Installation Cisco vWLC

>>> Virtual Wireless Controller Cisco 8.0.140

Description :

Le but de cette article est d'apprendre à mettre en place un contrôleur Wifi Cisco Virtuelle sur Vmware Workstation. Puis dans un second temps, l'article détaillera l'installation et la configuration du contrôleur WIFI.

Installation Cisco vWLC

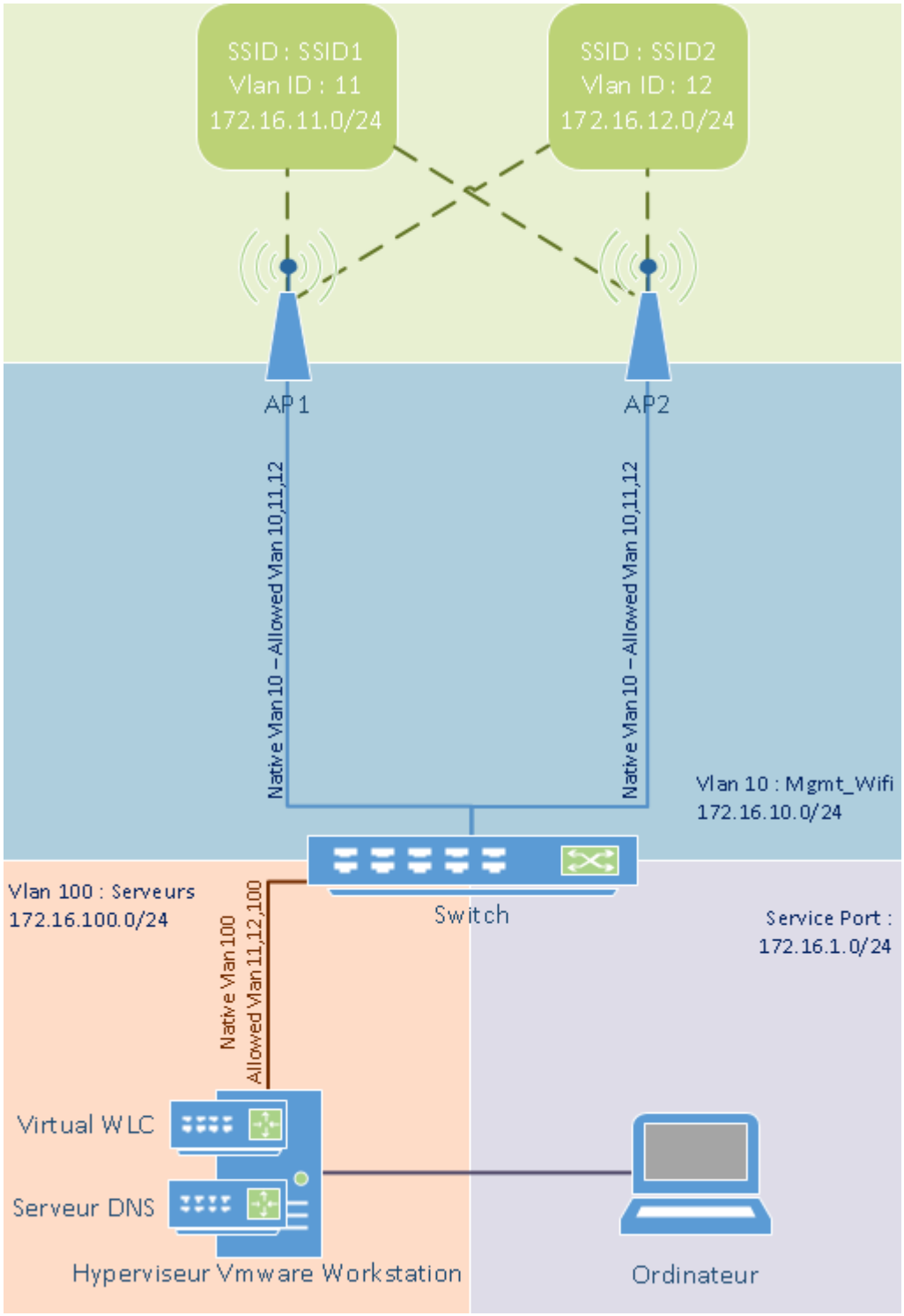
>>> Virtual Wireless Controller Cisco 8.0.140

Sommaire :

I) Introduction

Les contrôleurs Wifi permettent de gérer la couverture Wifi d'une entreprise, mono ou multi bâtiment.
Les contrôleurs sans fil sont responsables des politiques de sécurité, la prévention d'intrusion, la gestion de RF, la qualité du service (QoS), et la mobilité.
Ils offrent à l'administrateur plus de souplesse pour la mise en place de son réseau sans fil, la gestion, la maintenance et la sécurité.
Les contrôleurs sans fil s'intègrent facilement dans les réseaux existants d'entreprise. Ils communiquent avec les points d'accès au-dessus de la couche 2 (Ethernet) ou la couche 3 (IP) en utilisant le protocole léger de point d'accès (LWAPP).
Les contrôleurs Wifi virtuelle, permettent d'appliquer les avantages de la virtualisation à l'équipement réseaux.

Pour notre LAB, nous allons réaliser le réseau suivant :



Quelques informations :
Le contrôleur Wifi utilise 2 interfaces réseaux :

- Une interface pour le Service Port :
  - Interface d'administration du contrôleur
  - Correspond à notre réseau 172.16.1.0/24
  - Nous allons configurer l'adresse 172.16.1.200/24
- Une interface Management :
  - Interface pour dialoguer avec les bornes et les autres équipements réseaux (DNS, Radius)
  - Correspond à notre réseau 172.16.100.0/24
  - Nous allons configurer l'adresse 172.16.100.200/24

Notre LAB possède un serveur DNS (172.16.100.250) qui résout les noms suivants :

- cisco-lwapp-controller -> 172.16.100.200
- cisco-capwap-controller -> 172.16.100.200

- wlc-idum-lab -> 172.16.100.200
- sw-idum-lab -> 172.16.100.253
- Deb-idum-lab -> 172.16.100.250

Le switch de notre LAB, fait office de serveur DHCP.

II) Configuration du switch

1) config de base

Nous commençons par réaliser une configuration de base de notre switch.

- Configuration du domaine et des DNS :

```
switch(config)#hostname sw-idum-lab
sw-idum-lab(config)#ip domain-name idum.eu
sw-idum-lab(config)#ip name-server 172.16.100.250
```

- Configuration de l'accès au switch :

```
sw-idum-lab(config)#enable secret Mot_De_Passe
sw-idum-lab(config)#username admin privilege 15 secret Mot_De_Passe
sw-idum-lab(config)#crypto key generate rsa
sw-idum-lab(config)#Choose the size of the key modulus in the range of 360 to 4096 for your
General Purpose Keys. Choosing a key modulus greater than 512 may take
a few minutes.

How many bits in the modulus [512]:
2048
% Generating 2048 bit RSA keys, keys will be non-exportable...
sw-idum-lab(config)#ip ssh version 2
sw-idum-lab(config)#line vty 0 15
sw-idum-lab(config-line)#transport input
sw-idum-lab(config-line)#logging synchronous
sw-idum-lab(config-line)#login local
sw-idum-lab(config-line)#exit
```

- Déclaration des vlans :

```
sw-idum-lab(config)#vlan 10
sw-idum-lab(config-vlan)#name Mgmt_Wifi
sw-idum-lab(config-vlan)#exit
sw-idum-lab(config)#vlan 11
sw-idum-lab(config-vlan)#name SSID1
sw-idum-lab(config-vlan)#exit
sw-idum-lab(config)#vlan 12
sw-idum-lab(config-vlan)#name SSID2
sw-idum-lab(config-vlan)#exit
sw-idum-lab(config)#vlan 100
sw-idum-lab(config-vlan)#name Serveurs
sw-idum-lab(config-vlan)#exit
```

- Configuration des interfaces Vlans :

```
sw-idum-lab(config)#interface Vlan10
```

```
sw-idum-lab(config-if)#description Mgmt_Wifi
sw-idum-lab(config-if)#ip address 172.16.10.254 255.255.255.0
sw-idum-lab(config-if)#exit
sw-idum-lab(config)#interface Vlan11
sw-idum-lab(config-if)#description SSID1
sw-idum-lab(config-if)#ip address 172.16.11.254 255.255.255.0
sw-idum-lab(config-if)#exit
sw-idum-lab(config)#interface Vlan12
sw-idum-lab(config-if)#description SSID2
sw-idum-lab(config-if)#ip address 172.16.12.254 255.255.255.0
sw-idum-lab(config-if)#exit
sw-idum-lab(config)#interface Vlan100
sw-idum-lab(config-if)#description Serveurs
sw-idum-lab(config-if)#ip address 172.16.100.254 255.255.255.0
sw-idum-lab(config-if)#exit
```

2) Configuration du serveur DHCP

Nous allons configurer 4 pool DHCP, un pool pour les bornes, un pool pour le Vlan Serveurs et 2 pool pour les SSID.
- Pour éviter de configurer une adresse IP sur chaque borne. Ci-dessous la configuration du serveur DHCP pour le Vlan 10 :

```
sw-idum-lab(config)#ip dhcp pool Mgmt_Wifi
sw-idum-lab(dhcp-config)#network 172.16.10.0 255.255.255.0
sw-idum-lab(dhcp-config)#default-router 172.16.10.254
sw-idum-lab(dhcp-config)#domain-name idum.eu
sw-idum-lab(dhcp-config)#dns-server 172.16.100.250
```

- Ci-dessous la configuration du serveur DHCP pour le Vlan 100 :

```
sw-idum-lab(config)#ip dhcp pool Serveurs
sw-idum-lab(dhcp-config)#network 172.16.100.0 255.255.255.0
sw-idum-lab(dhcp-config)#default-router 172.16.100.254
sw-idum-lab(dhcp-config)#domain-name idum.eu
sw-idum-lab(dhcp-config)#dns-server 172.16.100.250
```

- Ci-dessous la configuration du serveur DHCP pour le Vlan 11 correspondant au SSID1 :

```
sw-idum-lab(config)#ip dhcp pool SSID1
sw-idum-lab(dhcp-config)#network 172.16.11.0 255.255.255.0
sw-idum-lab(dhcp-config)#default-router 172.16.11.254
sw-idum-lab(dhcp-config)#domain-name idum.eu
sw-idum-lab(dhcp-config)#dns-server 172.16.100.250
```

- Ci-dessous la configuration du serveur DHCP pour le Vlan 12 correspondant au SSID2 :

```
sw-idum-lab(config)#ip dhcp pool SSID2
sw-idum-lab(dhcp-config)#network 172.16.12.0 255.255.255.0
sw-idum-lab(dhcp-config)#default-router 172.16.12.254
sw-idum-lab(dhcp-config)#domain-name idum.eu
sw-idum-lab(dhcp-config)#dns-server 172.16.100.250
```

3) Configuration des interfaces

Mon switch est un Cisco 2960 avec :

- 8 interface FastEthernet
- 1 interface GigabitEthernet

La machine virtuelle du contrôleur Wifi est connecté sur l'interface Gi0/1. Les bornes seront connectés sur les interfaces fa 0/1 - 6.

- Voici la configuration pour le serveur :

```
sw-idum-lab(config)#interface GigabitEthernet0/1
sw-idum-lab(config-if)#description "Vers Serveurs"
sw-idum-lab(config-if)#switchport mode trunk
sw-idum-lab(config-if)#switchport trunk native vlan 100
sw-idum-lab(config-if)#switchport trunk allowed vlan 11-12,100
sw-idum-lab(config-if)#switchport nonegotiate
sw-idum-lab(config-if)#spanning-tree portfast
sw-idum-lab(config-if)#exit
```

- Voici la configuration des interfaces pour les bornes :

```
sw-idum-lab(config)#interface range fa0/1 - 7
sw-idum-lab(config-if)#description "Bornes Wifi"
sw-idum-lab(config-if)#switchport mode trunk
sw-idum-lab(config-if)#switchport trunk native vlan 10
sw-idum-lab(config-if)#switchport trunk allowed vlan 10-12
sw-idum-lab(config-if)#switchport nonegotiate
sw-idum-lab(config-if)#spanning-tree portfast
sw-idum-lab(config-if)#exit
```

- Voici la configuration des interfaces pour le Vlan Data :

```
sw-idum-lab(config)#interface fa0/8
sw-idum-lab(config-if)#description "PC Admin"
sw-idum-lab(config-if)#switchport mode access
sw-idum-lab(config-if)#switchport access vlan 100
sw-idum-lab(config-if)#switchport nonegotiate
sw-idum-lab(config-if)#spanning-tree portfast
sw-idum-lab(config-if)#exit
```

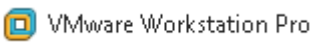
III) Déploiement OVA

Comme indiqué dans l'introduction, je vais commencer cette article par déployer le fichier OVA sur Vmware Workstation.

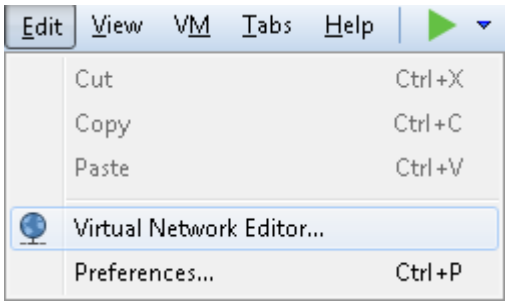
Vous trouverez le fichier OVA sur le site de cisco.com.

1) Préparation de Vmware

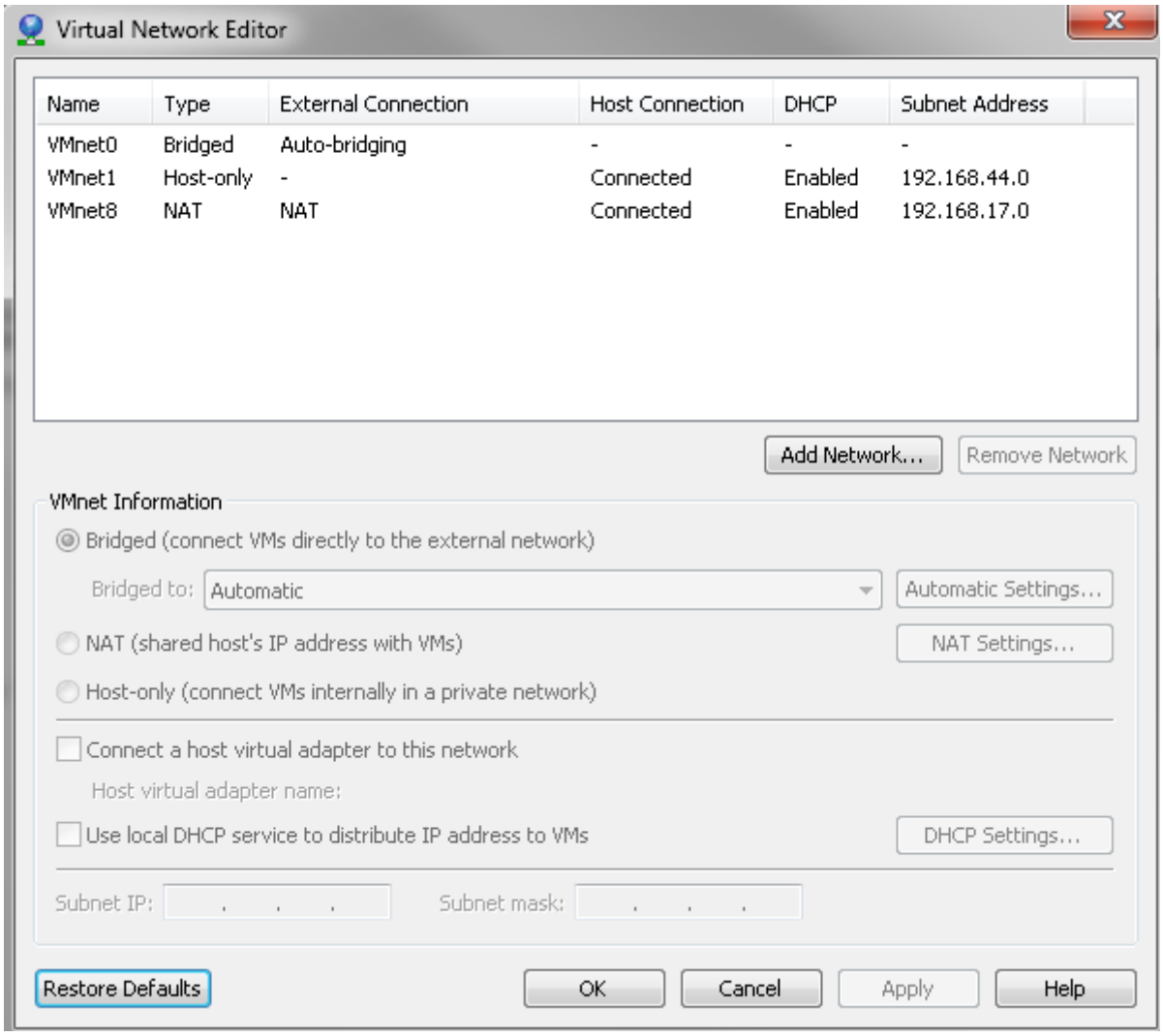
- Ouvrez VmWare Workstation.



- Dans le menu **"Edit"**, cliquez sur **"Virtual Network Editor"**.

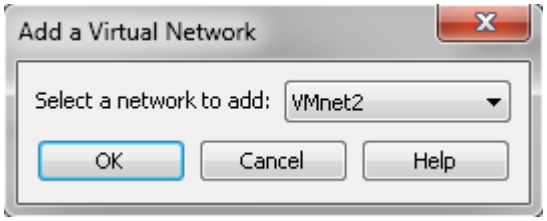


- Vous devez obtenir cette fenêtre :

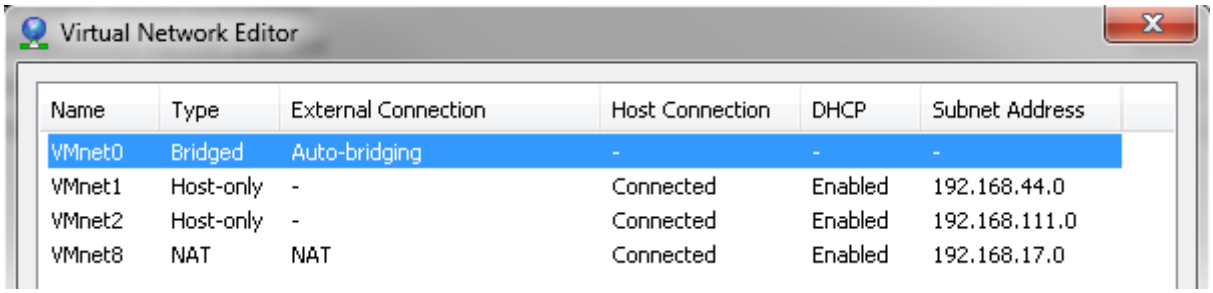


- Cliquez sur "**Add Network**".

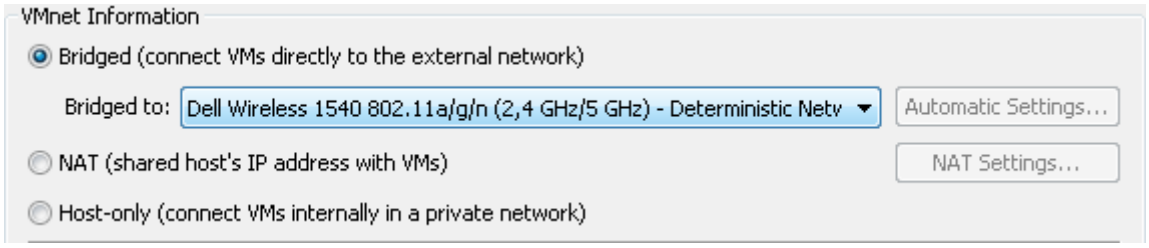
- Sélectionnez une interface dans la liste, puis cliquez sur "**OK**".



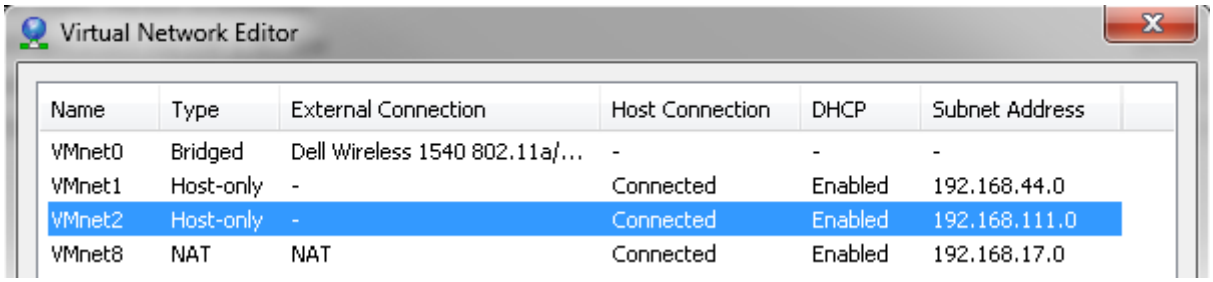
- Sélectionnez l'interface "**VMnet0**".



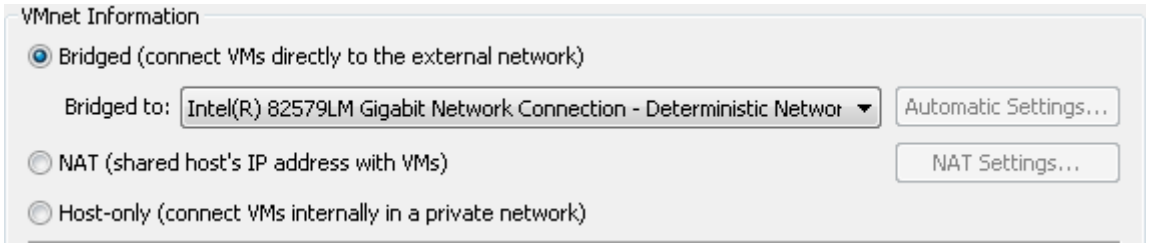
- Changez la valeur du menu déroulant pour sélectionner une interface physique.



- Sélectionnez l'interface que vous avez ajouté précédemment.



- Sélectionnez le mode "**Bridget**", puis changez la valeur du menu déroulant pour sélectionner une interface physique différente de VMnet0.

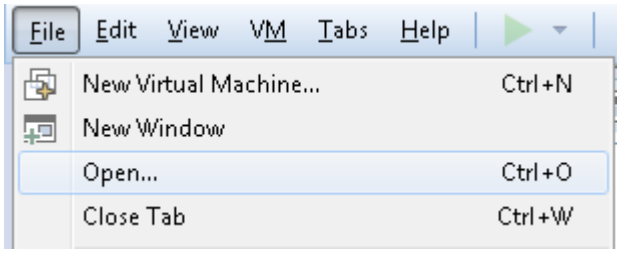


- Cliquez sur "**OK**".

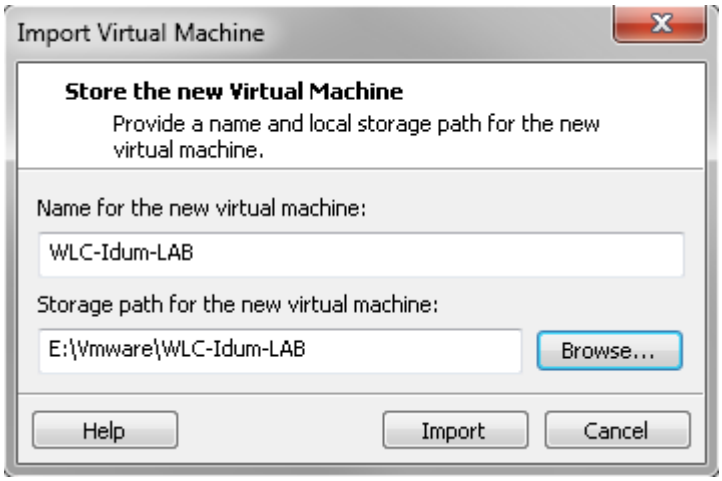
2) Déploiement OVA

Maintenant que la configuration de Vmware Workstation est prête, nous pouvons déployer l'OVA.

- Dans le menu "**File**", cliquez sur "**Open**".

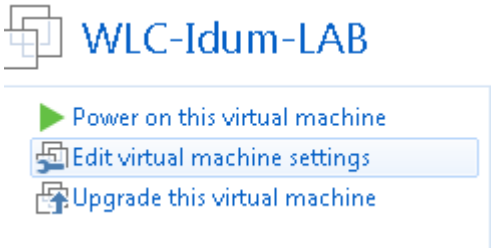


- Sélectionnez le fichier OVA. Puis définissez un nom à la VM. Cliquez sur "**Import**"

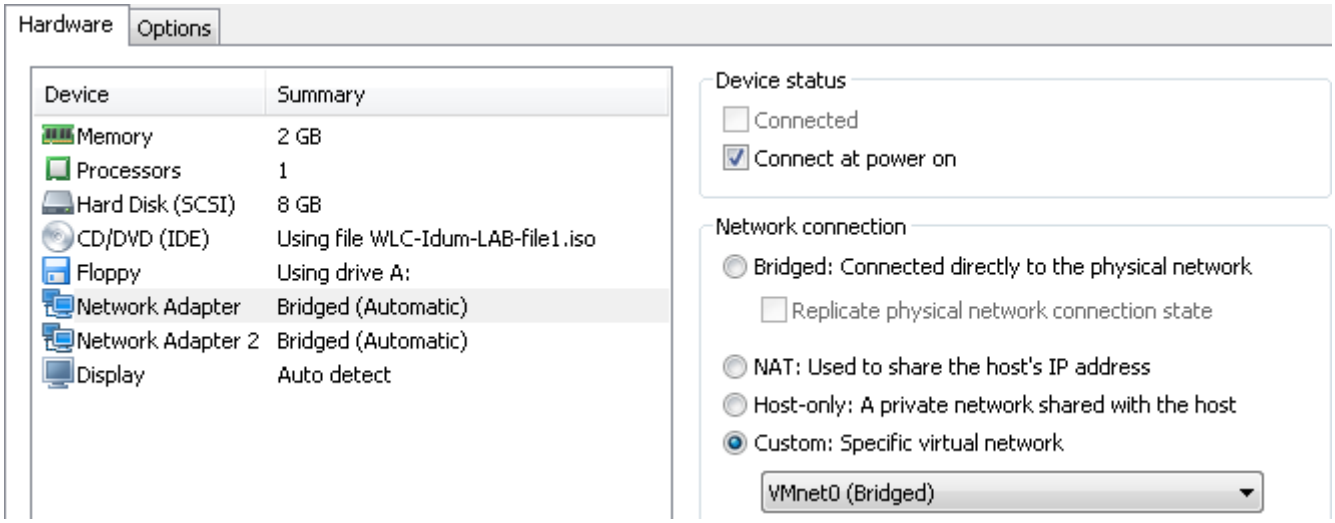


3) Modification de la VM

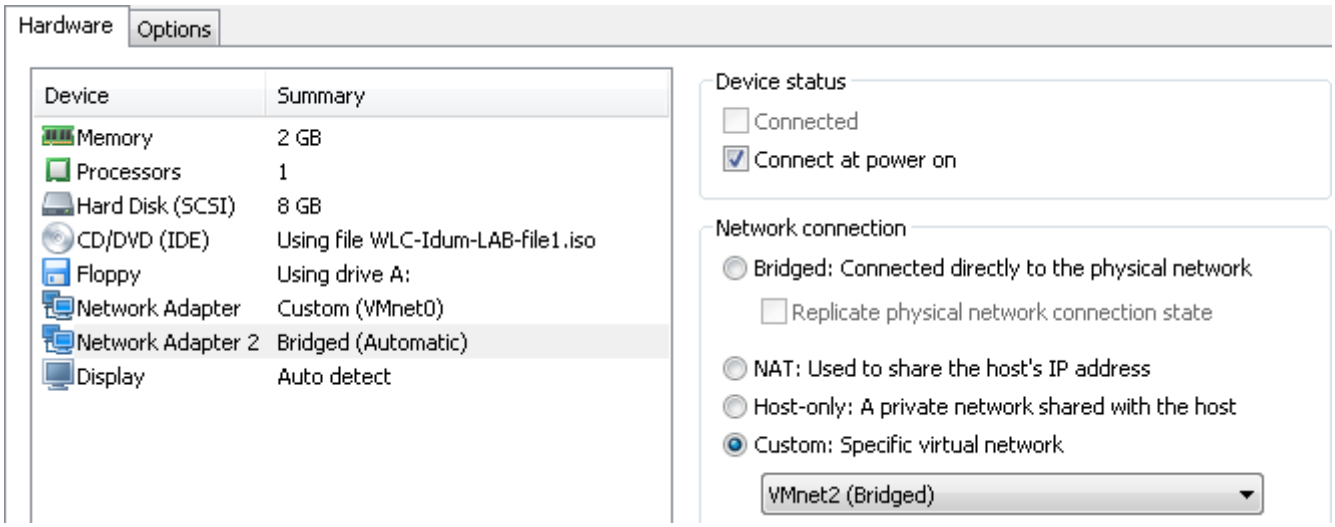
- Cliquez sur **"Edit virtual maching settign"**



- Sélectionnez **"Network Adapter"**, puis définissez le mode **"Custom"** et l'interface **"VMnet0"**.



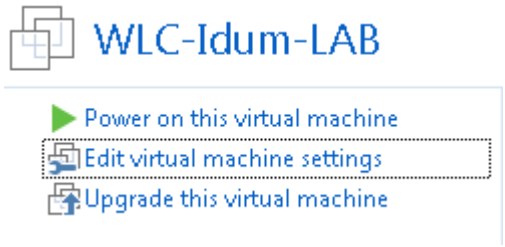
- Sélectionnez **"Network Adapter 2"**, puis définissez le mode **"Custom"** et l'interface **"VMnet2"**.



IV) Install & Config du vWLC

1) Installation

Pour installer le Contrôleur Wifi Virtuelle, cliquez sur **"Power on this virtual machine"**.



2) Pré-configuration

Lors de l'installation, le contrôleur a besoin de quelques informations afin de générer une configuration basique. Deux solutions sont possibles :

- Lors du démarrage, vous appuyez sur une touche afin d'entrer dans le terminal. ATTENTION Clavier QWERTY.
- Le serveur DHCP du switch va attribuer une adresse à l'interface Management du contrôleur. Il vous restera plus qu'à vous connecter dessus via un navigateur Web.

Dans cet article, j'utiliserai la deuxième méthode.

- Retrouvez l'adresse IP attribué par serveur DHCP.

Sur le switch tapez la commande ci-dessous pour retrouver les adresses délivrées :

```
show ip dhcp binding
```

Vous devez obtenir ceci :

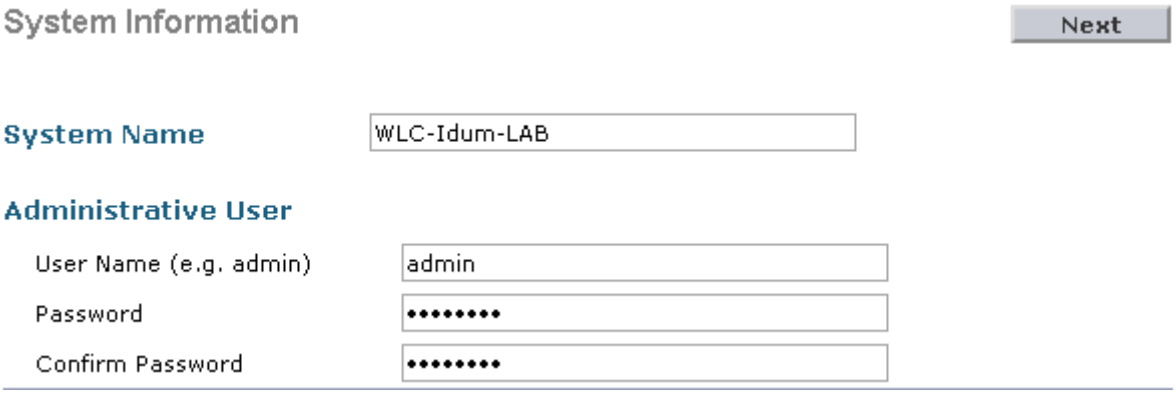
```
sw-idum-lab#sh ip dhcp binding
Bindings from all pools not associated with VRF:
IP address Client-ID/ Lease expiration Type
Hardware address/
```

```
User name
172.16.100.1 000c.296d.ec8b Mar 02 1993 12:55 AM Automatic
```

- Connectez-vous sur l’adresse IP via un navigateur web.

- Saisissez les paramètres suivants, puis cliquez sur **"Next"** :

- hostname
- username
- password



- Cliquez sur **"Next"**.

- Définissez l’adresse IP de l’interface "Service Port", puis cliquez sur **"Next"**.

General Information

Interface Name	service-port
MAC Address	00:0c:29:6d:ec:81

Interface Address

DHCP Protocol	Enabled
IP Address	172.16.1.200
Netmask	255.255.255.0

IPv6

SLAAC	Enable
Primary Address	::
Prefix Length	128

- Définissez l'adresse IP de l'interface "Management", ainsi que l'ID Vlan, puis cliquez sur **"Next"**.
- **ATTENTION** Vous devez définir un serveur DHCP autre que l'adresse **"1.1.1.1"**, sinon le contrôleur ne va jamais redémarrer.

General Information

Interface Name	management
MAC Address	00:0c:29:6d:ec:8b

Interface Address

VLAN Identifier	0
IP Address	172.16.100.200
Netmask	255.255.255.0
Gateway	172.16.100.254
Primary IPv6 Address	::
Prefix Length	128
Primary IPv6 Gateway	::

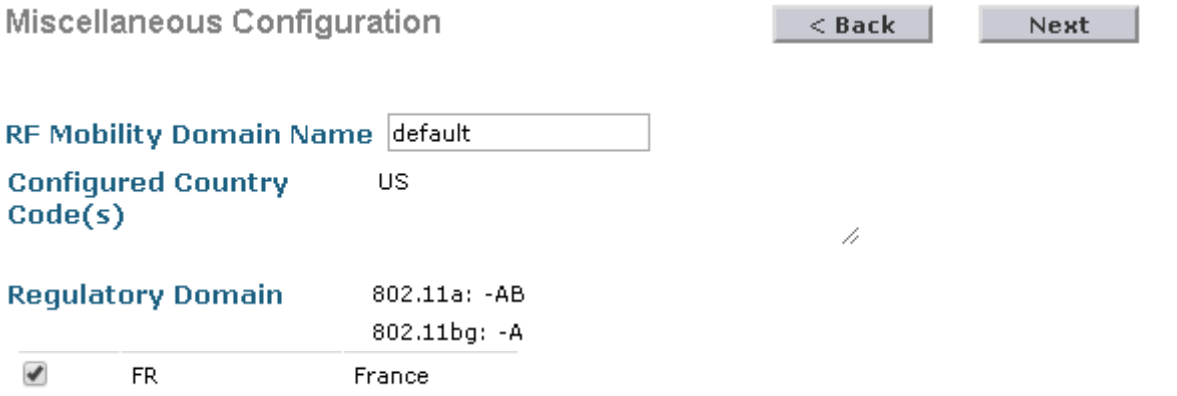
Physical Information

Port Number	1

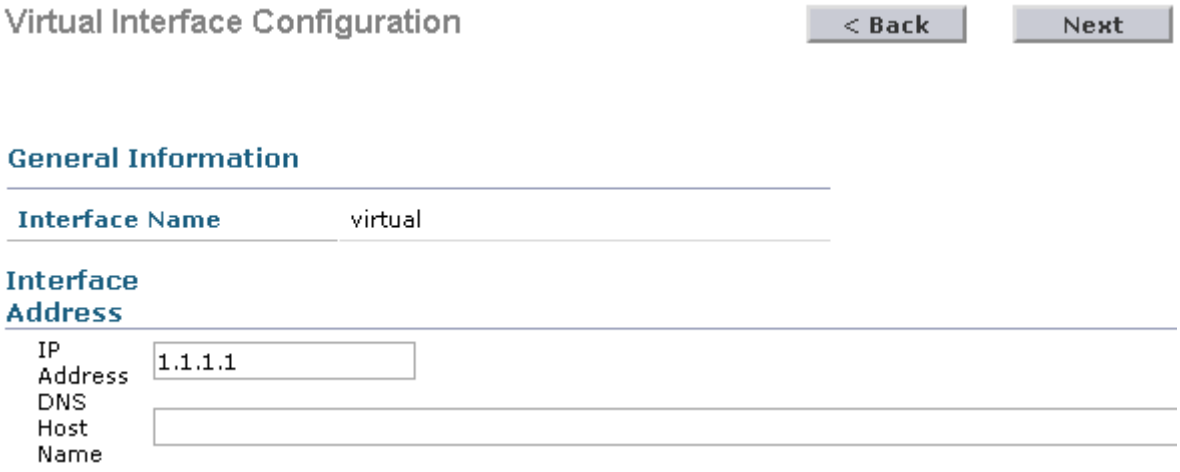
DHCP Information:
Ipv4

Primary DHCP Server	172.16.100.254
Secondary DHCP Server	0.0.0.0

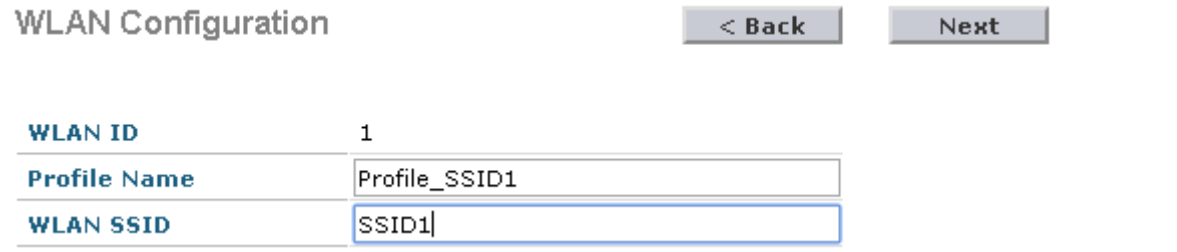
- Sélectionnez la région "**FR**", Désélectionnez la région "**US**", puis cliquez sur "**Next**".



- Cliquez sur "**Next**".



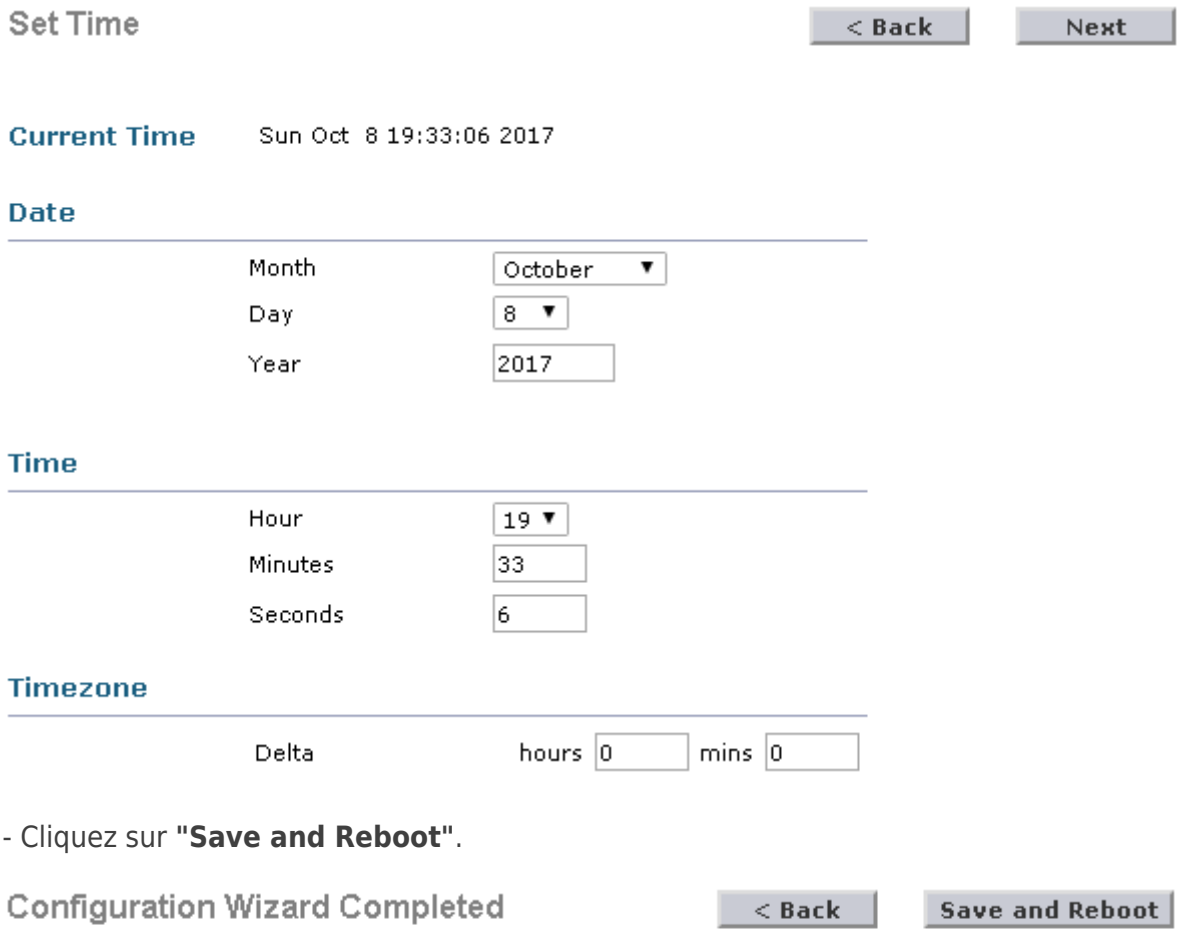
- Définissez un "**profile Name**" et un "**SSID**". Cliquez sur "**Next**".



- Cliquez sur "**Skip**".

- Cliquez sur "**Next**".

- Cliquez sur "**Next**".



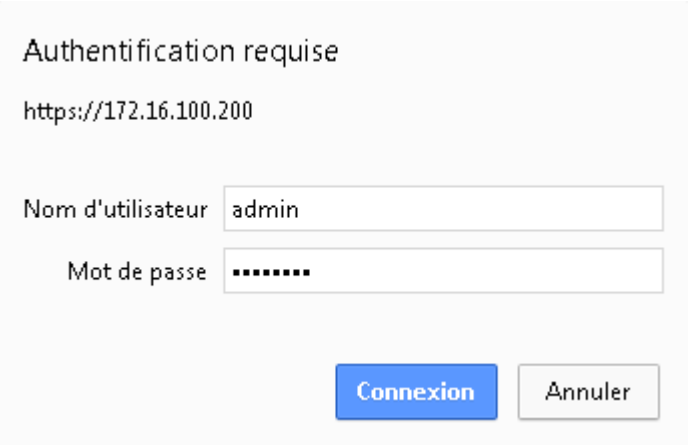
- Cliquez sur "**Save and Reboot**".

The configuration wizard is now complete. It is now necessary to save and reboot the system for the changes to take effect.

- Le contrôleur va redémarrer. Faites un ping continu pour savoir quand il sera disponible.

3) Connexion

Une fois prêt reconnectez-vous à l'interface Web en HTTPS et authentifiez-vous.

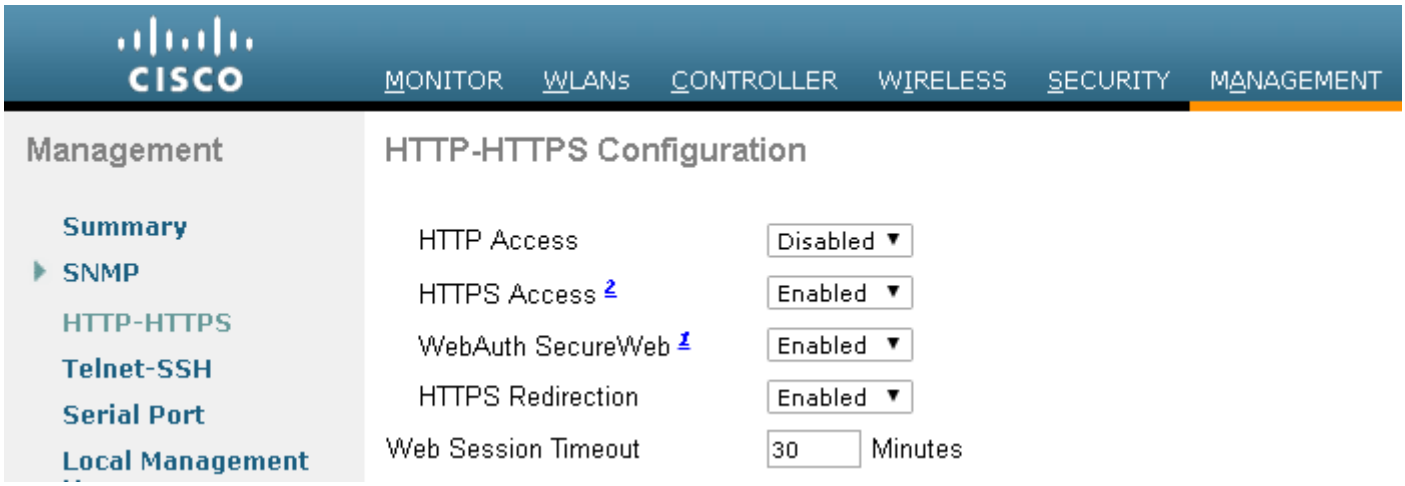


V) Configuration du vWLC

1) Configuration de base

a) Activation de la redirection HTTP vers HTTPS

- Dans le menu **"Management"**, cliquez sur **"HTTP-HTTPS"** puis activez l'option **"HTTPS Redirection"**.



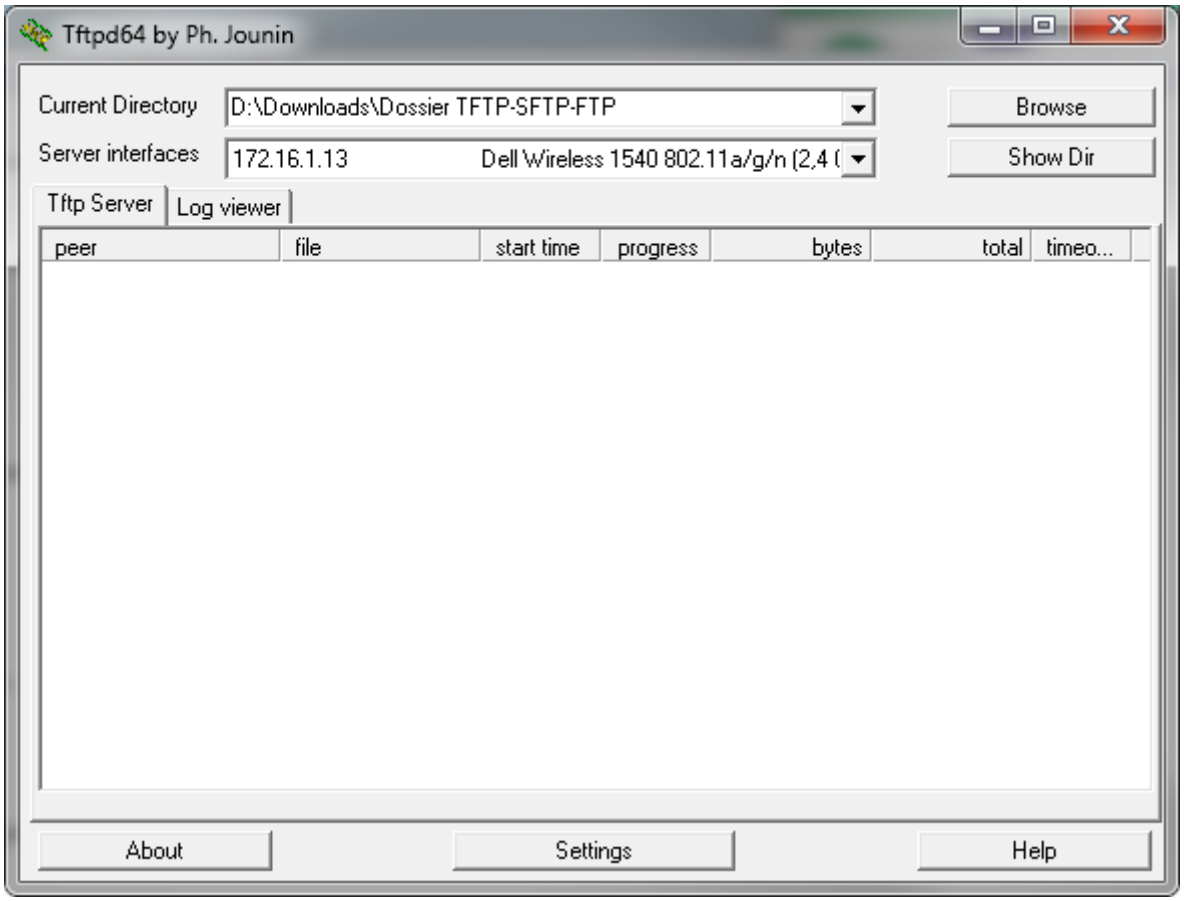
- Cliquez sur **"Apply"** pour valider.

b) Sauvegarder la configuration

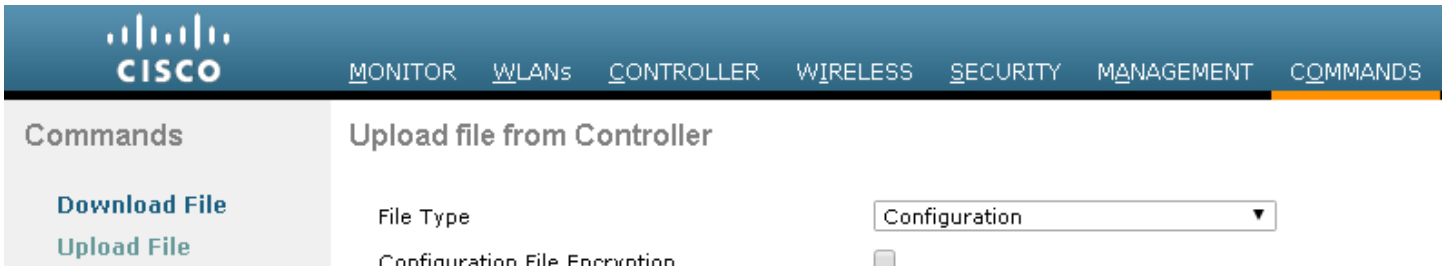
- Pour sauvegarder la configuration dans la flash du contrôleur, cliquez sur **"Save Configuration"** en haut à droite.

c) Télécharger la configuration

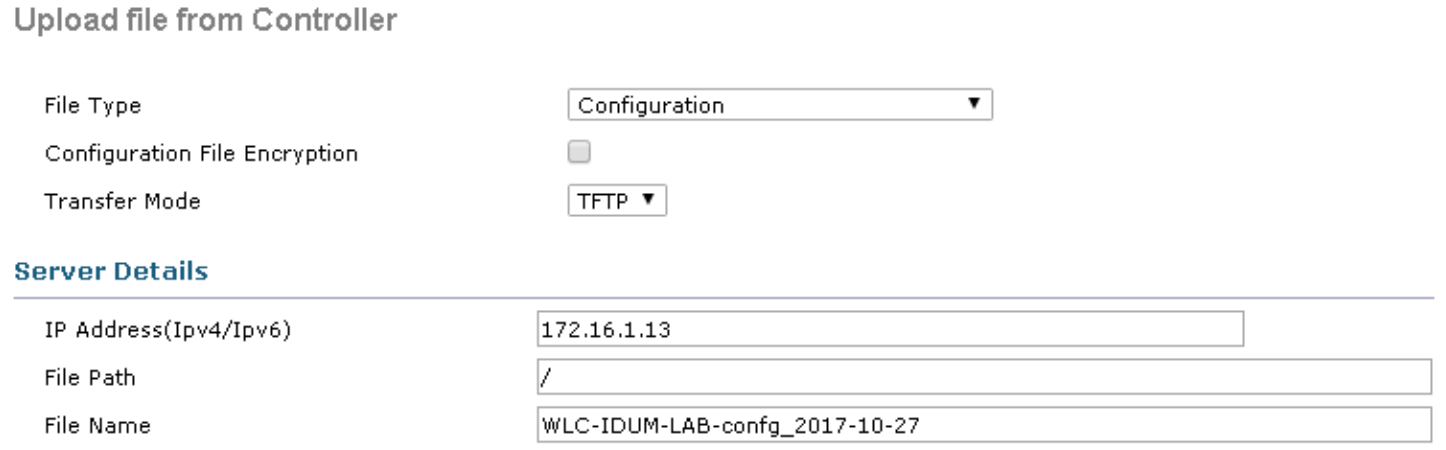
- Pour télécharger la configuration du contrôleur Wifi via un serveur TFTP, lancez au préalable votre serveur TFTP.



- Dans le menu **"Commandes"**, cliquez sur **"Upload File"**.



- Sélectionnez **"Configuration"**, le mode de transfert, l'adresse IP du serveur TFTP et le Filename.



- Cliquez sur le bouton **"Upload"**.

2) Configuration WLAN

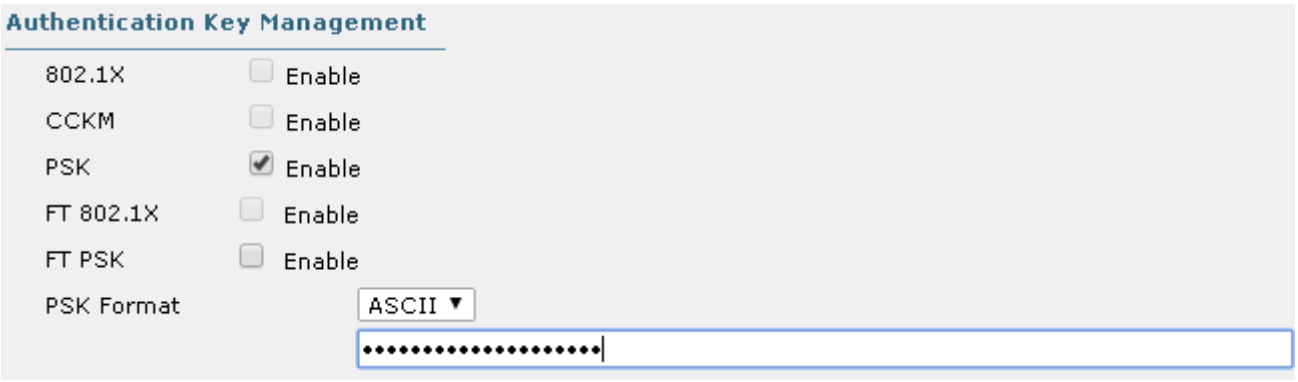
a) Configuration SSID1

Nous voulons modifier la configuration du SSID1 afin de mettre en place une sécurité de type WPA2 Personnal (Avec une Passphrase).

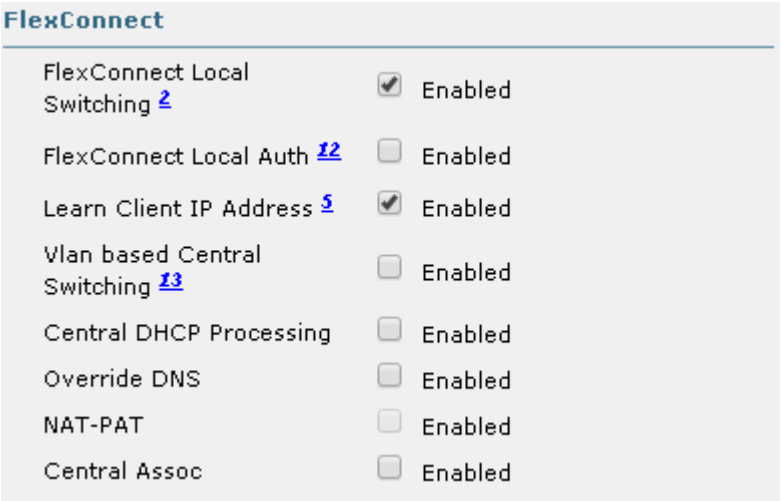
- Dans l'onglet **"WLANS"**, cliquez sur l'id WLAN que vous voulez configurez :

- Cliquez sur l'onglet **"Security"** :

- Cochez le type d'authentification **"PSK"**, puis définissez une passphrase.



- Dans l'onglet **"Advanced"**, cochez l'option **"FlexConnect Local Switching"**.



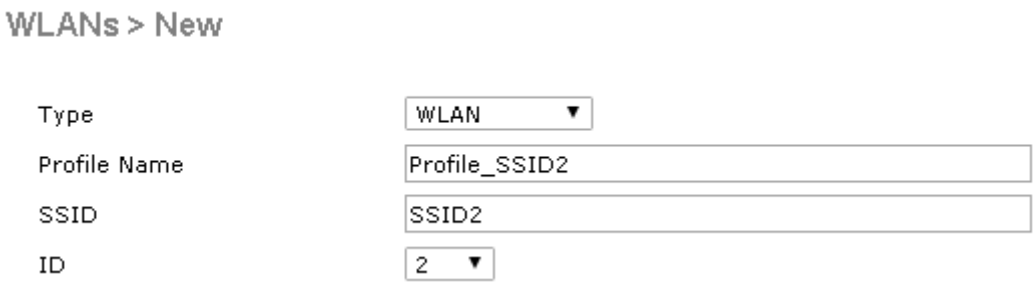
- Cliquez sur **"Apply"** pour valider les modifications.

b) Ajout d'un SSID2

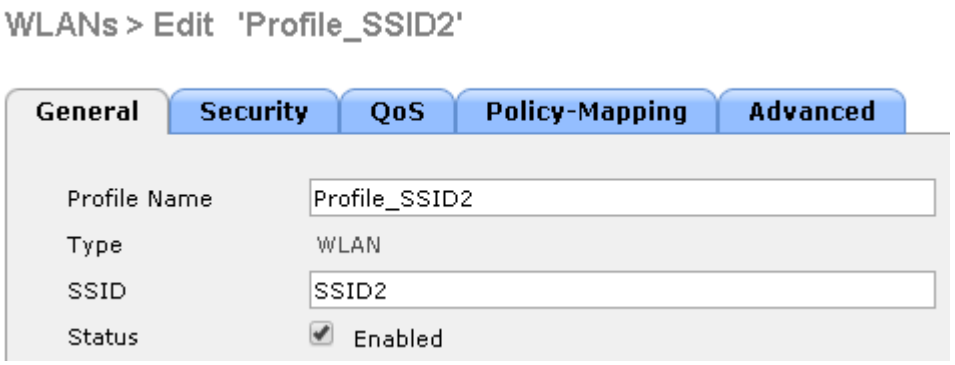
Nous voulons ajouter un nouveau SSID, avec une sécurité de type WPA2 Personnal.

- Dans l'onglet "**WLANS**", cliquez sur "**Go**".

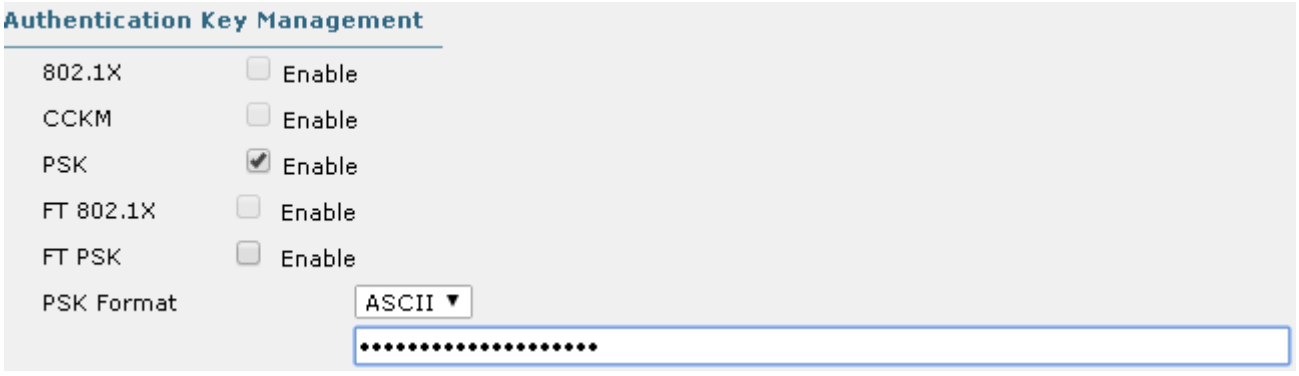
- Sélectionnez le type "**WLAN**", un profile Name, le nom du SSID et l'ID sur SSID. On valide en cliquant sur "**Apply**".



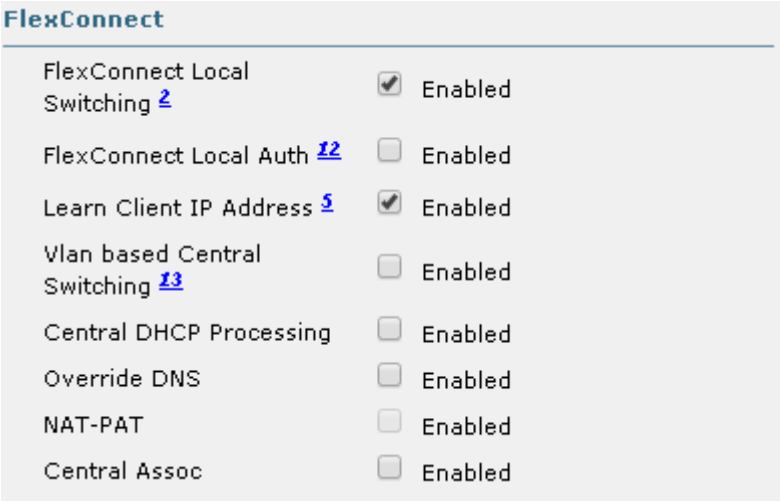
- Cochez le status "**Enabled**".



- Dans l'onglet "**Sécurité**", cochez le type d'authentification "**PSK**", puis définissez une passphrase.



- Dans l'onglet "**Advanced**", cochez l'option "**FlexConnect Local Switching**".



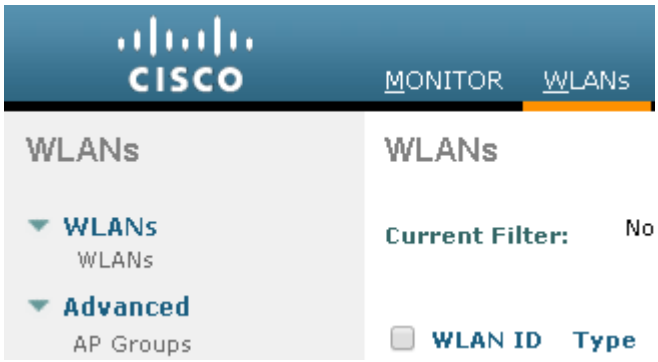
- Cliquez sur **"Apply"** pour valider les modifications.
- Vous devriez avoir ceci :

c) AP Groups

Les AP Group sont des groupes regroupant un ensemble de bornes diffusant les memes SSID.
Par exemple :

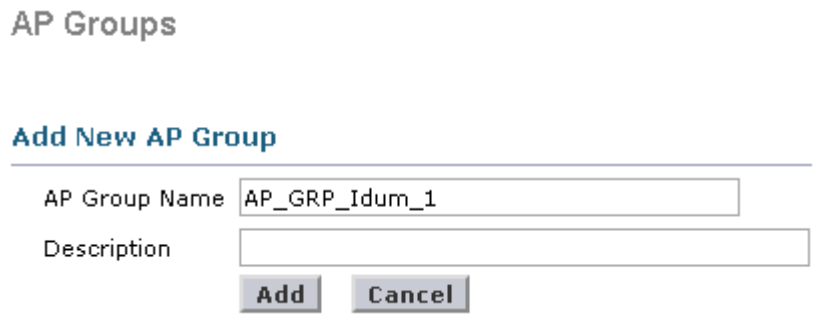
- Le groupe 1 diffuse le SSID1 et SSID2.
- Et on pourrait rajouter un groupe 2 qui diffuserai le SSID1 et SSID3

- Dans l'onglet **"WLANS"**, développez le menu **"Advanced"** et cliquez sur **"AP Groups"**.

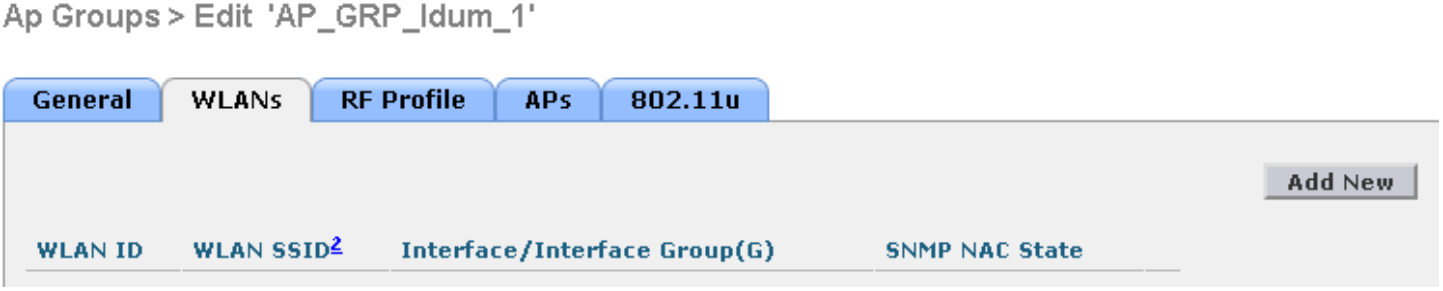


- Cliquez sur **"Add Group"**.

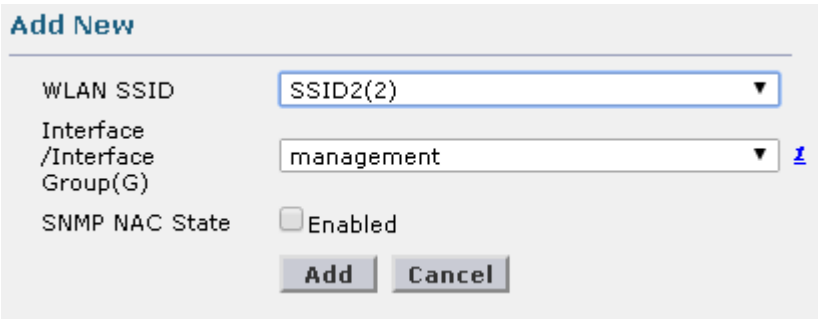
- Définissez un "AP Group Name" et cliquez sur **"Add"**.



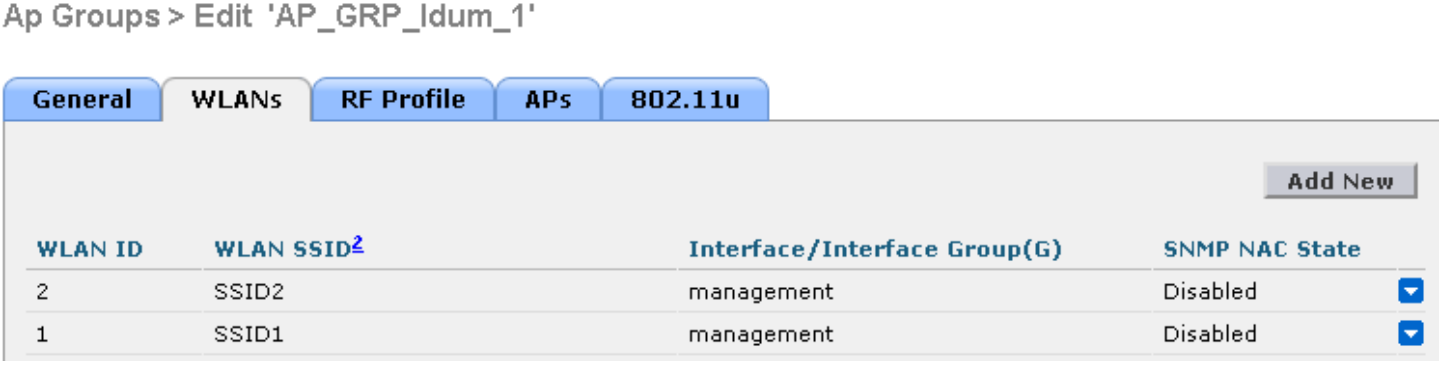
- Cliquez sur votre AP Group, puis cliquez sur l'onglet **"WLANs"** et enfin sur **"Add New"**.



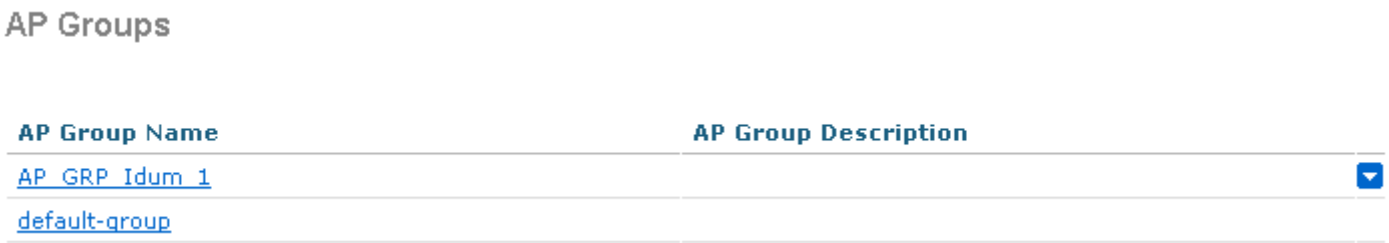
- Sélectionnez le SSID2, l'interface et cliquez sur **"Add"**.



- Faites la même chose pour SSID1.



- Vous devez obtenir ceci :



d) FlexConnect Group

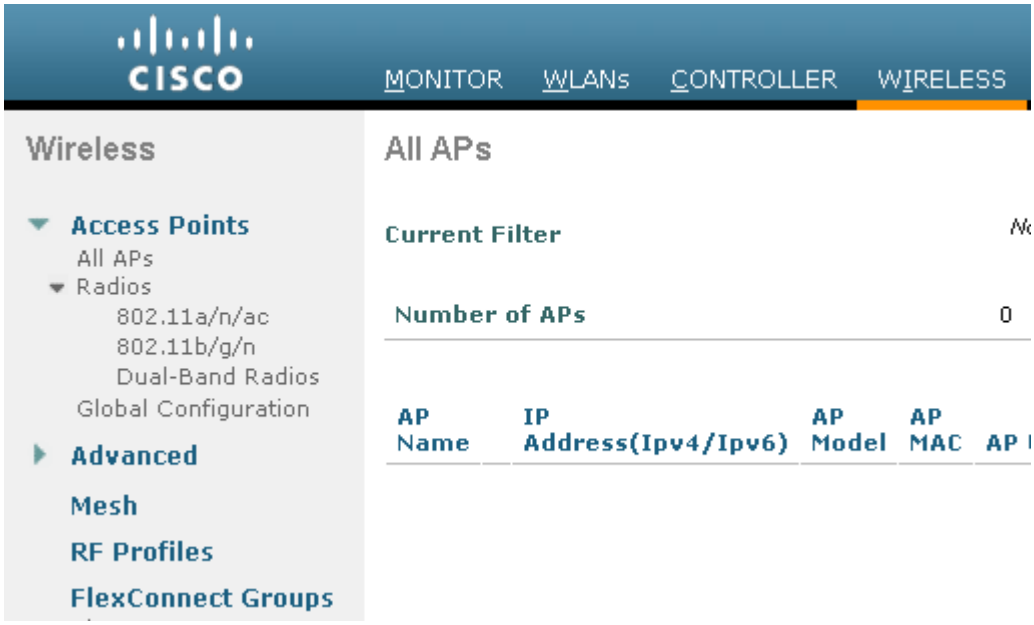
Pour rappel, le Flexconnect est une technologie Cisco permettant de rendre autonome une borne légère si

le contrôleur devient injoignable.

Un FlexConnect Group permet de regroupé toutes les bornes d'un même sites (par exemple) ayant les mêmes configurations VLAN associé au SSID.

Le FlexConnect Groupe est aussi très utile pour faire des mises à jour des bornes par lot.

- Dans l'onglet "**WIRELESS**", cliquez sur "**FlexConnect Groups**".

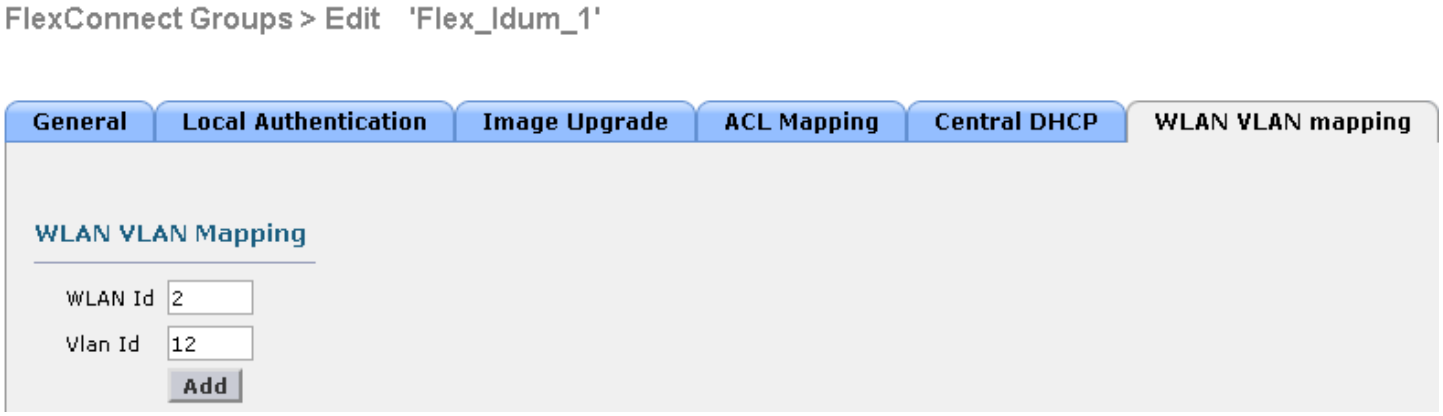


- Cliquez sur "**New...**"

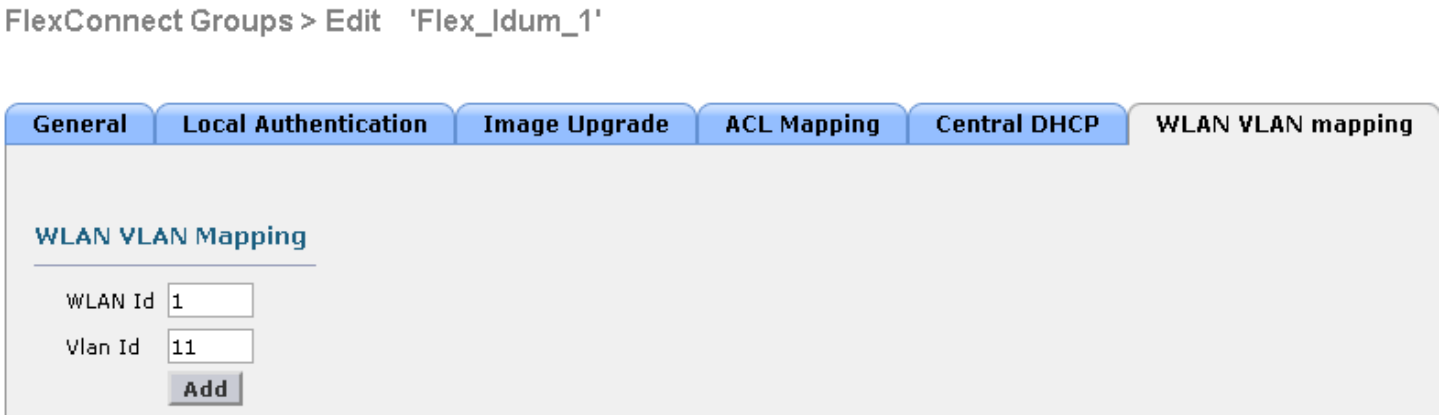
- Saisissez un nom de FlexConnect Group.

- Cliquez sur votre FlexConnect Group.

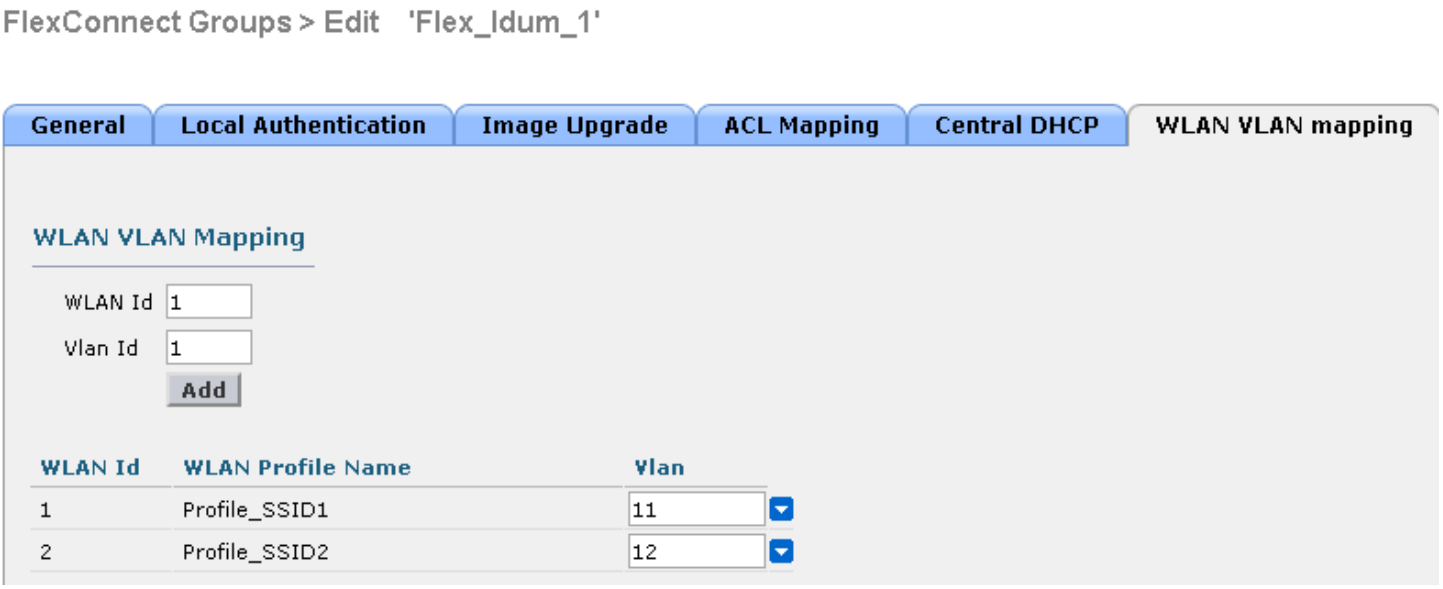
- Dans l'onglet "**WLAN VLAN mapping**", saisissez l'ID WLAN (ID SSID) et le Vlan a lui affecter.



Et



- Vous devez obtenir ceci :



ATTENTION Si vous essayer d'ajouter un SSID, où l'option **"FlexConnect Local Switching"** n'est pas activé, le contrôleur affichera un message d'erreur.

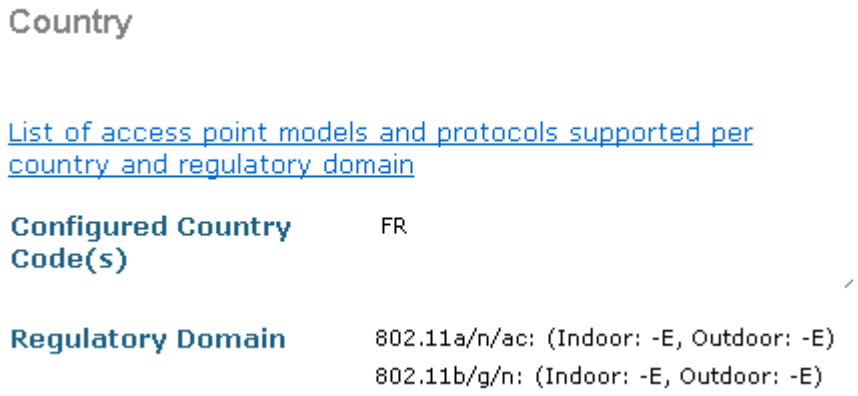
VI) Mise en place de 2 bornes Wifi

1) Vérification

Avant de connecter vos bornes, vérifiez que votre DHCP dans le Vlan 10 délivre bien une configuration IP. Et vérifiez que le serveur DNS résout bien les noms suivants :

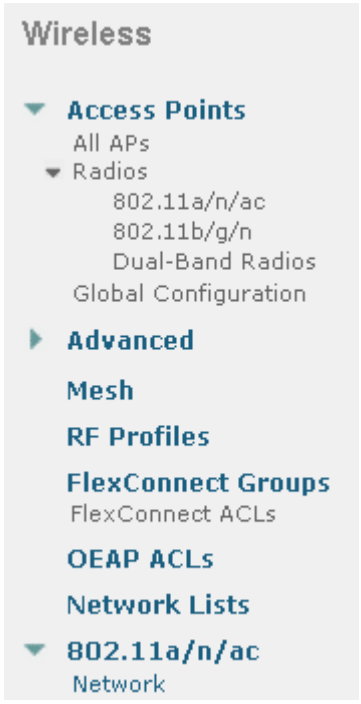
- cisco-lwapp-controller -> 172.16.100.200
- cisco-capwap-controller -> 172.16.100.200

- Dans l'onglet "**WIRELESS**", cliquez sur "**Country**" puis vérifiez que le "Configured Country Code" est bien "**FR**".

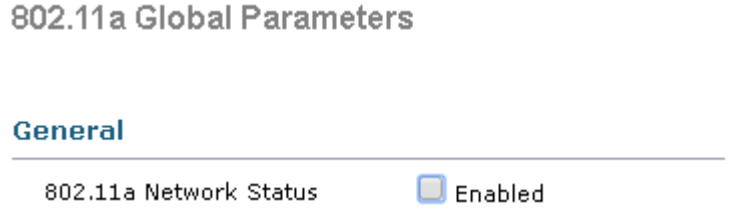


Si le "Configured Country Code" est "**US**", alors voici la procédure pour le changer :

- Dans l'onglet "**WIRELESS**", cliquez sur "**802.11a/n/ac**" puis sur "**Network**"

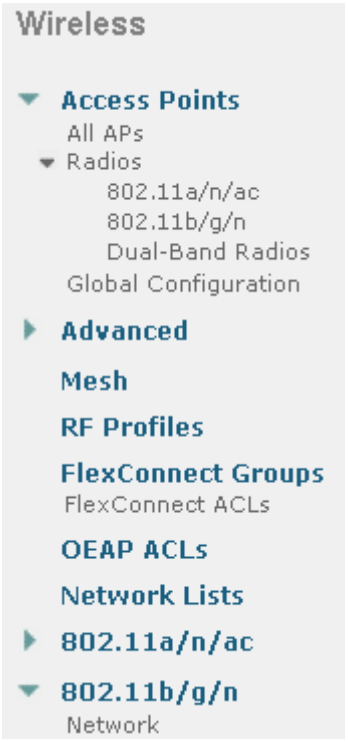


- Décochez l'option : "**802.11a Network Status**"

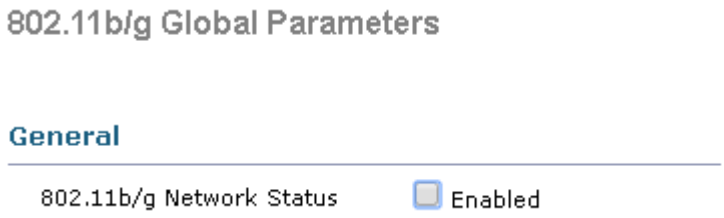


- Cliquez sur "**Apply**".

- Dans l'onglet "**WIRELESS**", cliquez sur "**802.11b/g/n**" puis sur "**Network**".

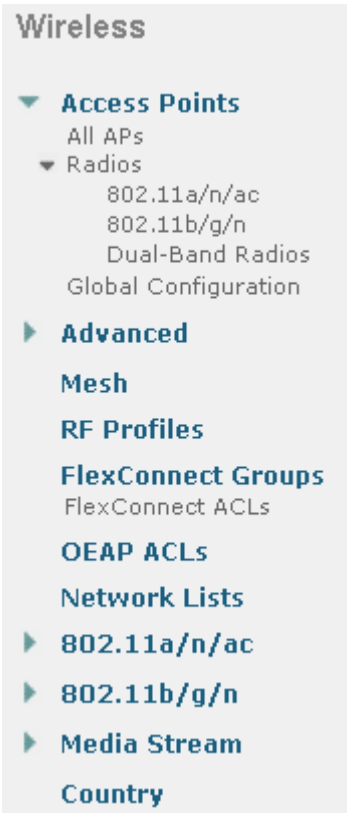


- Décochez l'option : **"802.11b/g Network Status"**



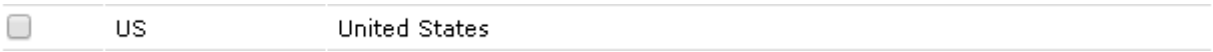
- Cliquez sur **"Apply"**.

- Dans le menu **"Country"**



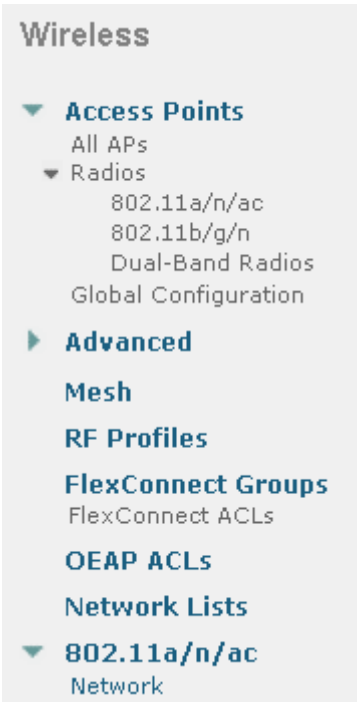
- Cochez l’option : **"FR"**

- Décochez l’option : **"US"**

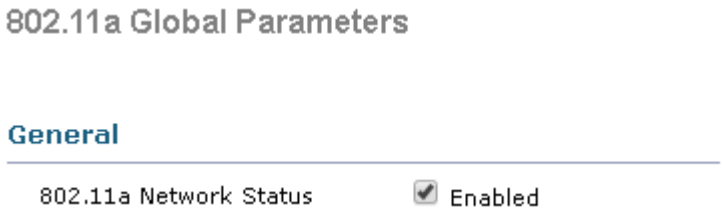


- Cliquez sur **"Apply"**.

- Dans l’onglet **"WIRELESS"**, cliquez sur **"802.11a/n/ac"** puis sur **"Network"**

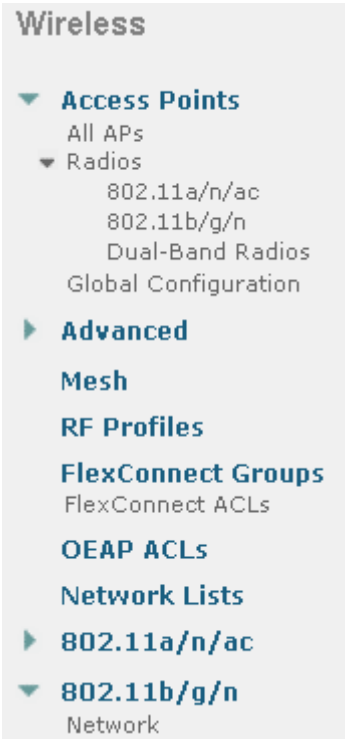


- Décochez l’option : **"802.11a Network Status"**

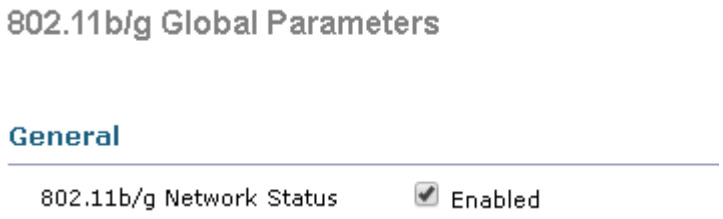


- Cliquez sur **"Apply"**.

- Dans l’onglet **"WIRELESS"**, cliquez sur **"802.11b/g/n"** puis sur **"Network"**.



- Décochez l'option : **"802.11b/g Network Status"**



- Cliquez sur **"Apply"**.

"ATTENTION" Si vous ne changez pas le paramètres vous pourrez rencontrer le problème ci-dessous :

```
AP has SHA2 MIC certificate - Using SHA2 MIC certificate for DTLS.

%CAPWAP-5-DTLSREQSEND: DTLS connection request sent peer_ip: 172.16.100.200 peer_port: 5246
%CAPWAP-5-DTLSREQSUCC: DTLS connection created sucessfully peer_ip: 172.16.100.200 peer_port: 5246
%CAPWAP-5-SENDJOIN: sending Join Request to 172.16.100.200
%DTLS-5-ALERT: Received WARNING : Close notify alert from 172.16.100.200
%DTLS-5-SEND_ALERT: Send FATAL : Close notify Alert to 172.16.100.200:5246
```

2) Démarrage des bornes

- Connectez les bornes sur le switch.
- Attendez quelles démarre.
- Vérifiez que le DHCP a bien délivré une config IP aux bornes, via la commande :

```
show ip dhcp binding
```

- Sur l'interface du contrôleur, vous pourrez observer qu'il a détecté une nouvelle borne :

Access Point Summary

	Total	Up	Down	
802.11a/n/ac Radios	0	0	0	Detail
802.11b/g/n Radios	0	0	0	Detail
Dual-Band Radios	0	0	0	Detail
All APs	1	0	0	Detail

- Dans un premier temps, la borne va télécharger le bon firmware. Vous pouvez voir le statut dans l'onglet **"WIRELESS"** :

Number of APs 1

AP Name	IP Address(Ipv4/Ipv6)	AP Model	AP MAC	AP Up Time	Admin Status	Operational Status
AP58ac.78c4.7a08	172.16.10.1	AIR-CAP2702I-E-K9	58:ac:78:c4:7a:08	0 d, 00 h 00 m 00 s	Enabled	Downloading

3) Configuration des bornes

Maintenant que les bornes sont remontées dans le contrôleur, nous pouvons les configurer.

- Cliquez sur la première borne :

AP Name
AP7cad.74db.6a94
AP58ac.78c4.7a08

- Définissez un **"AP Name"**, une **"Location"** et sélectionnez le mode **"FlexConnect"**

ATTENTION Avec un Virtual controller Wifi les bornes ne fonctionnent pas en mode **"Local"**.

All APs > Details for AP7cad.74db.6a94

General | Credentials | Interfaces | High Availab

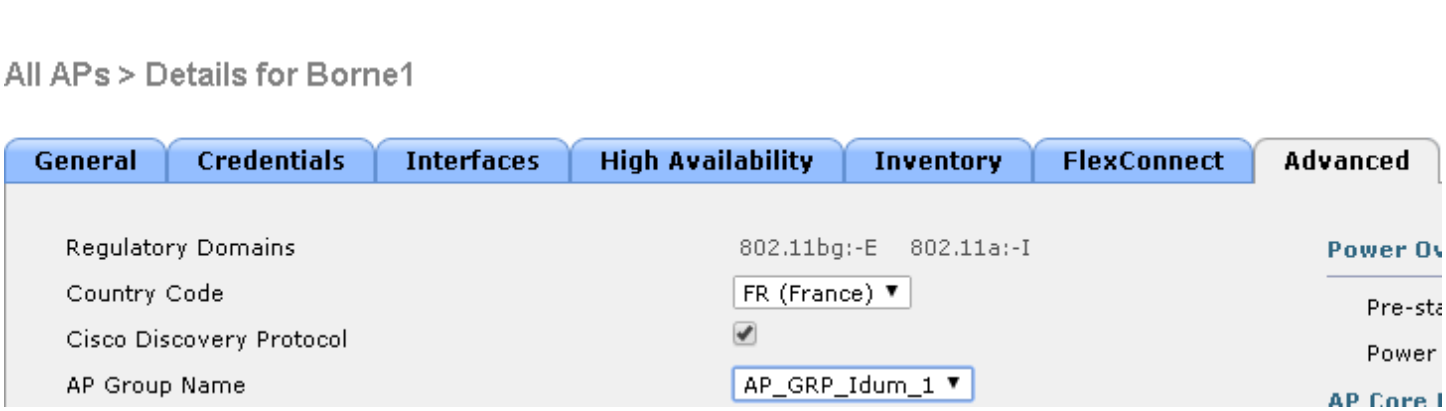
General

AP Name	Borne1
Location	Bat 1
AP MAC Address	7c:ad:74:db:6a:94
Base Radio MAC	08:cc:68:5f:57:c0
Admin Status	Enable
AP Mode	FlexConnect

- Cliquez sur **"Apply"**.

Apply

- Dans le menu **"Advanced"**, sélectionnez le "AP Group Name" : **"AP_GRP_IDUM_1"**.



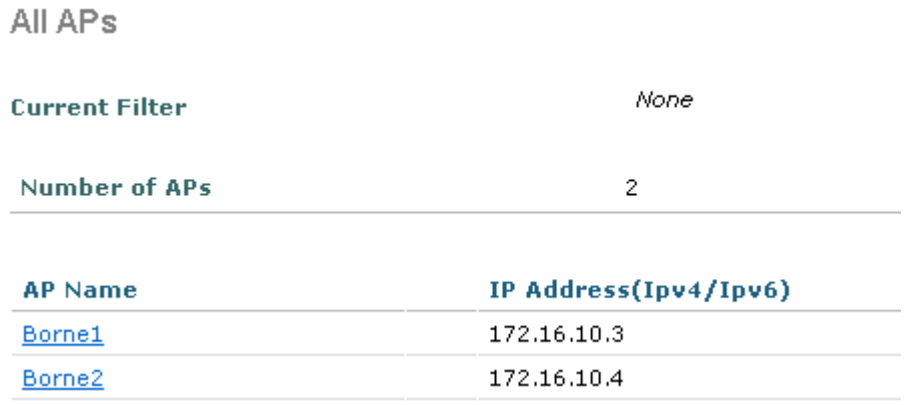
- Cliquez sur **"Apply"**. La borne va redémarrer.

- Attendez que la borne soit de nouveau visible sur le contrôleur.
- Puis retournez dans la configuration de la borne. Cliquez sur l'onglet **"FlexConnect"**.

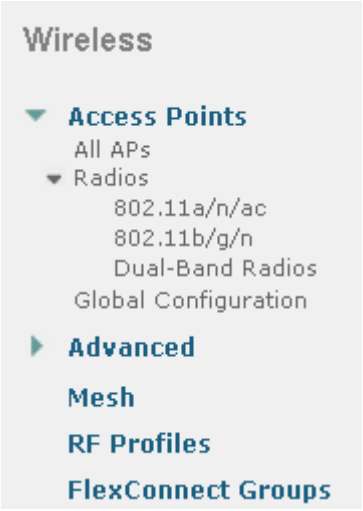
- Cochez l'option **"VLAN Support"** et définissez-le vlan native **"10"**.

- Cliquez sur **"Apply"**.

- Recommencez les mêmes étapes pour la deuxième borne.

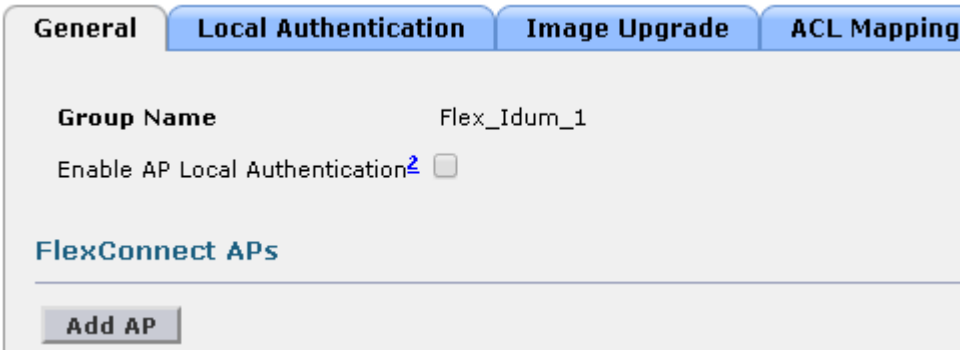


- Toujours dans l'onglet **"WIRELESS"**, cliquez sur **"FlexConnect Groups"**.

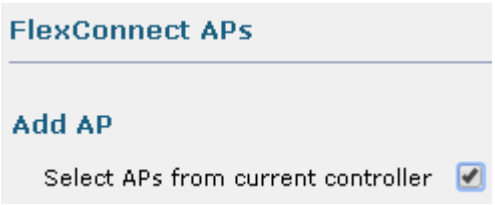


- Cliquez sur votre groupe Flexconnect, **"Flex_Idum_1"**.

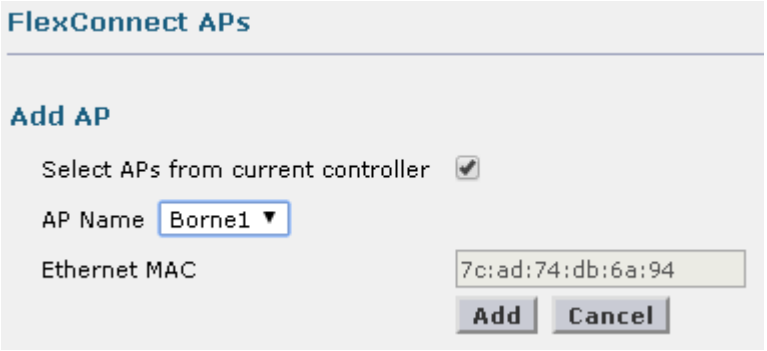
- Cliquez sur **"Add AP"**.



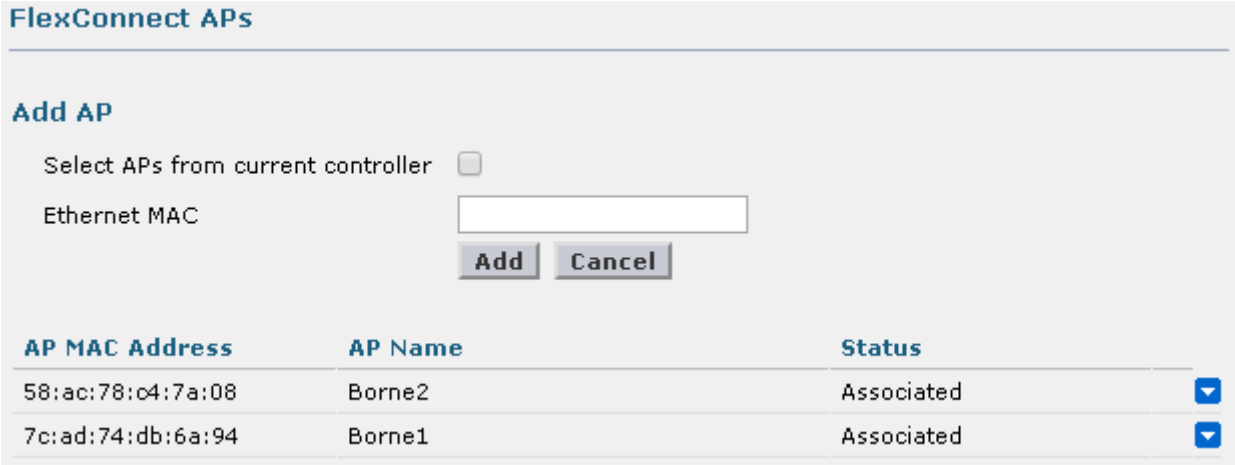
- Cochez l'option **"Select APs from current controller"**.



- Un menu déroulant apparait et vous permet de sélectionner la borne que vous souhaitez ajouter au group. Ajoutez les deux bornes.

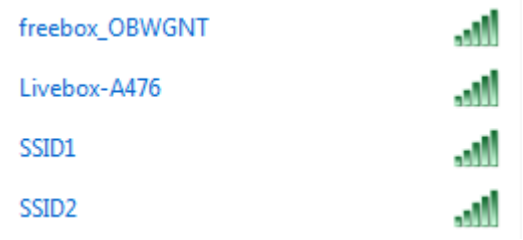


- Vous devez avoir ceci :



- Cliquez sur **"Apply"**.

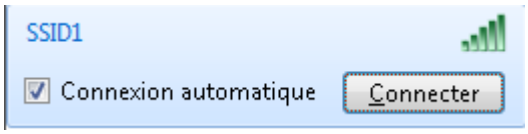
- Si vous regardez la couverture wifi, vous pourrez voir que les SSID sont diffusés.



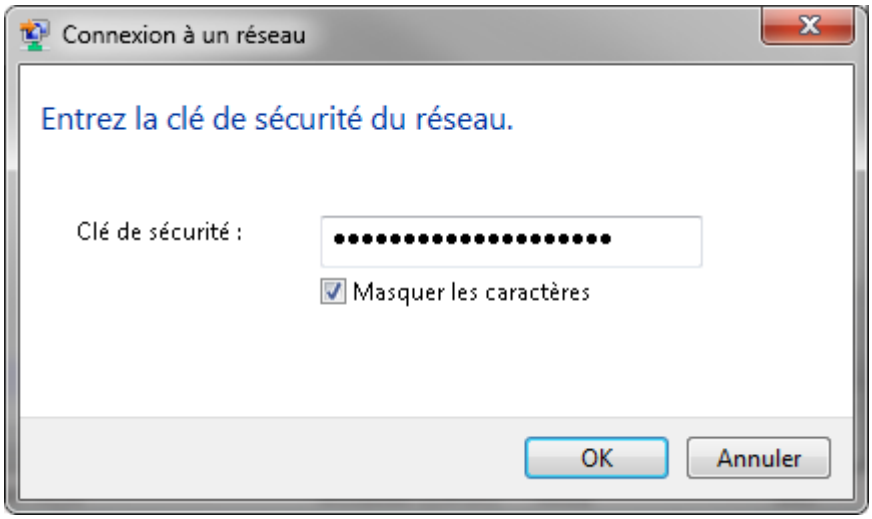
VII) Tests

1) Tests de connexion sur les SSID

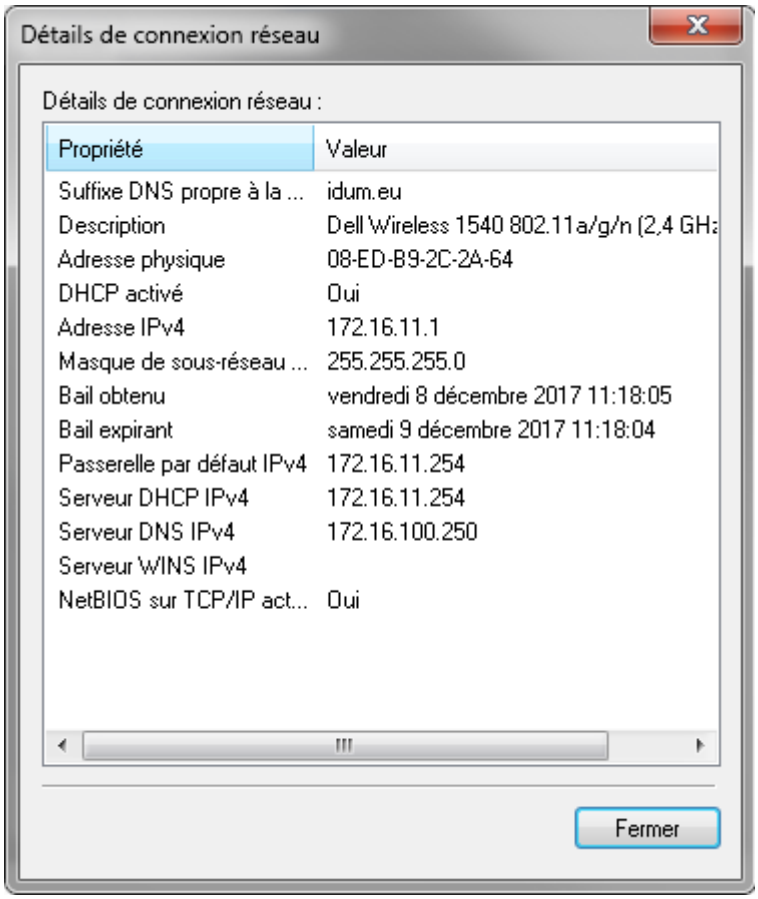
Maintenant que les deux bornes sont configurées, essayez de vous connecter.



- Authentifiez-vous en saisissant votre clef WPA2.



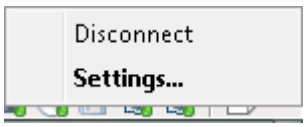
- Vérifiez que vous obtenez bien une adresse IP via le DHCP :



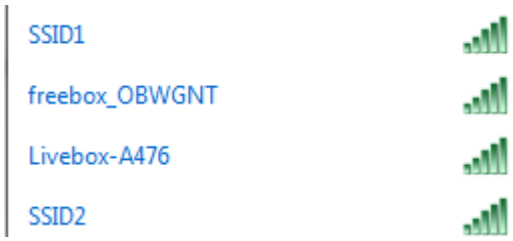
2) Tests perte contrôleur

Nous aimerions maintenant savoir comment réagit la couverture Wifi de notre entreprise lors de la perte du contrôleur Wifi. Pour cela nous allons faire un shut sur notre interface Vmware correspondant à l'interface de Management.

- Dans la fenêtre de VmWare Workstation, faite un clic droit sur l'interface réseau en bas à droite. Et cliquez sur **"Disconnect"**.

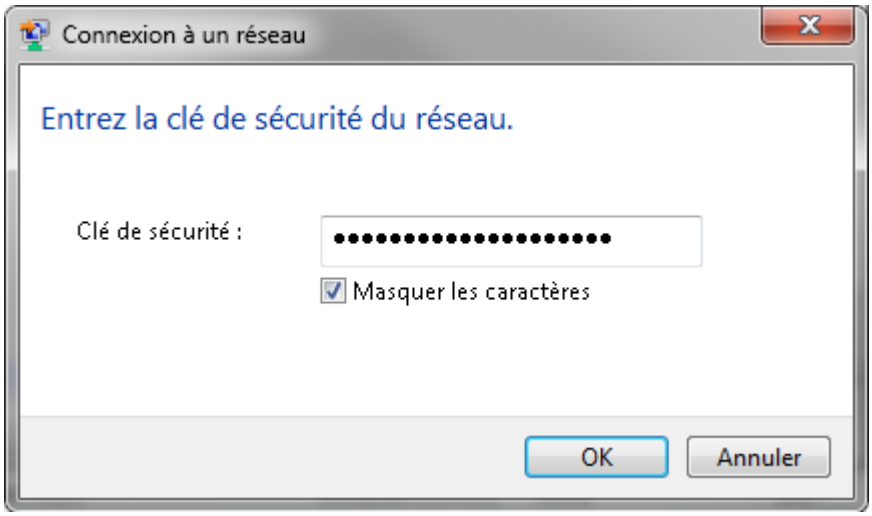


- Vérifiez dans un premier temps, que les bornes diffusent encore les SSID.

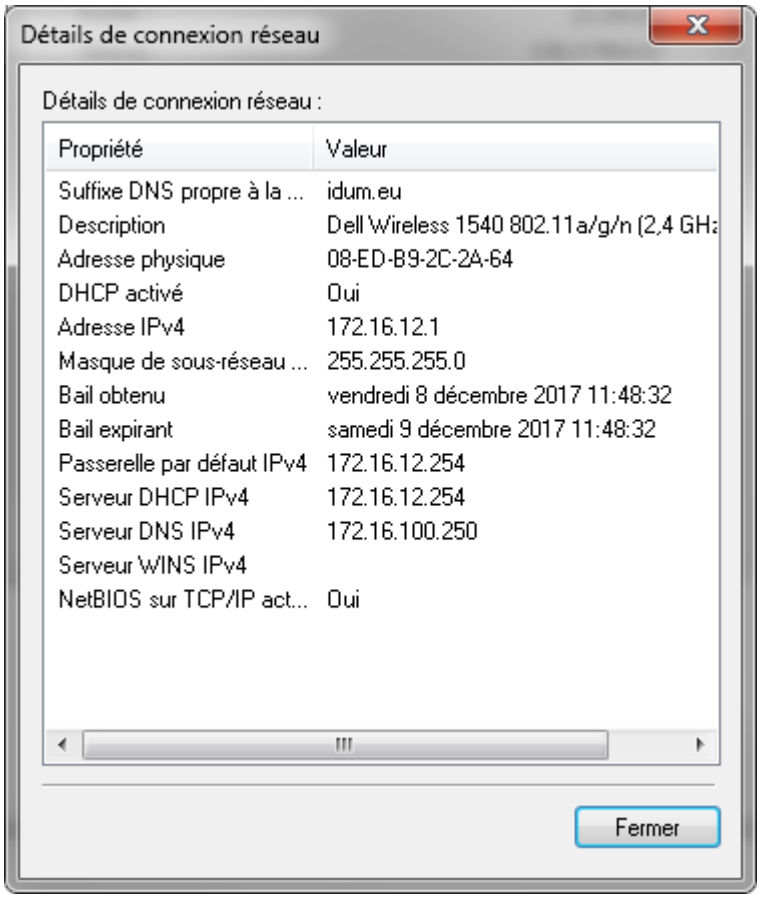


- Cliquez sur SSID2 pour vous connecter.

- Authentifiez-vous en saisissant votre clef WPA2.



- Vérifiez que vous obtenez bien une adresse IP via le DHCP :



Nous pouvons valider que les bornes fonctionnent toujours même si le contrôleur n’est plus joignable. Ce

miracle est rendu possible grâce au FlexConnect.

Idum