Dossier de Conception - Installation de Bornes WiFi

1. Présentation de l'entreprise

Nom de l'entreprise : [Valve]
Secteur d'activité : [Jeux-vidéos]
Nombre d'employés : [17]

L'entreprise souhaite améliorer la connectivité de ses locaux en installant un réseau WiFi sécurisé et segmenté selon trois catégories d'utilisateurs : les invités, la DSI (Direction des Systèmes d'Information) et les salariés.

---

2. Besoins et Objectifs

L'objectif principal est de fournir une connexion sans fil sécurisée et adaptée aux besoins de chaque type d'utilisateur :

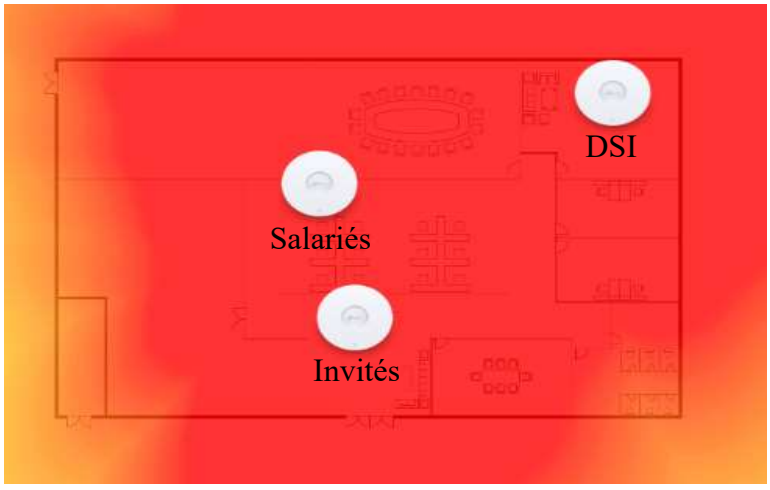
- **WiFi Invités** : Accès limité avec un système de Voucher (accès temporaire et contrôlé).
- **WiFi DSI** : Réseau sécurisé et isolé pour l'administration et la gestion informatique.
- **WiFi Salariés** : Accès au réseau interne avec des restrictions adaptées aux usages professionnels.

---

3. Architecture Réseau Prévue

L'infrastructure sera conçue pour garantir la **sécurité, la performance et la segmentation des flux**. Elle inclura :

- **Trois SSID distincts** (Valve_Invites, Valve_DSI, Valve_Salaries).
- **Contrôle d'accès et gestion des priorités** via un firewall et le contrôleur WiFi Omada.
- **Un serveur d’authentification** intégré au contrôleur Omada pour la gestion des vouchers.
- **Gestion centralisée des bornes WiFi** avec la plateforme Omada SDN.



4. Matériel et Logiciels Utilisés

Matériel

- **3 bornes WiFi Omada** (TP-Link EAP225, EAP245, ou EAP660HD).
- **1 routeur/firewall** (TP-Link ER605 ou autre modèle compatible Omada).
- **Switch**
- **Serveur d'authentification intégré à Omada pour le WiFi invités.**

Logiciels

- **Omada Controller** pour la gestion des bornes et des SSID.
- **Portail captif Omada** pour la gestion des vouchers invités.
- **Outils de monitoring et logs intégrés à Omada SDN.**

---

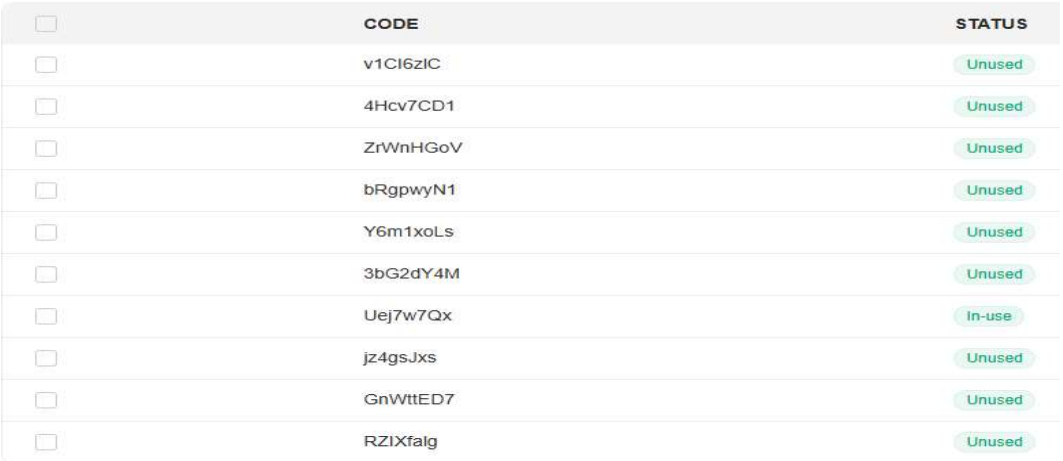
5. Mise en Place des Bornes WiFi et Système de Voucher

Configuration des SSID

SSID	Sécurité
Valve_Invites	WPA2 + portail captif avec voucher
Valve_DSI	WPA3-Enterprise avec authentification RADIUS
Valve_Salaries	WPA2-Enterprise avec accès restreint

Gestion des Vouchers pour les invités

- Utilisation du **portail captif intégré à Omada**.
- Génération de vouchers depuis l'interface Omada Controller.
- Durée de validité paramétrable 1 jour.
- Limitation de la bande passante et des accès selon les besoins.



	CODE	STATUS
☐	v1CI6zlC	Unused
☐	4Hcv7CD1	Unused
☐	ZrWnHGoV	Unused
☐	bRgpwyN1	Unused
☐	Y6m1xoLs	Unused
☐	3bG2dY4M	Unused
☐	Uej7w7Qx	In-use
☐	jz4gsJxs	Unused
☐	GnWttED7	Unused
☐	RZIXfalg	Unused

6. Plan de Sécurisation du Réseau

- **Isolation des SSID** : Aucune interconnexion directe entre les réseaux, sauf exceptions définies.
- **Filtrage des accès** :
  - Valve_Invites → Accès restreint à Internet uniquement.
  - Valve_Salaries → Accès aux ressources internes limité.
  - Valve_DSI → Accès complet mais avec authentification renforcée.
- **Activation du firewall Omada** pour restreindre les flux indésirables.
- **Surveillance et logs** : Activation des logs d'accès via Omada SDN.

---

7. Conclusion

Ce projet de mise en place d'un réseau WiFi segmenté avec Omada permettra de garantir **sécurité, performance et flexibilité** pour les différents types d'utilisateurs. La gestion des accès via Omada Controller et l'authentification centralisée assureront une meilleure protection des données et une administration simplifiée.