255.255.0
CE1(dhcp-config)#domain-name beerok.com
CE1(dhcp-config)#default-router 130.4.10.254
```

Il est important de souligner que toutes les commandes exécutées sur le switch et le routeur dans cette section ont été mises en œuvre dans le réseau du site Magasin, dans un souci de clarté et de compréhension.

### C. Configuration des PCs

Afin d'établir des communications entre les divers PC du réseau, la configuration des postes de travail a impliqué la réception d'adresses IP dynamiques via le protocole DHCP. Les étapes essentielles sont décrites ci-dessous :

Pour permettre aux PC de recevoir des adresses IP automatiquement, le fichier de configuration réseau situé dans **/etc/network/interfaces** a été modifié comme suit :

```
auto eth0 allow-hotplug
eth0 iface
eth0 inet dhcp
```

Suite à la modification du fichier de configuration, la commande **/etc/init.d/networking restart** a été exécutée pour redémarrer les services réseau sur les postes de travail.

Pour obtenir une nouvelle adresse IP, le processus DHCP précédent a été interrompu à l'aide de la commande **dhclient -r**, suivi de la recréation du processus avec **dhclient -v** pour demander une adresse IP via le protocole DHCP.

```
DHCPDISCOVER on eth0 to 255.255.255.255 port 67 interval 17
DHCPOffer of 130.4.20.2 from 130.4.20.254
DHCPREQUEST for 130.4.20.2 on eth0 to 255.255.255.255 port 67
DHCPACK of 130.4.20.2 from 130.4.20.254
bound to 130.4.20.2 -- renewal in 37356 seconds.
root@rt:~#
```

La demande d'adresse IP via DHCP est un processus client/serveur, où le serveur DHCP fournit automatiquement une adresse IP et d'autres paramètres de configuration, tels que les informations DNS et la passerelle par défaut, essentielles au bon fonctionnement du DHCP. Ces étapes ont été accomplies sur chaque poste de travail, garantissant ainsi une attribution dynamique des adresses IP et facilitant la communication entre les PC au sein du réseau.

b) Test de Communication entre VLANs

Après la réalisation de cette configuration, il devient possible d'effectuer un ping entre deux appareils qui ne sont pas membres du même VLAN. Dans ce scénario, toutes les communications de ce type transitent nécessairement par le routeur du site. Une méthode simple pour vérifier cette configuration consiste à utiliser des commandes telles que traceroute ou ping.

```
root@rt:~# ping 130.4.10.2
PING 130.4.10.2 (130.4.10.2) 56(84) bytes of data.
64 bytes from 130.4.10.2: icmp_seq=1 ttl=63 time=0.590 ms
64 bytes from 130.4.10.2: icmp_seq=2 ttl=63 time=0.570 ms
64 bytes from 130.4.10.2: icmp_seq=3 ttl=63 time=0.547 ms
^C
--- 130.4.10.2 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 46ms
rtt min/avg/max/mdev = 0.547/0.569/0.590/0.017 ms
```

## V. Services Réseaux

### A. Implantation des Services du siège

Dans le contexte de ce projet pédagogique, la mise en place des services au siège a été optimisée compte tenu des contraintes temporelles.

*a) Infrastructure Serveurs*

En dépit du délai restreint, des configurations initiales ont été effectuées pour les serveurs, avec une priorité accordée aux éléments essentiels tels que les bases de données. L'attribution d'adresses IP statiques a été réalisée pour garantir une stabilité minimale.

*b) Gestion Centralisée*

Une solution de DHCP a été rapidement instaurée pour rationaliser la gestion des adresses IP, accompagnée d'un serveur DNS facilitant la résolution des noms.

**B. Services pour les Magasins et le Showroom**

*a) Magasin*

Malgré les contraintes temporelles, les magasins ont été connectés au réseau central via des liaisons VPN. Bien que cela assure une connectivité de base, il convient de noter que des ajustements et des optimisations peuvent être envisagés dans des phases ultérieures du projet.

Bien que le déploiement de services spécifiques ait été limité, des possibilités d'implémentation ont été envisagées, notamment pour la gestion des stocks et d'autres fonctionnalités essentielles pour le fonctionnement d'un magasin.

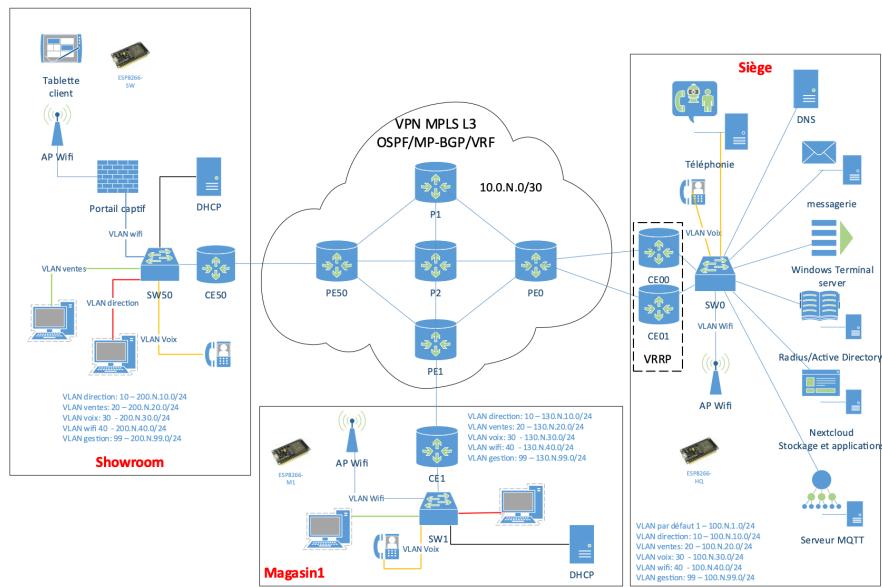
*b) Showroom*

Le showroom a bénéficié d'une infrastructure réseau dédiée, permettant une présentation basique des produits. Les délais contraignants ont restreint l'intégration de fonctionnalités avancées, mais une structure fonctionnelle a été mise en place.

La connexion entre le showroom et le siège a été établie grâce à des services VPN, assurant une sécurité élémentaire des données échangées. Des ajustements ultérieurs peuvent être envisagés pour améliorer la robustesse de cette connexion.

Malgré les défis, l'équipe a posé les bases des services réseau, axant ses efforts sur la simplicité et la fonctionnalité, compte tenu des contraintes de temps imposées par le projet pédagogique.

**C. Schéma du Projet (Détailé)**



## VI. Développement des Services

### A. Services de Base

#### a) Messagerie

La messagerie a été déployée avec succès en utilisant Proxmox pour la virtualisation, assurant ainsi une gestion efficace des ressources.

##### (1) Configuration du MSA/MTA avec Postfix :

- Enregistrement MX dans le DNS :** Tout d'abord, pour permettre la réception des courriels, un enregistrement MX a été ajouté dans le DNS, pointant vers le serveur de messagerie avec une priorité de 10. Cela indique aux autres serveurs de messagerie la manière de diriger les courriels vers votre serveur.
- Suppression d'Exim et installation de Postfix :** Le programme de messagerie Exim a été supprimé, et Postfix a été installé en tant que serveur de messagerie. La configuration a été réalisée en définissant Postfix comme un serveur de messagerie de type site internet.
- Configuration de Postfix :** La configuration de Postfix a impliqué l'autorisation du relais du courrier en laissant vide les champs lors de l'exécution de la commande "dpkg-reconfigure postfix". Des paramètres par défaut, tels que l'utilisation de la couche IPv4 et d'autres options, ont été acceptés.
- Vérification du bon fonctionnement de Postfix :** Pour s'assurer que Postfix fonctionne correctement, la commande "postfix -v check" a été utilisée.

```
root@Debian11:/tmp# postfix -v check
postfix: name_mask: ipv4
postfix: inet_addr local: configured 2 IPv4 addresses
root@Debian11:/tmp# █
```

- **Configuration des interfaces** : Les interfaces auxquelles Postfix doit écouter ont été spécifiées en modifiant le champ "inet\_interface" dans le fichier de configuration de Postfix (/etc/postfix/main.cf).
- **Test du serveur avec Telnet** : Les primitives SMTP (HELO, RCPT, MAIL, DATA) ont été utilisées via une session Telnet pour tester le bon fonctionnement du serveur.

```
root@Debian11:/tmp# telnet debserv 25
Trying 100.4.99.251...
Connected to debserv.beerok.com.
Escape character is '^]'.
220 Debian11 ESMTP Postfix (Debian/GNU)
HELO
501 Syntax: HELO hostname
HELO debserv
250 Debian11
MAIL FROM:jim@beerok.com
250 2.1.0 Ok
RCPT TO:joe@beerok.com
250 2.1.5 Ok
DATA
354 End data with <CR><LF>.<CR><LF>
Test de dimanche pour le rapport
.
250 2.0.0 Ok: queued as 0A79F100ED4
QUIT
221 2.0.0 Bye
Connection closed by foreign host.
root@Debian11:/tmp# █
```

- **Vérification des logs :** Les logs dans /var/log/syslog ont été vérifiés à l'aide de la commande "tail -40 /var/log/syslog | grep 0A79" pour confirmer l'envoi des courriels.

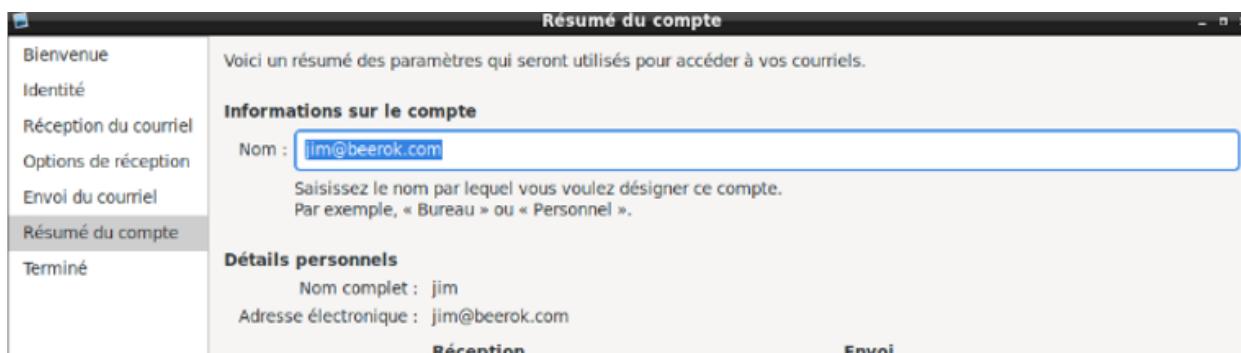
```
root@Debian11:/tmp# tail -40 /var/log/syslog | grep 0A79
Feb 8 19:49:47 Debian11 postfix/smtpd[48423]: 0A79F100ED4: client=pool-100-2-99-251.nycmny.fios.verizon.net[100.4.99.251]
Feb 8 19:50:04 Debian11 postfix/cleanup[48432]: 0A79F100ED4: message-id=<20240208184947.0A79F100ED4@Debian11>
Feb 8 19:50:04 Debian11 postfix/qmgr[47956]: 0A79F100ED4: from=<jim@beerok.com>, size=348, nrcpt=1 (queue active)
Feb 8 19:50:04 Debian11 postfix/local[48435]: 0A79F100ED4: to=<joe@beerok.com>, relay=local, delay=26, delays=26/0.02/0/0.02, dsn=2.0.0, status=sent (deliver
ed to mailbox)
Feb 8 19:50:04 Debian11 postfix/qmgr[47956]: 0A79F100ED4: removed
root@Debian11:/tmp#
```

(a) Configuration du MDA avec Dovecot :

- **Installation de Dovecot :** Dovecot a été installé pour agir en tant que MDA. Les paquets dovecot-pop3d et dovecot-imapd ont été installés pour permettre la récupération des courriels via les protocoles POP3 et IMAP.

(b) Client lourd avec Evolution :

- **Installation d'Evolution :** Evolution a été choisi comme client lourd, et son installation a été réalisée sur le système Linux.
- **Configuration d'Evolution pour Jim Dalton :** Evolution a été configuré pour le compte de Jim Dalton avec les paramètres appropriés, tels que le nom d'utilisateur, l'adresse de messagerie, le protocole IMAP, l'adresse IP du serveur mail, le port 143 pour la réception, le protocole SMTP, le port 25 pour l'envoi, etc.



- **Désactivation de l'authentification :** L'authentification dans Postfix et Dovecot a été désactivée en ajoutant les variables "smtpd\_use\_tls=no" dans /etc/postfix/main.cf et "disable\_plaintext\_auth=no" dans /etc/dovecot/conf.d/10-auth.conf.
- **Résumé de la configuration du client lourd :** Le client lourd Evolution a été configuré pour interagir avec le serveur de messagerie en utilisant les protocoles IMAP et SMTP.

En conclusion, l'ensemble du processus de configuration du serveur de messagerie inclut la mise en place réussie de Postfix en tant que MSA/MTA, Dovecot en tant que MDA, et Evolution en tant que client lourd, permettant ainsi l'envoi, la réception et la consultation des courriels de manière sécurisée et efficace.

b) Active Directory

Le déploiement d'Active Directory est une étape cruciale dans la gestion des ressources réseau, fournissant un annuaire LDAP pour les utilisateurs et les ordinateurs. Dans le cadre du projet Beerok.com, cette configuration est essentielle pour tous les services réseau Microsoft.

(1) Installation d'Active Directory :

- **Vérification des Paramètres :** Assurez-vous que le nom et les adresses IP du serveur correspondent au cahier des charges.
- **Désactivation de la Carte NAT :** La carte réseau NAT a été désactivée conformément aux spécifications.
- **Ajout du Rôle AD DS :** Utilisez le gestionnaire de serveur pour ajouter le rôle AD DS.
- **Configuration Post-Déploiement :**
  - Nouvelle Forêt : tpN.local
  - Niveau Fonctionnel de la Forêt : Windows Server
  - Mot de Passe de Restauration : Mot de passe Administrateur
  - Nom de Domaine NetBIOS : TPN

*Création des Unités Organisationnelles (OU) :*

Les OU ont été créées dans la console "Utilisateurs et Ordinateurs Active Directory", respectant la structure existante.

(2) Gestion des Groupes :

Suivant la méthode AGLP :

- **Détermination des Stratégies de Comptes :** Identification des stratégies de comptes pour le domaine.
- **Création des Modèles Utilisateurs :** Création de modèles utilisateurs par profil.
- **Création des Comptes Utilisateurs :** Copie des profils utilisateurs pour créer les comptes.
- **Création des Groupes Globaux :** En fonction des besoins de l'entreprise.
- **Placement dans les Groupes :** Les utilisateurs sont placés dans les groupes globaux.
- **Création des Groupes Locaux :** En fonction des ressources réseau.
- **Permissions aux Groupes Locaux :** Définition de permissions sur les partages, le système de fichiers NTFS et les imprimantes.

(3) Création des Répertoires Personnels

:

Dans le cadre du déploiement d'Active Directory pour le projet Beerok.com, la gestion des répertoires personnels constitue une étape essentielle pour assurer la sécurité et la personnalisation des espaces de stockage dédiés aux utilisateurs.

Premièrement, pour garantir une configuration personnalisée des répertoires personnels, l'héritage est désactivé sur ces dossiers. Cette désactivation de l'héritage signifie que les paramètres de sécurité spécifiques à ces répertoires ne seront pas automatiquement transmis aux sous-dossiers ou fichiers qu'ils contiennent. Ainsi, chaque répertoire personnel peut bénéficier de configurations de sécurité distinctes, assurant une gestion fine des autorisations.

Ensuite, des autorisations spécifiques sont ajoutées ou modifiées pour les groupes locaux, assurant un contrôle d'accès précis aux répertoires personnels. Les groupes locaux, tels que

G\_Ventes, G\_Prod, et G\_Dir, se voient attribuer des droits adaptés à leurs besoins respectifs. Par exemple, le groupe G\_Ventes peut recevoir des autorisations en lecture sur le répertoire des ventes, tandis que G\_Dir pourrait obtenir des droits de contrôle total sur le répertoire de la direction.

Cette approche méthodique de gestion des répertoires personnels offre une flexibilité et une sécurité accrues au sein de l'environnement Active Directory de Beerok.com. Chaque utilisateur bénéficie ainsi d'un espace de stockage dédié, configuré selon les besoins spécifiques de son service, tout en garantissant un contrôle d'accès précis et adapté à la structure organisationnelle de l'entreprise.

*(4) Création des Comptes d'Ordinateur :*

Dans cette étape cruciale du déploiement d'Active Directory pour le projet Beerok.com, la création des comptes d'ordinateur est soigneusement planifiée pour garantir une organisation optimale au sein de l'infrastructure réseau.

Tout d'abord, chaque compte d'ordinateur est créé au sein d'une Unité Organisationnelle (OU) distincte. Cette approche permet une gestion plus efficace des objets informatiques, offrant la possibilité d'appliquer des Stratégies de Groupe (GPO) spécifiques à cette catégorie d'objets. L'utilisation d'OU distinctes facilite également la gestion des autorisations et des configurations propres aux comptes d'ordinateur.

Une fois les comptes d'ordinateur créés dans leurs OU respectives, le processus de jonction au domaine est enclenché depuis les clients. Cette opération est réalisée en suivant des étapes simples pour garantir une intégration réussie des postes de travail dans l'environnement Active Directory.

Pour ajouter un ordinateur au domaine, les administrateurs se rendent sur les propriétés système de la machine à intégrer. En accédant à l'onglet "Nom de l'ordinateur" et en cliquant sur "Modifier", ils sélectionnent l'option "Membre d'un domaine" et fournissent le nom du domaine Active Directory, en l'occurrence, "beerok.com". Un message de bienvenue atteste du succès de cette jonction.

L'approche de création des comptes d'ordinateur dans des OUs distinctes avant leur jonction au domaine garantit une organisation claire et une gestion simplifiée au sein de l'infrastructure Active Directory de Beerok.com. Ce processus contribue à l'efficacité opérationnelle et à la facilité de maintenance de l'environnement informatique de l'entreprise.

*(5) Création des Comptes Utilisateurs :*

Création des utilisateurs suivants dans les OU appropriées :

- Joe Dalton - Direction/Siège
- Jack Dalton - Ventes/Showroom
- Jim Dalton - Informatique/Siège
- Averell Dalton - Ventes/Magasin1
- Lucky Luke - Direction/Siège

*c) Configuration RADIUS*

Le déploiement du serveur NPS (Network Policy Server) revêt une importance capitale dans l'établissement d'un système d'authentification et de sécurité pour les connexions à distance. Au cours de ce projet, nous avons exploité l'interface d'administration du serveur NPS pour configurer et gérer les stratégies d'accès réseau, mettant l'accent sur l'authentification centralisée des utilisateurs accédant au réseau de l'entreprise de manière distante.

L'interface d'administration du serveur NPS offre une vue d'ensemble de sa capacité à créer et appliquer des stratégies d'accès réseau spécifiques pour l'authentification RADIUS. La configuration standard a permis de définir le serveur NPS en tant que serveur RADIUS, jouant ainsi un rôle crucial dans la gestion de l'authentification, de l'autorisation et de la comptabilité des connexions VPN ou à distance.

La configuration ciblée indique explicitement que le serveur NPS fonctionnera comme un serveur RADIUS, responsable de la gestion des connexions VPN ou à distance. Cette fonctionnalité a permis la centralisation de l'authentification des utilisateurs, renforçant significativement la sécurité du réseau de l'entreprise.

En résumé, le déploiement du serveur NPS, orienté spécifiquement en tant que serveur RADIUS, pour la mise en place d'un système d'authentification et de sécurité pour les connexions VPN ou à distance, représente une étape essentielle dans la sécurisation des systèmes informatiques dans les environnements d'entreprise modernes. L'interface d'administration du serveur NPS offre des options de configuration standard et avancée, permettant une personnalisation approfondie en fonction des besoins spécifiques de l'entreprise.

*d) Téléphonie*

*Remarque : En raison des contraintes de temps, l'implémentation de la téléphonie n'a pas été achevée. Des solutions futures sont envisageables.*

*e) Stockage en Ligne/Applicatifs*

Le service de stockage en ligne a été mis en place avec Nextcloud, offrant une plateforme collaborative pour le partage de fichiers et la gestion des documents. Cette solution permet un accès sécurisé aux données à partir de divers emplacements.

NextCloud est un service de cloud local déployable sur un serveur ou une infrastructure. Il offre la possibilité de stocker et partager des données en local, assurant ainsi une gestion et une sécurité optimales des données. L'installation de NextCloud a été réalisée sur un système Linux, et le processus d'installation ainsi que les problèmes rencontrés sont expliqués ci-dessous.

**Prérequis d'installation :** Pour installer NextCloud, plusieurs prérequis sont nécessaires, notamment une base de données SQL (choisie ici comme MariaDB), un serveur web (Apache ou nginx, avec Apache2 dans ce cas), et un serveur PHP.

**Installation et configuration de la base de données MariaDB :** Les paquets nécessaires pour le bon fonctionnement de NextCloud ont été installés, couvrant Apache2, MariaDB, et divers modules PHP. La configuration de la base de données MariaDB a débuté par la sécurisation du serveur avec la commande `mysql_secure_installation`. Une base de données a été créée pour NextCloud, et des droits ont été accordés à l'utilisateur 'admin'. Les autorisations ont été mises à jour avec la commande `FLUSH PRIVILEGES`.

```
MariaDB [(none)]> show databases
    -> ;
+-----+
| Database      |
+-----+
| db23nextcloud |
| information_schema |
| mysql          |
| performance_schema |
+-----+
4 rows in set (0,003 sec)

MariaDB [(none)]> GRANT ALL ON db23nextcloud.* TO 'admin'@'localhost' IDENTIFIED BY 'fuel';
Query OK, 0 rows affected (0,016 sec)

MariaDB [(none)]> FLUSH PRIVILEGES;
Query OK, 0 rows affected (0,001 sec)

MariaDB [(none)]> █
```

**Installation de NextCloud :** La version 20.0.5 de NextCloud a été choisie pour assurer la compatibilité avec PHP7.4. Une fois téléchargée, l'archive a été décompressée dans le répertoire /var/www/html du serveur web. Cela permet à NextCloud d'être accessible via l'adresse <http://100.2.99.251/nextcloud>. Les droits des données de NextCloud ont été modifiés pour qu'ils appartiennent à l'utilisateur Apache2 avec la commande **chown -R www-data:www-data /var/www/html/nextcloud**.

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

MariaDB [(none)]> CREATE DATABASE db23nextcloud;
Query OK, 1 row affected (0,000 sec)

MariaDB [(none)]> GRANT ALL ON db23nextcloud.* TO 'usr23nextcloud'@'localhost' IDENTIFIED BY '████████';
Query OK, 0 rows affected (0,001 sec)

MariaDB [(none)]> FLUSH PRIVILEGES;
Query OK, 0 rows affected (0,000 sec)
```

**Vérification de l'accessibilité depuis le réseau :** Une vérification de l'accessibilité du Cloud depuis le réseau a été effectuée en accédant à NextCloud depuis un serveur Windows.

**Choix de la version de NextCloud :** NextCloud 20.0.5 a été choisi en raison de la compatibilité avec la version PHP7.4 disponible sur le serveur Linux. La dernière version (28.0.0) nécessitait une version plus récente de PHP (8.3.1), ce qui n'était pas disponible. Pour cette raison, les versions PHP compatibles ont été installées, et NextCloud 20.0.5 a été déployé.

En résumé, le serveur NextCloud a été déployé sur une infrastructure Linux avec une base de données MariaDB pour assurer le stockage sécurisé des données des utilisateurs. Les versions compatibles de PHP, Apache2, MariaDB, et NextCloud ont été installées pour garantir le bon fonctionnement de l'ensemble du système.



## B. Services Avancés

### a) DAAS : Serveur de Terminaux

Le déploiement du service Bureau à Distance sur un serveur Windows représente une étape clé dans la mise en œuvre d'une infrastructure permettant à plusieurs clients de se connecter simultanément et d'accéder à des applications à distance. Cette solution offre la possibilité d'exécuter des applications gourmandes en ressources directement depuis le serveur, améliorant ainsi la flexibilité et la gestion des ressources.

#### a) Préparation du Serveur TS (Terminal Server):

Avant toute mise en œuvre, il est essentiel de préparer le serveur Terminal Server en installant les composants nécessaires, notamment le Bureau à Distance, l'Accès Web, le Gestionnaire de licences, la Passerelle des services, et le Service Broker TS pour un équilibrage de charge des sessions.

#### b) Installation des Services Bureau à Distance:

- Installer le rôle Services Bureau à Distance sur le serveur Windows, à l'exception du service d'Hôte de virtualisation, en veillant à également installer le serveur NPS (Network Policy Server) lorsque cela est demandé.
- Lors de l'installation des services Bureau à Distance, choisir un "Déploiement standard" et opter pour un "Déploiement de bureaux basés sur une session" pour permettre l'utilisation des "RemoteApp" directement sur le serveur.
- Dans le gestionnaire de serveur, activer le Gestionnaire de licences et la Passerelle des services en sélectionnant le serveur correspondant.
- Dans les "Outils d'administration" > "Terminal Services" (ou "Services Bureau à distance"), accéder au "Gestionnaire de licence des services Bureau à distance".

Vérifier la configuration en s'assurant que le serveur de licences est correctement inscrit dans Active Directory et utilise le protocole SCP (Service Connection Point).

c) Configuration des Utilisateurs et Tests:

- Depuis la console "Utilisateurs et ordinateurs Active Directory", créer un utilisateur dédié, par exemple, TStest, dans le conteneur Users de votre domaine.
- Vérifier la capacité de l'utilisateur à se connecter depuis un poste Windows 10, confirmant ainsi le bon fonctionnement du service Bureau à Distance.

Cette démarche méthodique permet d'établir un environnement Bureau à Distance opérationnel, facilitant la connexion simultanée de multiples utilisateurs et la gestion à distance des applications, renforçant ainsi la flexibilité et la sécurité de l'infrastructure informatique de l'entreprise Beerok.com.

b) Gestion Technique des Bâtiments

*Remarque : En raison des contraintes temporelles, la gestion technique des bâtiments n'a pas été entièrement mise en place. Des développements futurs sont envisagés pour intégrer cette fonctionnalité.*

Malgré les contraintes, l'équipe a réussi à instaurer un stockage collaboratif efficace avec Nextcloud, améliorant ainsi la collaboration et la gestion des documents au sein de l'entreprise. Des plans d'extension et d'amélioration ont été esquissés pour les services qui n'ont pas pu être complètement déployés dans le cadre du projet pédagogique.

## VII. Services Spécifiques aux Magasins et Showroom

### A. Réseau Wi-Fi et Portail Captif

Le réseau Wi-Fi a été étendu grâce à l'utilisation de bornes Linksys, garantissant une connectivité fiable et performante dans les magasins et le showroom. Ces bornes Linksys bleues ont été stratégiquement positionnées pour assurer une couverture optimale, répondant aux besoins spécifiques de chaque zone.



### **B. Connexion Sécurisée au Showroom**

Afin d'assurer un accès sécurisé au réseau Wi-Fi, un portail captif a été mis en place. Ce portail captif permet une authentification contrôlée des utilisateurs, renforçant ainsi la sécurité du réseau. Les politiques d'accès ont été configurées pour garantir une utilisation appropriée des ressources Wi-Fi tout en minimisant les risques liés à une utilisation non autorisée.

## **VIII. Déroulement du Projet**

### **A. Planning et Méthode Kanban**

Pour garantir une gestion efficace du projet, nous avons opté pour la méthode Kanban en utilisant la plateforme Trello. Cela nous a permis de visualiser clairement l'avancement des tâches, d'attribuer des responsabilités et de suivre le flux de travail de manière transparente. En complément, un diagramme de Gantt a été élaboré pour avoir une vision chronologique des différentes phases du projet.

Trello, une plateforme de gestion de projet basée sur la méthode Kanban, a joué un rôle central dans l'orchestration du projet de restructuration du réseau pour Beerok. Cette plateforme offre une structure intuitive, se basant sur des tableaux, des listes et des cartes, adaptée à la gestion transparente et collaborative des différentes phases du projet.

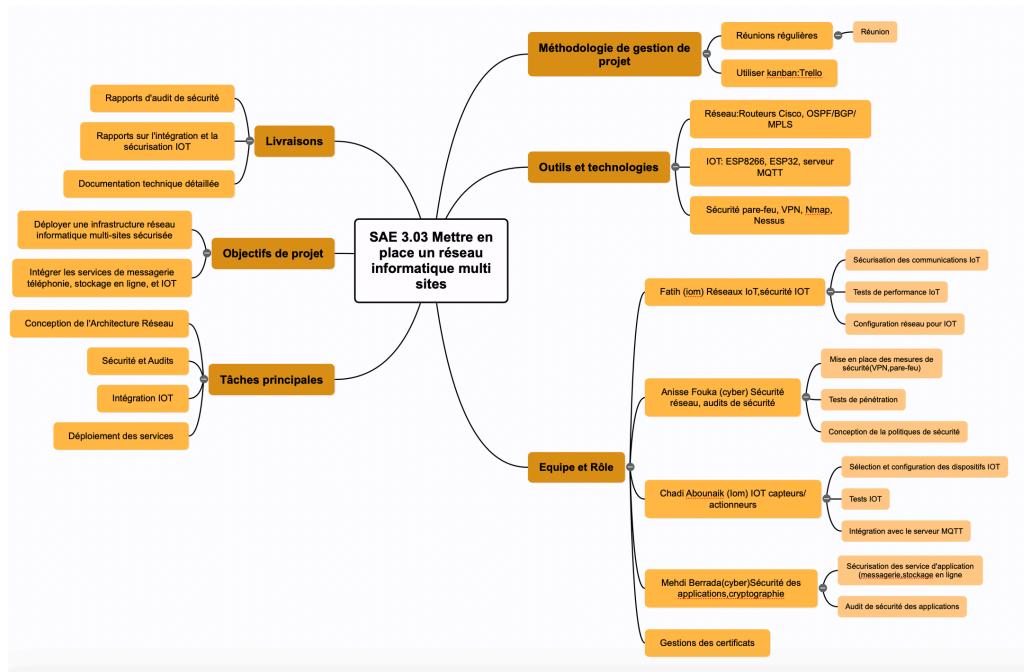
Chaque tableau sur Trello représentait une étape cruciale du projet, comme la planification, la configuration réseau, la sécurité, etc. À l'intérieur de chaque tableau, des listes ont été définies pour marquer les étapes clés du processus, tandis que les cartes représentaient des tâches spécifiques à accomplir.

Les membres de l'équipe, identifiés individuellement, ont utilisé les cartes pour détailler les actions à entreprendre. La capacité de déplacer ces cartes de liste en liste a symbolisé la progression des tâches tout au long du projet. Les commentaires, pièces jointes et échéances associés aux cartes ont facilité la communication et la coordination entre les membres de l'équipe.

Trello a fourni une vue visuelle instantanée de l'état d'avancement du projet, permettant à chaque collaborateur de rester informé et de contribuer de manière collaborative à l'ensemble du processus. Son interface conviviale a favorisé une gestion efficace du temps et des ressources, renforçant ainsi la coordination au sein de l'équipe pour atteindre les objectifs du projet dans le délai imparti.

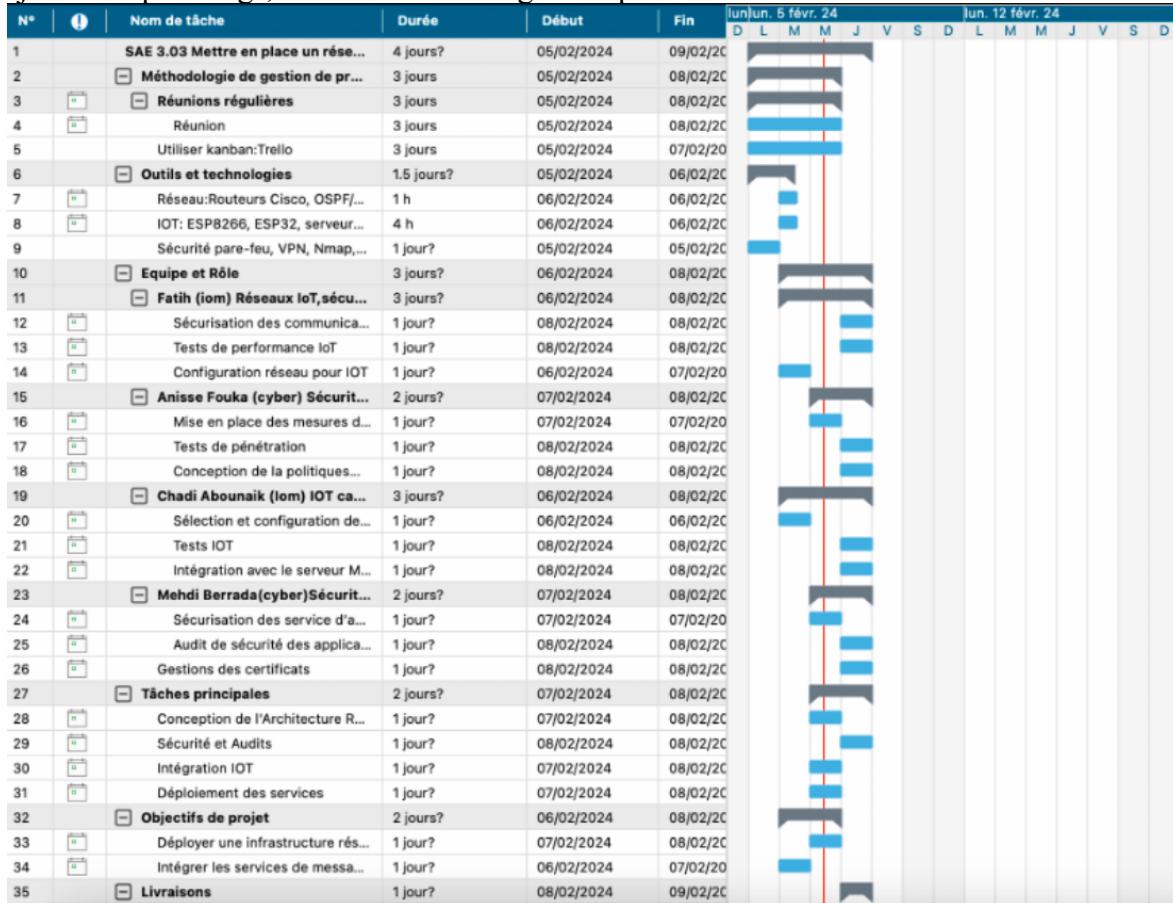
La carte mentale a servi à représenter de manière visuelle les différentes composantes du projet. MindView a offert une interface intuitive pour organiser les idées et les liens entre les différents aspects tels que la planification, la configuration réseau, la sécurité, etc. Chaque branche de la carte mentale représentait une catégorie majeure du projet, et les sous-branches détaillaient les éléments spécifiques à considérer.

L'équipe a pu collaborer de manière efficace en utilisant la carte mentale comme une toile dynamique pour générer des idées, explorer des relations complexes entre les différents éléments et identifier les dépendances entre les tâches.



MindView a également été utilisé pour créer un diagramme de Gantt, permettant de visualiser la planification temporelle du projet. Chaque tâche était représentée sous forme de barre horizontale, avec des dépendances claires entre elles. Cette représentation chronologique a fourni une compréhension approfondie des échéanciers, des retards potentiels et des moments clés du projet.

Les fonctionnalités de glisser-déposer de MindView ont facilité la mise à jour régulière du diagramme de Gantt en fonction des progrès réels du projet. Les membres de l'équipe ont pu suivre et ajuster les plannings, assurant ainsi une gestion proactive des délais et des ressources.



En résumé, Trello a été le pilier de notre gestion de projet, offrant une plateforme visuelle et collaborative basée sur la méthode Kanban. Les tableaux, listes et cartes ont facilité la planification et la communication au sein de l'équipe.

Complémentaire à Trello, MindView a ajouté une dimension visuelle cruciale. La carte mentale a clarifié les idées et les relations complexes, tandis que le diagramme de Gantt a assuré une planification temporelle précise.

Ensemble, ces outils ont été essentiels pour la réussite de notre projet, démontrant l'efficacité d'une approche intégrée de gestion de projet dans un contexte exigeant.

## B. Répartition des Tâches

**Fatih Kılıç :** En charge des objets connectés et de la configuration des routeurs, Fatih a joué un rôle crucial dans l'intégration des dispositifs IoT au sein du réseau. Il a également pris en charge la configuration détaillée des routeurs, assurant ainsi la connectivité et la fluidité du réseau.

**Anisse Fouka** : Responsable de la sécurité du réseau, Anisse a dirigé les efforts visant à garantir la robustesse et l'intégrité du système. Il a également pris en charge la configuration avancée des routeurs, renforçant ainsi les mesures de protection du réseau.

**Mehdi Berrada** : En charge de la sécurité et du déploiement des services réseau, Mehdi a dirigé la mise en œuvre des services de base et avancés. Son rôle a été central dans la concrétisation des fonctionnalités réseau essentielles malgré les contraintes de temps.

**Chadi Abouhnaik** : Responsable des objets connectés et de la configuration des routeurs, Chadi a collaboré étroitement avec Fatih pour garantir l'intégration réussie des dispositifs IoT. Son expertise dans la configuration des routeurs a contribué à l'efficacité opérationnelle du réseau.

## IX. Conclusion

### A. Réalisation des Objectifs

La restructuration du réseau Beerok a atteint ses objectifs pédagogiques malgré le défi temporel. Cependant, la mise en œuvre de la téléphonie a été sacrifiée en raison des contraintes de temps.

### B. Retours d'Expérience

Dans cette expérience intense, chaque membre de l'équipe a pu mettre en avant ses compétences, contribuant ainsi de manière significative à la réussite du projet.

Anisse a exprimé son enthousiasme pour cette opportunité, soulignant que cela a été une expérience enrichissante qui a considérablement amélioré ses compétences.

Fatih trouve que cette SAE a été très enrichissante car nous avons acquis de l'expérience et avons mis en œuvre tout ce que nous avons appris durant nos années de BUT en Réseaux et Télécommunications. Nous avons eu une situation qui se rapprochait le plus du monde professionnel.

Chadi a trouvé la SAE très complète car elle requiert toutes les connaissances acquises depuis le début de la formation et les met directement en relation avec le monde professionnel. Cependant un délai de 3 jours était peut-être un peu court pour mettre en place tous les services et les lier les uns aux autres.