



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.



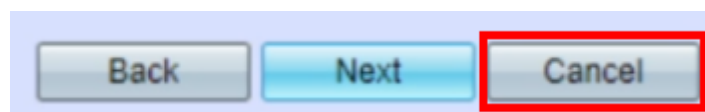
- Le point d'accès va redémarrer pendant une minute et sera ensuite prêt avec les paramètres par défaut.
- Sur votre serveur AD, dans le gestionnaire DHCP, se rendre dans la plage d'IP du VLAN 110 et récupérer l'IP attribuée à la borne Wi-Fi. Il est nécessaire de mettre le port du switch en mode access. 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 ».

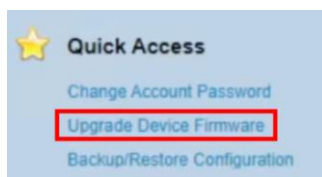


- Changer le mot de passe.



b) Mise à jour de la borne

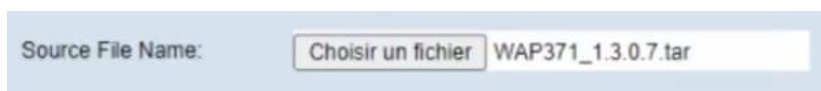
- Dans le menu « Quick Access », cliquer sur « Upgrade Device Firmware ».



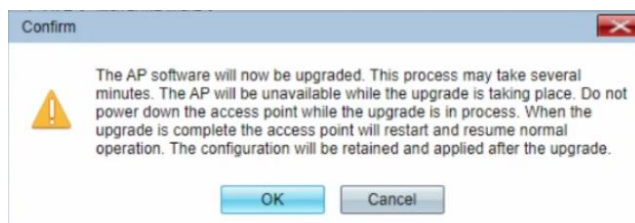
- Récupérer le firmware sur le site de Cisco :
<https://software.cisco.com/download/home/286154471/type/282463166/release/1.3.0.7>
- Sélectionner la méthode de transfert HTTP/HTTPS pour permettre le transfert du fichier via le navigateur Web. La méthode TFTP nécessite quelques manipulations supplémentaires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



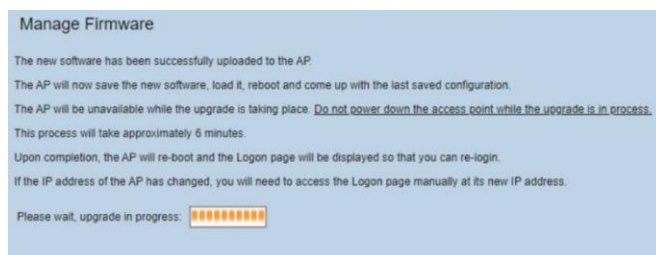
- Cliquer sur « Choisir un fichier » et sélectionner le fichier Firmware.



- 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.

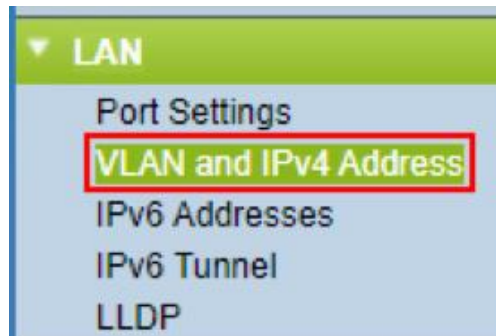


- Le point d'accès est désormais prêt à être configuré.



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



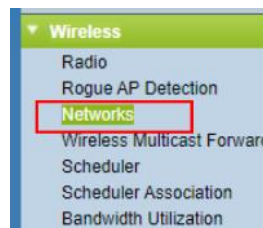
d) Création des points d'accès Wifi

Nous allons créer 3 points d'accès différents :

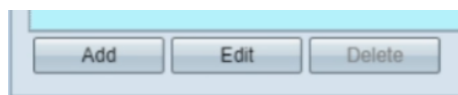
- Un point d'accès en WPA-Personal (Guest).
- Deux points d'accès en WPA-Enterprise (Admin et User) qui permettront de fournir la sécurité nécessaire pour les réseaux sans fil dans un environnement professionnel avec un serveur RADIUS.

Cellule WPA-Personal Invité

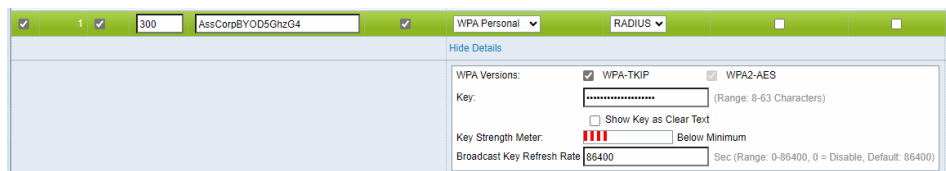
- Cliquer sur « Wireless » puis « Networks ».



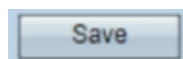
- Sur la radio 5Ghz, cliquer sur « Add ».



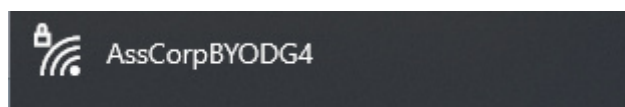
- Renseigner ensuite le SSID, le VLAN, la sécurité en « WPA Personal » et laisser le « SSID Broadcast » coché. Ajouter la clé de sécurité.



- 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)

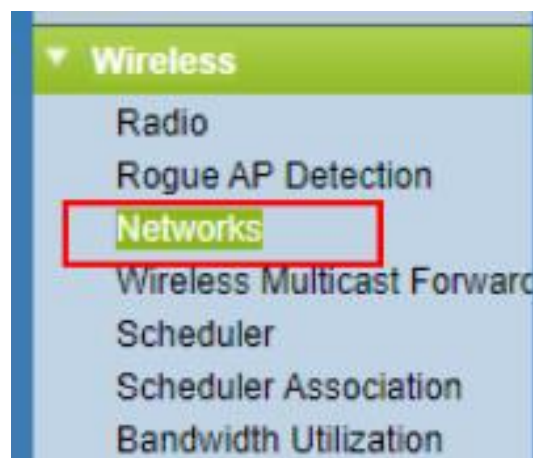
Key-2: (Range: 1 - 64 Characters)

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

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

RADIUS Accounting: Enable

- Retourner sur « Wireless » puis « Networks ».

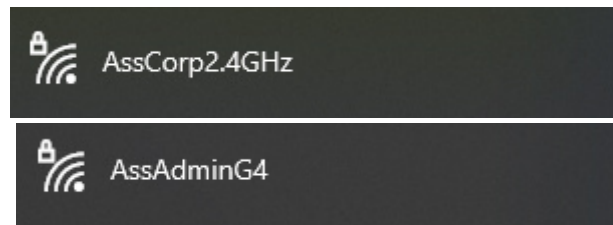




- Ajouter les points d'accès en « WPA Enterprise ». Renseigner le SSID, les VLANs et cocher la case « Use global RADIUS server settings ». Répéter l'opération pour les 2 bandes de fréquence.

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"/>	
Show Details									
<input type="checkbox"/>	<input checked="" type="checkbox"/>	300	AssCorpBYOD5GhzG4	<input checked="" type="checkbox"/>	WPA Personal	RADIUS	<input type="checkbox"/>	<input type="checkbox"/>	
Show Details									
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	110	AssAdmin5GhzG4	<input checked="" type="checkbox"/>	WPA Enterprise	RADIUS	<input type="checkbox"/>	<input type="checkbox"/>	
Hide Details									
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