



## 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
  - II) Configuration du switch
    - 1) config de base
    - 2) Configuration du serveur DHCP
    - 3) Configuration des interfaces
  - III) Déploiement OVA
    - 1) Préparation de Vmware
    - 2) Déploiement OVA
    - 3) Modification de la VM
  - IV) Install & Config du vWLC
    - 1) Installation
    - 2) Pré-configuration
    - 3) Connexion
  - V) Configuration du vWLC
    - 1) Configuration de base
    - 2) Configuration WLAN
  - VI) Mise en place de 2 bornes Wifi
    - 1) Vérification
    - 2) Démarrage des bornes
    - 3) Configuration des bornes
  - VII) Tests
    - 1) Tests de connexion sur les SSID
    - 2) Tests perte contrôleur
- 

## I) Introduction

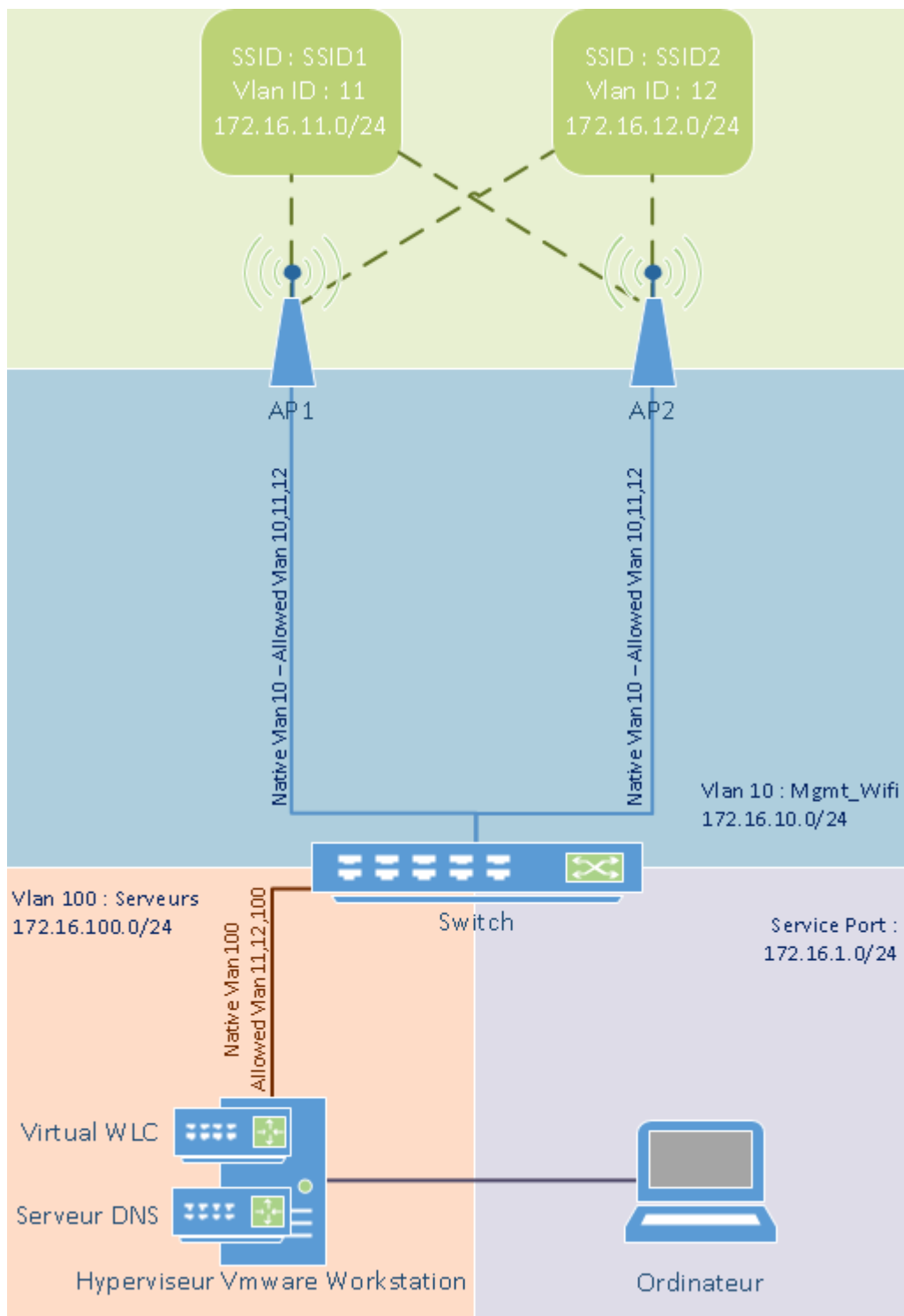
Les contrôleurs Wifi permettent de gérer la couverture Wifi d'une entreprise, mono ou multi bâtiment. Les contrôleurs sans fil sont responsables des politiques de sécurité, la prévention d'intrusion, la gestion de RF, la qualité du service (QoS), et la mobilité.

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
```

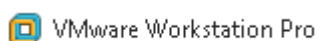
## III) Déploiement OVA

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

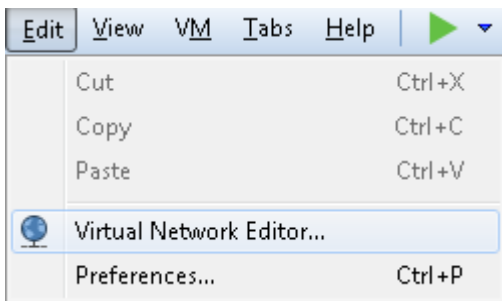
Vous trouverez le fichier OVA sur le site de cisco.com.

### 1) Préparation de VMware

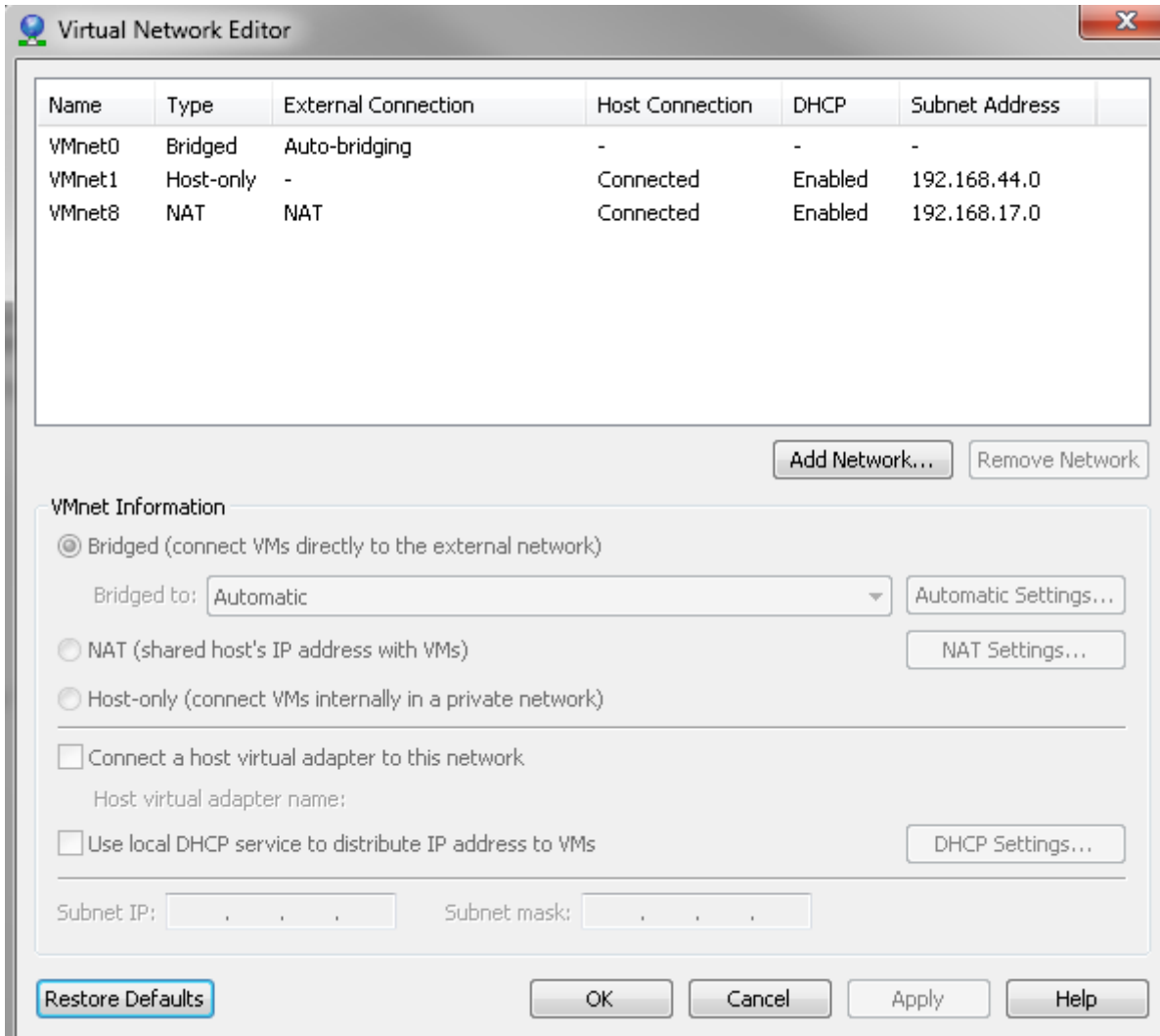
- Ouvrez VMware Workstation.



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



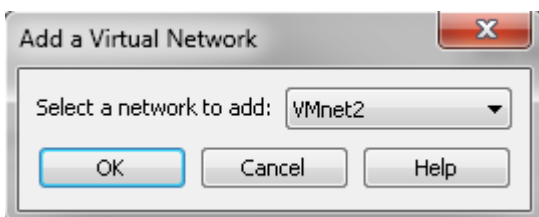
- Vous devez obtenir cette fenêtre :



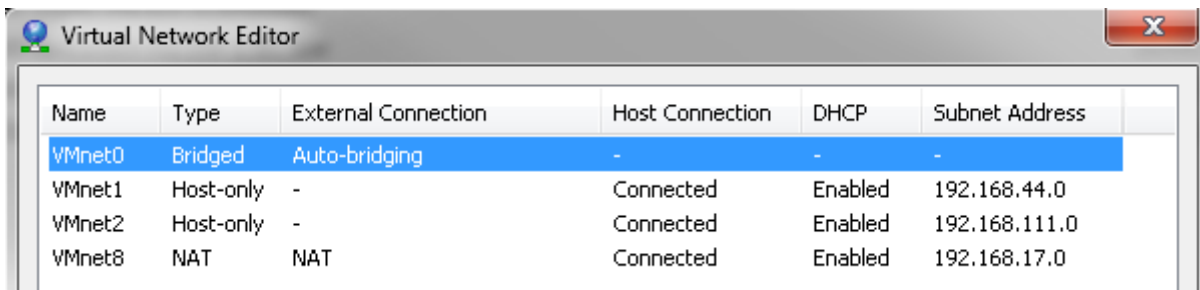
- Cliquez sur "**Add Network**".



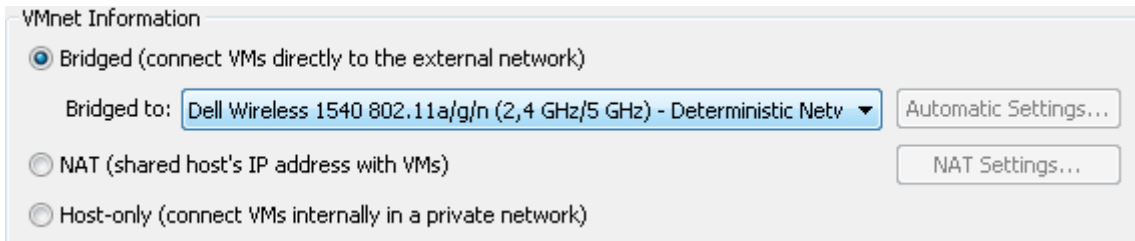
- Sélectionnez une interface dans la liste, puis cliquez sur "**OK**".



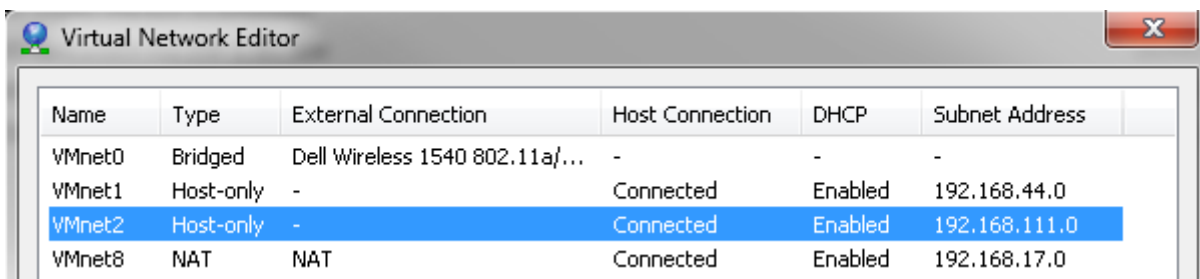
- Sélectionnez l'interface "**VMnet0**".



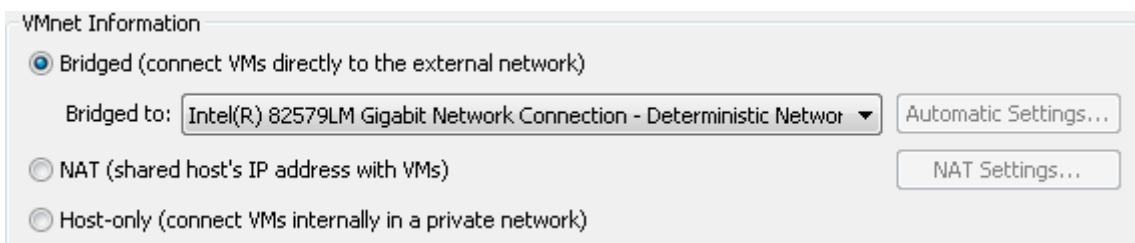
- Changez la valeur du menu déroulant pour sélectionner une interface physique.



- Sélectionnez l'interface que vous avez ajouté précédemment.



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

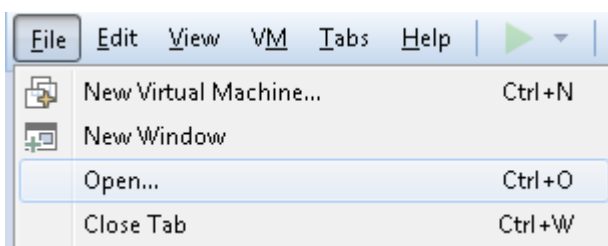


- Cliquez sur "**OK**".

## 2) Déploiement OVA

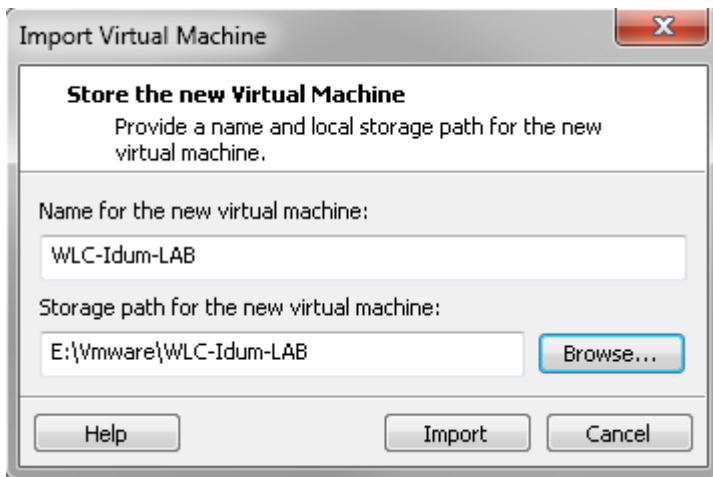
Maintenant que la configuration de VMware Workstation est prête, nous pouvons déployer l'OVA.

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



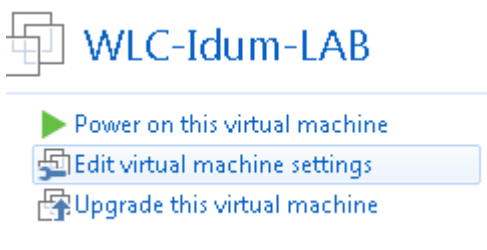
- Sélectionnez le fichier OVA. Puis définissez un nom à la VM. Cliquez sur "**Import**".



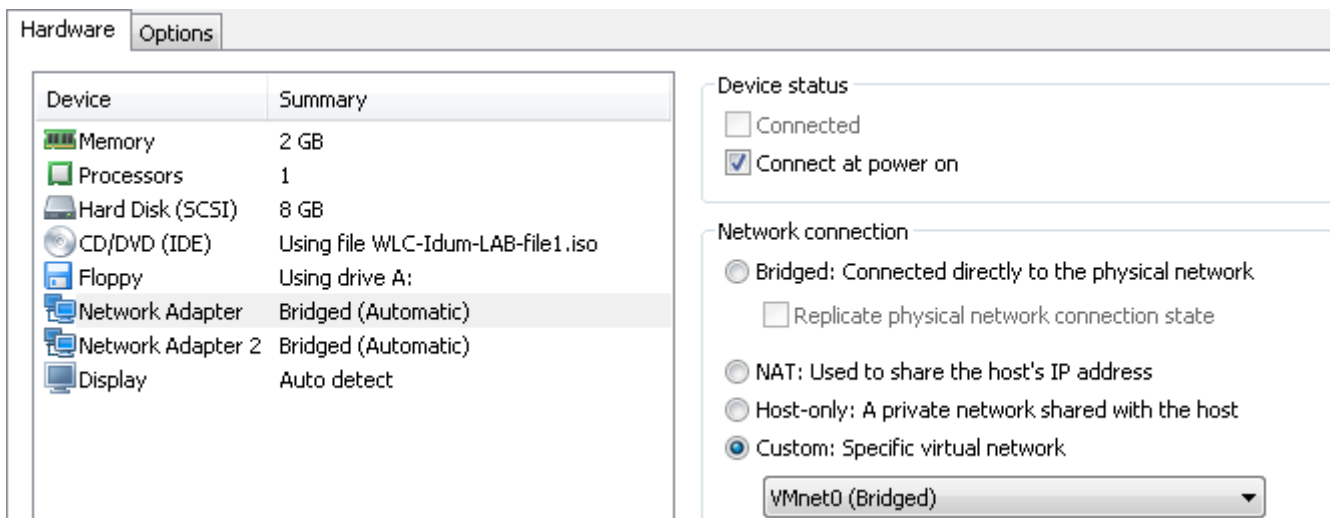


### 3) Modification de la VM

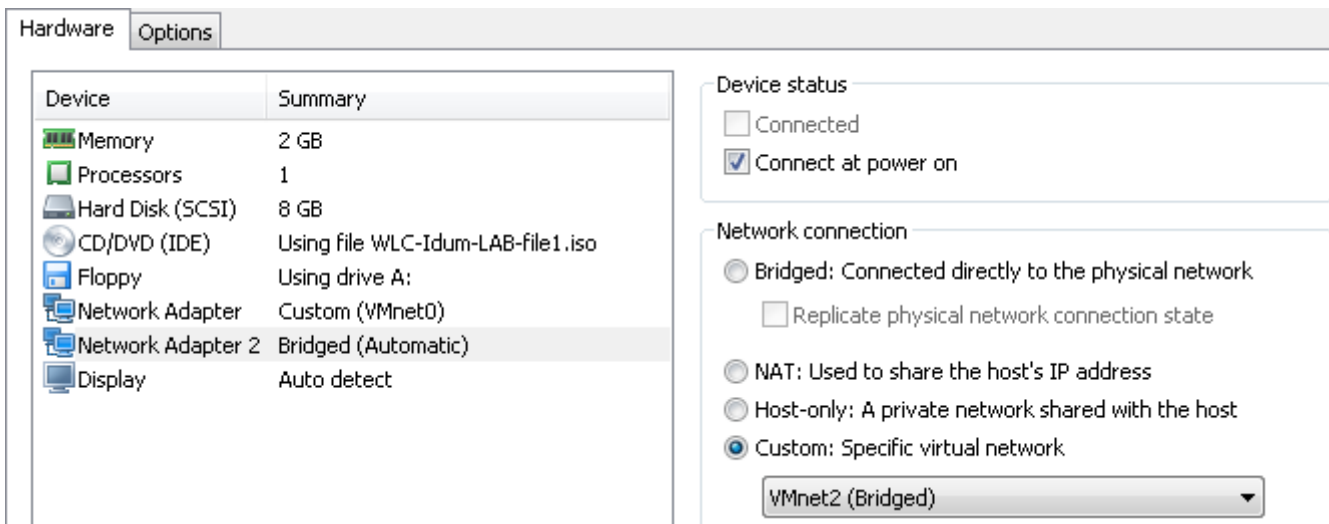
- Cliquez sur "**Edit virtual machine settings**"



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



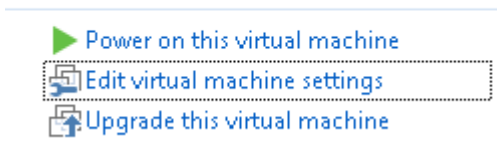
- Sélectionnez "**Network Adapter 2**", puis définissez le mode "**Custom**" et l'interface "**VMnet2**".



## 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.

Non sécurisé 172.16.100.1/screens/wizard\_frameset.html

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

- hostname
- username
- password

## System Information

Next

### System Name

WLC-Idum-LAB

### Administrative User

User Name (e.g. admin)

admin

Password

••••••••

Confirm Password

••••••••

- Cliquez sur "**Next**".

## SNMP Summary

< Back

Next

SNMP v1 Mode

Disable ▼

SNMP v2c Mode

Enable ▼

SNMP v3 Mode

Enable ▼

- 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

Netmask

### IPv6

---

SLAAC  Enable

Primary Address

Prefix Length

- 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.

## Management Interface Configuration

### General Information

---

**Interface Name** management

---

**MAC Address** 00:0c:29:6d:ec:8b

---

### Interface Address

---

VLAN Identifier

IP Address

Netmask

Gateway

Primary IPv6 Address

Prefix Length

Primary IPv6 Gateway

### Physical Information

---

Port Number 1

### DHCP Information:

#### Ipv4

---

Primary DHCP Server

Secondary DHCP Server

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

## Miscellaneous Configuration

< Back

Next

RF Mobility Domain Name

Configured Country Code(s) US

Regulatory Domain 802.11a: -AB  
802.11bg: -A

FR France

- Cliquez sur "**Next**".

## Virtual Interface Configuration

< Back

Next

### General Information

Interface Name

### Interface Address

IP Address

DNS Host Name

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

## WLAN Configuration

< Back

Next

WLAN ID

Profile Name

WLAN SSID

- Cliquez sur "**Skip**".

## RADIUS Server Configuration

[< Back](#)[Apply](#)[Skip](#)

Server IPv4 Address

Shared Secret Format

Shared Secret

Confirm Shared Secret

Port Number

Server Status

Server IPv6 Address

Shared Secret Format

Shared Secret

Confirm Shared Secret

Port Number

Server Status

- Cliquez sur "**Next**".

## 802.11 Configuration

[< Back](#)[Next](#)

802.11a Network Status  Enabled

802.11b Network Status  Enabled

802.11g Network Status  Enabled

Auto RF  Enabled

- Cliquez sur "**Next**".

**Current Time** Sun Oct 8 19:33:06 2017

### Date

Month  ▼  
Day  ▼  
Year

### Time

Hour  ▼  
Minutes   
Seconds

### Timezone

Delta hours  mins

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

**Configuration Wizard Completed**

&lt; Back

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.

Authentication requise

https://172.16.100.200

Nom d'utilisateur

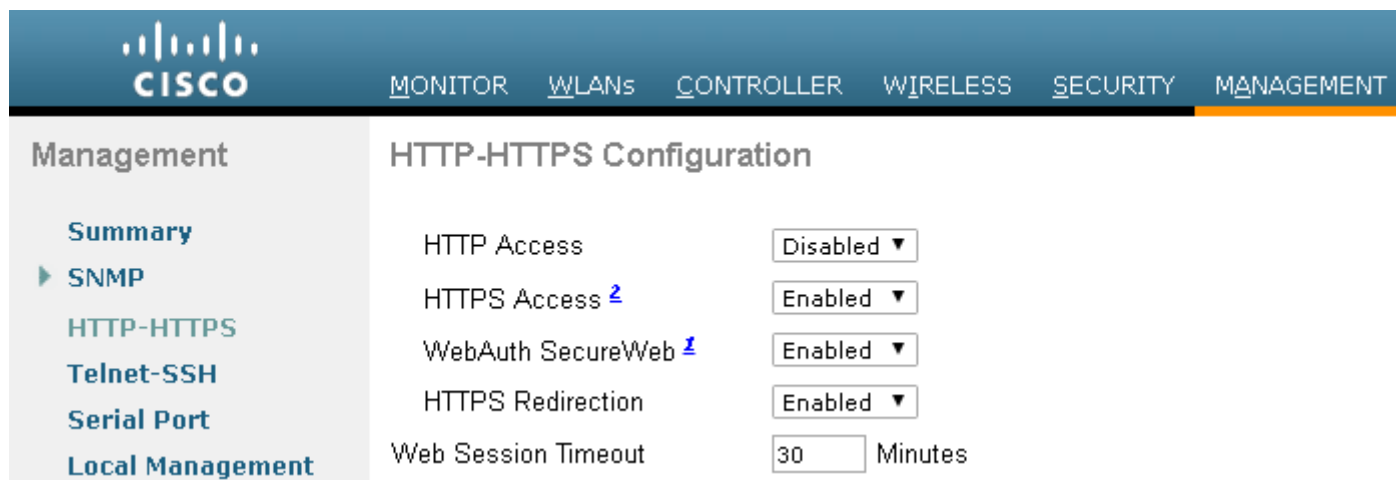
Mot de passe

## 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**".



The screenshot shows the Cisco Management interface. The top navigation bar includes the Cisco logo and tabs for MONITOR, WLANs, CONTROLLER, WIRELESS, SECURITY, and MANAGEMENT. The left sidebar shows the Management menu with options: Summary, SNMP, HTTP-HTTPS (selected), Telnet-SSH, Serial Port, and Local Management. The main content area is titled 'HTTP-HTTPS Configuration' and contains the following settings:

| Setting             | Value      |
|---------------------|------------|
| HTTP Access         | Disabled   |
| HTTPS Access        | Enabled    |
| WebAuth SecureWeb   | Enabled    |
| HTTPS Redirection   | Enabled    |
| Web Session Timeout | 30 Minutes |

- 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.

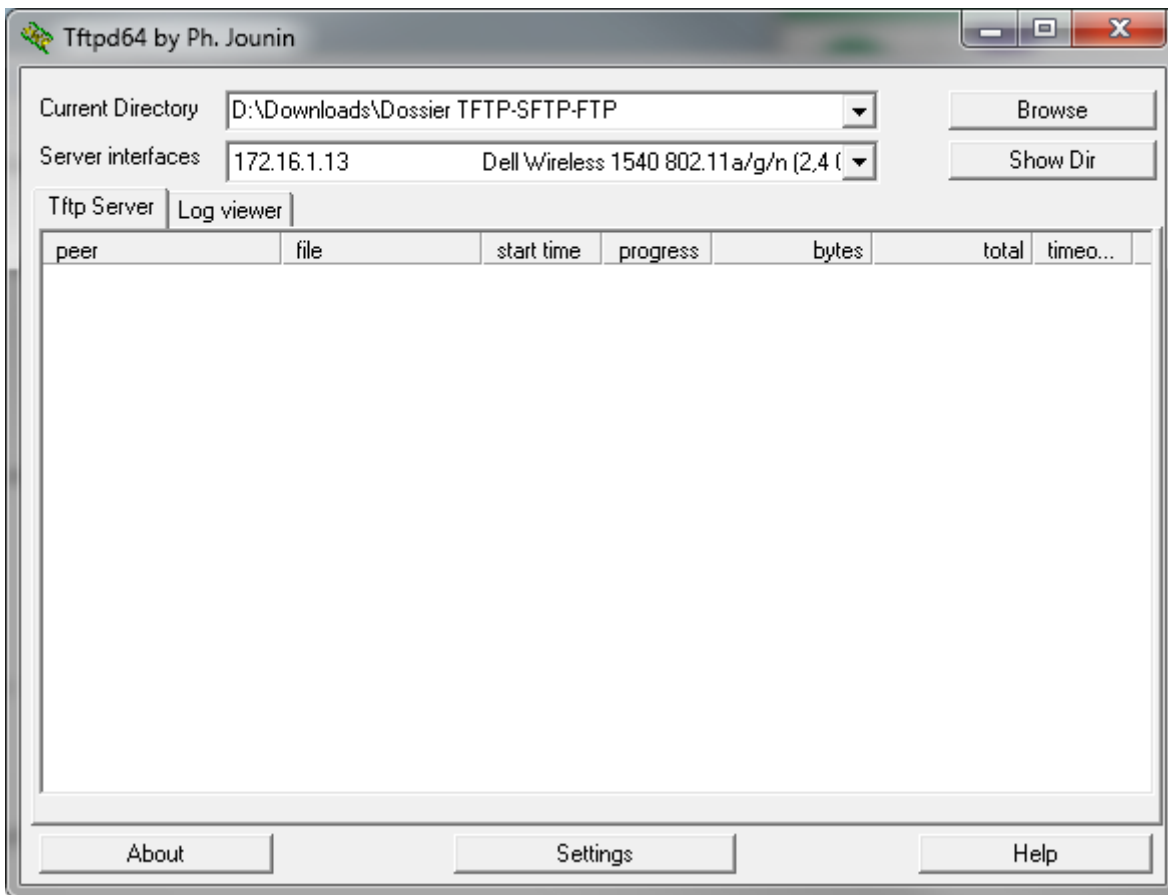


The screenshot shows a dark blue bar with the following links: Save Configuration | Ping | Logout | Refresh.

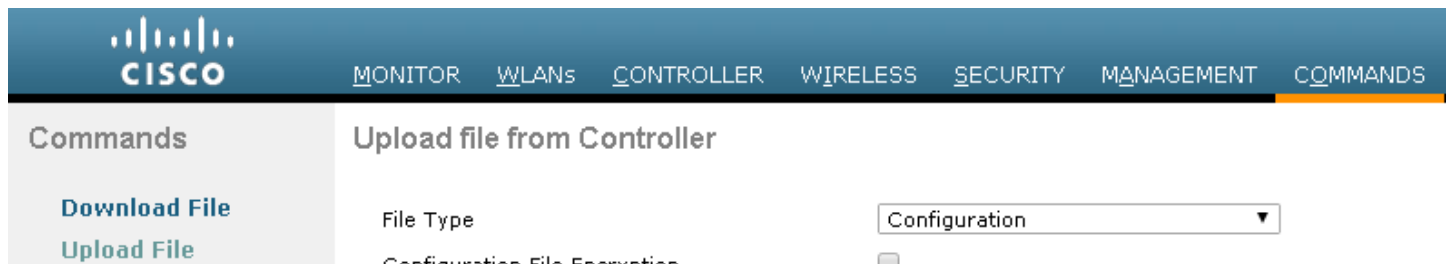
## c) Télécharger la configuration

- 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.

### Upload file from Controller

|                               |                          |
|-------------------------------|--------------------------|
| File Type                     | Configuration ▼          |
| Configuration File Encryption | <input type="checkbox"/> |
| Transfer Mode                 | TFTP ▼                   |

### Server Details

|                       |                                |
|-----------------------|--------------------------------|
| IP Address(Ipv4/Ipv6) | 172.16.1.13                    |
| File Path             | /                              |
| File Name             | WLC-IDUM-LAB-config_2017-10-27 |

- 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 Personal (Avec une Passphrase).

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

WLANS Entries 1 - 1 of 1

Current Filter: None [\[Change Filter\]](#) [\[Clear Filter\]](#) Create New

| <input type="checkbox"/> | WLAN ID           | Type | Profile Name  | WLAN SSID | Admin Status |
|--------------------------|-------------------|------|---------------|-----------|--------------|
| <input type="checkbox"/> | <a href="#">1</a> | WLAN | Profile_SSID1 | SSID1     | Enabled      |

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

WLANS > Edit 'Profile\_SSID1'

General Security QoS Policy-Mapping Advanced

Layer 2 Layer 3 AAA Servers

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

**Authentication Key Management**

|            |  |                                    |
|------------|--|------------------------------------|
| 802.1X     | <input type="checkbox"/>               | Enable                             |
| CCKM       | <input type="checkbox"/>               | Enable                             |
| PSK        | <input checked="" type="checkbox"/>    | Enable                             |
| FT 802.1X  | <input type="checkbox"/>               | Enable                             |
| FT PSK     | <input type="checkbox"/>               | Enable                             |
| PSK Format | ASCII <input type="button" value="v"/> | <input type="text" value="....."/> |

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

**FlexConnect**

|   |                                     |         |
|---|-------------------------------------|---------|
| FlexConnect Local Switching <a href="#">2</a>   | <input checked="" type="checkbox"/> | Enabled |
| FlexConnect Local Auth <a href="#">12</a>       | <input type="checkbox"/>            | Enabled |
| Learn Client IP Address <a href="#">3</a>       | <input checked="" type="checkbox"/> | Enabled |
| Vlan based Central Switching <a href="#">13</a> | <input type="checkbox"/>            | Enabled |
| Central DHCP Processing                         | <input type="checkbox"/>            | Enabled |
| Override DNS                                    | <input type="checkbox"/>            | Enabled |
| NAT-PAT   | <input type="checkbox"/>            | Enabled |
| Central Assoc                                   | <input type="checkbox"/>            | Enabled |

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

< Back

Apply

## b) Ajout d'un SSID2

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

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



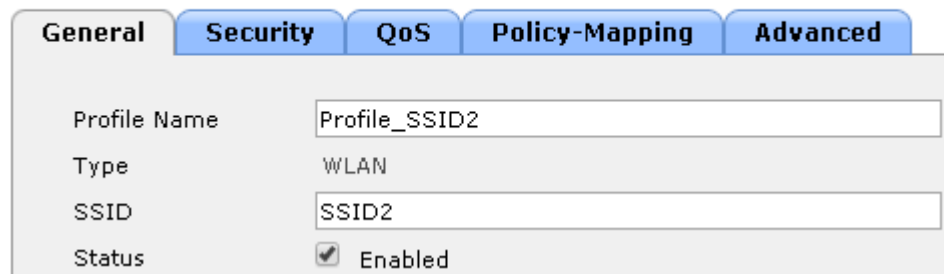
- Sélectionnez le type "**WLAN**", un profile Name, le nom du SSID et l'ID sur SSID. On valide en cliquant sur "**Apply**".

### WLANs > New

|              |               |
|--------------|---------------|
| Type         | WLAN ▼        |
| Profile Name | Profile_SSID2 |
| SSID         | SSID2         |
| ID           | 2 ▼           |

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

### WLANs > Edit 'Profile\_SSID2'



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



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

| FlexConnect                                     |   |
|---|---|
| FlexConnect Local Switching <a href="#">2</a>   | <input checked="" type="checkbox"/> Enabled |
| FlexConnect Local Auth <a href="#">12</a>       | <input type="checkbox"/> Enabled            |
| Learn Client IP Address <a href="#">5</a>       | <input checked="" type="checkbox"/> Enabled |
| Vlan based Central Switching <a href="#">13</a> | <input type="checkbox"/> Enabled            |
| Central DHCP Processing                         | <input type="checkbox"/> Enabled            |
| Override DNS                                    | <input type="checkbox"/> Enabled            |
| NAT-PAT   | <input type="checkbox"/> Enabled            |
| Central Assoc                                   | <input type="checkbox"/> Enabled            |

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

| MONITOR   <u>WLANS</u>   CONTROLLER   WIRELESS   SECURITY   MANAGEMENT   COMMANDS   HELP   FEEDBACK |                   |                                 |                                |   |                                   |                    |
|---|-------------------|---------------------------------|--------------------------------|---|-----------------------------------|--------------------|
| WLANS   |                   |                                 |                                |   |                                   | Entries 1 - 2 of 2 |
| Current Filter:   | None              | <a href="#">[Change Filter]</a> | <a href="#">[Clear Filter]</a> | <input type="button" value="Create New"/> | <input type="button" value="Go"/> |                    |
| <input type="checkbox"/>  | WLAN ID           | Type                            | Profile Name                   | WLAN SSID                                 | Admin Status                      | Security Policies  |
| <input type="checkbox"/>  | <a href="#">1</a> | WLAN                            | Profile_SSID1                  | SSID1                                     | Enabled                           | [WPA2][Auth(PSK)]  |
| <input type="checkbox"/>  | <a href="#">2</a> | WLAN                            | Profile_SSID2                  | SSID2                                     | Enabled                           | [WPA2][Auth(PSK)]  |

### 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**".

| CISCO   |                          | MONITOR | <u>WLANS</u> |
|---|--------------------------|---------|--------------|
| WLANS   |                          | WLANS   |              |
| <ul style="list-style-type: none"> <li>▼ <b>WLANS</b><br/>WLANS</li> <li>▼ <b>Advanced</b><br/>AP Groups</li> </ul> | Current Filter:          | No      |              |
|   | <input type="checkbox"/> | WLAN ID | Type         |

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

Entries 1 - 1 of 1

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

## AP Groups

### Add New AP Group

AP Group Name

Description

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

Ap Groups > Edit 'AP\_GRP\_Idum\_1'

**General** | **WLANs** | RF Profile | APs | 802.11u

| WLAN ID | WLAN SSID <sup>2</sup> | Interface/Interface Group(G) | SNMP NAC State |
|---------|------------------------|------------------------------|----------------|
|---------|------------------------|------------------------------|----------------|

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

**Add New**

WLAN SSID

Interface /Interface Group(G)

SNMP NAC State  Enabled

- Faites la même chose pour SSID1.

Ap Groups > Edit 'AP\_GRP\_Idum\_1'

**General** | **WLANs** | RF Profile | APs | 802.11u

| WLAN ID | WLAN SSID <sup>2</sup> | Interface/Interface Group(G) | SNMP NAC State                            |
|---------|------------------------|------------------------------|---|
| 2       | SSID2                  | management                   | Disabled <input type="button" value="v"/> |
| 1       | SSID1                  | management                   | Disabled <input type="button" value="v"/> |

- Vous devez obtenir ceci :

## AP Groups

| AP Group Name                 | AP Group Description             |
|-------------------------------|----------------------------------|
| <a href="#">AP_GRP_Idum_1</a> | <input type="button" value="v"/> |
| <a href="#">default-group</a> |                                  |

## 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 regrouper 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**".

The screenshot shows the Cisco Wireless configuration page. The 'WIRELESS' tab is selected. The left sidebar lists various wireless configuration options, with 'FlexConnect Groups' highlighted. The main area displays 'All APs' with a 'Current Filter' and a 'Number of APs' count of 0. A table with columns for AP Name, IP Address, AP Model, AP MAC, and AP I is visible.

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

New...

- Saisissez un nom de FlexConnect Group.

### FlexConnect Groups > New

Group Name

- Cliquez sur votre FlexConnect Group.

### FlexConnect Groups

Group Name

[Flex\\_Idum\\_1](#)



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

| General  | Local Authentication | Image Upgrade | ACL Mapping | Central DHCP | WLAN VLAN mapping |
|--|----------------------|---------------|-------------|--------------|-------------------|
| <p><b>WLAN VLAN Mapping</b></p> <p>WLAN Id <input type="text" value="2"/></p> <p>Vlan Id <input type="text" value="12"/></p> <p><input type="button" value="Add"/></p> |                      |               |             |              |                   |

Et

| General  | Local Authentication | Image Upgrade | ACL Mapping | Central DHCP | WLAN VLAN mapping |
|--|----------------------|---------------|-------------|--------------|-------------------|
| <p><b>WLAN VLAN Mapping</b></p> <p>WLAN Id <input type="text" value="1"/></p> <p>Vlan Id <input type="text" value="11"/></p> <p><input type="button" value="Add"/></p> |                      |               |             |              |                   |

- Vous devez obtenir ceci :

| General  | Local Authentication | Image Upgrade                     | ACL Mapping | Central DHCP | WLAN VLAN mapping |         |                   |      |   |               |                                   |   |               |                                   |
|--|----------------------|-----------------------------------|-------------|--------------|-------------------|---------|-------------------|------|---|---------------|-----------------------------------|---|---------------|-----------------------------------|
| <p><b>WLAN VLAN Mapping</b></p> <p>WLAN Id <input type="text" value="1"/></p> <p>Vlan Id <input type="text" value="1"/></p> <p><input type="button" value="Add"/></p>  |                      |                                   |             |              |                   |         |                   |      |   |               |                                   |   |               |                                   |
| <table border="1"> <thead> <tr> <th>WLAN Id</th> <th>WLAN Profile Name</th> <th>Vlan</th> </tr> </thead> <tbody> <tr> <td>1</td> <td>Profile_SSID1</td> <td><input type="text" value="11"/> ▼</td> </tr> <tr> <td>2</td> <td>Profile_SSID2</td> <td><input type="text" value="12"/> ▼</td> </tr> </tbody> </table> |                      |                                   |             |              |                   | WLAN Id | WLAN Profile Name | Vlan | 1 | Profile_SSID1 | <input type="text" value="11"/> ▼ | 2 | Profile_SSID2 | <input type="text" value="12"/> ▼ |
| WLAN Id  | WLAN Profile Name    | Vlan                              |             |              |                   |         |                   |      |   |               |                                   |   |               |                                   |
| 1  | Profile_SSID1        | <input type="text" value="11"/> ▼ |             |              |                   |         |                   |      |   |               |                                   |   |               |                                   |
| 2  | Profile_SSID2        | <input type="text" value="12"/> ▼ |             |              |                   |         |                   |      |   |               |                                   |   |               |                                   |

**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**".

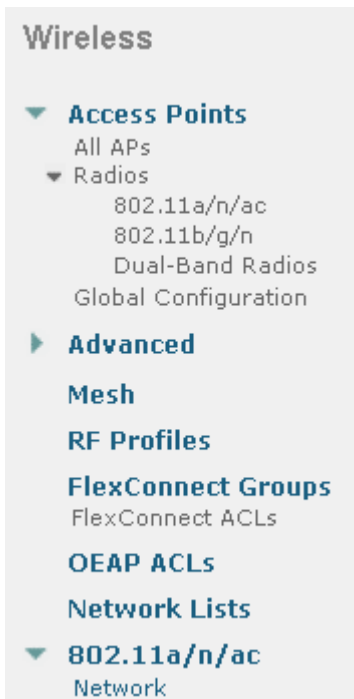
## Country

[List of access point models and protocols supported per country and regulatory domain](#)

|                                   |   |
|-----------------------------------|---|
| <b>Configured Country Code(s)</b> | FR  |
| <b>Regulatory Domain</b>          | 802.11a/n/ac: (Indoor: -E, Outdoor: -E)<br>802.11b/g/n: (Indoor: -E, Outdoor: -E) |

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**"

## 802.11a Global Parameters

### General

802.11a Network Status  Enabled

- Cliquez sur "**Apply**".

**Apply**

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



## Wireless

### ▼ Access Points

All APs

#### ▼ Radios

802.11a/n/ac

802.11b/g/n

Dual-Band Radios

Global Configuration

### ▶ Advanced

**Mesh**

**RF Profiles**

**FlexConnect Groups**

FlexConnect ACLs

**OEAP ACLs**

**Network Lists**

### ▶ 802.11a/n/ac

### ▼ 802.11b/g/n

Network

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

## 802.11b/g Global Parameters

### General

---

802.11b/g Network Status

Enabled

- Cliquez sur "**Apply**".

**Apply**

- Dans le menu "**Country**"

## Wireless

### ▼ Access Points

All APs

#### ▼ Radios

802.11a/n/ac

802.11b/g/n

Dual-Band Radios

Global Configuration

### ▶ Advanced

**Mesh**

**RF Profiles**

**FlexConnect Groups**

FlexConnect ACLs

**OEAP ACLs**

**Network Lists**

### ▶ 802.11a/n/ac

### ▶ 802.11b/g/n

### ▶ Media Stream

**Country**

- Cochez l'option : "**FR**"

|                                     |    |        |
|-------------------------------------|----|--------|
| <input checked="" type="checkbox"/> | FR | France |
|-------------------------------------|----|--------|

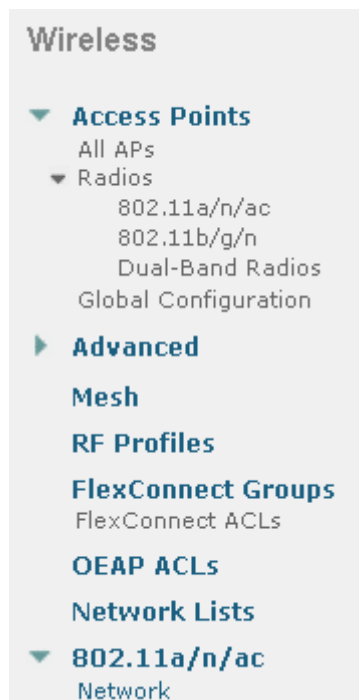
- Décochez l'option : "**US**"

|                          |    |               |
|--------------------------|----|---------------|
| <input type="checkbox"/> | US | United States |
|--------------------------|----|---------------|

- Cliquez sur "**Apply**".

**Apply**

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



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

### 802.11a Global Parameters

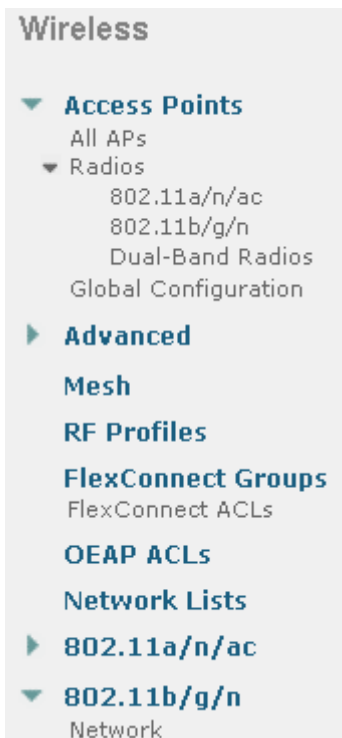
#### General

802.11a Network Status  Enabled

- Cliquez sur "**Apply**".

**Apply**

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



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

### 802.11b/g Global Parameters

#### General

802.11b/g Network Status  Enabled

- Cliquez sur **"Apply"**.

**Apply**

**"ATTENTION"** Si vous ne changez pas les 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 successfully 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 qu'elles démarrent.

- 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     | <span style="color: green;">●</span> 0 | <span style="color: red;">●</span> 0 | <a href="#">Detail</a> |
| 802.11b/g/n Radios  | 0     | <span style="color: green;">●</span> 0 | <span style="color: red;">●</span> 0 | <a href="#">Detail</a> |
| Dual-Band Radios    | 0     | <span style="color: green;">●</span> 0 | <span style="color: red;">●</span> 0 | <a href="#">Detail</a> |
| All APs             | 1     | <span style="color: green;">●</span> 0 | <span style="color: red;">●</span> 0 | <a href="#">Detail</a> |

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

| Number of APs                    |                       |                   |                   |                     |              |                    |
|----------------------------------|-----------------------|-------------------|-------------------|---------------------|--------------|--------------------|
| AP Name                          | IP Address(Ipv4/Ipv6) | AP Model          | AP MAC            | AP Up Time          | Admin Status | Operational Status |
| <a href="#">AP58ac.78c4.7a08</a> | 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 |
|----------------|--|------------|--------------|
| <b>General</b> |  |            |              |
| AP Name        | <input type="text" value="Borne1"/>          |            |              |
| Location       | <input type="text" value="Bat 1"/>           |            |              |
| AP MAC Address | 7c:ad:74:db:6a:94                            |            |              |
| Base Radio MAC | 08:cc:68:5f:57:c0                            |            |              |
| Admin Status   | <input type="button" value="Enable ▼"/>      |            |              |
| AP Mode        | <input type="button" value="FlexConnect ▼"/> |            |              |

- Cliquez sur "**Apply**".

- Dans le menu "**Advanced**", sélectionnez le "AP Group Name" : "**AP\_GRP\_IDUM\_1**".

## All APs > Details for Borne1

| General                  | Credentials                         | Interfaces | High Availability | Inventory | FlexConnect | Advanced         |
|--------------------------|-------------------------------------|------------|-------------------|-----------|-------------|------------------|
| Regulatory Domains       | 802.11bg:-E 802.11a:-I              |            |                   |           |             | <b>Power Ov</b>  |
| Country Code             | FR (France) ▼                       |            |                   |           |             | Pre-sta          |
| Cisco Discovery Protocol | <input checked="" type="checkbox"/> |            |                   |           |             | Power            |
| AP Group Name            | AP_GRP_Idum_1 ▼                     |            |                   |           |             | <b>AP Core I</b> |

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

**Apply**

- Attendez que la borne soit de nouveau visible sur le contrôleur.

- Puis retournez dans la configuration de la borne. Cliquez sur l'onglet "**FlexConnect**".

## All APs > Details for Borne2

| General | Credentials | Interfaces | High Availability | Inventory | FlexConnect |
|---------|-------------|------------|-------------------|-----------|-------------|
|---------|-------------|------------|-------------------|-----------|-------------|

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

|                        |                                     |                      |
|------------------------|-------------------------------------|----------------------|
| VLAN Support           | <input checked="" type="checkbox"/> |                      |
| Native VLAN ID         | 10                                  | <b>VLAN Mappings</b> |
| FlexConnect Group Name | Not Configured                      |                      |

- Cliquez sur "**Apply**".

**Apply**

- Recommencez les mêmes étapes pour la deuxième borne.

## All APs

**Current Filter**

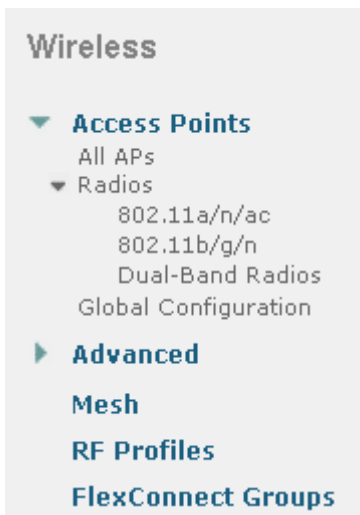
*None*

**Number of APs**

2

| AP Name                | IP Address(Ipv4/Ipv6) |
|------------------------|-----------------------|
| <a href="#">Borne1</a> | 172.16.10.3           |
| <a href="#">Borne2</a> | 172.16.10.4           |

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

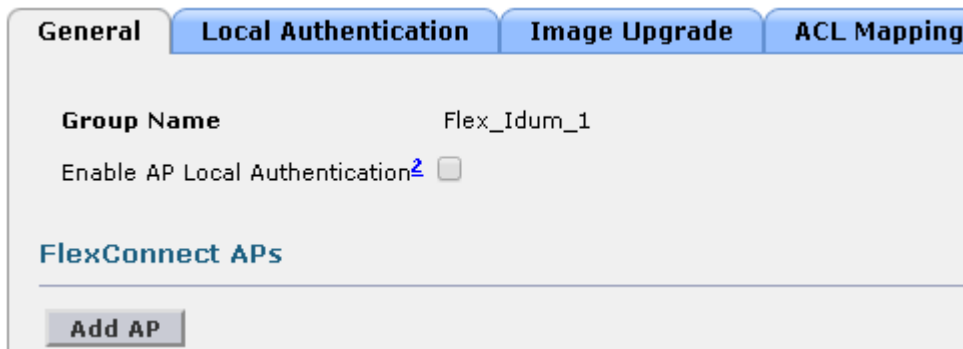


- Cliquez sur votre groupe Flexconnect, "**Flex\_Idum\_1**".

## FlexConnect Groups



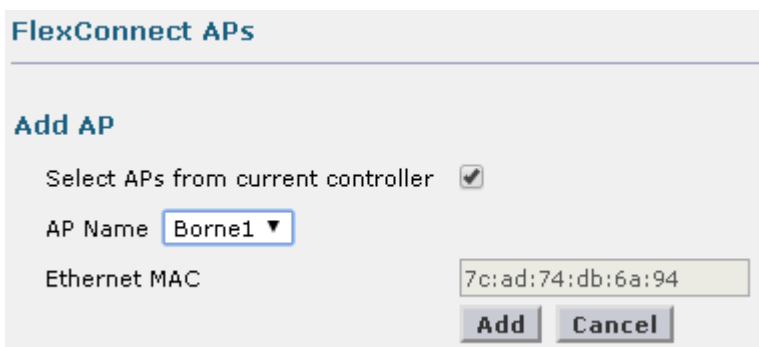
- Cliquez sur "**Add AP**".



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



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



- Vous devez avoir ceci :



**FlexConnect APs**

**Add AP**

Select APs from current controller

Ethernet MAC

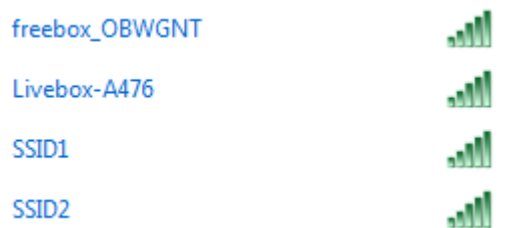
**Add** **Cancel**

| AP MAC Address    | AP Name | Status   |
|-------------------|---------|--|
| 58:ac:78:c4:7a:08 | Borne2  | Associated  |
| 7c:ad:74:db:6a:94 | Borne1  | Associated  |

- Cliquez sur "**Apply**".



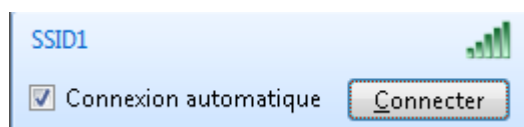
- Si vous regardez la couverture wifi, vous pourrez voir que les SSID sont diffusés.



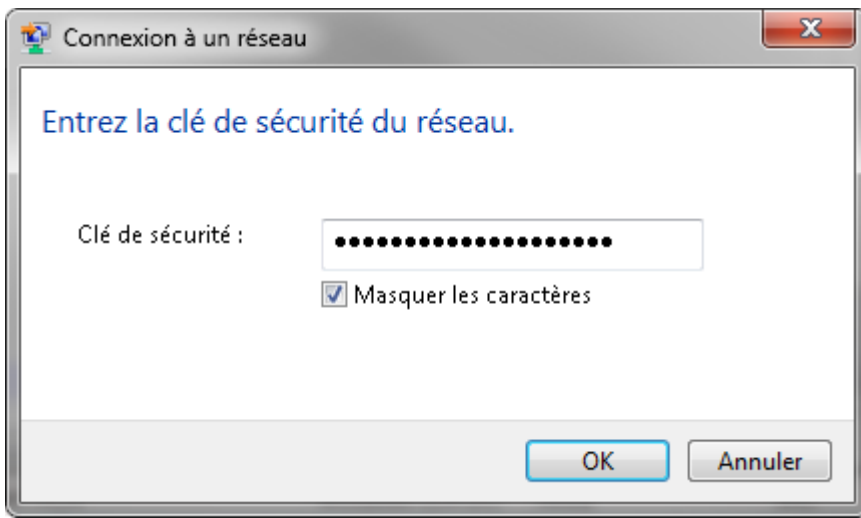
## VII) Tests

### 1) Tests de connexion sur les SSID

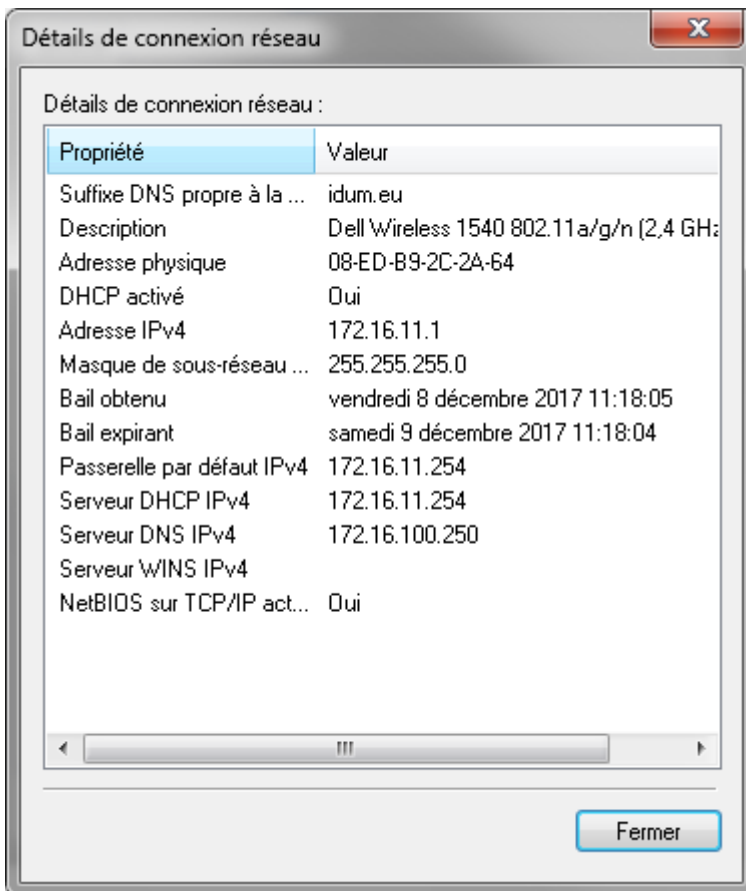
Maintenant que les deux bornes sont configurées, essayez de vous connecter.



- Authentifiez-vous en saisissant votre clef WPA2.



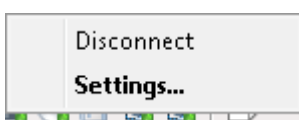
- Vérifiez que vous obtenez bien une adresse IP via le DHCP :



## 2) Tests perte contrôleur

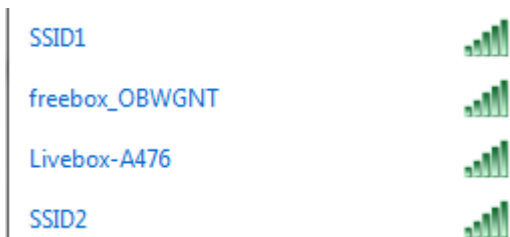
Nous aimerions maintenant savoir comment réagit la couverture Wifi de notre entreprise lors de la perte du contrôleur Wifi. Pour cela nous allons faire un shut sur notre interface VMware correspondant à l'interface de Management.

- 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.

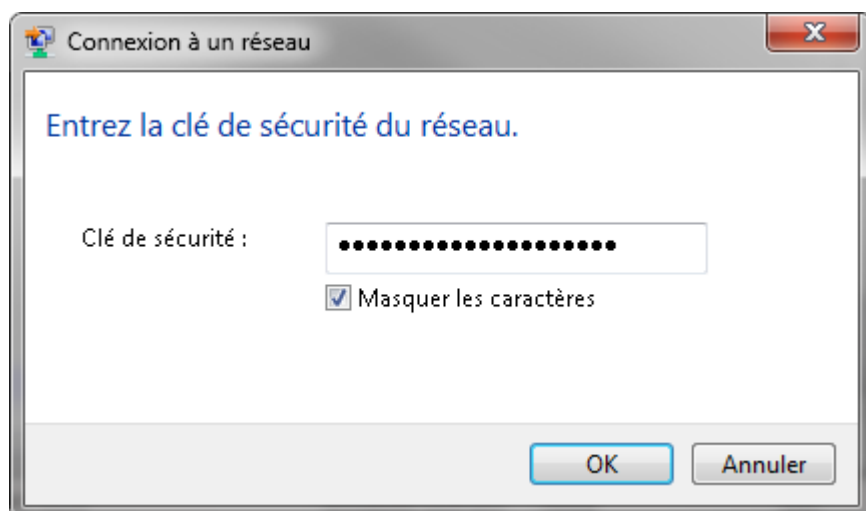




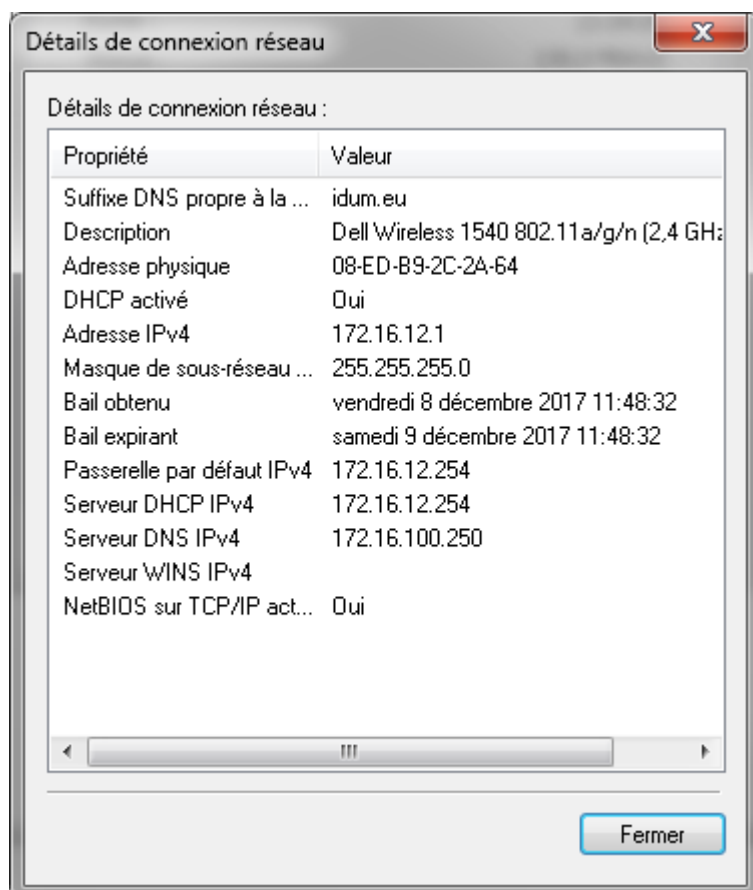
- Cliquez sur SSID2 pour vous connecter.



- 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.

30 avril 2018 -- N.Salmon -- article\_337.pdf



# Idum