Proof of Concept (POC) – Infrastructure Wi-Fi d’entreprise

Marchand Flavien
Duforets Thomas

1. Contexte et objectifs du POC

Dans le cadre d'un appel d'offres pour le déploiement d'une nouvelle infrastructure Wi-Fi d'entreprise, notre équipe technique a été missionnée afin de concevoir, déployer et valider une solution Wi-Fi fonctionnelle répondant aux besoins immédiats du client, tout en respectant de fortes contraintes budgétaires.

L'objectif principal de ce Proof of Concept (POC) est de démontrer la capacité de la solution proposée à répondre aux exigences :

- fonctionnelles,
- sécuritaires,
- radio (couverture et performances), tout en restant **évolutive** et **administrable de manière centralisée**.

Le client souhaite une mise en œuvre rapide, à coût réduit, en acceptant l'utilisation de matériels hétérogènes ou de générations différentes.

2. Besoins fonctionnels du client

Les services suivants devaient être mis en œuvre dans le cadre du POC :

- Sécurisation du LAN et isolation des flux Wi-Fi
- Mise en place de plusieurs SSID :
    - SSID IoT avec authentification simple par clé pré-partagée (PSK)
    - SSID Invité avec accès via portail captif local
    - Préparation d'un SSID sécurisé en WPA2-Entreprise (802.1X)
- Administration centralisée de l'infrastructure Wi-Fi
- Paramétrage radio adapté à un environnement à densité moyenne/élevée
- Réalisation d'un audit radio simplifié (site survey) sur une zone représentative

3. Architecture technique proposée

3.1 Principe général

L'architecture retenue repose sur :

- un **contrôleur Wi-Fi Aruba** permettant l'administration centralisée,
- plusieurs **points d'accès Aruba série 500**,
- un **switch PoE** assurant l'alimentation des bornes et la segmentation réseau.

Cette architecture permet :

- une gestion centralisée des SSID, de la sécurité et des paramètres radio,
- une évolutivité simple par ajout de points d'accès supplémentaires,
- une cohérence de configuration sur l'ensemble du réseau Wi-Fi.

3.2 Segmentation réseau et VLAN

Afin d'assurer l'isolation des flux et la sécurité du LAN, une segmentation par VLAN a été mise en place :

VLAN	Usage	Sous-réseau
VLAN 10	Management	192.168.10.0/24
VLAN 20	SSID IoT	192.168.20.0/24
VLAN 30	SSID Sécurisé	192.168.30.0/24
VLAN 40	SSID Invité	192.168.40.0/24

Chaque SSID est associé à un VLAN dédié, garantissant l'isolation des flux entre les différents types d'utilisateurs.

3.3 Configuration du switch et DHCP

Le switch est configuré avec :

- des ports en **mode trunk** pour les points d'accès,
- un VLAN natif dédié au management (VLAN 10),
- un service DHCP configuré par VLAN afin de fournir automatiquement une adresse IP aux clients Wi-Fi.

Exemple pour le VLAN management (VLAN des bornes) :

```
interface Vlan10
 ip address 192.168.10.254 255.255.255.0
 no ip route-cache

interface FastEthernet0/1
 switchport trunk native vlan 10
 switchport mode trunk
```

Le port est configuré en mode trunk afin de transporter l'ensemble des VLAN associés aux SSID.
Le VLAN natif est défini sur le VLAN 10, correspondant au réseau de management, permettant à la borne Wi-Fi d'obtenir une adresse IP de gestion.

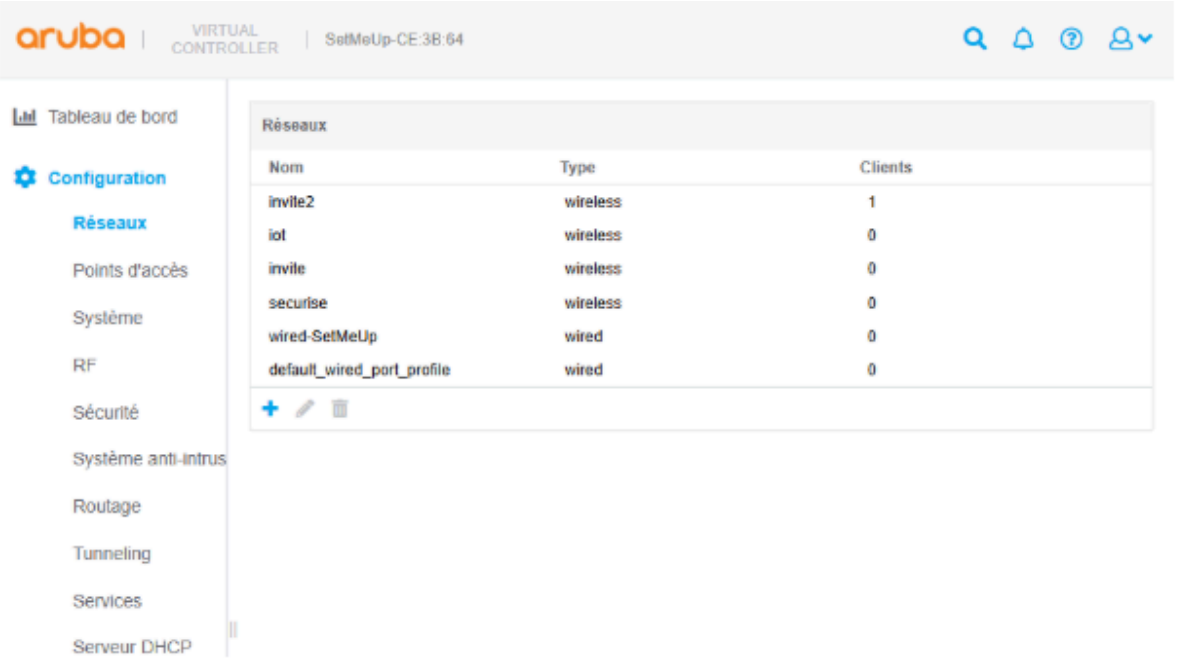
Chaque pool DHCP dispose :

- d'un plan d'adressage dédié,
- d'une passerelle par défaut en *.254.

Exemple pour le VLAN management (VLAN des bornes) :

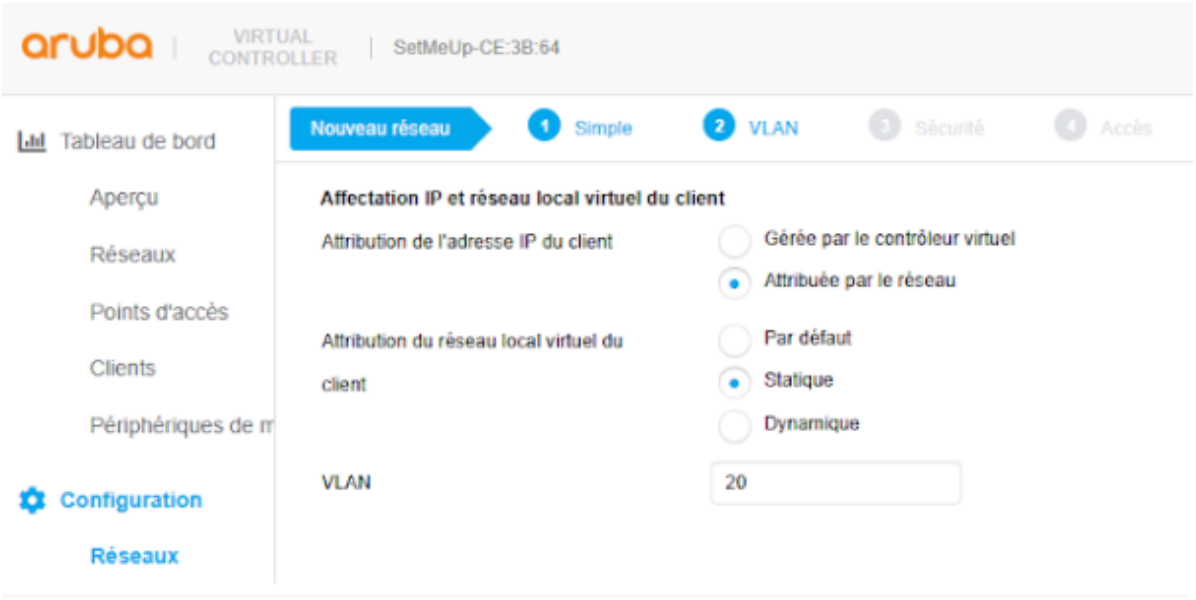
```
ip dhcp pool MANAGEMENT
 network 192.168.10.0 255.255.255.0
 default-router 192.168.10.254
```

4. Services Wi-Fi déployés dans le POC

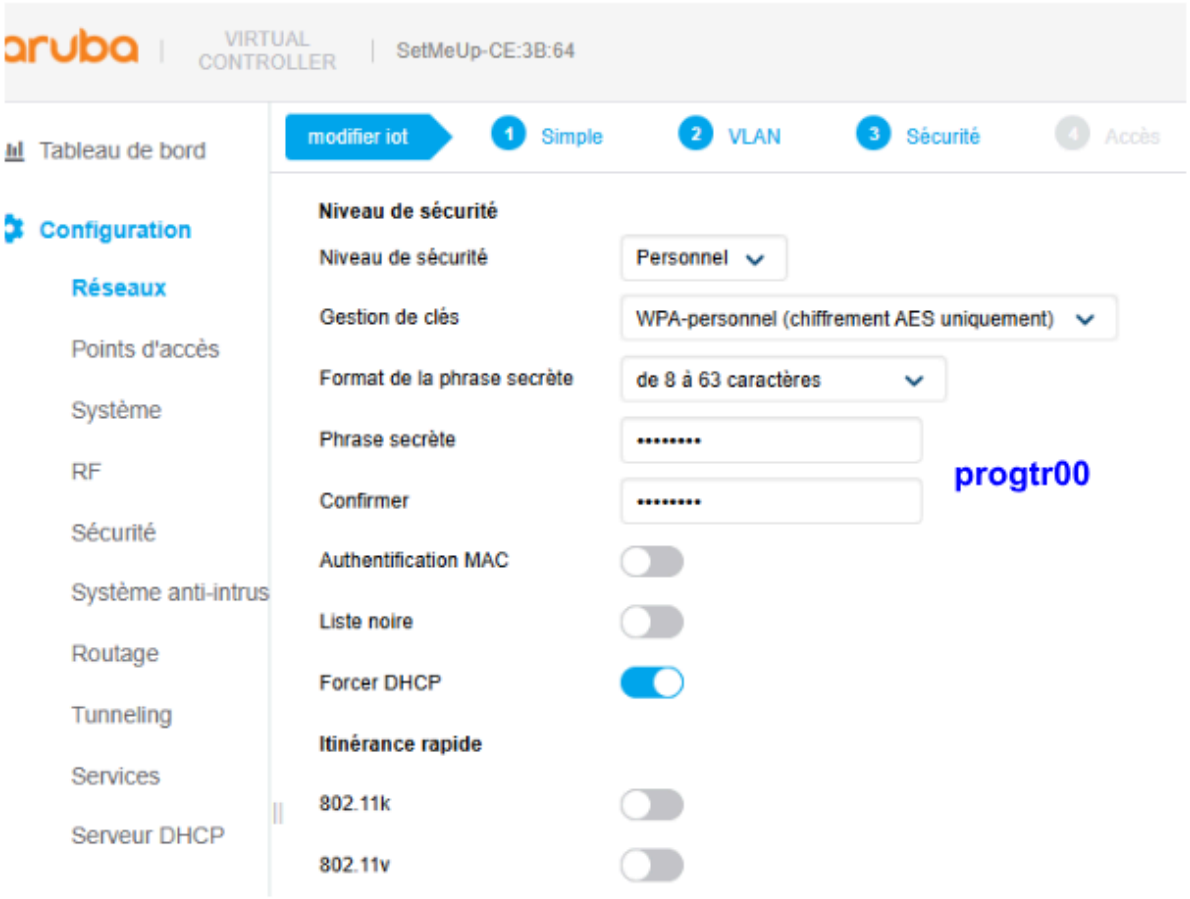


4.1 SSID IoT – Authentification PSK

- SSID : `iot`
- Sécurité : WPA-Personal (AES)
- VLAN associé : VLAN 20
- Attribution IP : DHCP



Ici on utilise les VLAN qui sont configurées sur le switch pour éviter de devoir faire un mappage entre les VLAN de la borne WIFI et les VLAN du switch.



Il ne faut pas oublier de cocher la case “Forcer DHCP” car sinon quand on va se connecter sur le Wifi, on ne va pas prendre d’IP sur le DHCP du switch et donc on ne va pas avoir de connexion.

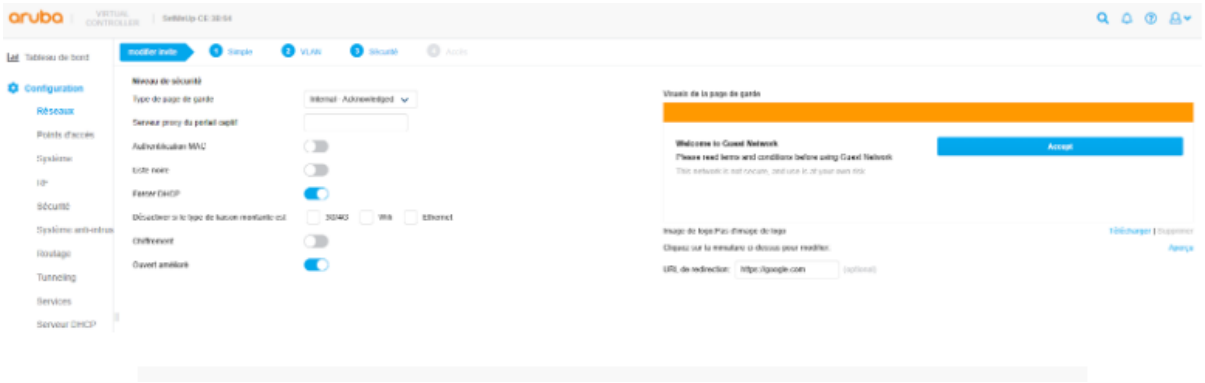
Ce SSID permet la connexion de terminaux IoT nécessitant une authentification simple tout en restant isolés du reste du réseau.

Les tests réalisés montrent :

- une association correcte au SSID,
- l'obtention d'une adresse IP dans le VLAN 20,
- un accès limité conformément au principe d'isolation.

4.2 SSID Invité – Portail captif local

- SSID : `invite`
- VLAN associé : VLAN 40
- Sécurité : portail captif local hébergé sur le contrôleur Wi-Fi



Ici on a choisi de mettre un portail captif au lieu d'un code d'authentification car ce réseau est le réseau invite, on configure donc pour avoir le portail captif lors de la connexion à ce réseau Wifi.

Lors de la connexion :

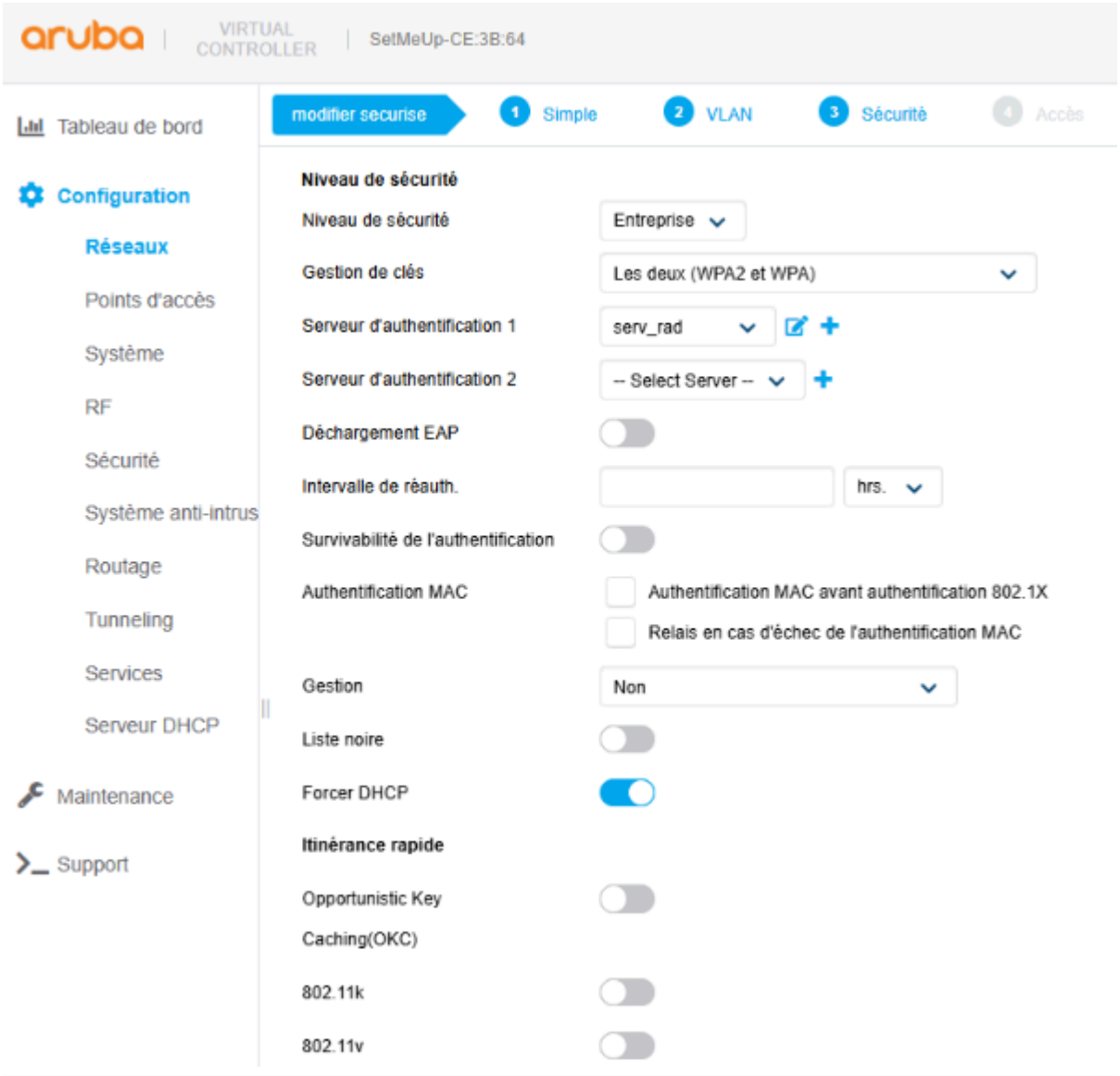
1. Le client obtient une adresse IP via DHCP.
2. Toute tentative d'accès web déclenche une redirection automatique vers le portail captif.
3. Après acceptation des conditions, l'accès réseau est autorisé selon les règles définies.

Ce mécanisme permet :

- de contrôler l'accès des utilisateurs invités,
- de maintenir une isolation stricte vis-à-vis du LAN interne.

4.3 SSID Sécurisé – Préparation WPA2-Entreprise (802.1X)

- SSID : `securise`
- Sécurité : WPA2-Entreprise
- Serveur d'authentification : RADIUS (`serv_rad`)
- VLAN associé : VLAN 30



Ici il faut qu'on crée le serveur d'authentification (serveur Radius) et une fois créé, on peut l'ajouter comme serveur d'authentification.

Dans le cadre du POC, ce SSID est configuré afin de démontrer la **préparation de l'architecture** à une authentification forte.

En environnement de production, ce SSID pourra être adossé à un annuaire (Active Directory / LDAP) afin de fournir :

- une authentification par identifiants personnels,
- une gestion fine des droits d'accès,
- une traçabilité des connexions.

5. Centralisation et évolutivité

Le contrôleur Wi-Fi permet :

- la gestion centralisée des points d'accès,
- la diffusion automatique des SSID sur les bornes,
- l'homogénéité des configurations sécurité et radio.

L'ajout de nouveaux points d'accès se fait sans reconfiguration lourde, ce qui rend la solution adaptée à un futur déploiement à plus grande échelle.

Il suffit de brancher la nouvelle borne au switch et de faire la même configuration que pour la première :

```
interface FastEthernet0/2
      switchport trunk native vlan 10
      switchport mode trunk
```

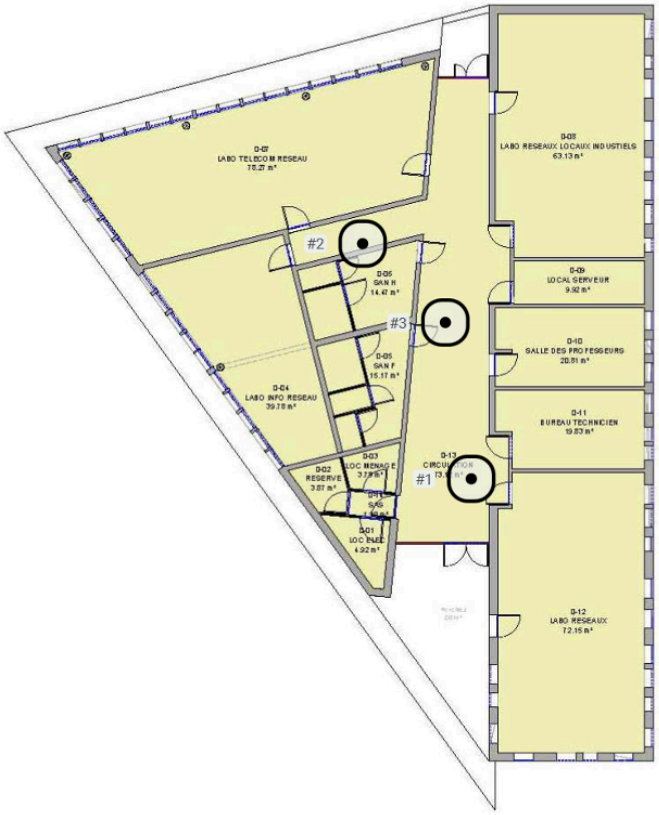
La borne se met automatiquement en esclave et récupère la configuration depuis le contrôleur (première borne configurée).

6. Audit radio – Étude Ekahau

6.1 Zone auditée et méthodologie

L'étude radio a été réalisée sur une zone représentative du site :

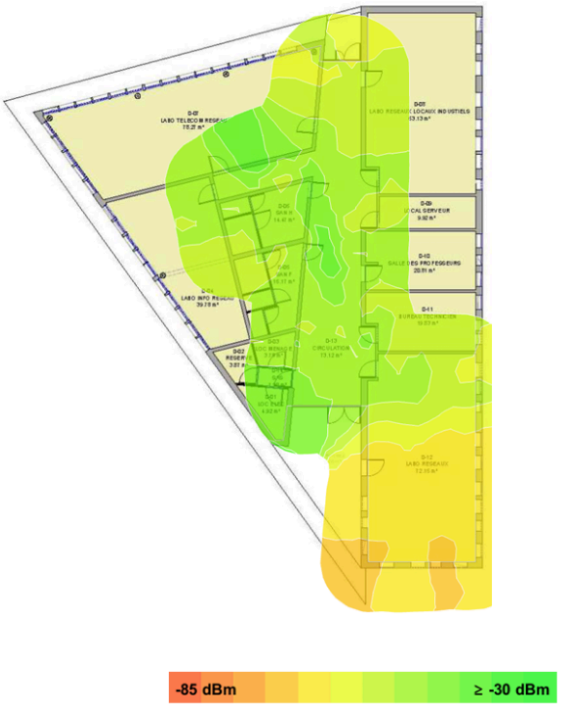
- **Bâtiment RT – surface d'environ 471 m²**

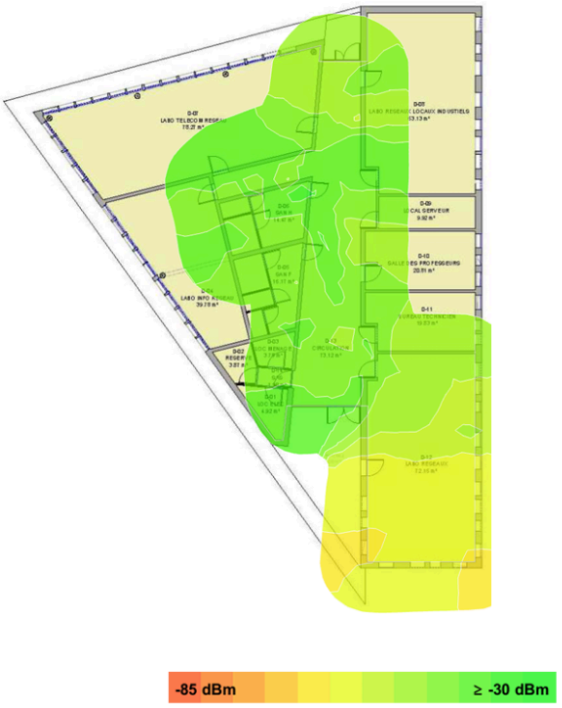


Les critères de qualité utilisés sont conformes aux bonnes pratiques (RSSI, SNR, débit minimum, couverture secondaire).

6.2 Analyse de la couverture radio

Intensité du signal :





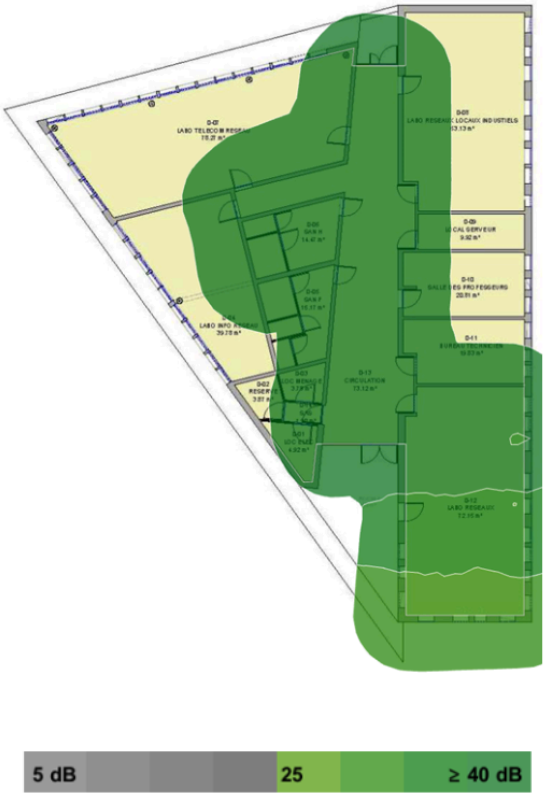
2.4GHz	5 GHz

Les cartes de couverture montrent :

- une couverture globalement satisfaisante en 5 GHz,
- des zones plus hétérogènes en 2.4 GHz, notamment en périphérie.

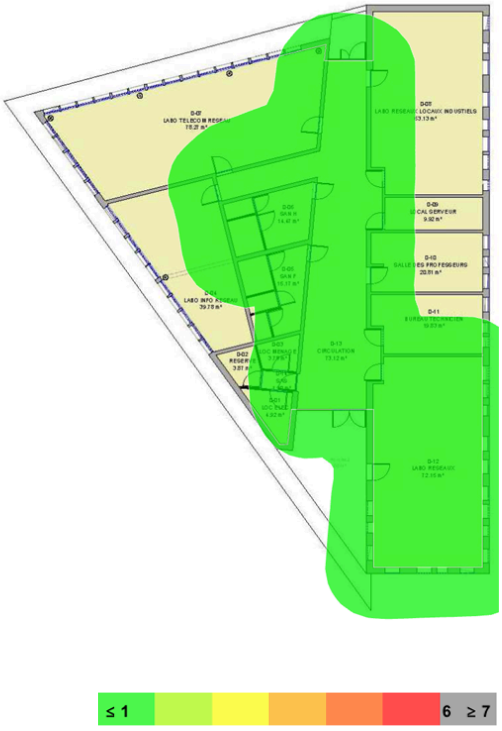
6.3 Qualité du signal et interférences

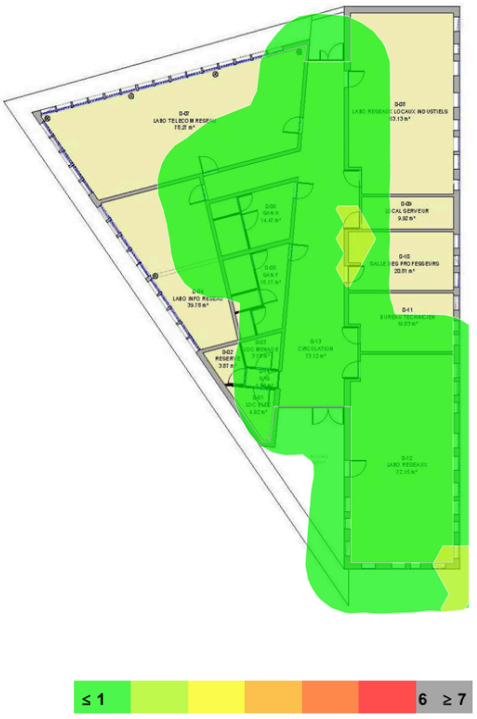
Rapport signal sur bruit (SNR) :



2.4GHz	5 GHz

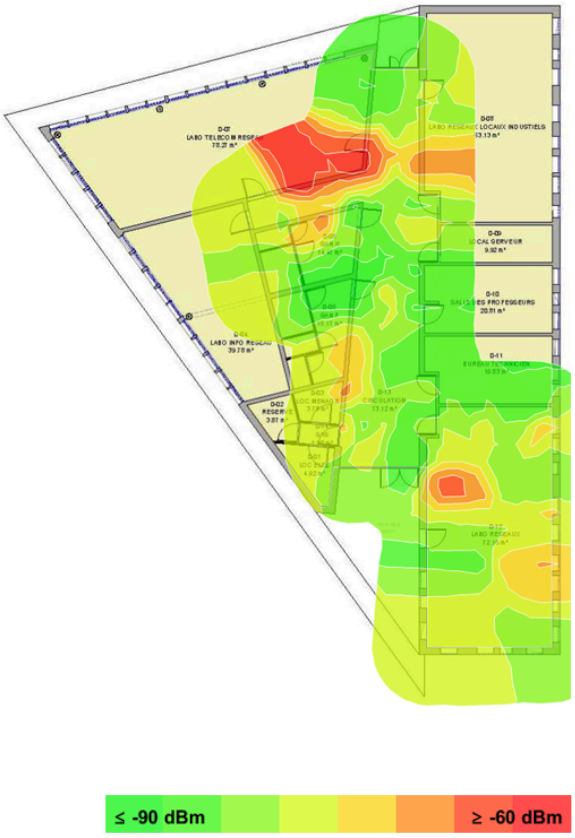
Interférence des canaux :

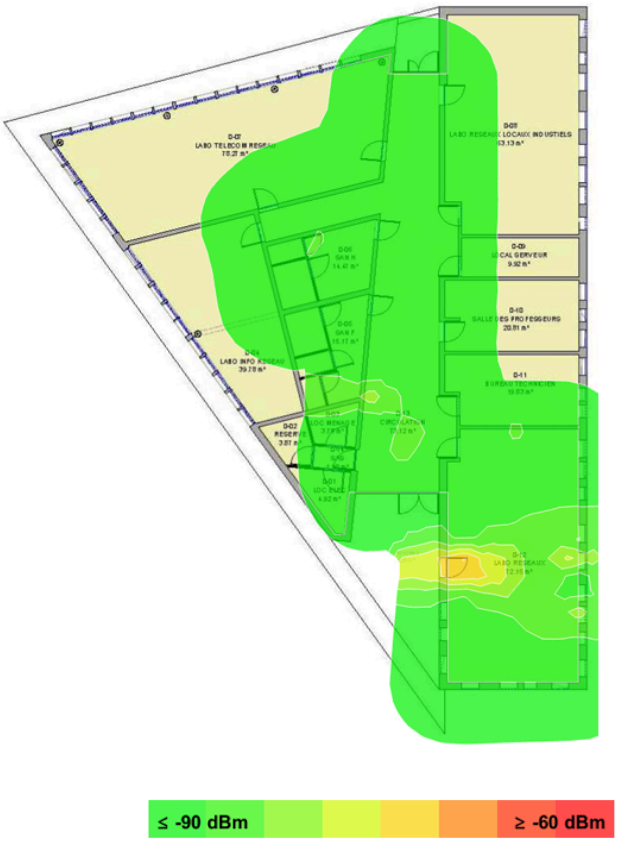




5 GHz	2.4 GHz

Bruit :

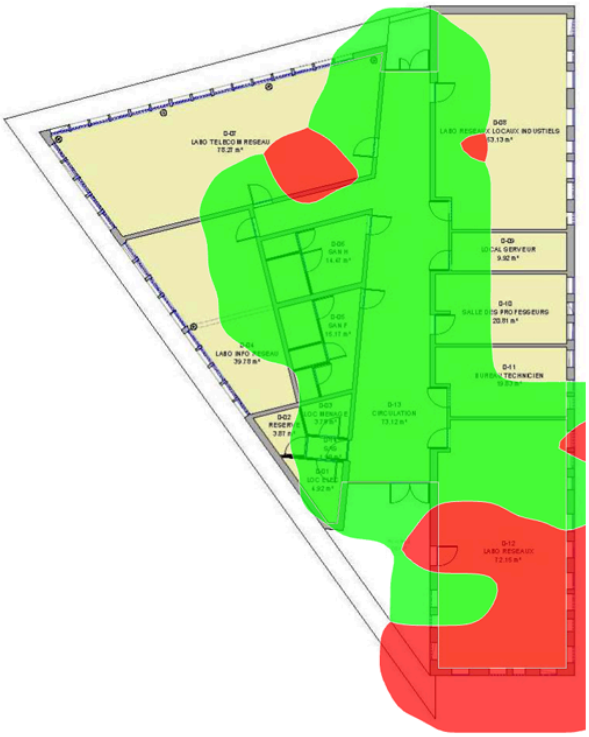




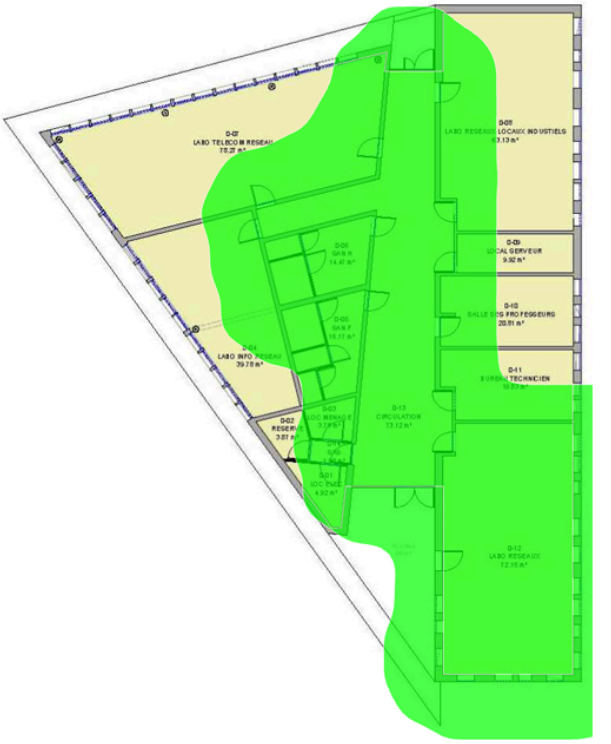
2.4GHz	5 GHz

- Le **SNR** est globalement meilleur en 5 GHz, indiquant un environnement radio plus propre.
- La bande **2.4 GHz** présente davantage de bruit et d'interférences non-Wi-Fi, impactant la qualité du réseau dans certaines zones.

6.4 Santé globale du réseau



Échec Passage



Échec Passage

2.4GHz	5 GHz

L'indicateur de santé du réseau met en évidence :

- quelques zones dégradées, principalement en 2.4 GHz,
- la nécessité d'optimiser le plan de canaux et la puissance d'émission.

7. Recommandations

7.1 Optimisations sans investissement supplémentaire

- Limiter la bande 2.4 GHz aux usages nécessaires (IoT).
- Favoriser la bande 5 GHz pour les terminaux récents.
- Utiliser des canaux 20 MHz en 2.4 GHz et limiter la puissance d'émission.
- Activer des mécanismes de steering vers le 5 GHz si disponibles.

7.2 Évolutions futures

Lorsque le budget le permettra :

- ajout de points d'accès pour améliorer la densité,
- déploiement complet d'un serveur RADIUS couplé à un annuaire,
- montée en gamme vers des bornes Wi-Fi 6/6E sur les zones à forte densité.

8. Conclusion

Ce Proof of Concept démontre qu'il est possible de déployer rapidement une infrastructure Wi-Fi d'entreprise :

- sécurisée,
- segmentée,
  administrable de manière centralisée,
- et adaptée aux contraintes budgétaires du client.

La solution proposée répond aux besoins immédiats tout en offrant une base solide et évolutive pour un futur déploiement à plus grande échelle.