



# Construire un réseau informatique

Module :

**SAE 2.1**

Professeur :

**M'LIK Morad**

Produit par

**RIASAT Asad-Ali, ROUCCOUMANADAN Srikanth, GUERMAT Mohamed-Yacob, HADDADI Kylian et SYLLAH Sankhou**

I.	Introduction	3
II.	Contexte et besoins de l'entreprise	3
III.	Méthodologie et organisation du travail	4
IV.	Conception de l'architecture réseau	5
V.	Plan d'adressage IP	6
VI.	Services réseau déployés	7
▶ DNS		7
▶ HTTP		8
▶ SSH & NFS		8
▶ DHCP		8
VII.	Routage inter-VLAN et translation d'adresses (NAT)	9
VIII.	Sécurisation du réseau	9
IX.	Tests et validation	10
X.	Difficultés rencontrées et solutions apportées	11
XI.	Conclusion	12

## I. Introduction

Dans le cadre de la SAÉ 2.01, notre groupe a été chargé de concevoir et de mettre en œuvre une infrastructure réseau complète pour une entreprise fictive, **GreenHome Solutions**, spécialisée dans les solutions domotiques.

Cette PME dispose de deux sites distants : un siège à Lyon et un atelier à Grenoble. L'objectif du projet était de **proposer une architecture réseau fonctionnelle, sécurisée, évolutive**, et capable de répondre aux besoins concrets d'une entreprise multi-sites.

Ce projet nous a permis de mobiliser de nombreuses compétences acquises au cours du semestre, aussi bien techniques que méthodologiques.

Au-delà de la configuration pure, il s'agissait de réfléchir à l'organisation du réseau, à la segmentation des utilisateurs, à la sécurité des flux, et à la gestion des services essentiels (DNS, HTTP, SSH, DHCP).

Nous avons adopté une démarche structurée, avec une répartition des rôles claire, des outils de collaboration efficaces, et une volonté commune de livrer un réseau réaliste et professionnel.

## II. Contexte et besoins de l'entreprise

**GreenHome Solutions** est une PME fictive spécialisée dans les solutions domotiques écoresponsables.

Elle est répartie sur deux sites géographiques :

- Le **siège social à Lyon**, accueillant principalement la direction, la comptabilité et les équipes commerciales.
- L'**atelier de production à Grenoble**, dédié à la fabrication, à la maintenance et au développement technique.

Les besoins exprimés par l'entreprise sont clairs et typiques d'une structure professionnelle :

- **Interconnexion fiable et sécurisée** entre les deux sites.

- Organisation du réseau en fonction des **différents services** internes (direction, comptabilité, production, etc.).
- Déploiement de **services réseau essentiels** accessibles depuis les deux sites : DNS, serveur web, SSH, DHCP.
- Mise en place d'un **accès Internet contrôlé** via NAT.
- **Sécurisation du réseau** via la segmentation (VLAN) et des règles de filtrage adaptées.
- Possibilité d'assurer une **administration distante sécurisée**.

En résumé, il s'agissait de concevoir un réseau à la fois **structuré, sécurisé, et évolutif**, capable de répondre à des contraintes professionnelles réalistes tout en restant compatible avec notre environnement de simulation.

### III. Méthodologie et organisation du travail

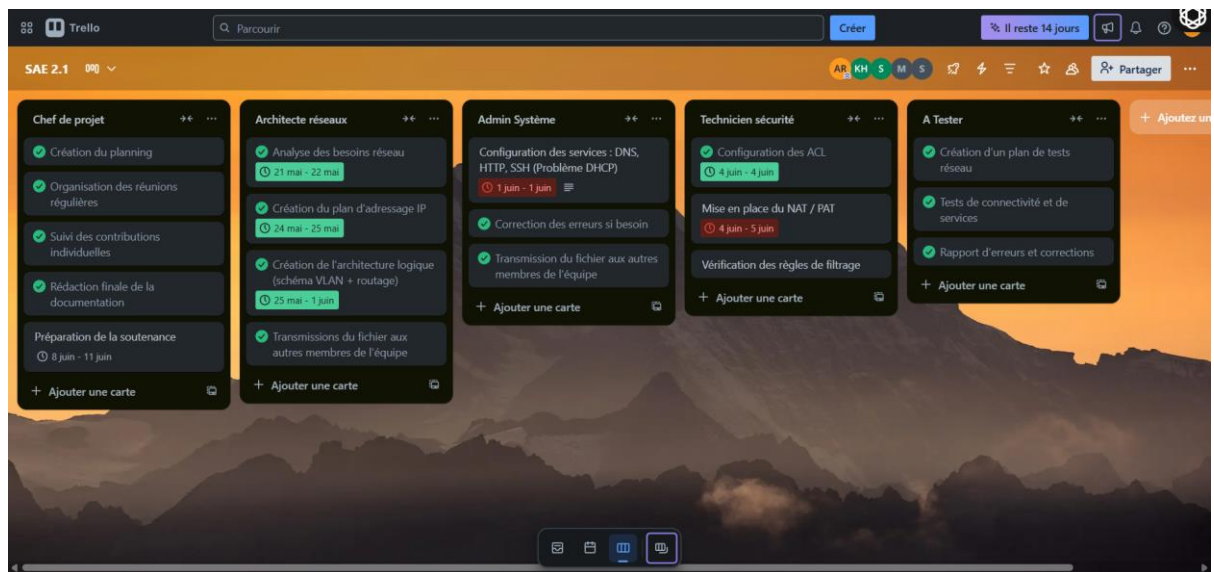
Dès le lancement du projet, nous avons adopté une **démarche de travail collaborative et structurée**, proche des méthodes utilisées en entreprise.

#### ► Répartition des rôles

Chaque membre du groupe s'est vu attribuer un rôle spécifique :

- **Chef de projet** : coordination, planification, suivi des tâches et rédaction finale
- **Architecte réseau** : conception de l'architecture, adressage IP, VLAN
- **Administrateur systèmes** : déploiement des services (DNS, HTTP, SSH, DHCP)
- **Technicien sécurité** : configuration des règles de sécurité (iptables, NAT, routage inter-VLAN)
- **Testeur** : validation technique, rédaction des retours et suivi des anomalies

Afin de suivre l'avancement, nous avons utilisé l'outil Trello, qui nous a permis d'organiser nos tâches selon les rôles et les étapes du projet. Chacun pouvait voir l'état d'avancement des autres, ce qui a favorisé l'autonomie mais aussi la cohésion du groupe. Nous avons également utilisé un groupe de messagerie pour échanger rapidement en dehors des séances encadrées, et tenu des réunions régulières pour faire le point sur les difficultés et réajuster notre travail si nécessaire.



Lien Trello :

<https://trello.com/invite/b/6845aec2096753bc0ce0beb2/ATTI13928a23e1a8d09217da1ac1c282e57d14AAD0EF/sae-21>

Grâce à cette organisation rigoureuse et collaborative, nous avons pu avancer efficacement, éviter les retards, et construire un réseau fonctionnel dans les délais impartis.

## IV. Conception de l'architecture réseau

L'architecture réseau que nous avons conçue repose sur deux sites : **Lyon**, qui héberge la direction, la comptabilité et les équipes commerciales, et **Grenoble**, dédié à la production.

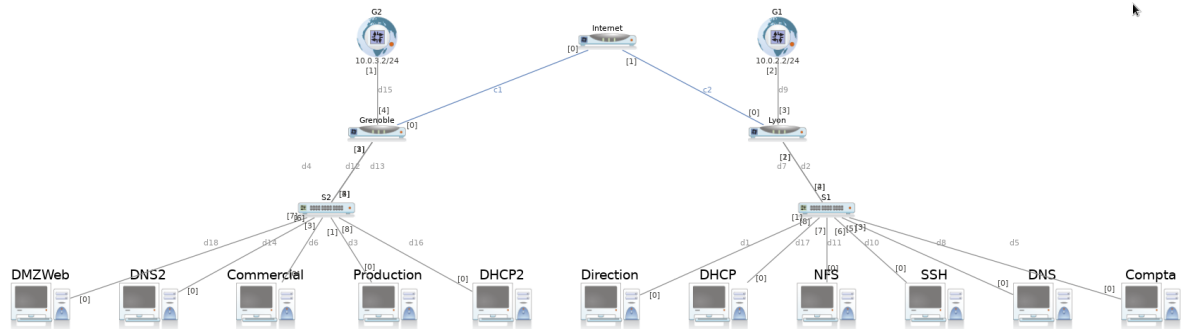
Nous avons construit un **schéma logique** structuré, dans lequel chaque service est isolé dans un **VLAN dédié**, afin de cloisonner les flux et d'améliorer la sécurité du réseau.

Les principaux VLANs sont répartis ainsi :

- VLAN 10 : Direction / Comptabilité
- VLAN 20 : Production
- VLAN 30 : Commercial
- VLAN 40 : Services réseau (DNS, HTTP, SSH)

Chaque site est relié à un **routeur central**, qui assure à la fois le **roulage inter-VLAN** et la **traduction d'adresses (NAT)** pour permettre un accès

Internet sécurisé. L'ensemble a été modélisé dans **Marionnet**, avec des machines virtuelles, des switches, et des liens IP simulés.



Ce schéma logique a servi de base à toutes les configurations suivantes : plan d'adressage IP, déploiement des services et mise en place de la sécurité.

## V. Plan d'adressage IP

Une fois l'architecture réseau définie, nous avons établi un **plan d'adressage IP structuré**, en associant une plage d'adresses spécifique à chaque VLAN.






















L'objectif était de garantir :

- une identification claire des machines par service,
- un routage inter-VLAN efficace,
- et une compatibilité avec le serveur DHCP.

Les VLANs ont été associés aux plages IP suivantes :

- **VLAN 10** (Direction/Comptabilité) → 192.168.10.0/24
- **VLAN 20** (Production) → 192.168.20.0/24
- **VLAN 30** (Commercial) → 192.168.30.0/24
- **VLAN 40** (Services – DNS, SSH, Web) → 192.168.40.0/24
- **VLAN 50** (DMZ Web) → 192.168.50.0/24

Les adresses des passerelles ont été positionnées en .254 pour chaque sous-réseau, afin de rester cohérents avec les conventions classiques.

Nom	Type	Adresse MAC	MTU	Adresse IPv4	Passer
▼ Grenoble					
port0		02:04:06:22:6d:c6	1500	192.168.2.254/24	
port1		02:04:06:89:65:63	1500	192.168.30.254/24	
port2		02:04:06:ed:40:df	1500	192.168.40.254/24	
port3		02:04:06:07:5e:87	1500	192.168.50.254/24	
port4		02:04:06:71:d6:12	1500	10.0.3.254/24	
port5		02:04:06:17:b3:ef	1500		
port6		02:04:06:76:d8:2c	1500		
port7		02:04:06:f7:6b:e9	1500		
▼ Lyon					
port0		02:04:06:fb:47:0e	1500	192.168.1.254/24	
port1		02:04:06:43:63:70	1500	192.168.10.254/24	
port2		02:04:06:e8:2f:00	1500	192.168.20.254/24	
port3		02:04:06:b2:34:7e	1500	10.0.2.254/24	
► Direction					
► Production					
▼ Internet					
port0		02:04:06:cf:52:46	1500	192.168.2.253/24	
port1		02:04:06:43:c2:20	1500	192.168.1.253/24	
port2		02:04:06:24:a1:e9	1500		
port3		02:04:06:9d:0a:c4	1500		

Cette organisation logique nous a permis de configurer les services, le routage et la sécurité de manière fiable et claire.

## VI. Services réseau déployés

Afin d'assurer le bon fonctionnement du réseau, nous avons mis en place plusieurs services essentiels, chacun affecté à un **VLAN spécifique**, selon sa fonction et sa localisation dans l'architecture.

### ► DNS

Le **DNS principal** a été installé dans le **VLAN 20**, sur le site de Lyon. Il assure la résolution de noms internes pour l'ensemble du réseau.

Nous avons également configuré un **DNS secondaire** dans le **VLAN 40**, situé à

Grenoble, afin de garantir une **redondance** en cas d'indisponibilité du serveur principal.

## ► HTTP

Un **serveur HTTP** a été mis en place dans le **VLAN 50**, dédié à la **DMZ**. Il héberge une page web interne, accessible depuis les deux sites. Grâce à la configuration **NAT/PAT** sur le routeur, cette page peut aussi être consultée depuis l'extérieur, simulant un service web exposé.

## ► SSH & NFS

Le **serveur SSH** et le **partage NFS** sont regroupés dans le **VLAN 20** avec le DNS principal. Le SSH permet l'administration distante des serveurs, tandis que NFS permet le **partage de fichiers** entre machines Linux internes, notamment entre les postes de travail de Grenoble.

## ► DHCP

Nous avons configuré **deux serveurs DHCP** pour permettre une gestion locale des adresses IP :

- Le **premier DHCP** se trouve dans le **VLAN 10** (site de Lyon). Il attribue les adresses aux postes de **Direction** et **Comptabilité**.
- Le **second DHCP** est dans le **VLAN 30** (site de Grenoble) et gère la distribution pour les services **Production** et **Commercial**.

Chaque serveur dispose de sa propre configuration, avec des plages d'adresses adaptées, une passerelle spécifique, et une interface réseau configurée dans Marionnet.

```
option domain-name-servers 192.168.10.50;

subnet 192.168.10.0 netmask 255.255.255.0 {
    range 192.168.10.100 192.168.10.200;
    option routers 192.168.10.254;
    max-lease-time 3600;
}
```

```
# On what interfaces should the DHCP server (dhcpcd) serve DHCP requests?
#     Separate multiple interfaces with spaces, e.g. "eth0 eth1".
INTERFACES="eth0"
```

*Figure : Exemple de la configuration DHCP sur le DHCP situé à Lyon.*



Cette configuration répartie permet de **gérer les adresses localement par site**, de **réduire la latence**, et d'assurer la continuité du service même en cas de coupure entre les deux sites.

## VII. Routage inter-VLAN et translation d'adresses (NAT)

La communication entre les différents VLANs et entre les deux sites de GreenHome Solutions a été rendue possible grâce à la mise en place d'un **routage inter-VLAN** via un routeur central.

Ce routeur, configuré dans Marionnet, dispose d'une interface connectée à chaque VLAN. Il agit comme **passerelle** entre les sous-réseaux, permettant aux machines de services différents de communiquer selon des règles précises.

Nous avons activé le **routage IP** au niveau du système (`net.ipv4.ip_forward=1`) et configuré manuellement les sous-interfaces et les passerelles (`.254`) pour chaque VLAN.

Des routes statiques ont également été ajoutées si nécessaire pour garantir la communication entre les deux sites.

En parallèle, nous avons mis en place un **NAT (Network Address Translation)** simple, permettant aux postes du réseau interne d'accéder à Internet à travers une seule adresse publique simulée.

Cette configuration a été effectuée avec **iptables**, en définissant une règle de **masquerading** sur l'interface de sortie.

Le NAT permet de masquer les adresses privées des clients, tout en autorisant la sortie vers l'extérieur, ce qui renforce la sécurité.

Le couple **routage + NAT** est donc au cœur du fonctionnement de notre réseau : il permet à la fois l'ouverture contrôlée entre les services internes et l'accès au Web, sans compromettre l'isolement ou la sécurité des machines internes.

## VIII. Sécurisation du réseau

La sécurité du réseau était un enjeu majeur dans la conception de l'infrastructure de GreenHome Solutions. Pour garantir un fonctionnement fiable et limiter les risques d'accès non autorisés, plusieurs mécanismes ont été mis en place.

La première couche de sécurité repose sur la **segmentation en VLANs**, qui permet de cloisonner les flux entre les différents services : la direction, la production, les services réseau, la DMZ, etc.

Ainsi, un poste du VLAN de production ne peut pas communiquer directement avec un poste de la direction, sauf si le routage est explicitement autorisé.

Le **protocole SSH**, utilisé pour l'administration distante, a été configuré avec des restrictions d'accès. Seules certaines machines internes peuvent s'y connecter, et les ports non nécessaires ont été désactivés pour limiter la surface d'attaque.

La protection la plus fine a été assurée par l'utilisation de **iptables**, configuré manuellement sur les machines sensibles, notamment les serveurs et le routeur. Nous avons mis en place des règles de filtrage strictes :

- blocage de tout trafic entrant par défaut (DROP)
- autorisation explicite de certains ports : 22 pour SSH, 80 pour HTTP, 53 pour DNS
- interdiction des flux inutiles ou suspects

Enfin, l'utilisation du **NAT** (simple) permet également de renforcer la sécurité en **masquant les adresses privées** des clients internes : seules les machines autorisées peuvent sortir vers Internet via l'adresse publique simulée du routeur.

Grâce à cette combinaison – VLANs, filtrage iptables, contrôle du SSH et NAT – nous avons mis en place un réseau à la fois **fonctionnel et protégé**, répondant aux exigences d'une petite structure professionnelle.

## IX. Tests et validation

Tout au long du projet, nous avons réalisé des tests à chaque étape de configuration pour nous assurer du bon fonctionnement du réseau et des services.

Pour la **connectivité**, nous avons utilisé la commande ping entre des machines de VLAN différents et entre les deux sites (Lyon ↔ Grenoble) pour vérifier le bon fonctionnement du routage inter-VLAN et la liaison inter-sites.

Concernant les **services**, plusieurs tests ont été réalisés :

- Pour le **DNS**, nous avons utilisé dig ou nslookup pour vérifier la résolution de noms internes à partir des postes clients.
- Le **serveur HTTP** a été testé en accédant à la page web via un navigateur ou un curl depuis un autre poste.
- Le **serveur DHCP** a été testé en redémarrant les clients pour s'assurer qu'ils recevaient bien une adresse IP adaptée à leur VLAN.
- Les connexions **SSH** ont été vérifiées avec succès depuis les machines autorisées, et refusées depuis les non-autorisées.

Enfin, nous avons aussi testé les **règles iptables** en simulant des flux bloqués (ex : ping bloqué depuis un VLAN non autorisé) pour confirmer que le filtrage était bien actif.

Ces tests nous ont permis de valider toutes les fonctionnalités prévues, et d'identifier rapidement les erreurs à corriger lors des phases de configuration.

## X. Difficultés rencontrées et solutions apportées

Comme tout projet technique, la mise en place de notre infrastructure réseau n'a pas été sans obstacles. Ces difficultés ont été autant d'occasions de **renforcer notre compréhension du réseau** et de **travailler en équipe pour les résoudre**.

L'un des premiers problèmes rencontrés concernait le **serveur DHCP**. Sur certains postes clients, la requête DHCPDISCOVER tournait en boucle sans recevoir de réponse. Après plusieurs vérifications, nous avons identifié une erreur dans le script de configuration du serveur. En modifiant les options réseau et en redémarrant correctement l'interface dédiée, nous avons pu corriger le comportement et rétablir l'attribution automatique d'adresses IP.

Nous avons également rencontré des difficultés lors de la **configuration d'iptables**. Certaines règles, mal ordonnées, bloquaient des flux pourtant autorisés, notamment les connexions SSH. Après avoir analysé les journaux (log), nous avons ajusté l'ordre des règles et restreint les autorisations de manière plus précise, ce qui a permis de maintenir la sécurité tout en assurant le bon fonctionnement des services.

Enfin, une erreur de **routage inter-VLAN** empêchait initialement la communication entre certains VLANs. Après vérification des sous-interfaces du routeur et des tables de routage, nous avons corrigé les adresses de passerelle mal positionnées et relancé le service de routage.

Ces incidents nous ont appris à diagnostiquer méthodiquement, à tester étape par étape, et à travailler de manière rigoureuse. Ils ont renforcé notre capacité à

collaborer efficacement et à adapter nos configurations en fonction des problèmes rencontrés.

## XI. Conclusion

Ce projet de mise en place d'un réseau pour une structure multi-site nous a permis de mobiliser et de croiser de nombreuses compétences acquises au cours de notre formation.

Nous avons travaillé sur des aspects techniques concrets comme l'adressage IP, la segmentation par VLAN, le routage, la configuration de services réseau et la sécurisation à l'aide de pare-feu et de translation d'adresses.

Mais nous avons également appris à organiser notre travail, à collaborer efficacement, à documenter nos choix et à faire face à des situations imprévues.

Par exemple, la configuration du DHCP, qui a initialement échoué à distribuer des adresses, nous a appris à **identifier un dysfonctionnement réseau**, à **remonter jusqu'à la cause**, et à le résoudre de manière propre.

La gestion des règles iptables nous a confrontés à la complexité d'un pare-feu réel, et nous a obligés à **mettre en place une logique de filtrage rigoureuse**, comme ce serait le cas dans une PME souhaitant sécuriser ses accès externes.

Ce projet nous a ainsi préparés à intervenir dans des situations professionnelles concrètes, où il faut à la fois **maîtriser les outils**, **travailler en équipe** et **réagir rapidement à des incidents techniques**.

Il nous a donné un aperçu réaliste de ce que peut être le rôle d'un technicien réseau dans une entreprise : rigoureux, polyvalent, mais aussi méthodique et capable d'adaptation.