



**Dossier de projet n°0 :**

Mise en place d'une solution Wi-Fi  
sécurisée

Dylan CHAU  
Axel BAUGÉ

2A-SISR

**ASSURMER**





Date de création : 17/01/2023

Version : 1.0

Pour validation : DSI

A destination : DSI

Mode de diffusion : Intranet Nombre

de pages : 86

## Métadonnées

Diffusion			
Périmètre de diffusion	Contrôlé	Interne	Libre

Historique des évolutions		
Auteur	Version	Objet de la version et liste des modifications
Dylan Chau et Axel Baugé	1.0	Initialisation du document

Validation			
Rédacteur		Valideur	
Nom	Date	Nom	Date
Dylan Chau et Axel Baugé	14/02/2023	DSI	14/02/2023
Date d'application : 14/02/2023			

## Table des matières



Métadonnées.....	2
Table des matières.....	3
I. Présentation du Wi-Fi et étude comparative.....	4
1. Qu'est-ce que le Wi-Fi ?.....	4
2. Les composantes.....	4
a) La porteuse.....	4
b) L'antenne.....	5
c) Les normes.....	6
3. Les protocoles de sécurité Wi-Fi : étude comparative.....	7
WEP (Wired Equivalent Privacy).....	7
WPA (Wi-Fi Protected Access).....	7
WPA2.....	8
WPA3.....	8
II. Procédure d'installation et de configuration des cellules Wi-Fi	<b>Erreur ! Signet non défini.</b>
III. Présentation et procédure Radius.....	<b>Erreur ! Signet non défini.</b>
IV. Tests d'intégration.....	<b>Erreur ! Signet non défini.</b>
V. Guide d'accompagnement utilisateur.....	<b>Erreur ! Signet non défini.</b>
VI. Planning et répartition des tâches.....	<b>Erreur ! Signet non défini.</b>
VII. Glossaire.....	<b>Erreur ! Signet non défini.</b>
VIII. Références.....	<b>Erreur ! Signet non défini.</b>
IX. Annexes.....	<b>Erreur ! Signet non défini.</b>



## 1. Qu'est-ce que le Wi-Fi ?

Le Wi-Fi (de l'anglais Wireless Fidelity) est une technologie de réseau sans fil permettant aux périphériques tels que les ordinateurs, les périphériques mobiles et les équipements divers (imprimantes, caméras) d'accéder à Internet mais également de communiquer entre eux sans besoin de connexion filaire.

Cette technologie permet la transmission de données grâce des ondes électromagnétiques et radioélectriques en haut-débit garantissant une liberté de mouvement au sein de la zone couverte par le réseau sans fil.

L'appellation Wi-Fi est à la base une marque déposée qui, à l'origine, désignait le nom de la certification donnée par la Wi-Fi Alliance, anciennement WECA (Wireless Ethernet Compatibility Alliance), organisme ayant pour mission de spécifier l'interopérabilité entre les matériels conformes à la norme 802.11 et de vendre le label « Wi-Fi » aux matériels répondant à ses spécifications.



Plus simple à retenir, le nom Wi-Fi est désormais aussi utilisé dans la vie de tous les jours pour désigner un réseau répondant la norme IEEE 802.11. Dans certains pays, on utilise également le terme « WLAN ».

## 2. Les composantes

### a) La porteuse

Afin de transporter les ondes électromagnétiques, il est nécessaire d'utiliser une « porteuse ». L'onde est modifiée pour transporter et transmettre l'information et sert de fondement à la communication sans fil entre un appareil et un réseau WiFi. Elle permet ainsi d'encoder les données à transmettre, en modulant la fréquence ou l'amplitude, où différentes valeurs du signal représentent différentes données numériques.

La porteuse, avec une fréquence spécifique (Le plus souvent en GHz : nombre de périodes du signal pendant une seconde), est essentielle pour la transmission et la réception efficaces des données dans un environnement Wi-Fi.

Plus la fréquence est élevée, plus le débit que l'on souhaite obtenir pourra être élevé.

## b) L'antenne



Afin de guider la porteuse, il est nécessaire d'avoir un guide d'ondes, que l'on désigne par le terme « antenne ».

Elle est utilisée pour émettre, mais aussi de réceptionner les ondes électromagnétiques. Divers types de données, y compris des informations informatiques peuvent alors être transmises. Cette capacité permet une utilisation quotidienne plus flexible sans nécessité d'une connexion filaire.

Selon sa forme et sa longueur, les ondes sont diffusées de différentes manières. Les deux types d'antennes Wi-Fi les plus courants sont les modèles :

- Omnidirectionnels (couverture à 360°), très répandues.
  - Dipôle (En tige, sur certains équipements comme les caméras)
  - Colinéaire (Sur les toits) ○ Patch (Principalement dans les smartphones) - Directionnels (faisceau focalisé).

### c) Les normes



Afin d'assurer l'interopérabilité entre les différents systèmes équipés de carte WiFi, la norme IEEE802.11 établit les bases des réseaux Wi-Fi.

Elle introduite pour la première fois en 1997 par l'Institut des Ingénieurs électriciens et électroniciens (IEEE). Elle a révolutionné la manière dont nous accédons à Internet en permettant la connexion sans fil à des réseaux locaux. Elle permet de choisir une fréquence porteuse entre 14 canaux différents afin de réduire les interférences, optimiser l'utilisation de la bande-passante et la flexibilité dans des environnements denses.

Depuis sa création, elle a connu de nombreuses évolutions afin d'être amélioré en termes de vitesse de transmission, portée et sécurité des connexions sans fil.

#### Tableau récapitulatif des principales normes IEEE 802.11 utilisées :

<b>IEEE 802.11n (Wi-Fi 4)</b>	Introduit en 2009, le Wi-Fi 4 a permis de supporter les bandes de fréquences de 2,4 GHz et 5 GHz et introduire le Multiple Input Multiple Output (MIMO) afin d'améliorer la vitesse de transmission et réduire les erreurs. Avec des débits pouvant atteindre 600 Mbit/s, cette norme a permis une utilisation plus large des réseaux WLAN en remplacement des réseaux filaires.
<b>IEEE 802.11ac (Wi-Fi 5)</b>	Lancée en 2013, la norme Wi-Fi 5 a permis d'atteindre des débits allant jusqu'à 3,5 Gbit/s grâce à une bande passante plus large, l'ajout de canaux supplémentaires, une meilleure modulation, et l'extension des capacités MIMO. Cette norme a fonctionné exclusivement sur la bande des 5 GHz, offrant ainsi des vitesses gigabit et réduisant les interférences avec d'autres appareils.
<b>IEEE 802.11ax (Wi-Fi 6)</b>	Le Wi-Fi 6, publié en 2021, se concentre sur l'amélioration de l'efficacité spectrale et la gestion de la densité du réseau. Bien que sa vitesse théorique atteigne 9,6 Gbit/s, l'objectif principal de cette norme est de gérer efficacement le trafic dans des zones à forte densité de Wi-Fi, grâce à des mécanismes multi-utilisateurs et à l'amélioration de la portée et de la consommation d'énergie pour les opérations extérieures.
<b>IEEE 802.11be (Wi-Fi 7)</b>	Le Wi-Fi 7 lancé en 2024 représente la norme la plus récente, prévu pour offrir des vitesses quatre fois plus rapides que le Wi-Fi 6, avec des débits théoriques d'environ 40 Gbit/s. Cette norme promet également de doubler la largeur de bande à 320 MHz et d'apporter des améliorations significatives en termes de latence, de prise en charge des appareils et de performances dans des environnements Wi-Fi encombrés.

Les bornes Wi-Fi d'ASSURMER fonctionnent avec les normes IEEE 802.11n et 802.11ac.

### 3. Les protocoles de sécurité Wi-Fi : étude comparative



Afin d'assurer la protection du réseau en matière de Wi-Fi, les données qui transitent entre deux machines d'un même réseau sont chiffrées à l'aide de protocoles de sécurité.

Pour rendre les réseaux sans fil plus sûrs et plus efficaces, ces protocoles font régulièrement l'objet de modifications et mises à jour pour faire face à de nouvelles failles de sécurité.

Ainsi, plusieurs protocoles de sécurité ont été développés et sont WEP, WPA, WPA2, WPA3. Ils ont le même objectif, mais leur fonctionnement est bien différent.

#### WEP (Wired Equivalent Privacy)

Introduit en 1999, le WEP a été la première solution de chiffrement pour protéger les réseaux Wi-Fi.

**Fonctionnement** : Le protocole utilise l'algorithme de chiffrement RC4 pour l'authentification et le chiffrement. Elle combine une clé de chiffrement prédéfinie de 64 bits ou 128 bits avec un vecteur d'initialisation (IV) de 24 bits pour renforcer le chiffrement.

**Sécurité** : Considéré comme faible en raison de la petite taille de l'IV et de la gestion des clés statiques qui permet un échange avec une clé unique, elle rend le réseau vulnérable aux attaques. L'information transite en clair sur le réseau. En raison des nombreuses failles que le WEP présente, il a été abandonné depuis 2004. En outre, il est très facile de casser la clé WEP avec aircrack-ng.

#### WPA (Wi-Fi Protected Access)

Régi par la norme IEEE802.11i et introduit en 2003, le WPA est une amélioration du WEP en corrigeant la majorité de ses problèmes.

**Fonctionnement** : Le protocole introduit l'utilisation du protocole TKIP (Temporal Key Integrity Protocol) pour améliorer la sécurité par rapport au WEP. TKIP utilise des clés de 256 bits, le mélange de clés par paquet, et une vérification d'intégrité du message. Le protocole WPA dispose également de 2 modes de fonctionnement : WPA-Personal et WPA-Enterprise, proposant ainsi 2 méthodes d'authentification différentes, PSK (Pre-Shared Key) et EAP (Extensible Authentication Protocol).

**Sécurité** : Plus sûr que le WEP, TKIP est également considéré comme vulnérable en raison de son utilisation continue de l'algorithme RC4 et de sa rétrocompatibilité avec WEP.

## WPA2



Introduit en 2004, le WPA2 est une amélioration du WPA et suit la continuité de la norme IEEE802.11i.

**Fonctionnement** : L'amélioration la plus significative est le remplacement du RC4/TKIP par l'AES (Advanced Encryption Standard) qui est un protocole de chiffrement symétrique et CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol), offrant une meilleure sécurité et intégrité des données. Le WPA2 utilise AES, mais peut également utiliser TKIP pour une rétrocompatibilité (pour qu'il puisse accepter les connexions WPA). Il propose également les 2 modes de fonctionnement du WPA.

**Sécurité** : Considéré comme très sécurisé, le protocole a été compromis en 2017 par la vulnérabilité KRACK (Key Reinstallation Attacks) qui exploitait une faiblesse dans la procédure de handshake quatre voies.

## WPA3

Introduit en 2018 et en réponse à la vulnérabilité KRACK, il s'agit du successeur du WPA2, introduisant des fonctionnalités et une couche de sécurité supplémentaire à la fois pour l'usage personnel et pour les entreprises.

**Fonctionnement** : Le protocole ajoute une meilleure protection contre les attaques par force brute grâce au protocole SAE (Simultaneous Authentication of Equals) basé sur Diffie-Hellman key exchange et utilise un chiffrement individuel des données avec des clés plus longues (jusqu'à 256 bits pour le mode entreprise).

**Sécurité** : Considéré comme le protocole le plus sécurisé à ce jour, il adresse les faiblesses des protocoles précédents et offre des protections supplémentaires contre les attaques modernes. Malheureusement, une faille (Dragonblood) a déjà mis à mal ce protocole sans pour autant le condamner.

### Tableau récapitulatif :

Protocole	Chiffrement	Authentification	Remarques
WEP	RC4 (64 ou 128 bits)	Clés statiques	Facilement piratable, désormais considéré comme obsolète.
WPA (Personal et Enterprise)	TKIP (128 bits)	PSK ou EAP	Plus sûr que le WEP, néanmoins vulnérable à des attaques par « injection de paquets ».
WPA2 (Personal et Enterprise)	AES (128 ou 256 bits)	PSK ou EAP	Standard actuel, offre une bonne sécurité et performance, vulnérable à KRACK.
WPA3	AES (192 ou 256 bits)	SAE	Plus sécurisé, protège contre les attaques par force brute, encore émergent.





Pour un dispositif moderne, il est recommandé d'utiliser WPA2 ou WPA3 pour assurer une sécurité optimale du réseau Wi-Fi.

WPA2 est actuellement le protocole le plus répandu et supporté par la plupart des appareils, tandis que WPA3 offre une meilleure sécurité nécessitant du matériel compatible plus récent (Obligatoire sur les équipements Wifi 6).

**/!\ WEP et WPA sont considérés comme moins sécurisés et doivent être évités absolue**





Dylan CHAU  
Axel BAUGÉ

2A-SISR

# Procédure d'installation et de configuration du Cisco WAP371

Date de création : 26/09/2023

Version : 1.0

Pour validation : DSI

A destination : DSI

Mode de diffusion : Intranet

Nombre de pages : 11

Auteur : CHAU Dylan



## Métadonnées

Diffusion			
Périmètre de diffusion	Contrôlé	Interne	Libre

Historique des évolutions		
Auteur	Version	Objet de la version et liste des modifications
Dylan Chau	1.0	Initialisation du document

Validation			
Rédacteur		Valideur	
Nom	Date	Nom	Date
Dylan Chau	22/11/2023	DSI	20/12/2023
Date d'application : 13/01/2024			



## Table des matières

Table des matières.....	3
Prérequis .....	3
Déploiement du Cisco WAP371 .....	4
1) Préparation de la borne Wifi.....	4
a) Réinitialisation en paramètre d'usine.....	4
b) Mise à jour de la borne .....	5
c) Configuration des paramètres réseaux .....	6
d) Création des points d'accès Wifi.....	8

## Prérequis

- Un switch avec les VLANs 110, 120, 300 configurés et les ports trunkés en R1 et SW48
- Un serveur AD, DNS, DHCP configuré + les étendues users et guests
- Un câble RJ45
- Le Cisco WAP371 branché sur le VLAN 110 et avec une IP DHCP



## Déploiement du Cisco WAP371

### 1) Préparation de la borne Wifi

#### a) Réinitialisation en paramètre d'usine

- Appuyer sur le bouton « RESET » à l'arrière de la borne avec un stylo ou un objet fin pendant environ 10 secondes.

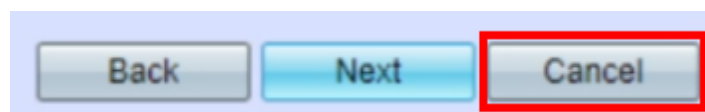


- Le point d'accès va redémarrer pendant une minute et sera ensuite prêt avec les paramètres par défaut.
- Sur votre serveur AD, dans le gestionnaire DHCP, se rendre dans la plage d'IP du VLAN 110 et récupérer l'IP attribuée à la borne Wi-Fi. Il est nécessaire de mettre le port du switch en mode access. Dans notre cas, il faudra taper : <https://172.16.0.101> pour accéder à l'interface de configuration.

	Adresse IP du client	Nom	Expiration du bail	Type	ID unique	Description	Protection d'accès réseau
DHCP	172.16.0.10	wap311a10.assurm...	Réservation (active)	DHCP	7001b5311...	AP	Accès complet

- Une page de connexion va s'afficher. Les credentials par défaut sont
  - o username : cisco
  - o password : cisco

- Une fenêtre de configuration rapide va apparaître, cliquer sur « Cancel ».

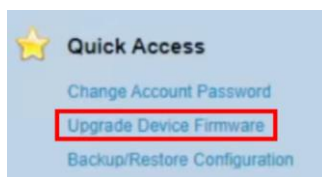


- Changer le mot de passe.



## b) Mise à jour de la borne

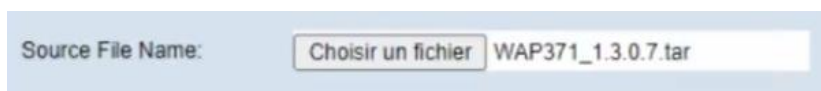
- Dans le menu « Quick Access », cliquer sur « Upgrade Device Firmware ».



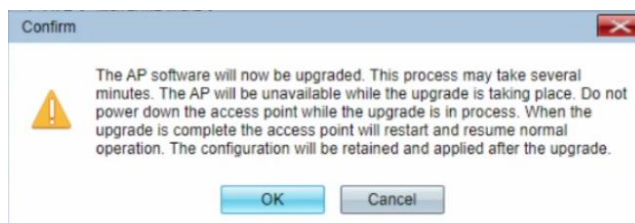
- Récupérer le firmware sur le site de Cisco :  
<https://software.cisco.com/download/home/286154471/type/282463166/release/1.3.0.7>
- Sélectionner la méthode de transfert HTTP/HTTPS pour permettre le transfert du fichier via le navigateur Web. La méthode TFTP nécessite quelques manipulations supplémentaires avec notamment un serveur TFTP.



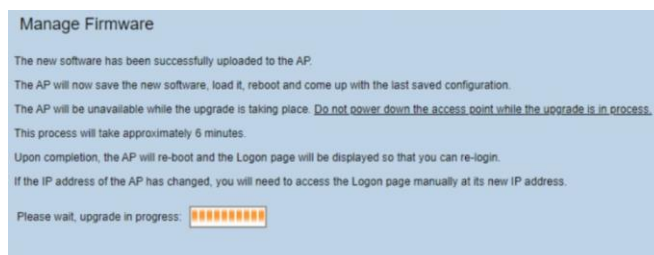
- Cliquer sur « Choisir un fichier » et sélectionner le fichier Firmware.



- Cliquer sur « Upgrade ». Une fenêtre de confirmation va apparaître. Cliquer sur « OK ». L'installation va démarrer.



- Une page de progression va apparaître. L'opération peut durer plusieurs minutes. Le point d'accès va ensuite redémarrer.

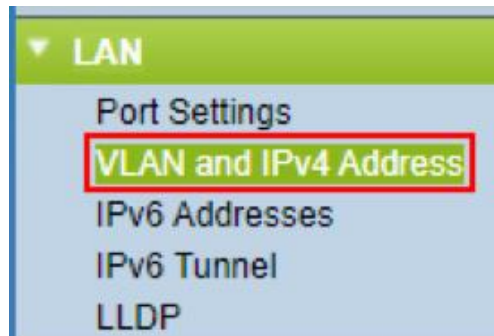


- Le point d'accès est désormais prêt à être configuré.



### c) Configuration des paramètres réseaux

- Cliquer sur « LAN » puis « VLAN and IPv4 Address ».



- Renseigner les informations dans « IPv4 Settings » en se basant sur la topologie Assumer.

IPv4 Settings

Connection Type:  DHCP  
 Static IP

Static IP Address: 172 . 16 . 0 . 10

Subnet Mask: 255 . 255 . 255 . 0

Default Gateway: 172 . 16 . 0 . 254

Domain Name Servers:  Dynamic  
 Manual

172 . 16 . 0 . 1

172 . 16 . 0 . 9

- Changer ensuite le VLAN de management afin de maintenir l'accès après la modification de la configuration du matériel réseau.

Global Settings

MAC Address: 70:01:B5:31:1A:10

Untagged VLAN:  Enable

Untagged VLAN ID: 1 (Range: 1 - 4094, Default: 1)

Management VLAN ID: 110 (Range: 1 - 4094, Default: 1)

- Se rendre dans l'onglet « Wireless » puis « Radio ».







- Dans « Basic Settings », cliquer sur « enable » pour activer les bandes de fréquences wifi 2.4GHz et 5Ghz.

**Radio Setting Per Interface**

Select the radio interface first, and then enter the configuration parameters.

Radio:  Radio 1 (5 GHz)  Radio 2 (2.4 GHz)

---

**Basic Settings**

Radio:  Enable

MAC Address: 70:01:B5:31:1A:10

Mode: 802.11a/n/ac

Channel Bandwidth: 80 MHz

Primary Channel: Lower

Channel: Auto

- En fonction de l'environnement, il est également possible de modifier des paramètres dans « Advanced Settings ».

**Advanced Settings**

DFS Support: On

Short Guard Interval Supported: Yes

Protection: Auto

Beacon Interval: 100 (Milliseconds (Range: 20 - 2000, Default: 100))

DTIM Period: 2 (Range: 1-255, Default: 2)

Fragmentation Threshold: 2346 (Even Numbers (Range: 256 - 2346, Default: 2346))

RTS Threshold: 65535 (Range: 0-65535, Default: 65535)

Maximum Associated Clients: 200 (Range: 0-200, Default: 200)

Transmit Power: Full - 100%

Frame-burst Support: Off (Boosts Downstream Throughput)

Fixed Multicast Rate: Auto Mbps

Legacy Rate Sets:

Rate (Mbps)	54	48	36	24	18	12	9	6
Supported	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Basic	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

- Dans « Administration » puis « HTTP/HTTPS service », cliquer sur « Generate SSL Certificate » pour activer le HTTPS.

**Administration**

- System Settings
- User Accounts
- Time Settings
- Log Settings
- Email Alert
- LED Display
- HTTP/HTTPS Service**
- Management Access Control
- Manage Firmware
- Download/Backup Configuration
- Configuration Files Properties
- Copy/Save Configuration
- Reboot
- Discovery - Bonjour
- Packet Capture
- Support Information

HTTPS Port: 443 (Range: 1025-65535)

Save

**Generate SSL Certificate**

Generate

**SSL Certificate File Status**

Certificate File Present: Yes

Certificate Expiration Date: Jan 25 11:46:49 2044 GMT

Certificate Issuer Common Name: CN=172.16.0.10



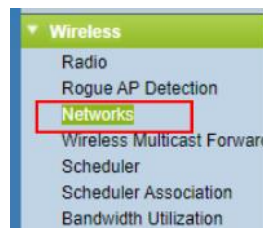
## d) Création des points d'accès Wifi

Nous allons créer 3 points d'accès différents :

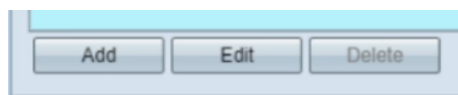
- Un point d'accès en WPA-Personal (Guest).
- Deux points d'accès en WPA-Enterprise (Admin et User) qui permettront de fournir la sécurité nécessaire pour les réseaux sans fil dans un environnement professionnel avec un serveur RADIUS.

### Cellule WPA-Personal Invité

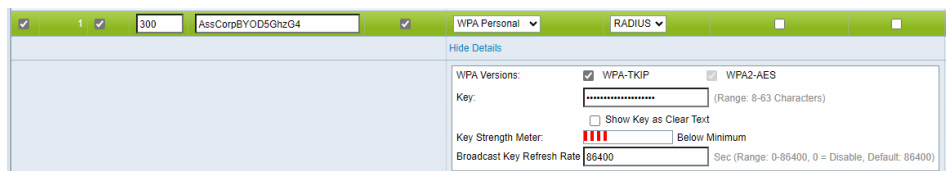
- Cliquer sur « Wireless » puis « Networks ».



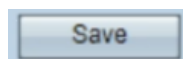
- Sur la radio 5Ghz, cliquer sur « Add ».



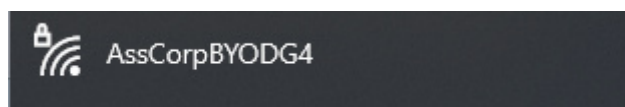
- Renseigner ensuite le SSID, le VLAN, la sécurité en « WPA Personal » et laisser le « SSID Broadcast » coché. Ajouter la clé de sécurité.



- En fonction des équipements de l'infrastructure, il se peut que certains ne soient pas compatibles avec la norme IEEE 802.11ac. Il faudra donc configurer la radio 2.4Ghz également (norme IEEE 802.11n et antérieures).
- Cliquer sur « Save ».



- Notre premier point d'accès est prêt. Il nécessite de connaître la clé de sécurité.





## Cellule WPA Enterprise Admin et Users

Nous allons maintenant créer les points d'accès en WPA-Enterprise qui fonctionneront avec un serveur Radius.

- Cliquer sur « System Security » puis « Radius Server ».



- Renseigner l'IP du serveur Radius, la clé secrète et cocher la case Radius accounting pour mesurer les ressources consommées.

RADIUS Server

Server IP Address Type:  IPv4  
 IPv6

Server IP Address-1:  (xxx.xxx.xxx.xxx)

Server IP Address-2:  (xxx.xxx.xxx.xxx)

Server IP Address-3:  (xxx.xxx.xxx.xxx)

Server IP Address-4:  (xxx.xxx.xxx.xxx)

Key-1:  (Range: 1 - 64 Characters)

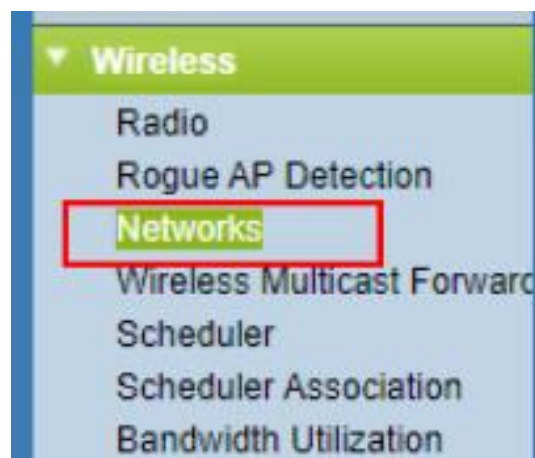
Key-2:  (Range: 1 - 64 Characters)

Key-3:  (Range: 1 - 64 Characters)

Key-4:  (Range: 1 - 64 Characters)

RADIUS Accounting:  Enable

- Retourner sur « Wireless » puis « Networks ».

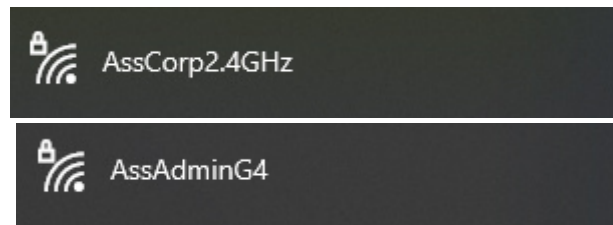




- Ajouter les points d'accès en « WPA Enterprise ». Renseigner le SSID, les VLANs et cocher la case « Use global RADIUS server settings ». Répéter l'opération pour les 2 bandes de fréquence.

Virtual Access Points (SSIDs)									
VAP No.	Enable	VLAN ID	SSID Name	SSID Broadcast	Security	MAC Filter	Channel Isolation	Band Steer	
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	120	AssCorp5GHz	<input checked="" type="checkbox"/>	WPA Enterprise	RADIUS	<input type="checkbox"/>	<input type="checkbox"/>	
<a href="#">Show Details</a>									
<input type="checkbox"/>	<input checked="" type="checkbox"/>	300	AssCorpBYOD5GhzG4	<input checked="" type="checkbox"/>	WPA Personal	RADIUS	<input type="checkbox"/>	<input type="checkbox"/>	
<a href="#">Show Details</a>									
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	110	AssAdmin5GhzG4	<input checked="" type="checkbox"/>	WPA Enterprise	RADIUS	<input type="checkbox"/>	<input type="checkbox"/>	
<a href="#">Hide Details</a>									
WPA Versions: <input checked="" type="checkbox"/> WPA-TKIP <input type="checkbox"/> WPA2-AES <input checked="" type="checkbox"/> Enable pre-authentication <input checked="" type="checkbox"/> Use global RADIUS server settings									

- Les point d'accès en WPA Enterprise sont prêts. Il faut faire des modifications sur le serveur NPS.



- Sur le firewall PfSense, ajouter les règles nécessaires pour empêcher un accès aux ressources internes sur le Wi-Fi Guest.

<input type="checkbox"/>	<input checked="" type="checkbox"/>	0/0 B	IPv4 TCP/UDP	172.16.201.0/24	*	DCs	*	*	none
<input type="checkbox"/>	<input checked="" type="checkbox"/>	0/0 B	IPv4 TCP/UDP	172.16.201.0/24	*	172.16.0.0/24	*	*	none
<input type="checkbox"/>	<input checked="" type="checkbox"/>	0/0 B	IPv4 TCP/UDP	172.16.201.0/24	*	DMZ net	*	*	none
<input type="checkbox"/>	<input checked="" type="checkbox"/>	0/0 B	IPv4 TCP/UDP	172.16.0.0/24	*	DMZ net	*	*	none