

Version 1.3

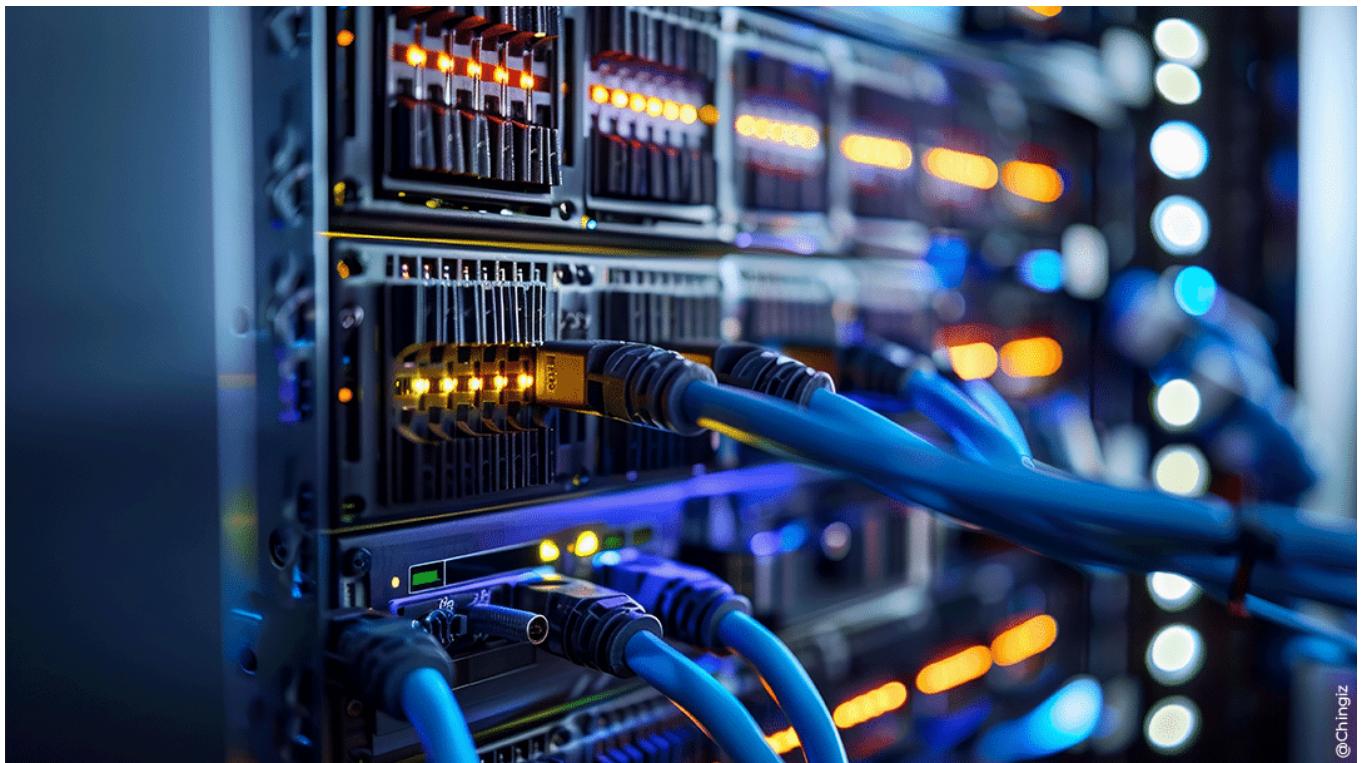
# Plan de sécurité

## Mairie de Maisons-Alfort

---



ROBUSTSÉCURITÉ



@Chingiz

Auteur : Malki Marwan, Bhrami Yazid, Mendil Hamza

Année 2025-2026

---

# Sommaire

<b>Sommaire</b>	<b>2</b>
<b>1. Introduction</b>	<b>3</b>
<b>2. Contexte du projet</b>	<b>3</b>
<b>3. Objectifs techniques</b>	<b>4</b>
<b>5. Topologie du réseau</b>	<b>6</b>
<b>6. Étapes de la réalisation</b>	<b>6</b>
6.1. Création des VLANs	6
6.2. Attribution des ports aux VLANs	7
6.3. Sécurisation des ports (Port Security)	8
6.4. Routage inter-VLAN	8
6.5. Plan d'adressage IP	9
<b>7. Simulation d'un IDS</b>	<b>10</b>
<b>8. Tests réalisés et vérification du fonctionnement</b>	<b>10</b>
<b>9. Charte informatique</b>	<b>11</b>
<b>10. Conclusion</b>	<b>11</b>
<b>11. Annexe</b>	<b>13</b>
11.1 Schéma Réseaux (fichier PKT inclus dans l'image)	13
11.2 Plan d'adressage IP	14
11.3 Attributions des ports dans les VLAN's	15
11.4 Désactivation des ports non utilisé	16
11.4 Autorisation d'une adresse mac par port utilisée	17
11.5 Activation du mode trunk	18
11.6 Bloque les protocoles non-utilisés	19
11.7 Routage inter-VLAN	19
11.8 Syslog (système de logs)	20

---

## 1. Introduction

Dans le cadre de sa démarche d'amélioration continue, la Mairie de Maisons-Alfort a exprimé le besoin de renforcer la sécurité de son réseau informatique. Cette demande concerne particulièrement une salle d'exposition ouverte au public, où sont présents des équipements réseau critiques, installés sans réelle protection physique.

Consciente des risques potentiels, tant externes qu'internes, la mairie a sollicité notre société, **Robustsecurité**, pour évaluer la situation, identifier les failles existantes et proposer des solutions réalistes, adaptées à son environnement.

Ce document présente l'approche suivie tout au long du projet, de la phase d'analyse jusqu'à la mise en place d'une simulation réseau sous Cisco Packet Tracer. Il vise à fournir une vision claire du travail réalisé, tout en servant de support technique aux équipes chargées de la gestion et de la maintenance du réseau.

## 2. Contexte du projet

La Mairie de Maisons-Alfort met à disposition de ses administrés une salle d'exposition ouverte au public. Dans cette salle, un local technique, actuellement non sécurisé, contient des commutateurs réseau connectés à l'infrastructure interne de la mairie.

Lors de notre visite sur site, nous avons constaté que ce placard, qui abrite la baie de brassage principale, est accessible sans restriction, ce qui constitue un risque important pour la sécurité du réseau. Cette situation peut permettre à un individu

---

---

malveillant, ou simplement mal informé, d'ajouter des équipements (comme un switch non autorisé), de détourner des connexions, voire d'interrompre les services informatiques municipaux.

Jusqu'à présent, l'attention portait principalement sur les attaques provenant d'internet. Toutefois, les menaces internes sont tout aussi critiques : elles peuvent provenir d'un collaborateur mécontent, d'une négligence, ou d'un accès non maîtrisé.

Face à ces constats, la mairie a sollicité une expertise technique afin de :

- mieux protéger les équipements existants,
- limiter les risques liés à l'accès physique,
- et améliorer l'organisation du réseau, sans pour autant impacter son bon fonctionnement.

Le projet consiste donc à concevoir une solution réseau sécurisée, évolutive et adaptée aux contraintes du terrain, tout en restant simple à administrer.

### **3. Objectifs techniques**

L'objectif de ce projet est de sécuriser et segmenter le réseau interne de la Mairie de Maisons-Alfort, en agissant exclusivement sur la configuration des switches. L'enjeu principal consiste à assurer l'intégrité et la disponibilité du réseau tout en réduisant les risques d'accès non autorisés.

Pour atteindre cet objectif, plusieurs actions ont été définies. La première consiste à mettre en place une segmentation logique grâce aux VLANs, afin de séparer les flux selon les

---

---

usages : serveurs, personnel administratif, visiteurs et collaborateurs techniques. Cette organisation permet de limiter les interactions non souhaitées et de renforcer la sécurité des données.

La deuxième étape repose sur la sécurisation des ports d'accès. L'utilisation de la fonctionnalité Port Security permet de contrôler les périphériques autorisés, d'empêcher l'ajout d'équipements non conformes et de bloquer automatiquement les interfaces en cas d'anomalie. De plus, les ports inutilisés sont désactivés et placés dans un VLAN isolé, garantissant une meilleure maîtrise de l'infrastructure.

Enfin, une réflexion sur la continuité de service a été menée. L'ajout éventuel d'un second switch, relié au premier par des liens redondants protégés par RSTP, permettrait d'améliorer la résilience et de limiter l'impact d'une panne matérielle.

Ces mesures, associées à un suivi régulier et à une supervision adaptée, garantissent un réseau plus fiable, plus sûr et mieux organisé pour répondre aux besoins de la mairie.

## 4. Sécurisation du matériels internes

Au-delà des aspects purement techniques, la sécurité du réseau dépend également de la protection physique des équipements. Lors de l'analyse des locaux, il a été constaté que les commutateurs sont installés dans un placard accessible au public, ce qui représente une faille majeure.

La première action recommandée consiste donc à sécuriser le local technique. L'accès doit être limité par une fermeture à clé ou un système de contrôle d'accès par badge. L'installation d'une vidéosurveillance ou d'un système de détection d'intrusion renforcerait encore cette protection.

En complément, un inventaire précis des équipements doit être tenu à jour, avec un étiquetage clair des ports et des câbles. Cela permet de réduire les erreurs lors des manipulations et de mieux contrôler l'infrastructure.

La combinaison de la sécurité physique et des mesures logiques mises en place sur les switches (VLANs, Port Security, désactivation des ports inutilisés) garantit une meilleure

---

---

protection contre les risques internes, qu'il s'agisse de négligence, d'erreurs humaines ou de tentatives malveillantes.

## 5. Topologie du réseau

La topologie adoptée est une topologie en étoile. Le premier switch est configuré avec deux VLANs : un pour les visiteurs et un pour le personnel. Le second switch est utilisé pour connecter le serveur. Les équipements sont reliés aux switches qui jouent le rôle de nœud central.

Un schéma de la topologie est disponible dans l'annexe

## 6. Étapes de la réalisation

Cette partie décrit l'ensemble des actions techniques réalisées pour concevoir et sécuriser le réseau de la salle d'exposition de la Mairie de Maisons-Alfort. L'objectif principal est de structurer le réseau à l'aide de VLANs, de sécuriser les ports d'accès et d'assurer une communication maîtrisée entre les différentes zones.

---

### 6.1. Création des VLANs

La première étape consiste à mettre en place la segmentation logique du réseau à l'aide des **VLANs** (Virtual Local Area Networks).

---

---

Cette configuration permet de séparer les flux réseau selon le type d'utilisateur ou de service, garantissant ainsi une meilleure sécurité et une gestion simplifiée.

Les VLANs suivants ont été créés sur le switch principal :

- **VLAN 10 - SERVEURS** : regroupe les équipements critiques (serveurs applicatifs, serveurs de fichiers, etc.).
- **VLAN 20 - PERSONNEL** : réservé au personnel administratif.
- **VLAN 30 - VISITEURS** : attribué aux utilisateurs invités ou externes.

---

Cette segmentation logique constitue la base de la politique de sécurité interne. Elle permet d'éviter les communications directes entre les différents services et de mieux maîtriser la propagation du trafic réseau.

---

## 6.2. Attribution des ports aux VLANs

Une fois les VLANs créés, les ports physiques du switch ont été attribués à chaque réseau en fonction de leur usage.

Le plan d'attribution est le suivant :

- **Fa0/1** : Serveur → VLAN 10
- **Fa0/2 - Fa0/3** : Personnel administratif → VLAN 20
- **Fa0/4 - Fa0/5** : Visiteurs → VLAN 30

---

Chaque port est configuré en **mode access** afin d'empêcher toute tentative de transformation en lien trunk. Cela renforce la sécurité en interdisant à un utilisateur d'introduire un commutateur tiers ou un appareil intermédiaire non autorisé.

---

### 6.3. Sécurisation des ports (Port Security)

Pour éviter toute connexion indésirable ou ajout de matériel non autorisé, la fonction **Port Security** a été activée sur chaque port utilisateur.

Cette fonctionnalité permet de contrôler le nombre d'adresses MAC autorisées par port et de bloquer automatiquement la connexion en cas de tentative suspecte.

La configuration retenue repose sur les principes suivants :

- **Limite d'une seule adresse MAC par port** pour éviter le branchement de plusieurs appareils sur la même prise réseau.
- **Mode de violation : shutdown**, entraînant la désactivation automatique du port en cas d'intrusion.
- **Apprentissage automatique (sticky MAC)** afin d'enregistrer l'adresse MAC légitime de l'appareil connecté.

De plus, les ports inutilisés ont été mis en mode « shutdown » pour interdire toute utilisation non prévue.

Grâce à ces mesures, chaque prise réseau est désormais sécurisée et contrôlée, ce qui limite fortement les risques de compromission interne.

---

### 6.4. Routage inter-VLAN

---

---

Le routage inter-VLAN n'a pas été modifié dans ce projet, car l'objectif était d'agir uniquement sur la configuration des switches.

Le routage existant, déjà opérationnel au niveau du routeur, permet la communication entre les différents réseaux logiques lorsque cela est nécessaire.

Toutefois, une **règle de pare-feu** a été ajoutée sur le routeur afin de **bloquer les requêtes ICMP (ping)** provenant de certains VLANs vers des zones sensibles du réseau, notamment le VLAN des serveurs.

Cette mesure renforce la confidentialité et empêche les utilisateurs non autorisés de sonder ou d'analyser la topologie interne du réseau.

La structure mise en place sur les switches assure donc une segmentation propre, complétée par un contrôle du trafic au niveau du routeur.

En cas d'évolution future, la configuration actuelle permettrait d'intégrer facilement d'autres filtres ou listes de contrôle d'accès (ACLs) selon les besoins de sécurité.

---

## 6.5. Plan d'adressage IP

Afin de maintenir une organisation claire et cohérente, un **plan d'adressage IP structuré** a été défini.

Chaque VLAN dispose de son propre sous-réseau, ce qui facilite l'identification des machines et la gestion du réseau.

VLAN	Nom	Plage d'adresses IP	Passerelle (routeur)
10	SERVEURS	192.168.10.0 /24	192.168.10.254
20	PERSONNEL	192.168.20.0 /24	192.168.20.254

---

---

30 VISITEURS 192.168.30.0 /24 192.168.30.254

Chaque poste de travail, serveur ou terminal connecté reçoit une adresse IP correspondant à son VLAN d'appartenance.

Ce plan d'adressage facilite la maintenance, la supervision et l'évolution du réseau à long terme.

## 7. Simulation d'un IDS

Afin de compléter la sécurisation du réseau de la Mairie de Maisons-Alfort, une **simulation d'IDS (Intrusion Detection System)** a été mise en place dans **Cisco Packet Tracer**.

L'objectif de cette étape est de démontrer la capacité du réseau à détecter des comportements anormaux ou non autorisés, tels que l'ajout d'un appareil inconnu, un balayage d'adresses IP ou un trafic suspect entre VLANs.

## 8. Tests réalisés et vérification du fonctionnement

Des tests ont été effectués sous **Cisco Packet Tracer** afin de vérifier le bon fonctionnement et la sécurité du réseau configuré. Les résultats ont confirmé la conformité de l'ensemble des objectifs techniques.

Tout d'abord, les tests de **connectivité** ont démontré que les équipements d'un même VLAN communiquent correctement. Les postes du VLAN 20 (visiteurs) et du VLAN 30 (personnel) ont échangé des paquets sans erreur, tandis que le serveur du VLAN 10 a répondu aux requêtes du routeur, validant ainsi la stabilité du réseau interne.

---

---

Les tests d'**isolation** ont prouvé que les VLANs sont bien séparés : aucune communication n'a été possible entre les VLANs 20, 30 et 10, garantissant la protection des données et la segmentation du trafic.

Le test du **Port Security** a confirmé l'efficacité du mécanisme de sécurité : lors du branchement d'un appareil non autorisé, le port s'est automatiquement bloqué, empêchant toute intrusion.

La **redondance** a également été validée. Lors de la coupure volontaire de la liaison principale entre les deux switches.

Enfin, la **simulation de l'IDS** a permis de détecter des tentatives d'accès non autorisées et des scans réseau. Le système a généré des alertes, confirmant la bonne surveillance du trafic.

L'ensemble des tests prouve que le réseau de la Mairie de Maisons-Alfort est désormais **fonctionnel, segmenté, sécurisé et tolérant aux pannes**, répondant pleinement aux exigences du projet.

## 9. Charte informatique

La charte informatique définit les règles d'utilisation des outils numériques mis à disposition par la mairie. Elle a pour but d'encadrer les usages afin d'assurer la sécurité des données, la confidentialité des informations et le respect des ressources partagées.

Elle précise également les bonnes pratiques attendues de la part des utilisateurs et fixe les sanctions applicables en cas de non-respect. Elle constitue donc un outil essentiel pour protéger le système d'information et responsabiliser les usagers.

## 10. Conclusion

---

---

À l'issue de ce projet, la Mairie de Maisons-Alfort dispose d'un réseau plus **fiable, structuré et sécurisé**, répondant aux besoins techniques et organisationnels identifiés au départ. L'étude et la mise en œuvre ont permis de renforcer à la fois la **sécurité logique** et la **sécurité physique** du système d'information, tout en garantissant une **meilleure continuité de service**.

La création et la configuration des VLANs ont permis de segmenter efficacement le réseau selon les différents profils d'utilisateurs : serveurs, personnel, visiteurs et collaborateurs. Cette séparation logique améliore la gestion du trafic et limite les risques d'accès non autorisé entre les services.

La mise en place du **Port Security** sur les ports d'accès a permis de protéger le réseau contre les connexions non autorisées et d'assurer un contrôle strict des périphériques connectés. De plus, les tests ont démontré que le réseau réagit correctement en cas de tentative d'intrusion interne ou de branchement d'un appareil inconnu.

Concernant la **redondance**, l'ajout de deux commutateurs reliés entre eux et au routeur assure une continuité de fonctionnement même en cas de panne sur un lien ou un équipement principal. Cette architecture permet d'éviter une coupure totale du réseau et garantit la stabilité des communications.

La **simulation d'un IDS** a permis de compléter cette approche en apportant une couche de détection des anomalies réseau. Le système a su repérer et signaler les comportements suspects, prouvant la pertinence des mécanismes de surveillance mis en place.

Les **tests réalisés** ont confirmé le bon fonctionnement global de l'infrastructure : communication entre les VLANs via le routeur, isolation des segments, sécurisation des ports et maintien du service en cas de défaillance partielle.

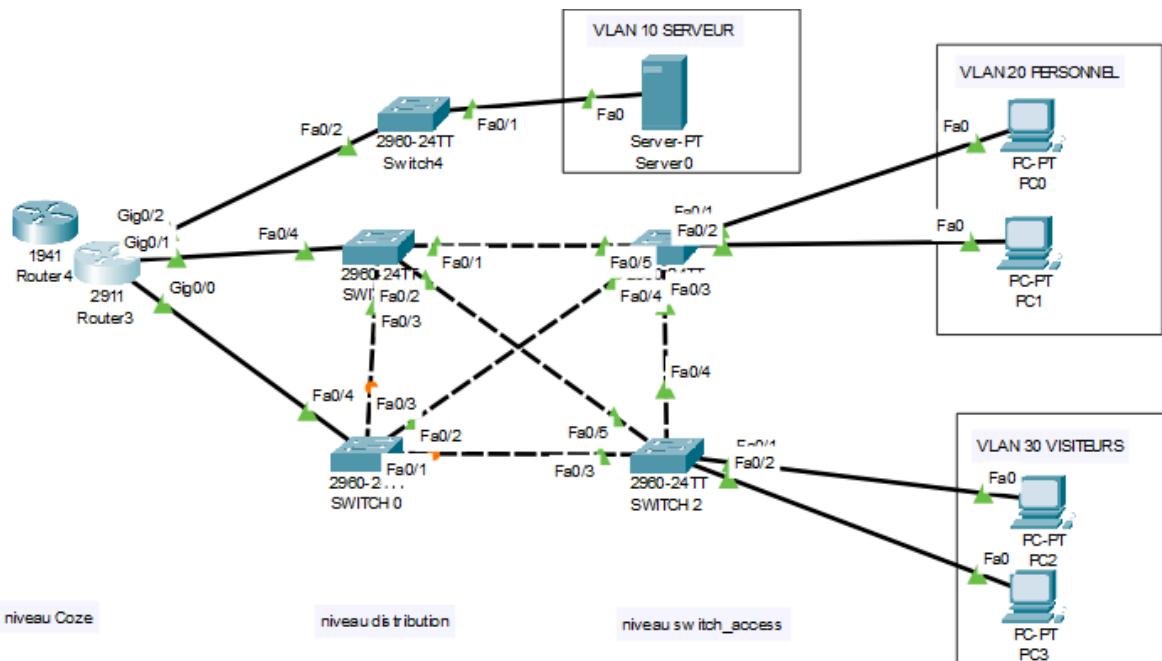
En conclusion, ce projet a permis d'établir une infrastructure réseau **claire, évolutive et sécurisée**, conforme aux bonnes pratiques de gestion et de cybersécurité.

La Mairie de Maisons-Alfort dispose désormais d'un réseau stable, mieux organisé et capable d'évoluer selon les besoins futurs tout en assurant la **sécurité et la fiabilité** de ses services informatiques.

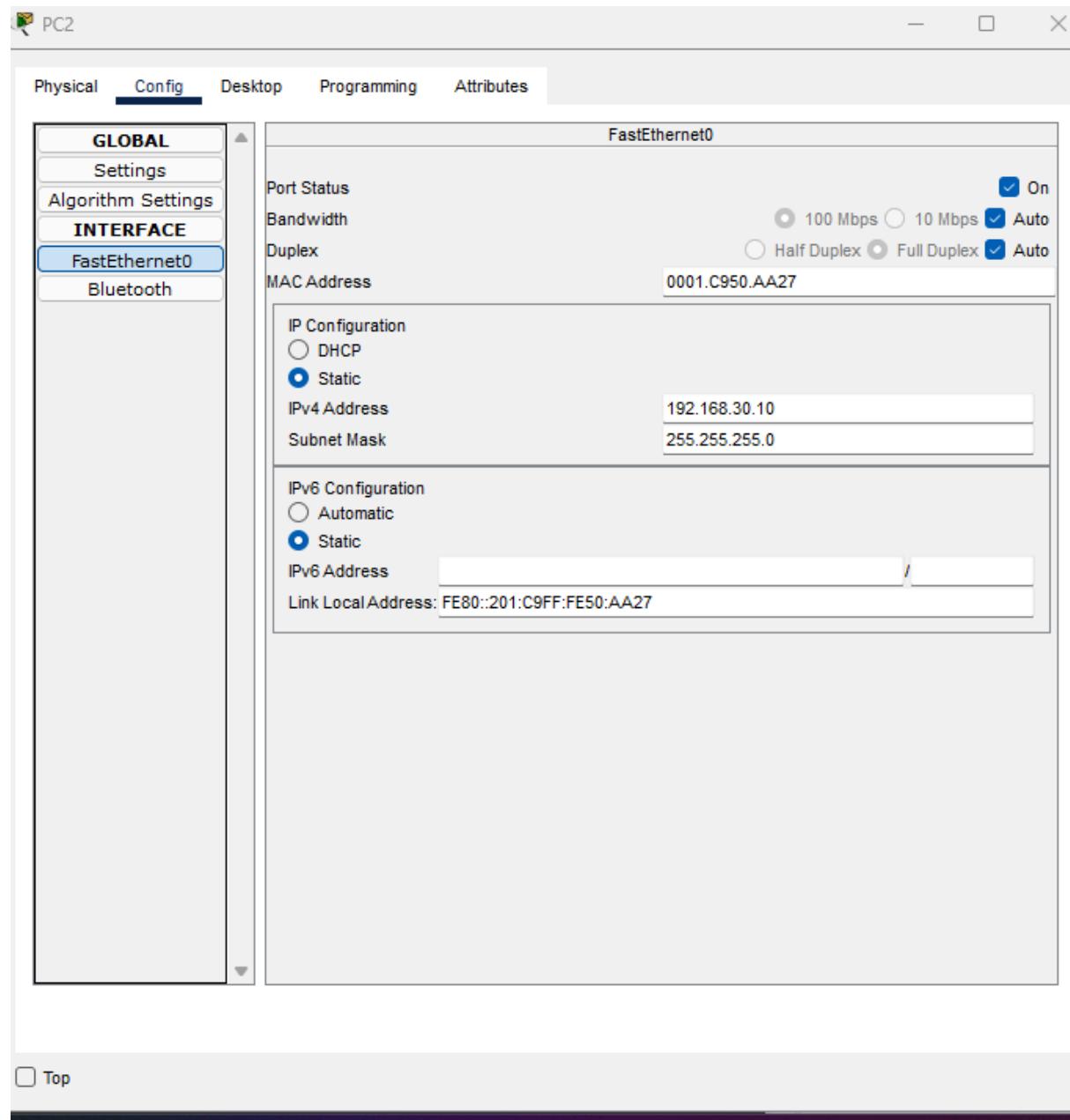
---

# 11. Annexe

## 11.1 Schéma Réseaux (fichier PKT inclus dans l'image)



## 11.2 Plan d'adressage IP



## 11.3 Attributions des ports dans les VLAN's

---

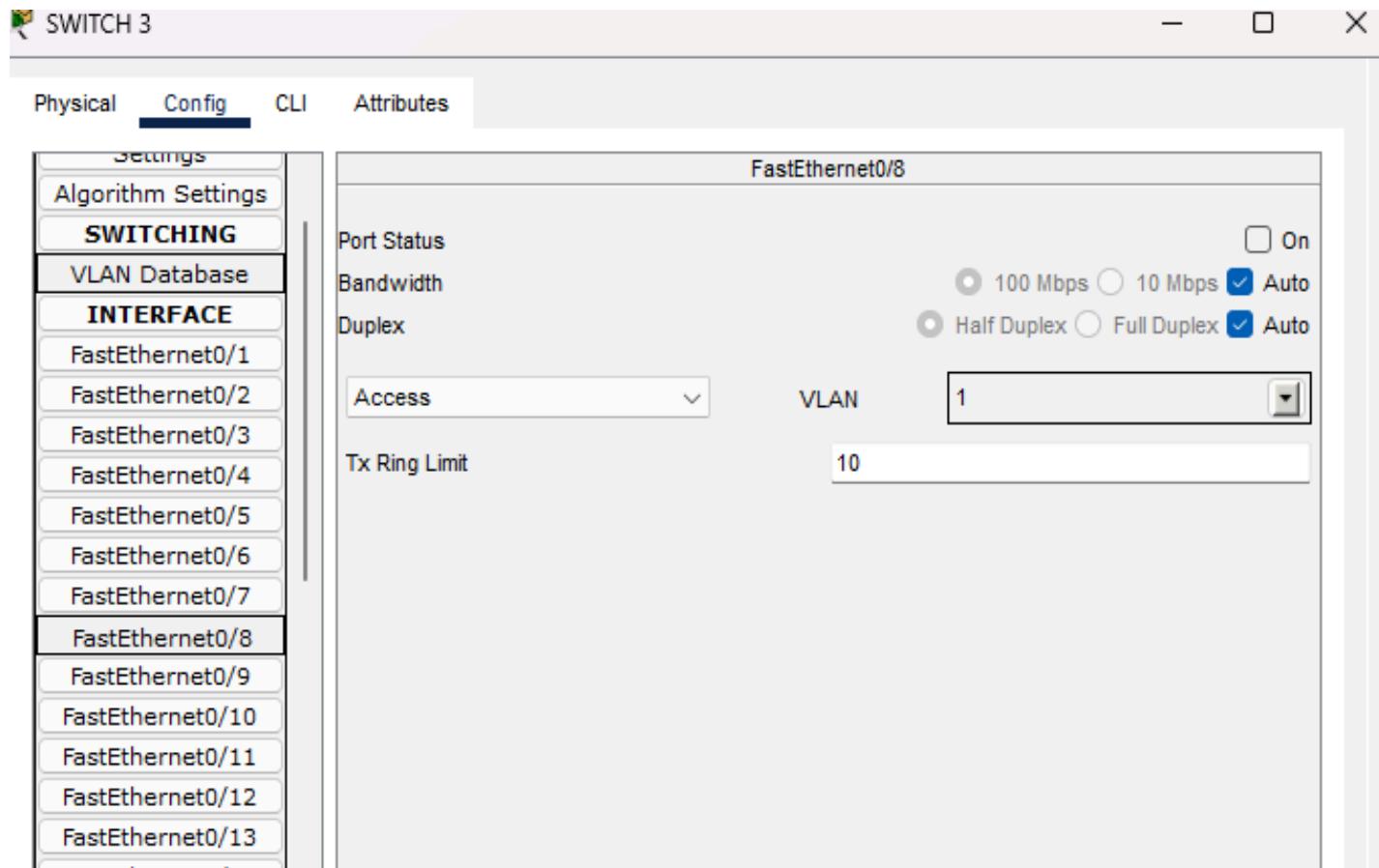
```
Switch(config)#int range fa0/1
Switch(config-if-range)#switchport mode acces
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan 20
Switch(config-if-range)#exit
Switch(config)#exit
Switch#
%SYS-5-CONFIG_I: Configured from console by console

Switch#sh vlan

VLAN Name          Status      Ports
---- -----
1    default        active     Fa0/3, Fa0/4, Fa0/5, Fa0/6
                           Fa0/7, Fa0/8, Fa0/9, Fa0/10
                           Fa0/11, Fa0/12, Fa0/13, Fa0/14
                           Fa0/15, Fa0/16, Fa0/17, Fa0/18
                           Fa0/19, Fa0/20, Fa0/21, Fa0/22
                           Fa0/23, Fa0/24, Gig0/1, Gig0/2
20   Personnel      active     Fa0/1, Fa0/2
```

## 11.4 Désactivation des ports non utilisé

---



## 11.4 Autorisation d'une adresse mac par port utilisée

---

```
Switch(config-if)#exit
Switch(config)#interface range fa0/1 - 2
Switch(config-if-range)#switchport port-security
Switch(config-if-range)#switchport port-security maximum 1
Switch(config-if-range)# switchport port-security violation shutdown
Switch(config-if-range)#switchport port-security mac-address sticky
Switch(config-if-range)#+
```

---

## 11.5 Activation du mode trunk

Physical    **Config**    CLI    Attributes

GLOBAL	
Settings	
Algorithm Settings	
SWITCHING	
VLAN Database	
INTERFACE	
FastEthernet0/1	
FastEthernet0/2	
<b>FastEthernet0/3</b>	
FastEthernet0/4	
FastEthernet0/5	
FastEthernet0/6	
FastEthernet0/7	
FastEthernet0/8	
FastEthernet0/9	
FastEthernet0/10	
FastEthernet0/11	
FastEthernet0/12	

FastEthernet0/3

Port Status  On  
 100 Mbps  10 Mbps  Auto

Bandwidth  
Duplex  
Trunk      VLAN 1  
Tx Ring Limit 10

Equivalent IOS Commands

```
*LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up

Switch(config-if)#switchport mode access
Switch(config-if)#
Switch(config-if)#exit
Switch(config)#interface FastEthernet0/3
Switch(config-if)#
Switch(config-if)#switchport mode trunk

Switch(config-if)#
*LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3, changed state to down
*LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3, changed state to up
```

---

## 11.6 Bloque les protocoles non-utilisés

```
Switch>
Switch>en
Switch#conf t
Enter configuration commands, one per line. End with Ctrl-Z
Switch(config)#no cdp run
Switch(config)#no ip domain-lookup
Switch(config)#end
```

## 11.7 Routage inter-VLAN

```
Router#show ip interface brief
Interface                  IP-Address      OK? Method Status
GigabitEthernet0/0          unassigned     YES unset   up
GigabitEthernet0/0.1        192.168.30.254 YES manual up
GigabitEthernet0/1           unassigned     YES unset   up
GigabitEthernet0/1.1        192.168.20.254 YES manual up
GigabitEthernet0/2           unassigned     YES unset   up
GigabitEthernet0/2.1        192.168.10.254 YES manual up
Vlan1                      unassigned     YES unset   administratively down
```

---

## 11.8 Syslog (système de logs)

---

## Syslog

Service

On

Off

Time	HostName	Message
------	----------	---------