**Lab Configuration d’un point d’accès WI-FI Cisco Airone**

**Dans ce laboratoire, nous allons configurer un réseau Wi-Fi à l'aide d'un point d'accès Cisco PoE et d'un commutateur. Ce lab permet de comprendre le processus de mise en place d'un réseau sans fil sécurisé en utilisant des équipements Cisco et des commandes de base. En suivant les instructions pas à pas, vous mettrez en place un réseau Wi-Fi fonctionnel, sécuriserez les transmissions et validerez que le SSID est visible pour les clients sans fil.**

**Matériel Requis :**

* 1 commutateurs Cisco 3750 PoE(Power Over Ethernet) .
* 1 PC .
* 1 AP point d'accès Wi-Fi Cisco PoE .
* Câbles Ethernet .
* Câble série RS232.
* Adaptateur USB/RS232.

**Schéma Maquettte physique :**

**SW**

**Port Eth PoE**

AP wifi Cisco

**Câble série RS232/ USB**

PC



**Étape 1 : Connexion au point d'accès**

Connectez un pc équipé d'un émulateur de terminal tel Putty ou minicom(ubuntu) a l’interfaces console de l’AP a laide d'un câble console et de l’adaptateur USB/RS232 et bronchez l’AP via un câble Ethernet sur au port PoE du SW.

**Étape 2 : Réinitialiser la configuration de l’AP**

ap> enable Password: [Entrez le mot de passe «Cisco» ap#erase startup-config ap#reload

**Étape 3 : Configuration du SSID et de la sécurité**

Dans ce scénario, nous allons configurer un SSID (nom du réseau wifi) et activer la sécurité WPA avec une clé pré-partagée (PSK).

ap> enable Password: [Entrez le mot de passe «Cisco»

ap#conf t Enter configuration commands, one per line. End with CNTL/Z. ap(config)#

ap(config)# no logging console

(config) # dot11 ssid equipeX

(config-ssid) # authentication open

(config-ssid) # authentication key-management wpa

(config-ssid) # wpa-psk ascii equipeXX

(config-ssid)# guest-mode

(config-ssid) # exit

**Explication :**

**no logging console :** Est utilisée pour désactiver l’affichage des messages de journalisation

(logging) dans la consolen de l'appareil. Lorsque l'administrateur travaille directement dans la console de l'appareil, les messages de journalisation constants peuvent perturber les tâches de configuration ou de diagnostic. **dot11 ssid equipeX** : Définit un nouveau SSID (équipeX) pour le réseau Wi-Fi.

**authentication open** : Configure l'authentification en mode "open". Cela signifie que l'authentification sera ouverte, permettant à n'importe quel périphérique de tenter de s'authentifier.

**authentication key-management wpa** : Configure la gestion des clés en utilisant le protocole WPA (Wi-Fi Protected Access). WPA améliore la sécurité par rapport au protocole d'authentification WEP (Wired Equivalent Privacy).

**wpa-psk ascii equipeXX** : :Est utilisé pour configurer la clé pré-partagée (PSK) WPA, qui est essentiellement le mot de passe permettant l'authentification sur le réseau Wi-Fi. Le choix du mot de passe est déterminé par la partie ascii equipeX, où "equipeX" est le mot de passe réel (ou la clé pré-partagée).

**Étape 4 : Configuration de l'interface radio**

Nous allons maintenant configurer l'interface radio du point d'accès.

(config) # interface dot11Radio 0

(config-if) # encryption mode ciphers aes-ccm

(config-if) # ssid equipeX

(config-if) # channel least-congested

(config-if) # no shutdown

(config-if) # exit **Explication :**

**interface dot11Radio 0** : Cela indique que vous souhaitez accéder à la configuration de l'interface sans fil (radio) numéro 0.

**encryption mode ciphers aes-ccmi :** indique que le point d'accès Wi-Fi Cisco utilisera l'algorithme AES en mode CCM pour chiffrer les données sur le réseau Wi-Fi, assurant ainsi la confidentialité et l'intégrité des transmissions. Ces paramètres sont typiquement utilisés dans le contexte de la sécurité WPA (Wi-Fi Protected Access) sur les réseaux sans fil.

**ssid equipeX** : Associe l'interface au SSID (équipeX) spécifié. Cela indique que cette interface sera utilisée pour le réseau Wi-

Fi avec le SSID "équipeX".

**channel least-congested** : Configure le canal Wi-Fi pour être automatiquement déterminé comme le canal le moins encombré. Cela peut améliorer les performances en évitant les canaux congestionnés.

**Étape 5 : Sauvegarde de la configuration**

Enfin, assurez-vous de sauvegarder votre configuration pour qu'elle persiste après un redémarrage.

Ap # write memory

**Étape 6 : Vérification de la visibilité du SSID "equipeX"**

Pour vous assurer que le SSID "equipeX" est correctement configuré et visible, suivez ces étapes :

1. Sur le PC client, assurez-vous que la carte Wi-Fi est activée.
2. Ouvrez le gestionnaire de réseaux sans fil sur le PC client.

Sous Windows, cela peut être fait en cliquant sur l'icône Wi-Fi dans la barre des tâches.

Sous Linux, vous pouvez utiliser des commandes comme iwlist ou des gestionnaires de réseaux spécifiques.

Sous macOS, utilisez l'icône Wi-Fi dans la barre de menus.

1. Recherchez la liste des réseaux Wi-Fi disponibles.

Vous devriez voir le SSID "equipeX" dans la liste des réseaux disponibles.

1. Vérifiez que le SSID "equipeX" est affiché avec la sécurité WPA activée.

Cela confirme que le SSID est diffusé par le point d'accès, et il est configuré avec la sécurité WPA que vous avez définie précédemment.

Cette vérification s'assure que le réseau Wi-Fi que vous avez configuré est visible et prêt à être utilisé par les périphériques clients.