RAPPORT DE TP :

Réalisation d’un POC Wi-Fi

Auteur : Pierre FAMCHON
Formation : R&T - 3ème Année
Année : 2025-2026
Date : 15/12/2025

SOMMAIRE DÉTAILLÉ

I. ANALYSE DU BESOIN ET CONTEXTE

1.1. Contexte du client et enjeux stratégiques

L'entreprise traverse actuellement une période de rationalisation budgétaire stricte (OPEX/CAPEX limités), tout en faisant face à une urgence opérationnelle nécessitant la remise à niveau immédiate de sa connectivité sans-fil.

Le défi majeur de ce projet ne réside pas uniquement dans la technique, mais dans l'adéquation entre **performance** et **économie**. Le client exige une solution :

- **Immédiatement opérationnelle :** Déploiement rapide sans travaux lourds.
- **Économique :** Réutilisation de l'existant, absence d'achat de contrôleur physique dédié.
- **Évolutive :** La solution déployée aujourd'hui (POC) doit pouvoir grandir demain sans tout remplacer.

1.2. Recueil des besoins techniques

Suite à l'analyse de l'appel d'offre, nous avons identifié quatre piliers fonctionnels indispensables :

Besoin	Description Technique	Contrainte associée
Sécurisation du LAN	*Isolation stricte des flux (Employés vs Invités vs Objets).*	*Segmentation par VLANs (802.1Q).*
Connectivité IoT	*Connexion d'équipements tiers (capteurs, imprimantes).*	*Authentification WPA2-PSK (Simple mais robuste).*
Accès Invités	*Accès internet uniquement, légalement conforme.*	*Portail Captif local (sans serveur externe).*
Haute Densité	*Maintien des performances avec de nombreux terminaux.*	*Wi-Fi 6 (802.11ax) et gestion radio optimisée.*

1.3. Objectifs du POC (Proof of Concept)

Ce "Preuve de Concept" a pour but de valider, sur un périmètre restreint (une zone représentative), que l'architecture proposée est viable. Il doit démontrer que :

1. L'architecture "sans contrôleur physique" tient la charge.
2. La sécurité n'est pas sacrifiée malgré le budget réduit.
3. La couverture radio est adaptée aux matériaux du bâtiment (validé par audit Ekahau).

1.4. Planification et répartition des tâches

Tâche	Statut	Responsable
ANALYSE DU BESOIN ET CONTEXTE	Terminé	Nicolas Édouard Pierre Famchon
PHASE 1 : ARCHITECTURE DE LA SOLUTION PROPOSÉE	Terminé	Pierre Famchon
PHASE 2 : MISE EN OEUVRE TECHNIQUE (Le POC)	En cours	Nicolas Édouard
PHASE 3 : AUDIT RADIO ET COUVERTURE (Site Survey)	En cours	Pierre Famchon
PHASE 4 : TESTS ET VALIDATION	En cours	Pierre Famchon
PHASE 5 : RECOMMANDATIONS ET ÉVOLUTIONS	En cours	Nicolas Édouard
PHASE 6 : CONCLUSION	En cours	Pierre Famchon
RÉDACTION DES DOCUMENTS	En cours	Pierre Famchon

II. ARCHITECTURE DE LA SOLUTION PROPOSÉE

2.1. Philosophie : L'architecture Aruba Instant (IAP)

Au lieu d'investir dans une appliance de gestion coûteuse (Contrôleur matériel), nous utilisons l'intelligence embarquée des bornes **Aruba AP-505**.

- **Le principe du Virtual Controller (VC) :**

  Une des bornes (l'AP-505 "Master") est élue chef d'orchestre. Elle héberge l'interface d'administration, la configuration des SSID et le portail captif pour tout le cluster.

- **Redondance native :**

  Si la borne "Master" tombe en panne, la borne "Slave" reprend automatiquement le rôle de chef. Cela garantit une haute disponibilité à coût zéro.

- **Déploiement "Zero Touch" :**

  Toute nouvelle borne branchée sur le réseau détecte le Master et télécharge sa configuration automatiquement. C'est la réponse à l'exigence de "déploiement rapide".

2.2. Choix Matériels et Logiciels

L'infrastructure repose sur des équipements de gamme Entreprise, robustes et pérennes :

- **1 Aruba AP 505 (Master IAP)** : Choisi pour sa capacité à opérer en mode "Instant" (IAP). Cette borne joue le rôle de contrôleur virtuel (Virtual Controller) pour l'ensemble du réseau.

  Justification : Elle permet de centraliser la configuration, la sécurité et le portail captif sans nécessiter l'achat d'un contrôleur physique coûteux, répondant ainsi aux contraintes budgétaires du client tout en offrant des fonctionnalités d'entreprise (Firewall applicatif, WPA3, Wi-Fi 6).

- **1 Aruba AP 505 (Slave IAP) :**Point d'accès Wi-Fi 6 (802.11ax) agissant en mode dépendant.

  Justification : Elle démontre la capacité d'extension du réseau (scalabilité). Dès son raccordement, elle récupère automatiquement la configuration du Master (Zero Touch Provisioning), assurant une continuité de service et une itinérance (roaming) fluide pour les utilisateurs.

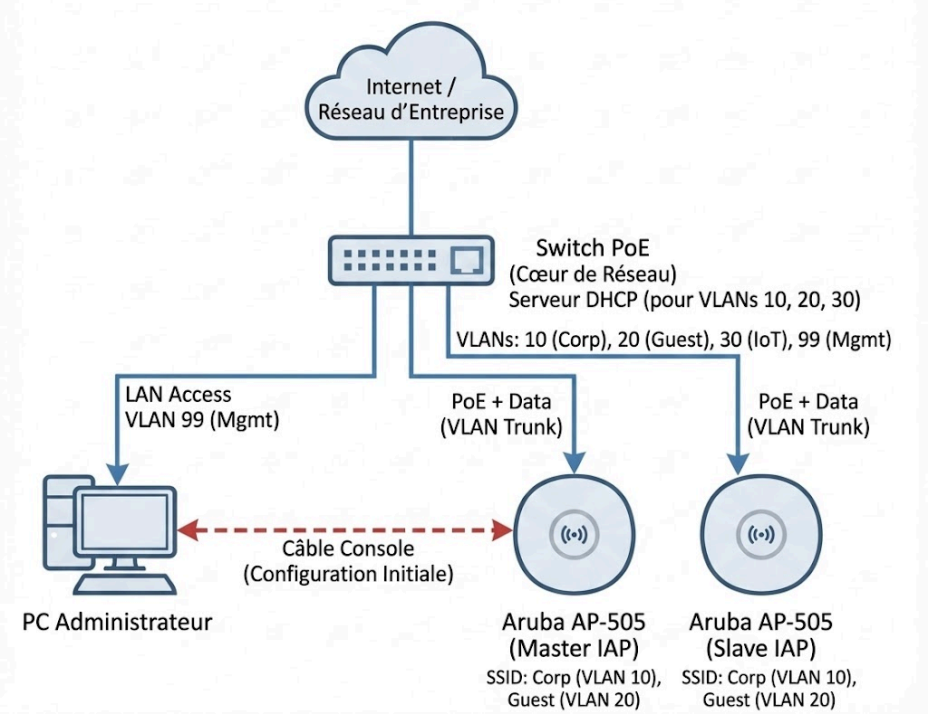
- **1 Switch PoE :** Élément central de la connectivité filaire et de l'alimentation électrique.

  Justification : Il assure l'alimentation des bornes via la norme PoE (802.3at/af), éliminant le besoin de blocs d'alimentation externes. Il est configuré pour gérer la segmentation réseau (VLANs 802.1Q), garantissant l'isolation stricte des flux demandée par le client (Invités vs Employés vs IoT).

- **Outils : Ekahau + Sidekick :** Solution de référence mondiale pour l'analyse spectrale et la planification Wi-Fi.

  Justification : L'association du logiciel Ekahau et de la sonde Sidekick permet de réaliser un audit précis de l'environnement radio (Site Survey). Cela nous permettra de valider la couverture, de détecter les sources d'interférences non-Wi-Fi et de positionner les bornes de manière optimale pour éviter les zones blanches.

2.3. Schéma d'architecture (Topologie)



L'architecture repose sur une segmentation stricte via des VLANs (Réseaux Locaux Virtuels).

Matrice des Flux Wi-Fi :

Nom du SSID (Wi-Fi)	**Authentification**	**VLAN ID**	**Accès Réseau Autorisé**
CORP-SECURE	*WPA2/WPA3 Enterprise (802.1X)*	*VLAN 10*	*Accès complet LAN + Internet*
GUEST-WIFI	*Portail Captif (Open + Web Auth)*	*VLAN 20*	*Internet Uniquement (Isolation client)*
IOT-DEVICE	*WPA2-PSK (Clé partagée)*	*VLAN 30*	*Accès Internet + Serveurs IoT spécifiques*
MGMT	*(Filaire / Hidden SSID)*	*VLAN 99*	*Administration des bornes uniquement*

Schéma de fonctionnement des ports Switch : Les ports reliant les bornes au switch sont configurés en mode **TRUNK**. Cela permet de faire transiter les paquets de tous les VLANs (10, 20, 30) sur le même câble, la borne se chargeant de distribuer le bon paquet au bon utilisateur Wi-Fi.

Tableau Global d'Adressage IP - POC Wi-Fi

Équipement / Service	Interface / Rôle	VLAN ID	Adresse IP / Masque	Passerelle (Gateway)	Type d'IP
Switch PoE (Coeur)	*Vlan99*	*99*	*192.168.99.**254** /24*	-	*Statique*
Switch PoE (Coeur)	*Vlan10*	*10*	*192.168.10.**254** /24*	-	*Statique*
Switch PoE (Coeur)	*Vlan20*	*20*	*192.168.20.**254** /24*	-	*Statique*
Switch PoE (Coeur)	*Vlan30*	*30*	*192.168.30.**254** /24*	-	*Statique*
Aruba AP-505 (Master)	*MGMT*	*99*	*192.168.99.**2** /24*	*192.168.99.**254***	*Statique*
Aruba AP-505 (Slave)	*MGMT*	*99*	*192.168.99.**11** /24*	*192.168.99.**254***	*DHCP*
Cluster Aruba (VIP)	*Virtual Controller*	*99*	*192.168.99.**15** /24*	*192.168.99.**254***	*Statique (Virtuelle)*
PC Admin	*Carte Ethernet*	*99*	*192.168.99.**10** /24*	*192.168.99.**254***	*Statique*
Clients CORP	*CORP-SECURE*	*10*	*Plage DHCP : **.10** à **.200***	*192.168.10.**254***	*DHCP (via Switch)*
Clients GUEST	*GUEST-WIFI*	*20*	*Plage DHCP : **.10** à **.200***	*192.168.20.**254***	*DHCP (via Switch)*
Clients IoT	*MGMT*	*30*	*Plage DHCP : **.10** à **.200***	*192.168.30.**254***	*DHCP (via Switch)*

Stratégie d'adressage IP : Pour garantir une exploitation simplifiée et une maintenance aisée, nous avons appliqué une règle de nommage logique : le 3ème octet de l'adresse IP correspond systématiquement à l'ID du VLAN.

2.4. Évolutivité de la solution

Cette architecture POC est conçue pour passer à l'échelle (Scale-up) sans refonte :

1. **Ajout de capacité :**

   Il suffit de brancher une nouvelle AP-505 pour étendre la couverture.

2. **Migration future :**

   Si le parc dépasse 50 ou 100 bornes, ces mêmes AP-505 pourront être basculées vers une gestion Cloud (Aruba Central) ou un contrôleur physique sans rachat de matériel, protégeant ainsi l'investissement initial du client.

III. MISE EN OEUVRE TECHNIQUE (Le POC)

Cette section détaille les opérations de configuration réalisées pour transformer le matériel brut en une infrastructure opérationnelle. Nous avons suivi une approche "Bottom-Up" : d'abord le réseau filaire (Switch), puis le réseau sans-fil (Aruba Instant).

3.1. Infrastructure Réseau et Sécurité LAN

Le switch PoE est la clé de voûte de l'architecture. Il assure trois fonctions vitales : l'alimentation des bornes, la segmentation (VLANs) et la distribution des adresses IP (DHCP).

A. Création des VLANs (Segmentation) Pour respecter l'isolation des flux demandée, nous avons déclaré les VLANs suivants sur le switch :

- **VLAN 99 (Mgmt) :** Administration des équipements.
- **VLAN 10 (Corp) :** Flux collaborateurs (Prioritaire).
- **VLAN 20 (Guest) :** Flux invités (Accès Internet strict).
- **VLAN 30 (IoT) :** Flux objets connectés.

# Création VLANs	# Configuration des IPs
en	en
conf t	conf t
vlan 99	interface vlan 99
name MGMT	ip address 192.168.99.254 255.255.255.0
vlan 10	no shut
name CORP	interface vlan 10
vlan 20	ip address 192.168.10.254 255.255.255.0
name GUEST	no shut
vlan 30	interface vlan 20
name IOT	ip address 192.168.20.254 255.255.255.0
	no shut
exit	interface vlan 30
	ip address 192.168.30.254 255.255.255.0
	no shut

B. Configuration du Service DHCP (Sur le Switch) Conformément à l'architecture cible, le Switch agit comme serveur DHCP pour délivrer les IP aux clients Wi-Fi. Cela allège la charge sur les bornes.

- *Configuration réalisée :* Création de 3 "Pools DHCP" distincts correspondant aux VLANs 10, 20 et 30, avec pour chacun la passerelle par défaut et les DNS (ex: 8.8.8.8 pour les invités).

```
# Configuration du DHCP
service dhcp

ip dhcp pool POOL-CORP
 network 192.168.10.0 255.255.255.0
 default-router 192.168.10.254
 dns-server 8.8.8.8

ip dhcp pool POOL-GUEST
 network 192.168.20.0 255.255.255.0
 default-router 192.168.20.254
 dns-server 8.8.8.8

ip dhcp pool POOL-IOT
 network 192.168.30.0 255.255.255.0
 default-router 192.168.30.254
 dns-server 8.8.8.8
```

C. Configuration des Ports (Trunking) Les ports connectés aux bornes Aruba AP-505 (ex: ports 2 et 3) ont été configurés en mode **TRUNK (802.1Q)**.

- *Objectif :* Permettre aux bornes de "taguer" les paquets. Si un utilisateur se connecte sur le SSID Invité, la borne tague son trafic en "20" et l'envoie au switch. Le port Trunk accepte ce tag et le dirige vers le bon réseau.

```
# Configuration des Ports
interface range GigabitEthernet 0/2 - 3
 switchport trunk encapsulation dot1q # non nécessaire sur les switch récents
 switchport mode trunk
 switchport trunk native vlan 99
 switchport trunk allowed vlan 10,20,30,99
 no shut
```

3.2. Configuration du Cluster Aruba Instant (IAP)

La force de la solution proposée réside dans sa simplicité de déploiement via le mode IAP (Instant Access Point).

Phase 1 : Initialisation du Master (Virtual Controller)

1. Connexion en console série sur la première borne AP-505.
2. Assignation d'une IP statique de management (VLAN 99) pour garantir l'accès futur.
3. Connexion via l'interface Web (GUI) : Création du cluster nommé "POC-WIFI-ENTREPRISE".

L'administration centralisée du cluster s'effectue via une interface unique, sans nécessiter de matériel dédié.

Phase 2 : Adhésion de l'Esclave (Zero Touch Provisioning)

1. Raccordement de la seconde AP-505 sur le switch.
2. **Résultat observé :**

   La borne a démarré, récupéré une IP, détecté le Master via le protocole IAP, et téléchargé automatiquement la configuration et le firmware.

3. La borne est devenue opérationnelle en moins de 5 minutes sans intervention humaine supplémentaire.

3.3. Déploiement des Services Wi-Fi (SSID)

Trois réseaux sans-fil distincts ont été configurés via l'interface centralisée du Virtual Controller.

1. SSID "GUEST-WIFI" (Invités)

- **Type :** Réseau Invité avec Portail Captif interne.

- **Fonctionnement :**

  L'utilisateur se connecte à un réseau ouvert. À la première requête HTTP, l'AP intercepte le flux et affiche une page d'accueil (Splash Page) stockée localement sur la borne.

- **Sécurité :**

  Une règle de pare-feu (ACL) a été appliquée pour interdire tout accès aux réseaux privés (192.168.10.x, etc.) et n'autoriser que l'accès HTTP/HTTPS vers Internet.

- **VLAN :** Mappé sur le VLAN 20.

2. SSID "IOT-DEVICE" (Objets Connectés)

- **Type :** Réseau Employé (Employee Network) avec sécurité WPA2-Personal (PSK).

- **Justification :**

  La majorité des capteurs et imprimantes ne supportent pas l'authentification web. Une clé pré-partagée complexe a été définie.

- **Optimisation :**

  La fréquence 2.4 GHz a été privilégiée pour ce SSID afin d'assurer une meilleure pénétration des murs pour les capteurs lointains.

- **VLAN :** Mappé sur le VLAN 30.

3. SSID "CORP-SECURE" (Collaborateurs)

- **Type :** WPA2-Enterprise / 802.1X.

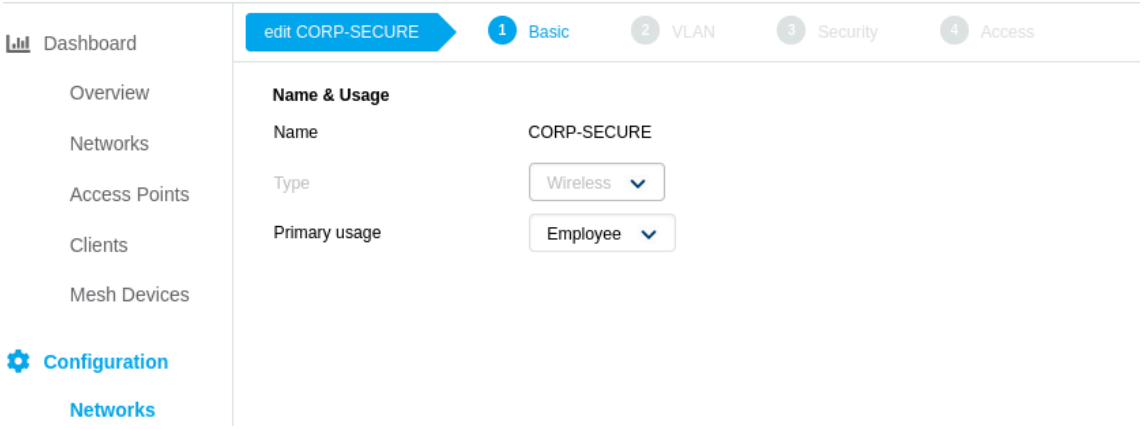
- **Fonctionnement :**

  Ce réseau demande une authentification forte (Login/Mot de passe utilisateur).

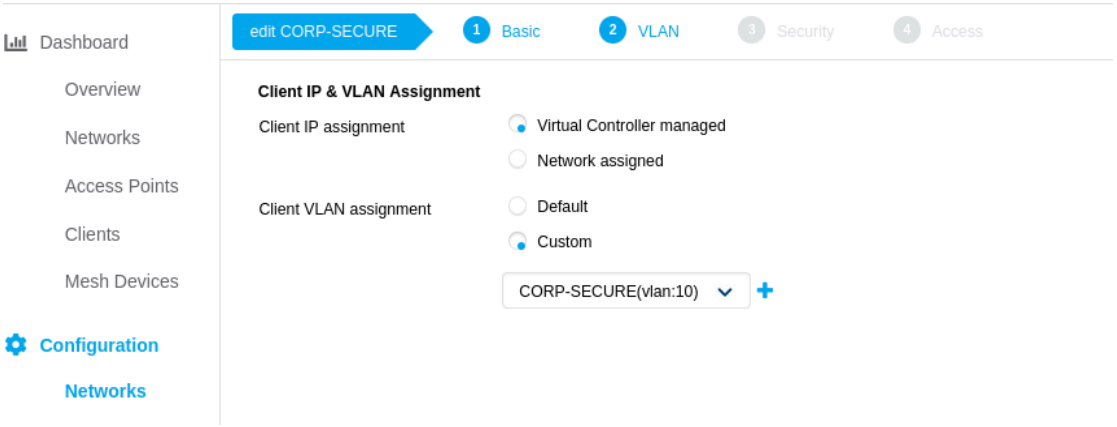
- **VLAN :** Mappé sur le VLAN 10.

Création du SSID avec la configuration de son VLAN

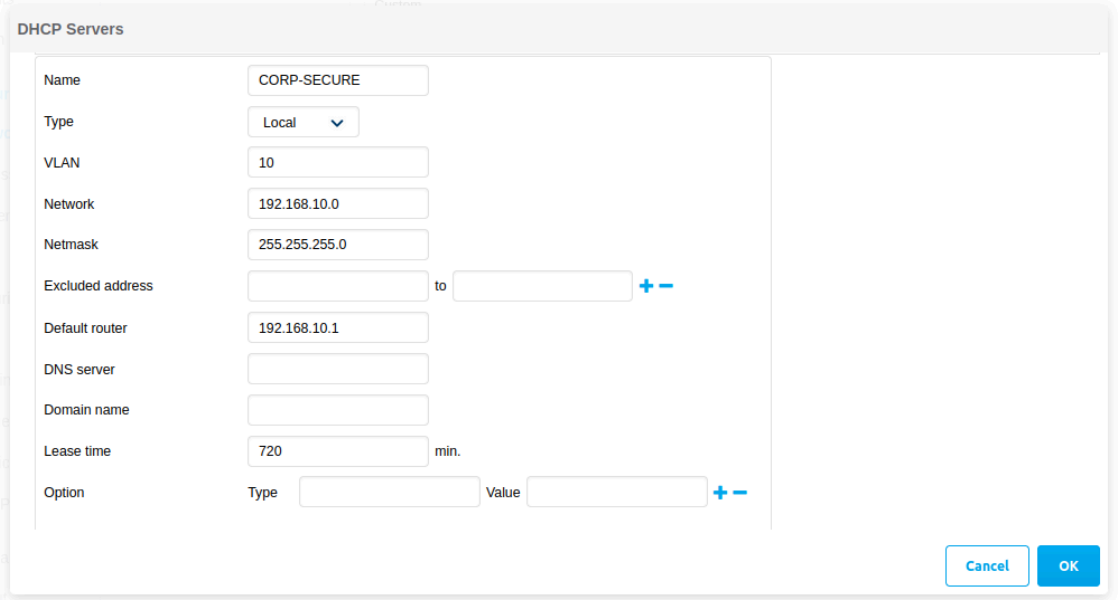
et des différentes règles mises en place pour ce réseau :



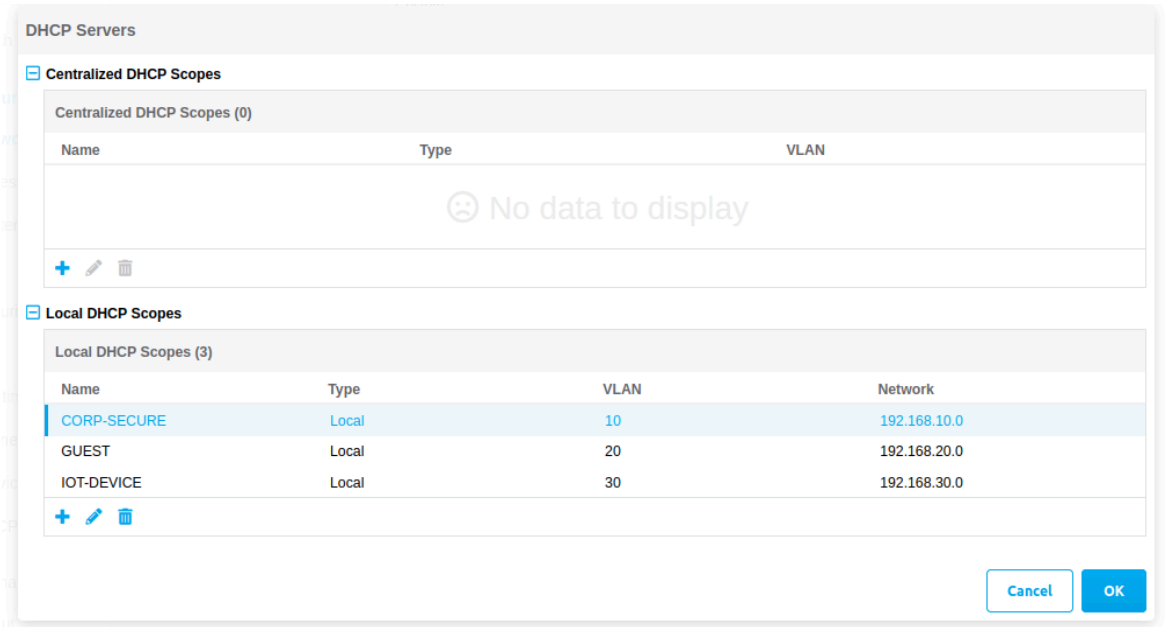
Paramétrage du rôle (Employee) et du type d'accès (Wireless).

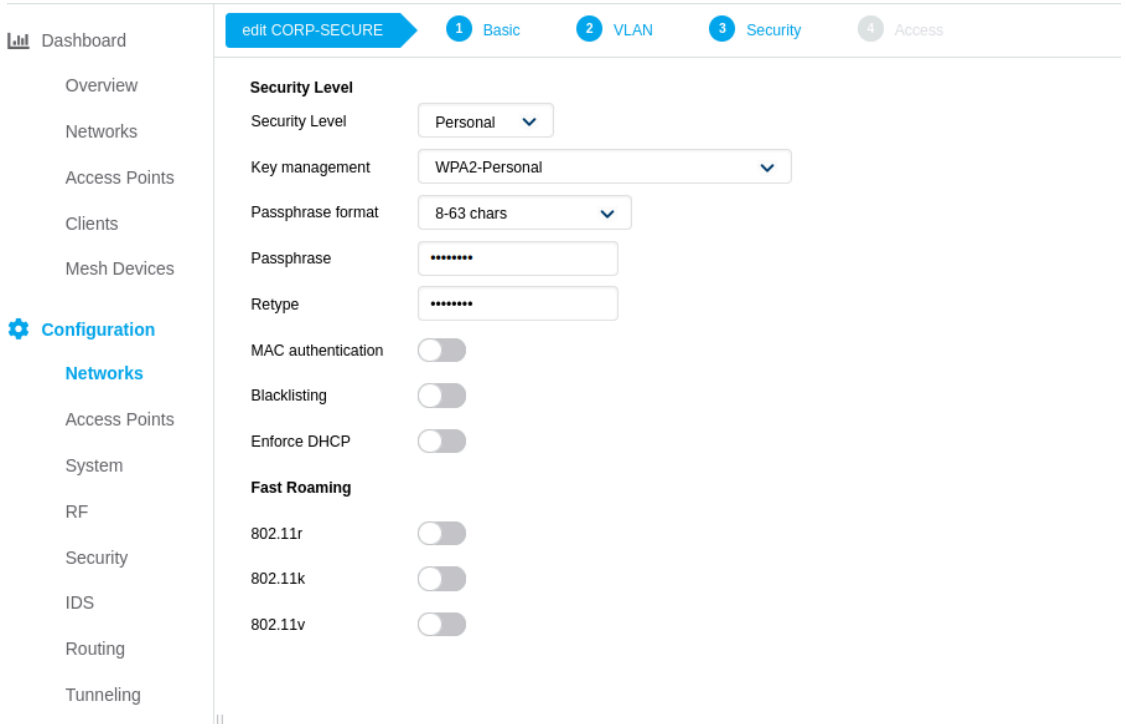


Association du SSID au VLAN 10 (Zone de Confiance).

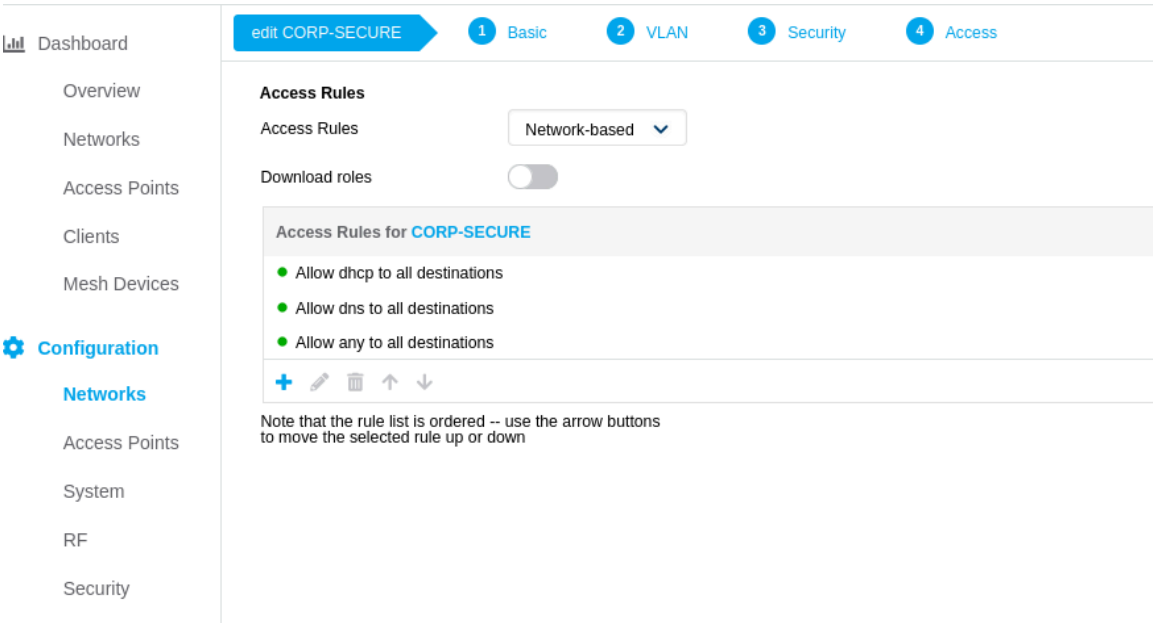


Déclaration des sous-réseaux 10, 20 et 30 sur le contrôleur Wi-Fi afin d'assurer la correspondance (mapping) avec la segmentation configurée sur le switch de cœur de réseau.





Implémentation de la couche de sécurité L2 et gestion des clés de chiffrement.



Configuration du pare-feu applicatif (PEF) : Application des politiques d'accès réseau.

3.4. Optimisation "Haute Densité"

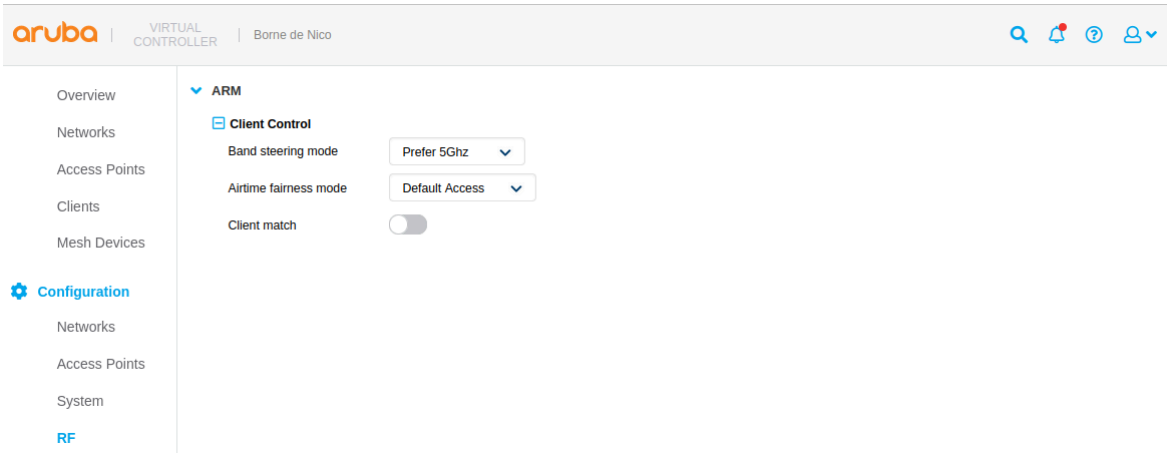
Pour répondre à l'exigence de performance dans les zones denses (salles de réunion), nous avons activé les fonctionnalités radio avancées des Aruba 505 :

1. **Suppression des bas débits :**

   Les vitesses 1, 2, 5.5 et 11 Mbps ont été désactivées. Cela force les clients à se connecter à haute vitesse et libère du "temps d'antenne" (Airtime) pour les autres.

2. **Band Steering :**

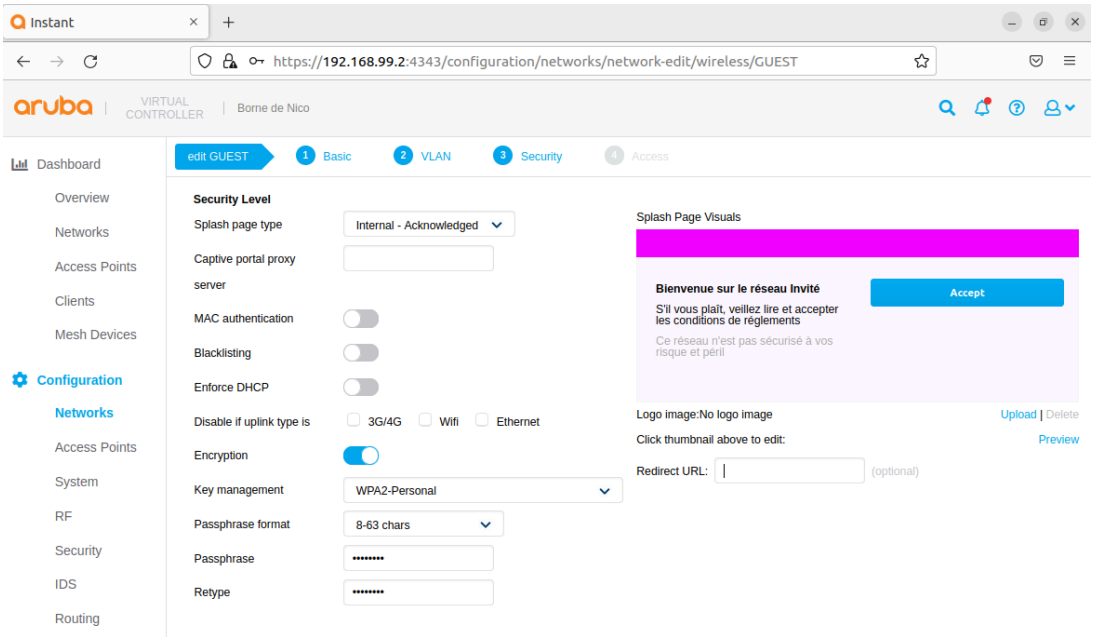
   Le mode "Prefer 5GHz" a été activé pour inciter les terminaux modernes (PC, Smartphones) à quitter la bande 2.4 GHz (souvent saturée) pour la bande 5 GHz (plus rapide).



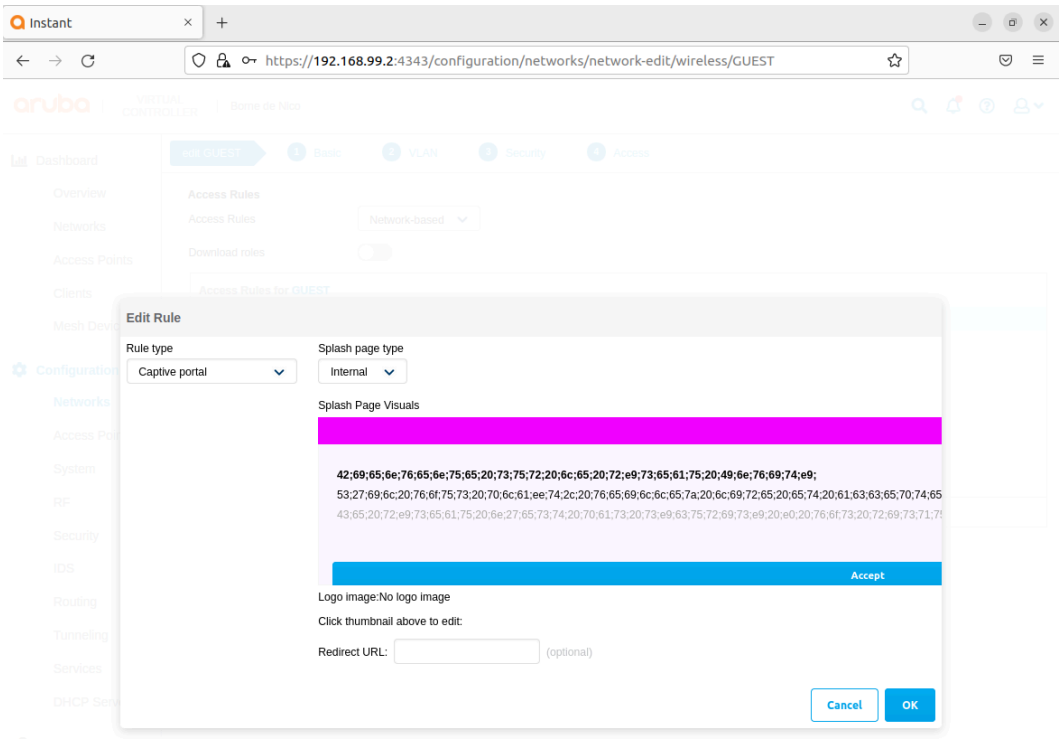
3. **Client Match :**

   Cette technologie Aruba surveille la "santé" de la connexion des clients et les force intelligemment à changer de borne (Roaming) s'ils s'éloignent trop, évitant le problème du "Sticky Client" (client qui reste accroché à une borne lointaine).

3.5. Portail captif local



Implémentation de l'authentification Invité : Service hébergé localement sur le Cluster IAP (Controller Less).



Configuration UX : Adaptation graphique du portail local sans recours à un serveur web externe.

IV. AUDIT RADIO ET COUVERTURE (Site Survey)

Afin de valider la faisabilité du déploiement et d'identifier les contraintes environnementales du "Bâtiment RT", une étude de site (Site Survey) a été réalisée. Cette étape est critique pour garantir que la solution Aruba proposée fonctionnera dans l'environnement réel.

4.1. Méthodologie et Périmètre

- **Outils utilisés :**

  Logiciel **Ekahau AI Pro** couplé à la sonde spectrale **Ekahau Sidekick** pour une précision métrologique.

- **Zone auditée :**

  Bâtiment RT, surface d'environ 437 m² comprenant des zones techniques (Labo Telecom, Labo Info) et des bureaux.

- **Critères de validation (SLA) :**

  Nous nous sommes basés sur les "Cisco Design Guidelines" pour la voix et la vidéo:

  - Intensité du signal cible : -65 dBm minimum.
  - Rapport Signal/Bruit (SNR) : 25 dB minimum.
  - Perte de paquets max : 2.0%.

BâtimentRT (437 m²)

Exigence de couverture: **Cisco Design Guideline**		
2.4 GHz	intensité du signal Min	-65.0 dBm
	Puissance du signal secondaire Min	-75.0 dBm
	Rapport signal sur bruit Min	25.0 dB
	Débit Min	12 Mbits/s
	Interférence de canal Max	1 un minimum de -86.0 dBm
	Durée de la rotation Ping Max	300 ms
	Perte de paquets Max	2.0 %
5 GHz	intensité du signal Min	-65.0 dBm
	Puissance du signal secondaire Min	-75.0 dBm
	Rapport signal sur bruit Min	25.0 dB
	Débit Min	12 Mbits/s
	Interférence de canal Max	1 un minimum de -86.0 dBm
	Durée de la rotation Ping Max	300 ms
	Perte de paquets Max	2.0 %
6 GHz	intensité du signal Min	-65.0 dBm
	Puissance du signal secondaire Min	-75.0 dBm
	Rapport signal sur bruit Min	25.0 dB
	Débit Min	12 Mbits/s
	Interférence de canal Max	1 un minimum de -86.0 dBm
	Durée de la rotation Ping Max	300 ms
	Perte de paquets Max	2.0 %

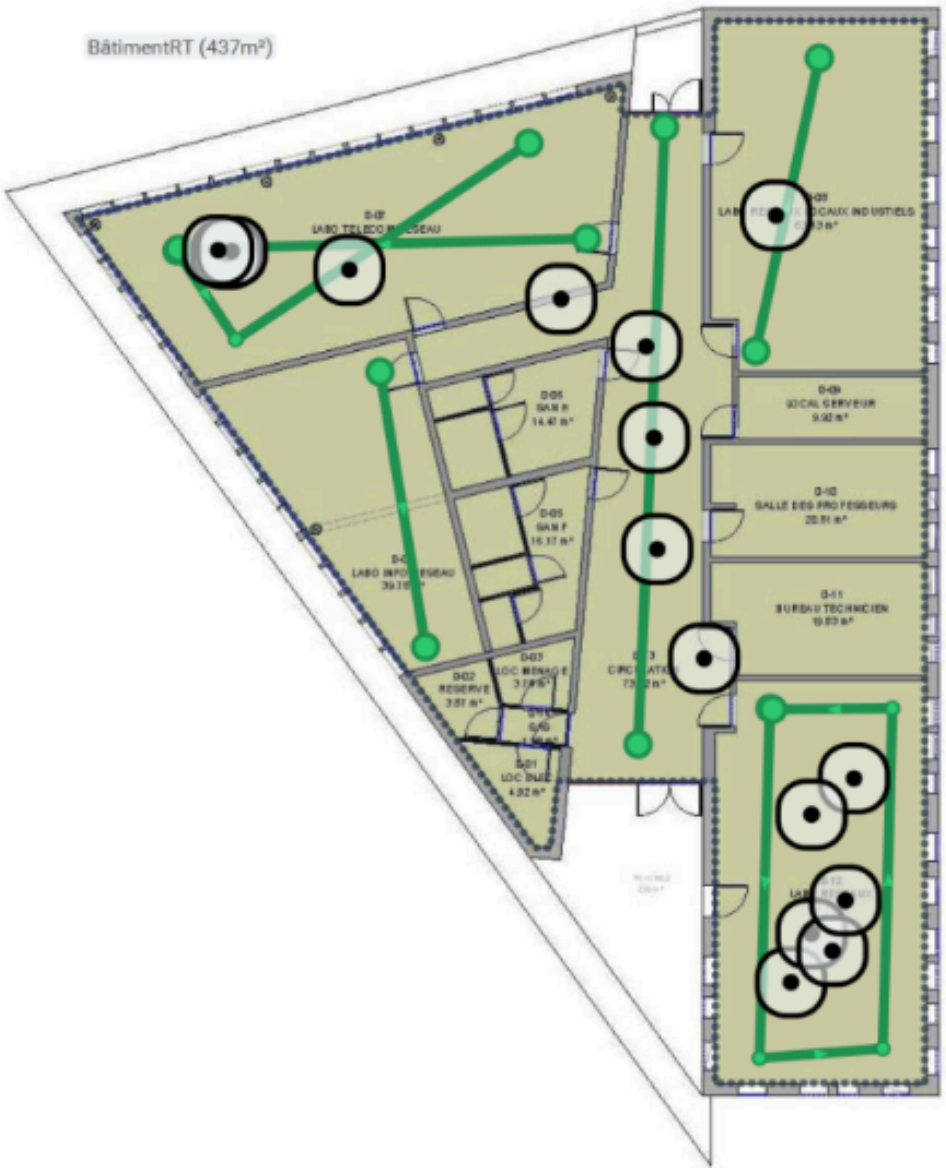


Schéma du Bâtiment RT

4.2. Analyse de la Couverture Actuelle (État des lieux)

L'audit a permis de mesurer la propagation des ondes sur les deux bandes de fréquences.

A. Bande de fréquences 2.4 GHz

- **Couverture (RSSI) :**

  La couverture est globalement satisfaisante sur la majorité du plateau (zones vertes > -65 dBm). Cependant, des faiblesses sont notées dans les angles du bâtiment (ex: Labo Telecom Réseau), où le signal chute vers -70/-75 dBm.

- **Santé du Réseau :**

  Malgré un signal fort, l'indicateur "Santé du réseau" affiche un statut "Échec" (Rouge) sur une grande partie de la surface. Cela indique que bien que le signal soit présent, la qualité de la liaison est dégradée, probablement due à des interférences ou une mauvaise configuration des canaux.

B. Bande de fréquences 5 GHz (Critique pour la Haute Densité)

- **Couverture (RSSI) :**

  La pénétration est logiquement plus faible qu'en 2.4 GHz. La zone centrale (couloir) est bien couverte, mais l'atténuation des murs (cloisons sèches/vitres) impacte les bureaux périphériques.

- **Redondance (Recouvrement) :**

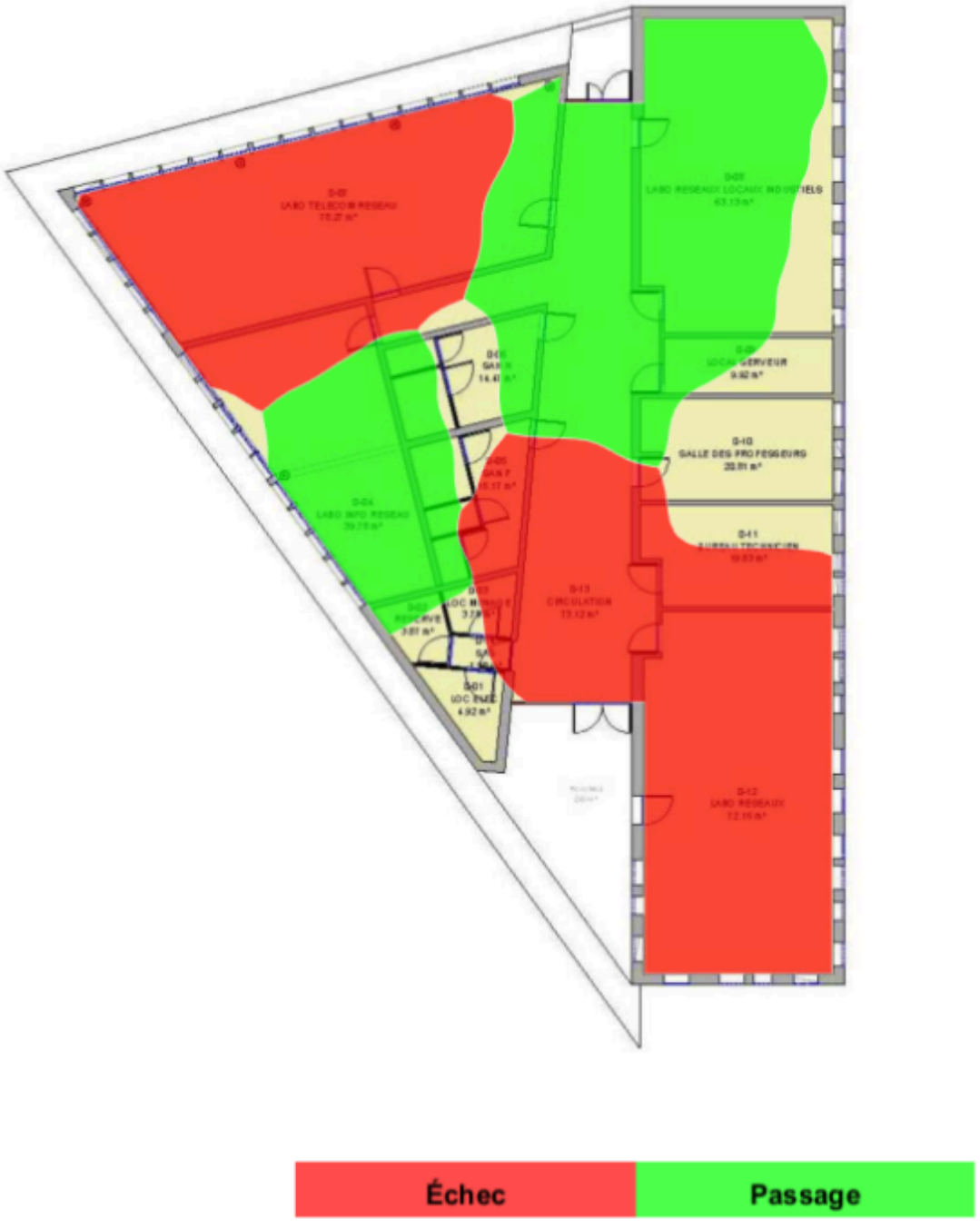
  La "puissance du signal secondaire" est insuffisante dans les bureaux (< -75 dBm).

  - Impact : En cas de panne d'une borne, les utilisateurs situés dans les bureaux (Technicien, Professeurs) perdront leur connexion. Le roaming (itinérance) risque d'être brutal.

Intensité du signal pour le Bâtiment RT à Bande de 5 GHz

On observe une atténuation significative du signal (zones jaunes/grises) à l'intérieur des bureaux périphériques, due à la traverse des cloisons.

Santé du réseau pour Bâtiment RT à Bande de 5 GHz.



Les zones rouges indiquent les emplacements où le réseau ne respecte pas les pré-requis de débit ou de stabilité pour des usages multimédias.

4.3. Analyse Spectrale et Interférences (Point Critique)

L'analyseur de spectre Sidekick a révélé des problèmes majeurs qui justifient le remplacement de l'infrastructure actuelle.

1. Présence d'Interférences Non-Wi-Fi (Continuous Transmitter)

L'audit révèle des zones rouges critiques sur la bande 5 GHz identifiées comme "Continuous Transmitter".

- **Observation :**

  Une source d'émission continue perturbe gravement le signal dans le couloir central et les zones adjacentes.

- **Conséquence :**

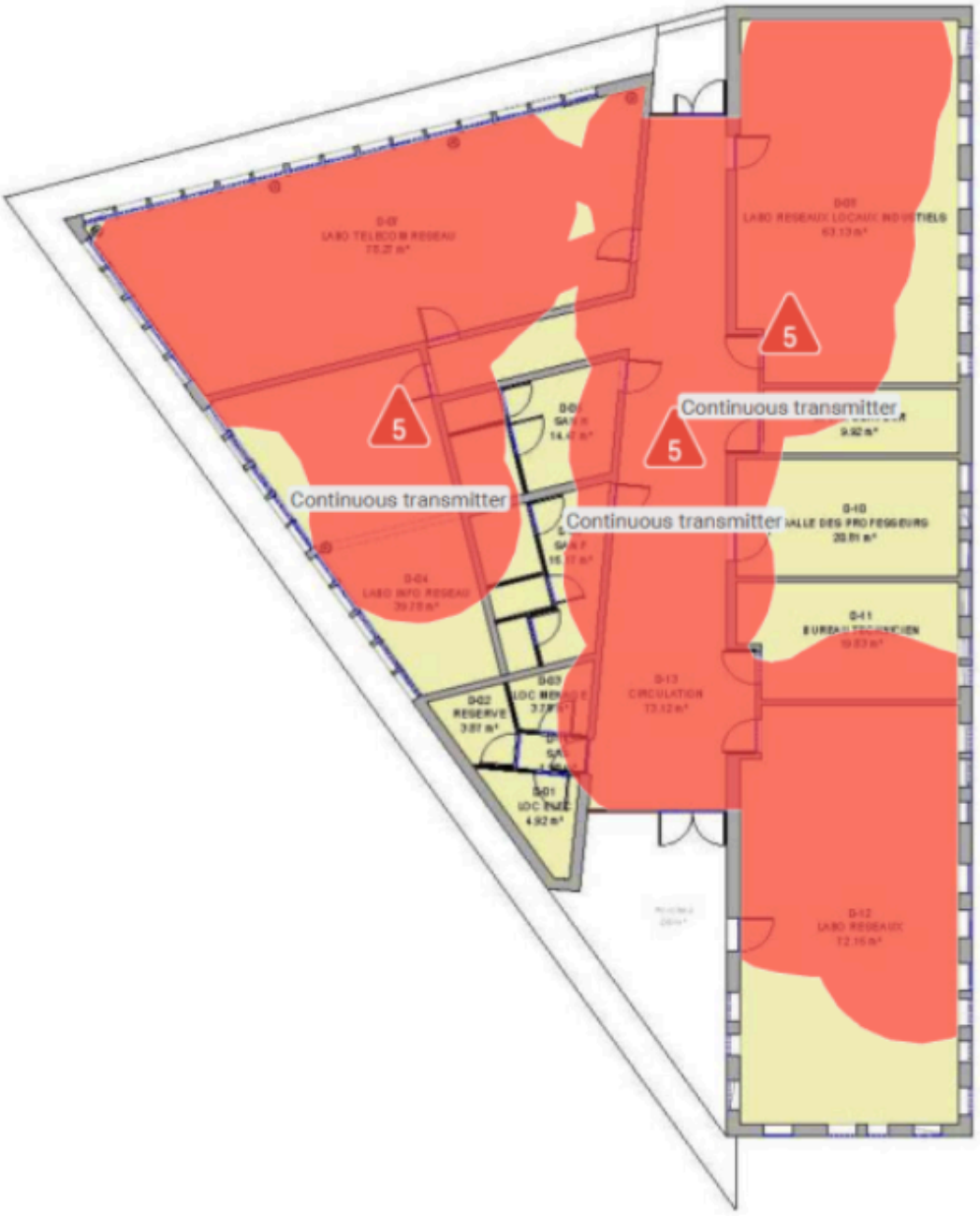
  Ce type d'interférence (souvent dû à des capteurs de mouvement défectueux, des caméras sans fil analogiques ou des équipements radar) sature le temps d'antenne. C'est la cause probable des "Échecs" constatés dans la santé du réseau.

2. Occupation des Canaux

L'infrastructure actuelle (bornes Cisco détectées) utilise des largeurs de canal hétérogènes.

- Certains canaux sont saturés à 100% d'utilisation, ce qui explique les lenteurs ressenties par le client.

Périphérique générant des interférences à Bande de 5 GHz.



Identification d'un émetteur continu (Continuous Transmitter) saturant la bande de fréquence 5 GHz et causant des pertes de paquets sévères dans la zone centrale.

4.4. Inventaire des Équipements Détectés

L'audit a permis de cartographier l'existant :

- **Matériel en place :**

  Points d'accès **Cisco** (Wi-Fi 6).

- **SSID diffusés :**

  EDUROAM, BIP_IUT, Irsf_UArtois, BEI_Tab.

- **Positionnement :**

  Les bornes sont principalement installées dans les couloirs (Mode "Carpeted hallway"). Ce positionnement est économique mais inadapté aux cloisons actuelles qui bloquent le 5 GHz vers les bureaux.

4.5. Préconisations pour le Déploiement Aruba (POC)

Sur la base de ces mesures, voici nos recommandations pour la nouvelle architecture :

1. **Changement de positionnement :**

   Ne pas remettre les bornes Aruba AP-505 exactement à la place des anciennes Cisco. Il faut privilégier une installation en quinconce entrant dans les grands bureaux (Labo Info, Labo Telecom) pour contourner l'atténuation des murs.

2. **Plan de Fréquences :**
   - Fixer la largeur de canal à **20 MHz sur la bande 2.4 GHz** pour éviter le recouvrement (seulement 3 canaux utilisables : 1, 6, 11).
   - Utiliser **40 MHz sur la bande 5 GHz** pour augmenter le débit sans trop risquer d'interférence.

3. **Traitement de l'interférence :**

   Avant la mise en production définitive, une "chasse à l'interférence" physique doit être menée pour localiser et éteindre l'émetteur "Continuous Transmitter" détecté en page 47 du rapport, sans quoi même le nouveau matériel Aruba subira des pertes de paquets.

V. TESTS ET VALIDATION

5.1. Tests de connectivité

Objectif : Prouver que chaque SSID distribue bien une adresse IP dans le bon VLAN et permet l'accès à Internet.

Protocole de test :

Pour chaque réseau (SSID), nous avons effectuer la manipulation suivante avec un PC portable ou un smartphone :

1. Se connecter au Wi-Fi (ex: CORP-SECURE).
2. Vérifier l'adresse IP obtenue.
3. Lancer un Ping vers Internet (Google DNS).

Preuve SSID CORP : On doit voir une IP en 192.168.10.x.
Preuve SSID GUEST : On doit voir une IP en 192.168.20.x.
Preuve SSID IOT : On doit voir une IP en 192.168.30.x.

Comme le démontrent les captures ci-dessous, le mécanisme DHCP est fonctionnel. Le PC connecté au SSID 'CORP-SECURE' a bien reçu l'adresse 192.168.10.51, confirmant son appartenance au VLAN 10.

5.2. Tests de l'itinérance (Roaming)

Objectif : Prouver que l'utilisateur ne perd pas sa connexion en passant d'une borne à l'autre (Haute disponibilité).

Protocole de test :

1. Se connecter au SSID CORP-SECURE.
2. On se place près de la Borne 1 (Master).
3. On lance un "Ping infini" vers Google pour surveiller la coupure.
    - Commande : ping 8.8.8.8 -t
4. L'action :
    - *Méthode Labo (sur table) :* Débranchez brutalement le câble Ethernet de la Borne 1.
    - *Méthode Réelle :* Marchez vers la Borne 2 jusqu'à ce que le PC bascule.

5. On observe le ping. On peut voir "Délai d'attente dépassé" une ou deux fois, puis ça repart.
6. On arrête le ping avec CTRL + C.

Lors de l'arrêt simulé de la borne Master, le service a basculé automatiquement sur la borne Esclave. Nous observons la perte d'un seul paquet ICMP (ping), ce qui est imperceptible pour l'utilisateur (ex: appel VoIP ou vidéo).

5.3. Validation de la sécurité(Isolation / ACL)

Objectif : C'est le test le plus important pour le client. Prouver qu'un Invité (Guest) ne peut pas pirater le réseau de l'entreprise.

Protocole de test :

1. Dans un premier temps, on se connecte au SSID GUEST-WIFI (VLAN 20).
2. Ensuite nous tentons d'accéder à Internet.
    - ping 8.8.8.8 → Succès.
3. Puis, on tente de "pinguer" la passerelle de management.
    - ping 192.168.99.254 → Échec (Délai d'attente dépassé). Ce qui prouve que cela fonctionne.
4. Et pour finir, on tente de "pinguer" un PC imaginaire du réseau Employé.
    - ping 192.168.10.254 → Échec. Ce qui ne fonctionne pas grâce au ACL.

Le test de segmentation confirme l'étanchéité des réseaux. Un utilisateur connecté au profil Invité a accès à Internet mais reçoit un 'Délai d'attente dépassé' lorsqu'il tente de joindre l'infrastructure interne. Les règles de pare-feu (ACL) sont donc effectives.

VI. RECOMMANDATIONS ET ÉVOLUTIONS

Suite à la validation technique du POC et à l'analyse de l'environnement radio, nous formulons les recommandations suivantes. Elles sont classées par horizon temporel afin de respecter les contraintes budgétaires actuelles tout en préparant l'avenir.

6.1. Recommandations à Court Terme (Déploiement immédiat)

Ces actions doivent être entreprises dès la mise en production des équipements pour garantir la stabilité du réseau sans coût supplémentaire.

A. Installation Physique et Câblage

- **Positionnement des bornes :** Conformément aux résultats de l'étude prédictive Ekahau, les bornes Aruba AP-505 doivent impérativement être installées au plafond (montage horizontal).
    - Justification : Les antennes omnidirectionnelles intégrées sont conçues pour diffuser le signal vers le bas ("effet douche"). Un montage mural vertical réduirait la portée utile de 40%.

- **Câblage :** Utilisation requise de câbles Catégorie 6 ou 6A.
    - Justification : Le Wi-Fi 6 (AX) peut dépasser le gigabit de débit. Un vieux câblage (Cat 5e) risquerait de créer un goulot d'étranglement.

B. Durcissement de la Configuration Radio (RF)

- **Gestion des canaux :** Bien que la technologie ARM (Adaptive Radio Management) d'Aruba gère les canaux automatiquement, nous recommandons de fixer manuellement la puissance de transmission (TX Power) entre 12 dBm (min) et 18 dBm (max).
    - Objectif : Éviter que les bornes ne "crient" trop fort, ce qui créerait des interférences entre elles (Co-channel interference) dans les zones denses.

- **Désactivation des protocoles hérités :** Confirmation de la désactivation du Wi-Fi 802.11b (obsolète) pour libérer du temps d'antenne (Airtime) au profit des terminaux récents.

6.2. Évolutions à Moyen Terme (Quand le budget le permettra)

A. Transition vers le Cloud (Aruba Central)

Actuellement, le réseau est géré localement (IAP). Nous recommandons à terme la migration vers **Aruba Central**.

- **Avantage :** Gestion unifiée via le Cloud, mises à jour programmées la nuit, et surtout accès à l'intelligence artificielle (AIOps) pour dépanner les lenteurs automatiquement.

- **Modèle économique :** Passage en mode abonnement (OpEx), évitant un gros investissement matériel.

B. Sécurité Avancée (NAC - ClearPass)

Pour renforcer la sécurité du réseau "CORP-SECURE", l'ajout d'un serveur **NAC (Network Access Control)** comme Aruba ClearPass est préconisé.

- **Plus-value :** Au lieu d'une simple vérification mot de passe, le réseau vérifiera l'état de santé du PC (Antivirus à jour ? Windows patché ?) avant d'autoriser l'accès.

- **Gestion des Invités :** Mise en place d'un portail "Sponsorisé" où l'invité reçoit ses codes par SMS ou est validé par l'employé qu'il visite.

6.3. Gestion du Cycle de Vie

- **Renouvellement du Switch de Cœur :** Le switch actuel assure le service, mais pour tirer pleinement profit du Wi-Fi 6, un passage vers des switches **Multi-Gigabit (SmartRate)** sera à envisager d'ici 3 ans pour supporter des débits supérieurs à 1 Gbps par borne.

- **WPA3 :** Dès que le parc de PC portables de l'entreprise sera renouvelé (compatibilité des cartes réseaux), nous recommandons de basculer le SSID "CORP" exclusivement en **WPA3-Enterprise** pour une sécurité inviolable.

VII. CONCLUSION

Conclusion Générale du Rapport

Le POC réalisé démontre que la solution basée sur les bornes **Aruba AP-505** en mode Instant (**IAP**) répond parfaitement aux exigences du cahier des charges :

1. **Économique :**

   Aucune acquisition de contrôleur physique n'est nécessaire.

2. **Performante :**

   La technologie Wi-Fi 6 et l'optimisation "Haute Densité" assurent une expérience utilisateur fluide.

3. **Sécurisée :**

   La segmentation stricte par VLANs (10, 20, 30) et les pare-feux intégrés garantissent l'étanchéité des flux.

L'équipe technique valide donc la faisabilité du déploiement à grande échelle sur la base de cette architecture.