



# Station F Paris

## plan

Résumé exécutif

L'équipe d'ingénierie réseau de **Station F – Paris**, composée de 12 spécialistes en systèmes et réseaux, accompagne les **startups hébergées sur le campus** dans la conception et la modernisation de leurs infrastructures informatiques.

Notre mission s'inscrit dans un contexte d'innovation et de performance, où la **stabilité du réseau**, la **sécurité des données**, et la **connectivité sans faille** sont des priorités stratégiques pour les jeunes entreprises du site.

# Chef d'équipe réseau / Responsable réseau

## Information

---

Email

clement.remoissenets@gmail.com

Address

📍 Paris

## Acteurs de l'entreprise

---

Nom de l'entreprise

STATION F

Industrie

IT & Networking

---

# Acteurs de l'entreprise

Administrateurs Réseaux	1-12 employees ▾
Clients, startups & employés	Over 1000 employees ▾
Taille de l'entreprise	

Administrateurs Réseaux	Brightman
Thomas	Evan
Arthur	Kanikathir
Assa	Diego
Kinsy	Anas
Abdel	Eldelmira

Composants et services à configurer

Les Besoins		
Élément	Rôle	Détail technique
Proxmox VE	Hyperviseur	Création et gestion des machines virtuelles (VM), configuration des bridges réseau, gestion des VLAN.
Stormshield SN	Pare-feu	Routage inter-VLAN, NAT sortant, filtrage des flux, supervision et VPN sécurisé pour accès distant.
ADDS (Windows Server 2025)	Contrôleur de domaine	Gestion centralisée des comptes utilisateurs, attribution d'adresses IP (DHCP), résolution DNS interne, politiques de sécurité de domaine.
FileServer (Windows Server 2025)	Serveur de fichiers (Partage SMB)	Hébergement des fichiers partagés, gestion des droits NTFS selon les groupes Active Directory.
Switchs Cisco	Commutation VLAN	Création et affectation des VLAN 10/20/30, configuration des ports trunk vers le Stormshield et les serveurs Proxmox.
Wi-Fi (Borne Azure)	Accès sans fil mobile	SSID interne isolé, VLAN Wi-Fi dédié, authentification WPA2/Azure, couverture réseau pour les utilisateurs mobiles.

# Objectifs principaux/ Requêtes

- *Centraliser les fichiers sur un serveur de fichiers sécurisé.*
- *Gérer les utilisateurs et les droits via Active Directory (ADDS).*
- *Distribuer automatiquement les adresses IP via DHCP.*
- *Fournir une résolution de noms interne (DNS).*
- *Sécuriser l'accès Internet grâce à un pare-feu Stormshield.*
- *Permettre une connexion Wi-Fi fiable et sécurisée pour les utilisateurs mobiles.*
- *Créer des vlans de 12 startups et les autres acteurs de l'entreprise tels que office, mana, etc.*
- *Mise en place des mesures de sécurité à l'infrastructure.*

## Contraintes techniques

- *Virtualisation : Proxmox VE.*
- *Systèmes d'exploitation : Windows Server 2025, Windows 11 (client).*
- *Segmentation réseau : VLAN distincts pour management, serveurs, invités, Wi-Fi, DMZ.*

- **Sécurité :**
  - **Droits NTFS par groupes AD**
  - **Authentification SSH limitée aux IP du VLAN Mana**
  - **Pare-feu Stormshield configuré en filtrage par zones**
- **Sauvegardes : snapshots automatiques (Proxmox) + sauvegarde partagée sur SRV-FILES.**
- **Documentation : plan IP, VLAN, rôles des VM, configurations Stormshield.**
- **Outils réseau : MobaXterm, PuTTY, RDP, SSH**

# Sécurité et bonnes pratiques

- **Pare-feu Stormshield : routage inter-VLAN, NAT, filtrage par zones, journalisation.**
- **Active Directory : gestion centralisée des comptes, politiques de mot de passe.**
- **Partages : droits NTFS selon les groupes AD.**
- **Wi-Fi : SSID isolé, VLAN dédié, WPA2/Azure.**
- **Switchs : SSH autorisé uniquement depuis VLAN Mana, Telnet désactivé.**
- **Sauvegardes : snapshots Proxmox automatiques, sauvegarde planifiée sur SRV-FILES.**

## Difficultés rencontrées et solutions Globale

Difficulté rencontrée	Description	Solution apportée
<b>Problèmes de routage inter-VLAN</b>	Les machines de différents VLAN (client, serveur, management, Wi-Fi) ne pouvaient pas communiquer entre elles.	Configuration du routage sur le pare-feu Stormshield, vérification des passerelles et des sous-réseaux, tests avec <b>ping</b> et <b>tracert</b> .
<b>Mauvaise attribution DHCP</b>	Les clients ne recevaient pas d'adresse IP ou recevaient une mauvaise passerelle.	Vérification du rôle DHCP sur le serveur AD/DHCP/DNS, définition des portées correctes et activation du relais DHCP si nécessaire.
<b>Résolution DNS incorrecte</b>	Les noms d'hôtes internes n'étaient pas résolus correctement (erreurs d'accès aux partages réseau).	Configuration du DNS interne sur le serveur AD, ajout des enregistrements A et PTR, vidage du cache DNS client.
<b>Accès SSH non fonctionnel sur les switches</b>	Impossible de se connecter en SSH pour l'administration réseau.	Activation du service SSH uniquement sur l'IP de gestion dans le VLAN Mana et ouverture du port 21.
<b>Erreur de configuration Proxmox (VMBR)</b>	Les VM n'avaient pas d'accès réseau ou IP.	Reconfiguration des bridges : un VMBR pour l'administration, un autre pour les VLAN serveurs. Test de la connectivité après redémarrage.
<b>Pare-feu trop restrictif</b>	Certaines communications internes (ex : Proxmox ↔ SRV-FILES) étaient bloquées.	Révision des règles Stormshield, autorisation des flux nécessaires (SMB, DNS, LDAP, DHCP).
<b>Problème de NAT / Internet</b>	Les postes clients n'avaient pas accès à Internet.	Activation du NAT sortant sur le Stormshield pour le VLAN Client, vérification des routes et DNS externe.
<b>Découpage réseau mal défini</b>	VLAN mal isolés ou sous-réseaux mal répartis, entraînant conflits IP et confusion dans la gestion du réseau.	Redéfinition du plan d'adressage et du découpage logique (VLAN Client, Serveur, Mana, Wi-Fi).
<b>Boucles réseau ou erreurs de câblage</b>	Paquets perdus ou réseau instable.	Vérification physique du câblage, activation du Spanning Tree Protocol (STP) sur les switches.

<b>Performance réseau faible</b>	Débits très faibles entre les VM et les clients.	Vérification du duplex et vitesse sur les ports, tests avec <code>iperf</code> , optimisation du trunking VLAN.
<b>Erreur de droits sur les partages SMB</b>	Certains utilisateurs n'avaient pas accès aux bons dossiers.	Configuration des droits NTFS selon les groupes AD (Lecture/Écriture selon rôle).
<b>Conflits d'adressage IP</b>	Deux équipements utilisaient la même IP statique.	Centralisation du plan d'adressage et vérification avec <code>arp -a</code> . Réservation DHCP si nécessaire.
<b>Authentification Proxmox limitée</b>	Un seul compte d'administration est disponible, limitant la traçabilité et la sécurité.	Mise en place d'un compte unique sécurisé avec mot de passe fort et documentation des accès.
<b>Wi-Fi instable</b>	Déconnexions fréquentes et VLAN non appliqué correctement.	Vérification du SSID, VLAN tagging sur le switch, mot de passe WPA2 fort et canal radio fixe.
<b>Sauvegardes mal organisées</b>	Planification des snapshots Proxmox incomplète, risques de perte de données.	Mise en place d'une procédure claire, création de snapshots réguliers et planification de sauvegardes sur SRV-FILES.
<b>Sauvegarde bâclée</b>	Certains dossiers critiques non inclus et restauration non testée.	Vérification et test complet de la restauration, ajout de tous les partages critiques dans le plan de sauvegarde.
<b>Documentation insuffisante</b>	Choix techniques et configurations réseau mal documentés, compliquant la maintenance.	Création d'une documentation complète : plan d'adressage, VLAN, rôle des VM, procédures d'administration et sauvegarde.
<b>Gestion des VLAN côté switch complexe</b>	Certains ports mal configurés ou VLAN non taggés.	Reconfiguration des ports sur les switchs, vérification des trunks et des VLAN assignés.
<b>Mauvaise organisation globale</b>	Planification initiale incomplète, doublons dans les IP et confusion entre VLANs.	Revue complète de l'architecture, documentation et vérification systématique des configurations.



# Sommaire

## LOT 1

*Mettre en place une infrastructure réseau sécurisée, segmentée et performante, conforme aux bonnes pratiques d'administration et de cybersécurité.*

*Ce lot vise à assurer :*

- *la séparation logique des réseaux via des VLANs ;*
- *le routage inter-VLAN et le NAT vers Internet ;*
- *la définition du plan d'adressage IP (logique et physique) ;*
- *la sécurisation des flux grâce à des règles de filtrage réseau ;*
- *et la validation de la connectivité entre les postes, serveurs et Internet.*

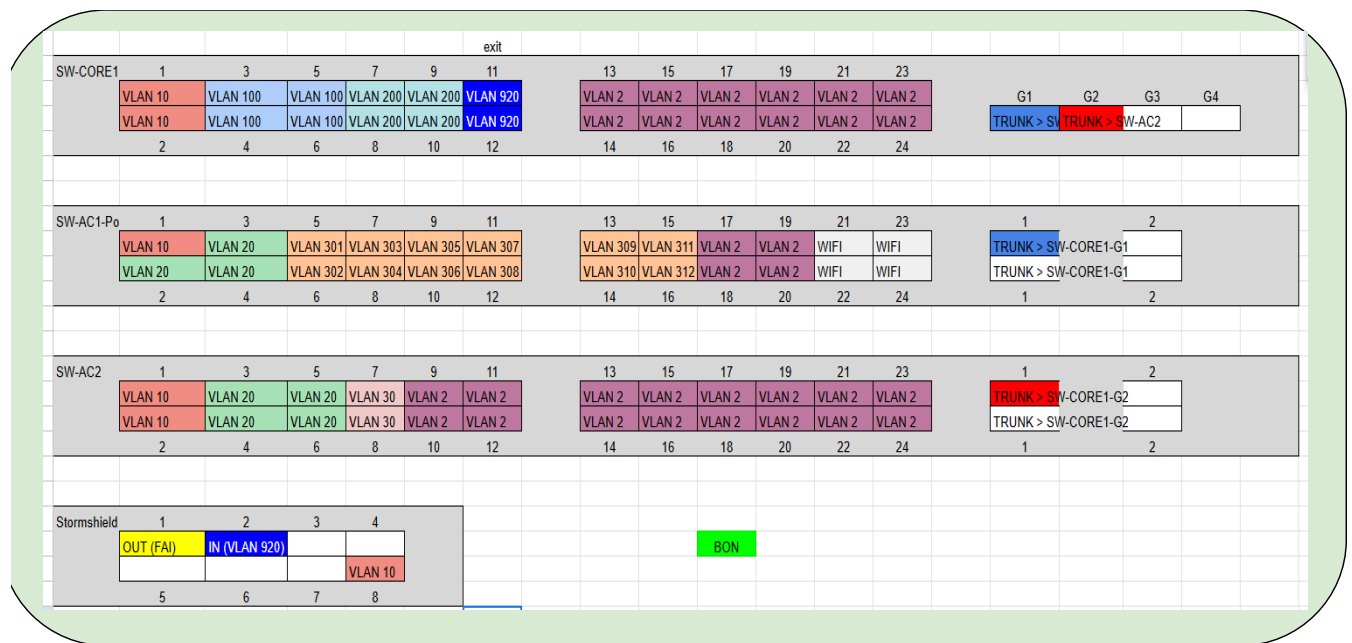
*Ce lot concerne uniquement la couche réseau :*

- *le Switch Core (L3) assurant le routage inter-VLAN ;*
- *les deux switches d'accès (L2) ;*
- *les liens trunk et les ports d'accès ;*
- *le plan d'adressage VLAN ;*
- *et la configuration des règles de sécurité associées.*

**Les Schémas logique et physique**

**Plan Logique**





Les addresses @IP

LES VLANS	NOMS	MASQUE/	@IP SVI	Premier @IP	Dernière @IP
VLAN 10	MANA	172.16.0.0/19	172.16.31.254	172.16.0.1	172.16.31.253
VLAN 20	OFFICE	172.16.32.0/19	172.16.63.254	172.16.32.1	172.16.63.253
VLAN 30	INVITÉS	172.16.192.0/19	172.16.192.254	/N en trunk	/N en trunk
VLAN 100	Public	172.16.96.0/20	172.16.111.254	172.16.96.1	172.16.111.253
VLAN 200	Privés	172.16.96.0/20	172.16.127.254	172.16.112.1	172.16.127.253
VLAN 920	Exit	172.16.254.0/28	172.16.254.0	172.16.254.1	172.16.254.13
VLAN 300	Startups	172.16.64.0/27	/N propre à chacun	/N propre à chacun	/N propre à chacun
VLAN 2	Blackhole	/N	/N	/N	/N

## Les startups AVANT

Les Startups sur sw et core	Les noms	Les @ip
VLAN 301	evan	172.16.64.30
VLAN 302	thomas	172.16.64.62
VLAN 303	assa	172.16.64.94
VLAN 304	arthur	172.16.64.126
VLAN 305	clement	172.16.64.158
VLAN 306	brightman	172.16.64.190
VLAN 307	anas	172.16.64.222
VLAN 308	kinsy	172.16.64.254
VLAN 309	kanikathir	172.16.65.30
VLAN 310	abdel	172.16.65.62
VLAN 311	eldelmira	172.16.65.94
VLAN 312	diego	172.16.65.126

## Le Plan de Nommage

Sw_A1	Sw-Core	Sw-Core	172.16.0.1/19
Sw_A1	Sw-A1	Sw-A1	172.16.0.2/19
Sw_acces-users	Sw-A2	Sw-A2	172.16.0.3/19

## Les Ip attribuée aux périphériques

Elément réseau			
Elément réseau	Nommage	@ IP/MSR	Interface
Switch Acces1 Poe	Sw-A1	172.16.0.3/19	eth 1
Switch Acces2	Sw-A2	172.16.0.2/19	eth1
Switch Core 1	Sw-C1	172.16.31.254/19	
Stormshield	SN310	10.0.0.254/8	eth 3
Active Directory	ADDS2025	172.16.127.253/20	
File Server	fileserv	172.16.127.252/20	
Proxmox 1	proxmox	172.16.31.253/24	EN01
Proxmox 2	proxmox	172.16.31.253/24	EN03
Borne Wifi 1	WIFI_StationF1	172.16.0.251/19	

noms startups				
Startup	Nom	ID	N° VLAN	SVI (passerelle)
Startup 1 digimedia	Evan	200101	301	172.16.64.30
Startup 2 atema	Thomas	200201	302	172.16.64.62
Startup 3 hostit	Assa	200301	303	172.16.64.94
Startup 4 donicharity	Arthur	200401	304	172.16.64.126
Startup 5 antiquecafe	Clément	200501	305	172.16.64.158
Startup 6 elflyer	Brightman	200601	306	172.16.64.190
startup 7 cycle	Anas	200701	307	172.16.64.222
Startup 8 finexo	Kinsy	200801	308	172.16.64.254
Startup 9 restaurant	Kanikathir	200901	309	172.16.65.30
Startup 10 littlefashion	Abdel	201001	310	172.16.65.62
Startup 11 onyxdigital	Eldelmira	201101	311	172.16.65.94
Startup 12 dicet tv	Diego	201201	312	172.16.65.126

## Configuration réseau

Afin de configurer le réseau, nous avons commencé à configurer le switch core.

Premièrement, nous avons mis en place le VTP pour la gestion des VLAN. L'objectif était de centraliser la gestion en configurant les VLAN sur le switch core afin qu'il les distribue sur les switch accès.

Deuxièmement, nous avons mis en place le SSH pour une connexion à distance sécurisée.

\$

L'objectif est de pouvoir se connecter à distance depuis le VLAN management pour administrer les équipements et de se tenir au courant des actions effectuées par techniciens/administrateurs.

Ensuite, nous avons créer les VLAN

*“Au cours de la mise en place de l’infrastructure réseau, j’ai pu renforcer ma compréhension du fonctionnement d’un système d’information : Plan d’adressage ip, segmentation par VLAN, routage inter-VLAN, ACL, SSH, la mise en place de l’ip address- helper donc par l’administration des switchs Core/Access.”-OnyxDigital*

## Les tests

Jeu de test	
Etape	exemple VLAN office
ping sa propre SVI	ping 172.16.63.254
ping une autre SVI	ping 172.16.31.254
ping un serveur	ping 172.16.127.253
ping internet	ping 8.8.8.8

**Les ACL sont appliquées principalement sur le Switch Core (L3) afin de filtrer les flux non autorisés. Tous les flux inter-VLAN passent obligatoirement par le pare-feu Stormshield, garantissant un contrôle complet.**

## LOT 2

### Partie lots 2

Proxmox

Comment créer un utilisateur proxmox

Aller dans pve:

**Sur le shell (en root) →**

```
adduser etudiant
```

1. → ça crée le compte Linux (donc reconnu par PAM).

2. **Ensuite, dans l'interface web de Proxmox (GUI) →**

- Aller dans **Datacenter** → **Permissions** → **Users**

- Cliquer sur **Add** → **User**

- Choisir :

- **User ID** : `etudiant`

- **Realm** : `PAM`

3. **Puis aller dans :**

- **Datacenter** → **Permissions** → **Add** → **User Permission**

- Sélectionner :

- **User** : `etudiant@pam`

- **Path** : `/`

- **Role** : `Administrator`

pour unlock une vm : `qm unlock #n°`

Qui	Login	Mdp_proxmox	mdp_ssh_réseau	
Brightman	brightman	Sio.2026	paris.2026	



Arthur	arthur	Sio.2026	paris.2026	
thomas	thomas	Sio.2026	paris.2026	
Diego	diego	Sio.2026	paris.2026	
Kinsy	kinsys	Sio.2026	paris.2026	
Anas	anas	Sio.2026	paris.2026	
Abdel	abdel	Sio.2026	paris.2026	
Clement	clement	Sio.2026	paris.2026	
Eldelmira	eldelmira	Sio.2026	paris.2026	
Evan	evan	Sio.2026	paris.2026	
Kanikathir	kathir	Sio.2026	paris.2026	
Assa	assa	Sio.2026	paris.2026	

## DHCP

L'objectif suivant était de distribuer automatiquement les adresses IP via un serveur DHCP.

Pour attribuer automatiquement les adresses IP, nous avons créé des étendues DHCP pour les VLAN via la vlan office et pour chaque startup.

La VLAN possède ainsi sa propre plage d'adresses IP définie dans une étendue spécifique, ce qui permet une gestion claire et organisée du réseau.

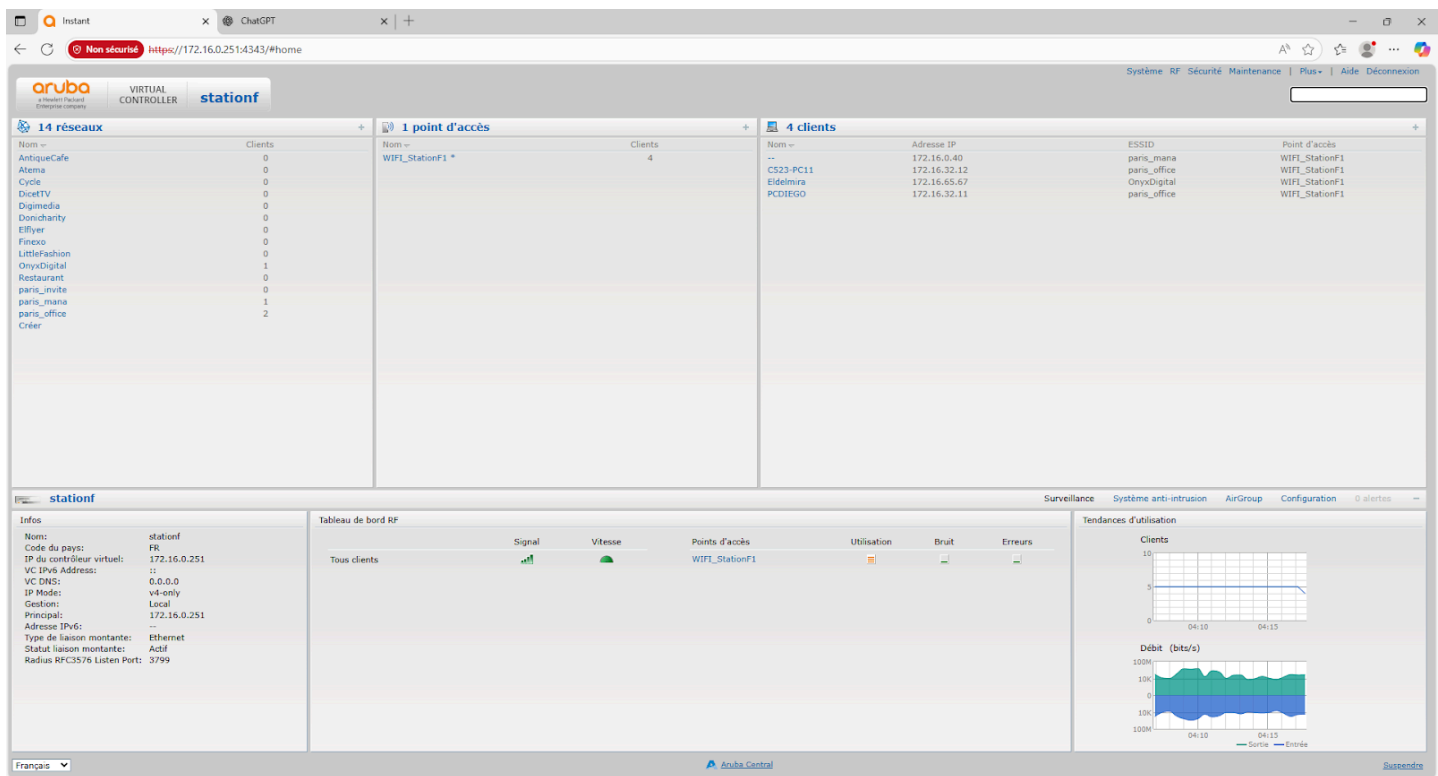
Concernant les startups, nous avons choisi d'utiliser uniquement les dix premières adresses de chaque réseau .

### **Borne WIFI :**

L'objectif de cette manipulation est de mettre en place et superviser un réseau Wi-Fi (172.16.0.251) à l'aide d'un contrôleur virtuel Aruba.

Cette configuration permet de gérer plusieurs réseaux sans fil (SSID), de centraliser l'administration des points d'accès et de surveiller en temps réel les connexions des clients.

L'objectif secondaire est de vérifier la connectivité, la répartition des startups et le bon fonctionnement du point d'accès.



Trois réseaux Wi-Fi (SSID) ont été créés à part les startups et configurés pour différents usages :

- paris\_invite (réseau invité) = ok
- paris\_mana (réseau principal interne) = fixe bon et dhcp pas bon
- paris\_office (réseau de bureau) = bon

## LOT 3

### 1. Création de l'infrastructure Active Directory

Nous avons commencé par créer deux unités d'organisation (UO) :

- Office
- Startup

Dans l'UO Office, nous avons créé deux sous-groupes :

- Administrateurs
- Ressources Humaines (RH)

Ensuite, nous avons ajouté les utilisateurs :

- Pour les administrateurs, des comptes numérotés de 1001 à 1012
- Pour les RH, des comptes numérotés de 10001 à 10002

Dans l'UO Startup, nous avons créé les 12 startups (Startup1 à Startup12), chacune avec ses utilisateurs.  
Par exemple :

- L'utilisateur 200101 appartient à Startup1
- L'utilisateur 201201 appartient à Startup12

## 2. Configuration du serveur de fichiers

Nous avons ensuite configuré le serveur de fichiers en le renommant et en l'intégrant au domaine "paris.stationf".

Des dossiers ont été créés pour :

- Les profils itinérants
- Les données partagées

Les droits NTFS ont été configurés afin d'assurer la sécurité et la gestion des accès aux différents dossiers.

## 3. Problèmes rencontrés

Au cours de la première configuration, nous avons rencontré plusieurs difficultés :

- Changement d'adresses IP, ce qui a entraîné la déconnexion du serveur de l'Active Directory
- Suppression accidentelle de l'Active Directory, nécessitant une reconfiguration complète du système

Nous avons donc dû tout recommencer avec l'aide de Monsieur Pichon, ce qui nous a permis de mieux comprendre le fonctionnement global du réseau et du domaine Active Directory.

noms startups				
Startup	Nom	ID	N° VLAN	SVI (passerelle)
Startup 1 digimedia	Evan	200101	301	172.16.64.30
Startup 2 atema	Thomas	200201	302	172.16.64.62
Startup 3 hostit	Assa	200301	303	172.16.64.94
Startup 4 donicharity	Arthur	200401	304	172.16.64.126
Startup 5 antiquecafe	Clément	200501	305	172.16.64.158
Startup 6 elflyer	Brightman	200601	306	172.16.64.190
startup 7 cycle	Anas	200701	307	172.16.64.222




Startup 8 finexo	Kinsy	200801	308	172.16.64.254
Startup 9 restaurant	Kanikathir	200901	309	172.16.65.30
Startup 10 littlefashion	Abdel	201001	310	172.16.65.62
Startup 11 onyxdigital	Eldelmira	201101	311	172.16.65.94
Startup 12 dicet tv	Diego	201201	312	172.16.65.126

noms startups				
Startup	Nom	ID	MDP	N° VLAN
Startup 1 digimedia	Evan	200101	Sio2026	301
Startup 2 atema	Thomas	200201	Sio2026	302
Startup 3 hostit	Assa	200301	Sio2026	303
Startup 4 donicharity	Arthur	200401	Sio2026	304
Startup 5 antiquecafe	Clément	200501	Sio2026	305
Startup 6 elflyer	Brightman	200601	Sio2026	306
startup 7 cycle	Anas	200701	Sio2026	307
Startup 8 finexo	Kinsy	200801	Sio2026	308
Startup 9 restaurant	Kanikathir	200901	Sio2026	309
Startup 10 littlefashion	Abdel	201001	Sio2026	310
Startup 11 onyxdigital	Eldelmira	201101	Sio2026	311
Startup 12 dicet tv	Diego	201201	Sio2026	312

SESSION			
administrateur /rh	Qui	ID	MDP
administrateur	arthur	1001	Sio2026
administrateur	Thomas	1002	Sio2026
administrateur	Assa	1007	Sio2026
administrateur	evan	1010	Sio2026
administrateur	Clément	1005	Sio2026
administrateur	Brightman	1003	Sio2026
administrateur	Anas	1006	Sio2026
administrateur	Kinsy	1012	Sio2026
administrateur	Kanikathir	1011	Sio2026
administrateur	Abdel	1009	Sio2026
administrateur	Eldelmira	1008	Sio2026
administrateur	Diego	1004	Sio2026
administrateur	Fabien pichon	fpichon	Sio2026
rh	francis dominique	10001	Sio2026

rh	gagou fifi	10002	Sio2026
----	------------	-------	---------

# Annexes

 Information general.xlsx  schéma architecture réseau.pdf  paris\_stationf1.pkt .