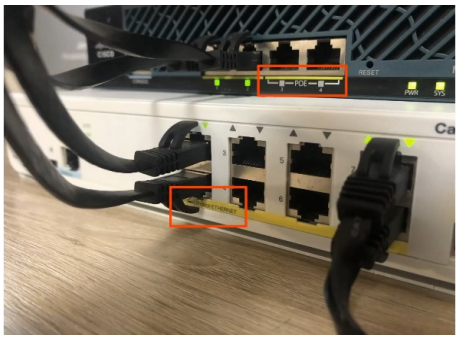
Cours 58 : Configuration Sans Fil

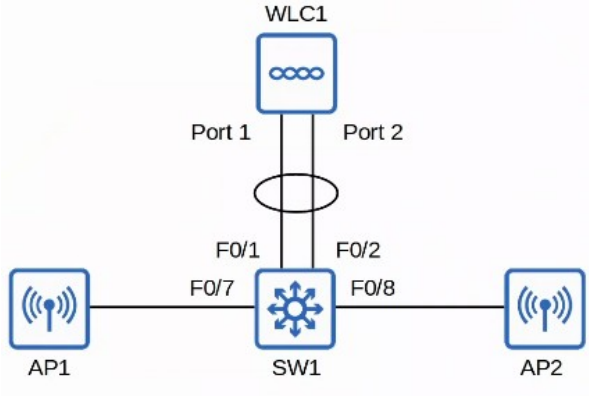
Dans ce cours nous verrons la configuration sans fil.
Nous ferons d'abord une introduction sur les topologies réseaux que nous utiliserons.
Nous ferons aussi une introduction sur la configuration nécessaire sur un Switch avant d'y connecter tous les appareils à ce Switch central.
Nous verrons la mise en place de base des contrôleurs sans fil LAN nous pourrons accéder au GUI (Graphical User Interface) et faire la configuration. Nous verrons ensuite comment configurer les interfaces WLC, et nous configurerons quelques WLAN. En dernier temps nous verrons quelques fonctionnalités additionnels de WLC.

La topologie du réseau que nous utiliserons sera la suivante :

Sur cette topologie on peut voir 1 Switch, UN WLC controler et 2 point d'accès (AP pou access Point). On peut voir que les points d'accès ne sont pas alimentés par des alimentations, elles sont alimentés par les câbles Ethernet qui fournissent l'énergie en PoE.
Comme on peut le voir sur l'image suivante le Switch supporte le PoE, tout comme le WLC (en haut)



La topologie du réseau en le suivant :

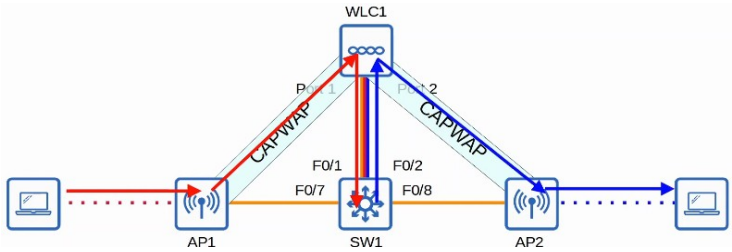


Le WLC est connecté au Switch par un LAG (Link Aggregation Group) ou EtherChannel.
Les WLC supportent uniquement le LAG Statique et non pas PagP ou LACP.

Nous utiliserons dans ce réseau 3 VLAN :
VLAN 10 : Management, 192.168.1.0/24
VLAN 100 : Internal, SSID : Internal, 10.0.0.0/24
VLAN 200 : Guest, SSID : Guest, 10.1.0.0/24

Le Vlan 10 est utile seulement dans la gestion des appareils, modifier leurs configurations etc..
Les VLAN 100 et 200 seront utile dans l'usage des utilisateurs.

Le switch aura un SVI pour chaque VLAN à chaque fois l'adresse finissant par .1 de chaque sous réseau. Le WLC aura lui aussi une adresse IP de chaque VLAN aussi avec pour adresse finissant par .100 dans chaque sous réseau.
Le Switch a été configuré pour être à la fois le serveur DHCP et le serveur NTP.
Seulement le lien avec le WLC doit être configuré avec le Switch pour être un port Trunk.
Par exemple lorsqu'un client se connecte à l'un des points d'accès, les données sont transmises avec CAPWAP vers le WLC qui lui même fais le transfert vers le Switch. Le Switch transfère ensuite ses données au client en passant par le même chemin, c'est à dire le WLC puis le point d'accès.
Maintenant que se passe t-il si le client du VLAN 100 (Interne) veut communiquer avec un autre client du VLAN 200 (Guest) ? Le client enverra le trafique vers son Gateway, qui transmettra au WLC puis au Switch. Le Switch va redistribuer le trafique vers le WLC qui le transmettra au Switch puis au point d'accès afin de le faire passer vers le client de l'autre VLAN.
Comme sur le schéma suivant :



Commençons par faire la configuration du Switch, con utilise les commandes suivantes :

```
SW1(config)#vlan 10
SW1(config-vlan)#name Management
SW1(config-vlan)#vlan 100
SW1(config-vlan)#name Internal
SW1(config-vlan)#vlan 200
SW1(config-vlan)#name Guest

SW1(config)#int range f0/6 - 8
SW1(config-if-range)#switchport mode access
SW1(config-if-range)#switchport access vlan 10
SW1(config-if-range)#spanning-tree portfast

SW1(config-if-range)#interface range f0/1 - 2
SW1(config-if-range)#channel-group 1 mode on

SW1(config-if-range)#interface port-channel 1
SW1(config-if)#switchport mode trunk
SW1(config-if)#switchport trunk allowed vlan 10,100,200
```

On commence par créer les 3 VLAN, et leur donner un nom avec les commandes suivantes

```
SW1(config)#vlan 10
SW1(config-vlan)#name Management
SW1(config-vlan)#vlan 100
SW1(config-vlan)#name Internal
SW1(config-vlan)#vlan 200
SW1(config-vlan)#name Guest
```

On configure ensuite les interface pour spécifier le « mode access » :

```
SW1(config)#int range f0/6 - 8
SW1(config-if-range)#switchport mode access
SW1(config-if-range)#switchport access vlan 10
SW1(config-if-range)#spanning-tree portfast
```

On configure les interfaces vers le WLC en Etherchannel (LAG) avec les commandes suivantes :
WLC supporte uniquement le LAG statique et non pas PagP ou LACP.

```
SW1(config-if-range)#interface range f0/1 - 2
SW1(config-if-range)#channel-group 1 mode on
```

On configure les interface port channel en mode Trunk avec les commandes :

```
SW1(config-if-range)#interface port-channel 1
SW1(config-if)#switchport mode trunk
SW1(config-if)#switchport trunk allowed vlan 10,100,200
```

Une fois ces cela configuré on lance ensuite les commandes suivantes pour la configuration des SVI (Switch Virtual Interface) des VLAN, du serveur DHCP et de NTP :

```
SW1(config)#interface vlan 10
SW1(config-if)#ip address 192.168.1.1 255.255.255.0
SW1(config-if)#interface vlan 100
SW1(config-if)#ip address 10.0.0.1 255.255.255.0
SW1(config-if)#interface vlan 200
SW1(config-if)#ip address 10.1.0.1 255.255.255.0

SW1(config)#ip dhcp pool VLAN10
SW1(dhcp-config)#network 192.168.1.0 255.255.255.0
SW1(dhcp-config)#default-router 192.168.1.1
SW1(dhcp-config)#option 43 ip 192.168.1.100

SW1(config)#ip dhcp pool VLAN100
SW1(dhcp-config)#network 10.0.0.0 255.255.255.0
SW1(dhcp-config)#default-router 10.0.0.1

SW1(config)#ip dhcp pool VLAN200
SW1(dhcp-config)#network 10.1.0.0 255.255.255.0
SW1(dhcp-config)#default-router 10.1.0.1

SW1(config)#ntp master
```

On configure les SVI (Switch Virtual Interface) des Vlan, ces adresses sont utilisés comme passerelle par défaut de leur sous réseau, on lance les commandes suivantes :

```
SW1(config)#interface vlan 10
SW1(config-if)#ip address 192.168.1.1 255.255.255.0
SW1(config-if)#interface vlan 100
SW1(config-if)#ip address 10.0.0.1 255.255.255.0
SW1(config-if)#interface vlan 200
SW1(config-if)#ip address 10.1.0.1 255.255.255.0
```

On configure ensuite les pool DHCP avec les commandes suivantes :
Le VLAN 10 a la commande option 43 lancé, cette commande permet de dire aux points d'accès l'adresse IP de leur WLC (ici l'adresse du WLC est 192.168.1.100).

```
SW1(config)#ip dhcp pool VLAN 10
SW1(dhcp-config)#network 192.168.1.0 255.255.255.0
SW1(dhcp-config)#default-router 192.168.1.1
SW1(dhcp-config)#option 43 ip 192.168.1.100

SW1(config)#ip dhcp pool VLAN100
SW1(dhcp-config)#network 10.0.0.0 255.255.255.0
SW1(dhcp-config)#default-router 10.0.0.1

SW1(dhcp-config)#dhcp pool VLAN200
SW1(dhcp-config)#network 10.1.0.0 255.255.255.0
SW1(dhcp-config)#default-router 10.1.0.1
```

On lance en dernier temps la commande suivante pour activer le serveur NTP :
`SW1(config)#ntp master`

Voyons à présent comment le WLC :

```
Welcome to the Cisco Wizard Configuration Tool
Use the '-' character to backup


Would you like to terminate autoinstall? [yes]:

System Name [Cisco_10:65:64] (31 characters max): WLC1
Enter Administrative User Name (24 characters max): admin
Enter Administrative Password (3 to 24 characters): *********
Re-enter Administrative Password                : *********

Enable Link Aggregation (LAG) [yes][NO]: yes

Management Interface IP Address: 192.168.1.100
Management Interface Netmask: 255.255.255.0
Management Interface Default Router: 192.168.1.1
Management Interface VLAN Identifier (0 = untagged): 10
Management Interface DHCP Server IP Address: 192.168.1.1
```

Lorsque l'on se connecte au WLC on utilise un câble console, le premier message que l'on peut voir apparaître est qu'il demande s'il est nécessaire de faire la terminer la configuration avec « autoinstall » qui va récupérer la configuration à partir d'un serveur TFTP.
On configure ensuite le nom de système, le nom d'utilisateur et le mot de passe.
On spécifie si l'on veut activer LAG (Link Aggregation), on indique « yes » car la réponse par défaut est ici « NO ». On indique les adresses voulue à configurer.

On continue la configuration basique du WLC en répondant aux question au lieu de lancer les commandes de configuration directement sur une ligne de commande :

```
Virtual Gateway IP Address: 172.16.1.1

Multicast IP Address: 239.239.239.239

Mobility/RF Group Name: jITlab

Network Name (SSID): Internal

Configure DHCP Bridging Mode [yes][NO]: no

Allow Static IP Addresses [YES][no]: yes

Configure a RADIUS Server now? [YES][no]: no
Warning! The default WLAN security policy requires a RADIUS server.
Please see documentation for more details.

Enter Country Code list (enter 'help' for a list of countries) [US]: FR
```

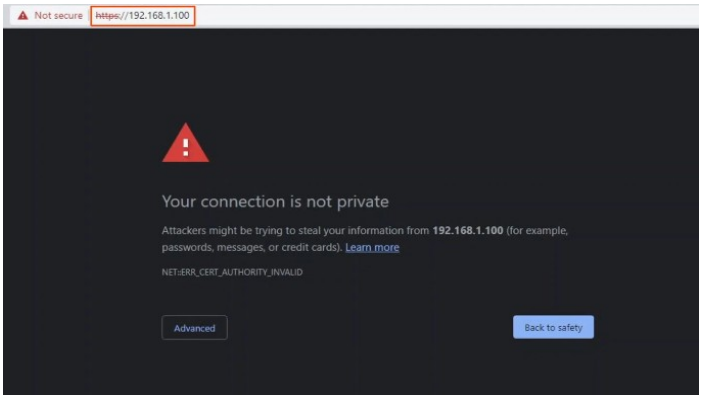
Les trois première options sont utile, le Virtual Gateway IP est une adresse utilisé lorsque le WLC pour communiquer directement avec ses clients sans fil.
L'adresse Multicast est l'adresse utilisé pour transmettre le trafique vers ces IP.
Le Mobility/RF Group Name est utilisé lorsque l'on a par exemple plusieurs WLC et que l'on veut qu'ils fonctionnent ensemble.
A la suite de la configuration est demandé de configurer le SSID, on en configure pour l'instant 1 et on laisse le reste de la configuration avec les réponses par défaut.
On ne configure pas pour l'instant de serveur RADIUS nous changerons la politique de sécurité WLAN vers PSK donc il ne sera plus nécessaire de configurer de serveur RADIUS.
On entre le code du pays « FR » pour « France », ici on configure la France comme pays car le modèle est compatible avec l'Europe, le nom du modèle du point d'accès est avec un « E » pour Europe. (Modèle : AIR-CAP3502I-E-K9)

On continue la configuration du WLC :

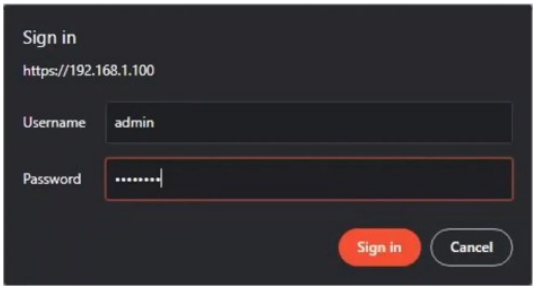
```
Enable 802.11b Network [YES][no]:
Enable 802.11a Network [YES][no]:
Enable 802.11g Network [YES][no]:
Enable Auto-RF [YES][no]:

Configure a NTP server now? [YES][no]: yes
Enter the NTP server's IP address: 192.168.1.1
Enter a polling interval between 3600 and 604800 secs: 3600

Configuration correct? If yes, system will save it and reset. [yes][NO]:
yes

Configuration saved!
Resetting system with new configuration...
```

On choisie ici d'activer les mode 802.11b, 802.11a, 802.11g.
On configure ensuite le serveur NTP pour que le WLC ait le temps correct.
On sauvegarde les paramètre et l'appareil se réinitialise.

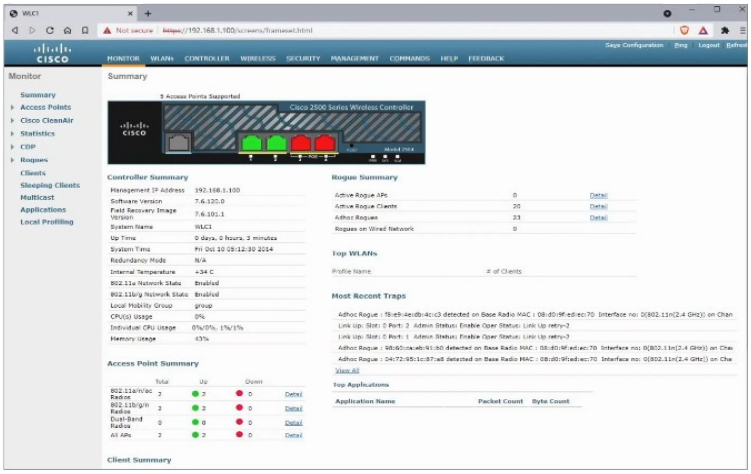
Une fois tout cela configuré il est possible de se connecter au WLC par le moyen d'un navigateur web. On lance donc l'adresse du WLC (192.168.1.100) depuis le navigateur.



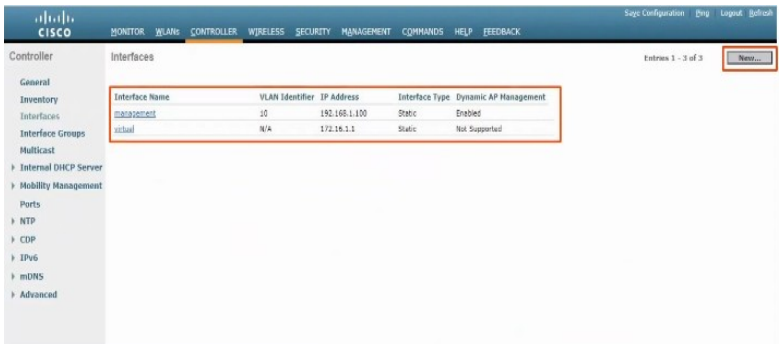
Il faut cliquer sur Advanced et « accéder à 192.168.1.100 »
On peut à présent accéder à l'interface de gestion du WLC, on clique sur « Login » puis on entre les identifiant et mot de passe configuré au départ :



Voici le panel de gestion du WLC :

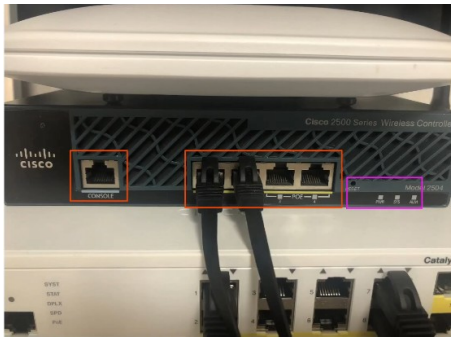


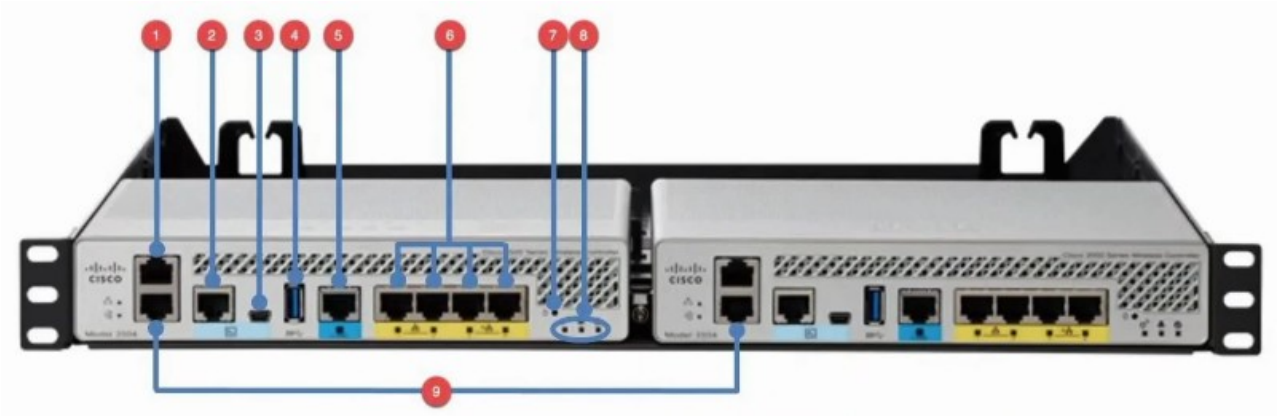
On peut voir quelle interface sont active et des informations divers sur le WLC avec les points d'accès connectés etc..
Sur la page « Controller » on clique sur « Interfaces », on peut voir la VLAN que l'on configuré au départ, il n'y a pour le moment que le VLAN 10. On clique sur « New » pour en ajouter une nouvelle.



Les ports de WLC sont des ports physique sur lesquelles des câbles se connectent.
Les interfaces WLC sont des interfaces logique inclus dans le WLC (Par exemple le SVI sur un Switch), WLC a plusieurs sorte de ports :
- Service port : Un port de gestion dédié utilisé pour la gestion. Il doit être connecté à un port access du Switch car il ne supporte qu'une seule VLAN. Ce port peut être utilisé pour se connecter à l'appareil tant que celui ci démarre, récupère le système, etc...
- Distribution system port : Ce sont les ports standard du réseau qui connectent au système de distribution (réseau câblé) et qui est utilisé pour le trafique de donnée. Ces ports se connectent aux ports Switch Trunk, et si plusieurs ports de distribution sont utilisé ils peuvent former un LAG.
- Port console : C'est le port console standard, avec un port RJ45 ou USB.
- Port de redondance : Ce port est utilisé pour se connecter à un autre WLC pour former une pair de haute disponibilité (High Availability en Anglais).

On peut voir ici 4 ports de distribution, et un port Console.



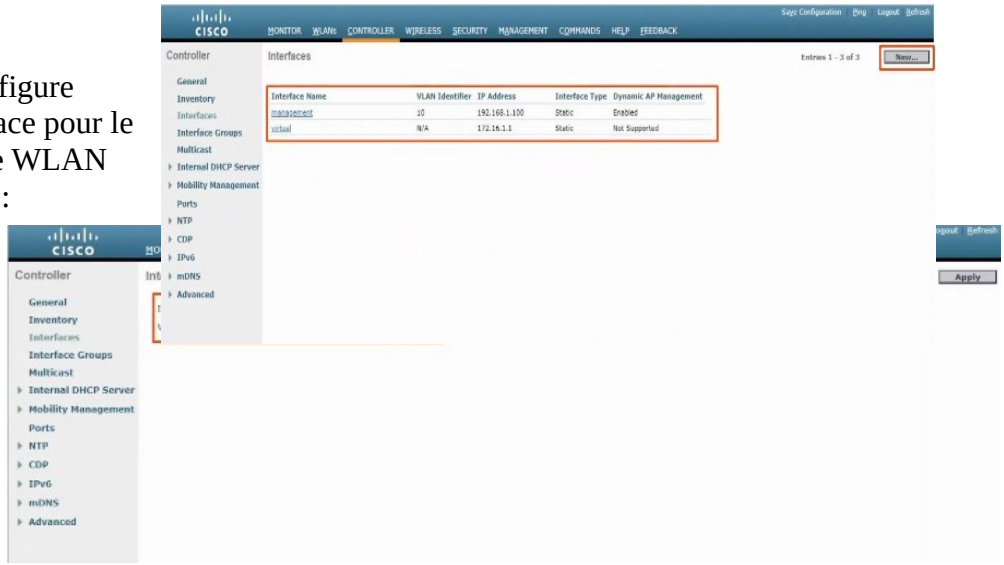


Voici un réseau avec une pair de 2 WLC, voyons chacun des numéro de 1 à 9 :
1) Le Service Port
2) Port Console (RJ45)
3) Port Console (USB)
4) USB (Pour mis à jour logicielle)
5) Port système de Distribution (Multi-gigabit)
6) Port système de Distribution (1-gig)
7) Bouton Reset
8) LED de Statut
9) Port de Redondance

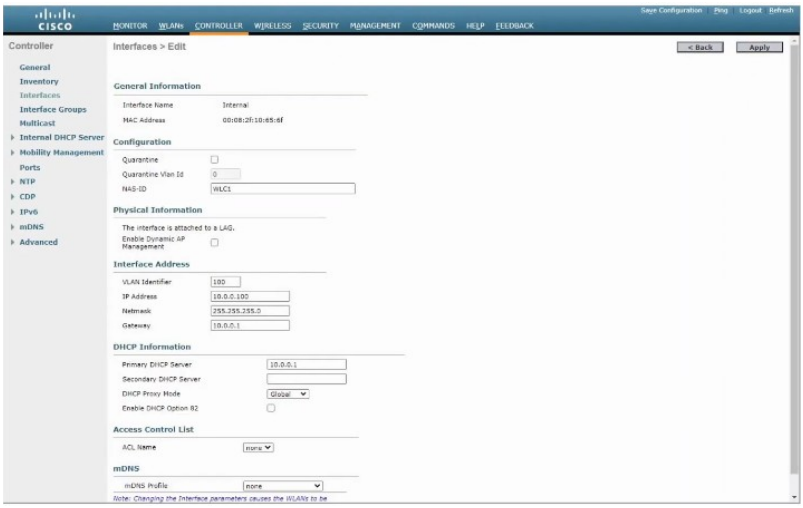
Les WLC ont différents type d'interfaces :
- Interface de gestion : utilisé pour gérer le trafique comme Telnet, SSH, HTTP, HTTPS, Authentification RADIUS, NTP, Syslog, etc... Tunnels CAPWAP sont aussi formés vers/depuis l'interface de gestion du WLC.
- Interface de gestion de redondance : Lorsque deux WLC sont connectés par leurs ports de redondance, un WLC est « active » et l'autre est en « standby ». Cette interface est utilisé pour connecter et gérer le WLC « standby ».
- Interface Virtuel : Cette interface est utilisé lorsque l'on communique avec les clients sans fil vers le relai de requête DHCP, que l'on fait fonctionner une authentification web client, etc...
- Interface de port de Service : Si le port de service est utilisé, cette interface est lié vers celle ci et utilisé pour la gestion externe.
- Dynamic interface : Ce sont les interfaces utilisé pour cartographier un WLAN vers un VLAN. Par exemple, le trafique depuis le WLAN « internal » sera envoyé vers le réseau câblé depuis l'interface dynamic du WLC « internal »

Retournons à présent sur l'interface GUI pour configurer des interfaces Dynamique :

On configure l'interface pour le trafique WLAN interne :

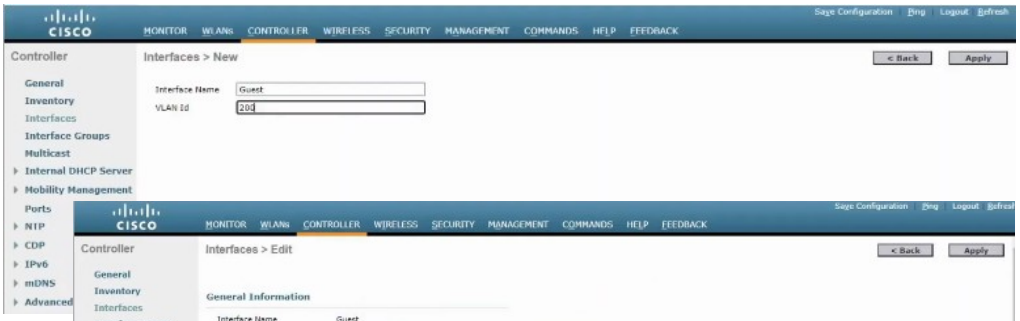


L’écran affiche la page suivante :
On indique l’adresse IP du vlan et son masque de sous réseau puis on applique les modifications en cliquant sur « Apply »

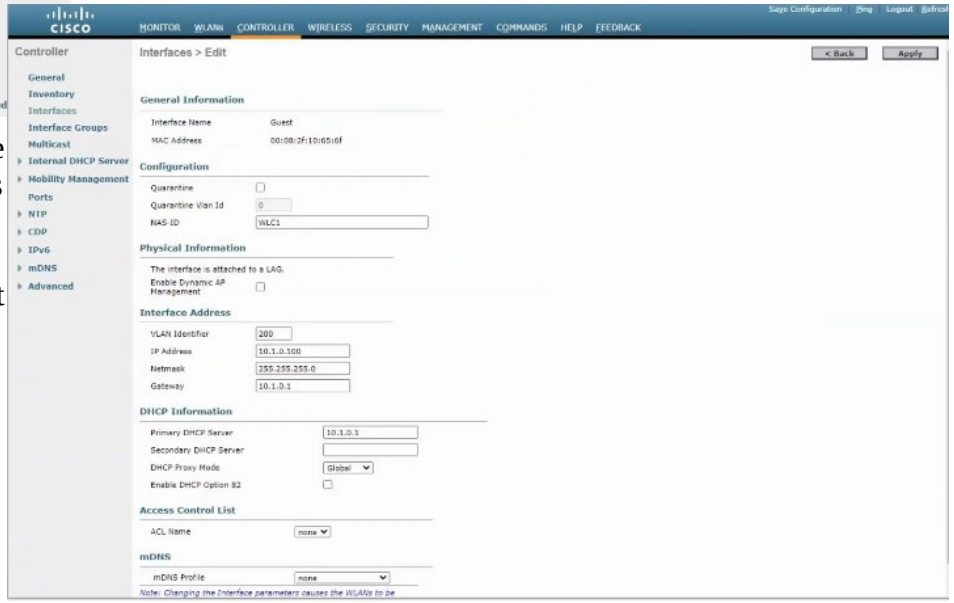


Depuis le menu Dynamic on peut à présent voir les 3 interfaces, dont celle venant d’être crée qui est « Internal »

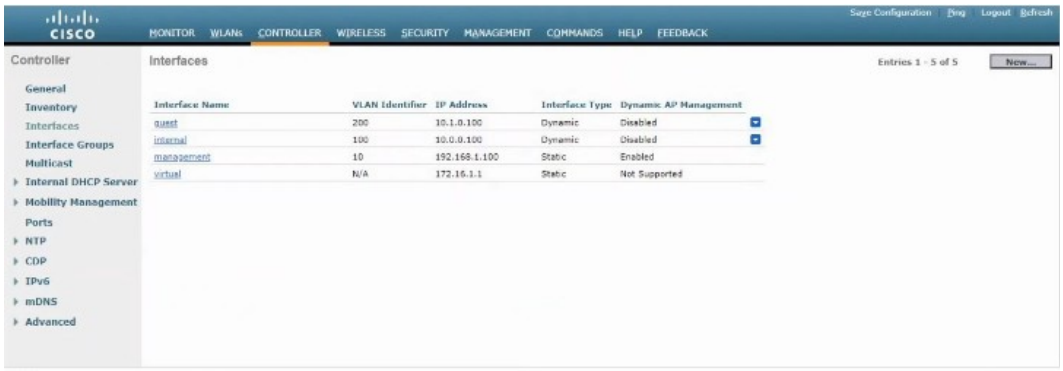
Il reste à créer l’interface « Guest », pour cela on procède comme auparavant en spécifiant les paramètre voulant être appliqué pour l’interface « Guest » :



Sur cette page on indique les adresse IP nécessaire correspondant au VLAN :

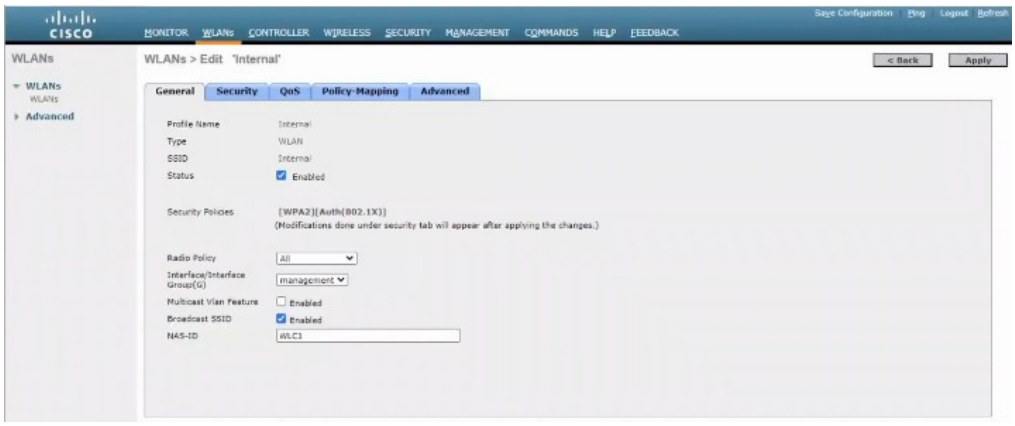


Toutes les interfaces sont à présent bien configurés :

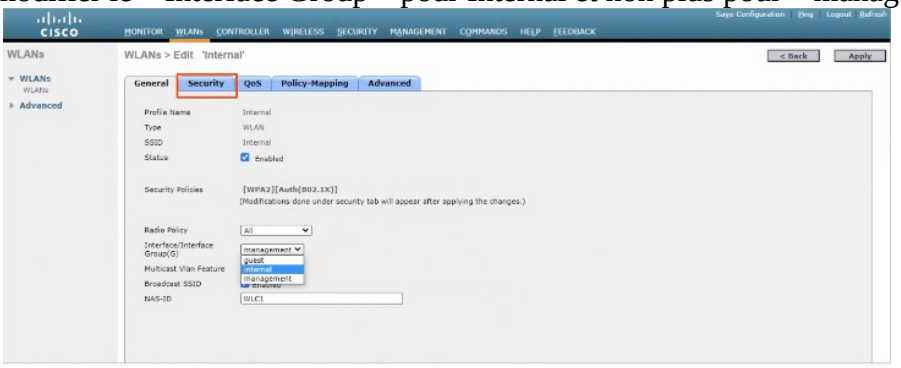


Faisons la configuration des WLAN :

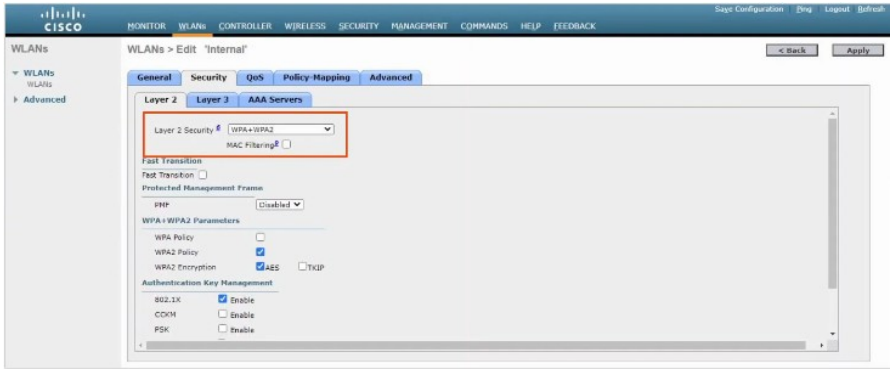
Il n’y en a ici qu’une seul, le mode de politique de sécurité est WPA2, 802.1X, donc le mode Enterprise, nous allons configurer le mode PSK.
En cliquant sur le « 1 » à gauche il est possible de modifier ce WLAN.



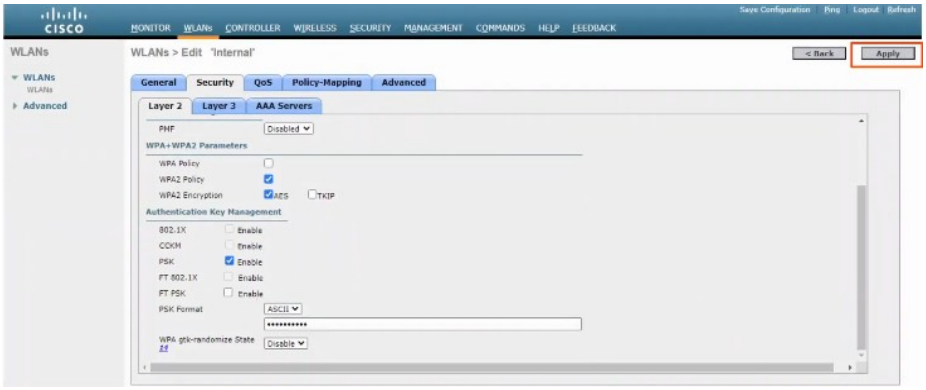
Nous allons modifier le « Interface Group » pour Internal et non plus pour « management ».



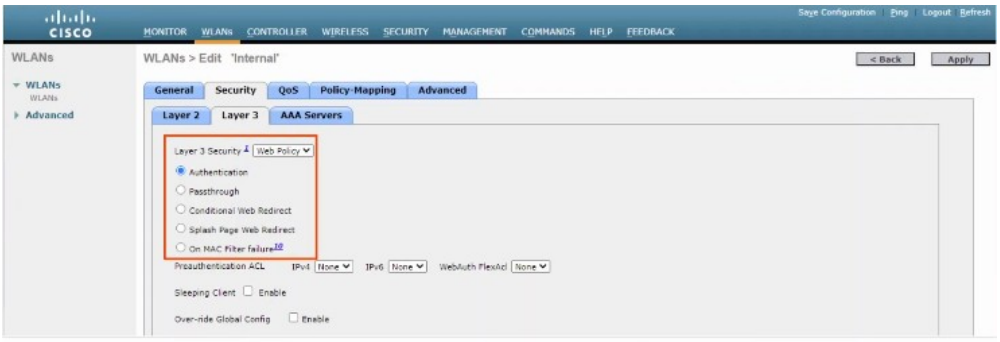
Pour modifier afin d'utiliser le mode PSK, on se rend sur l'onglet « Security »



Et nous modifions la gestion des clefs d'authentification et sélectionnons PSK :

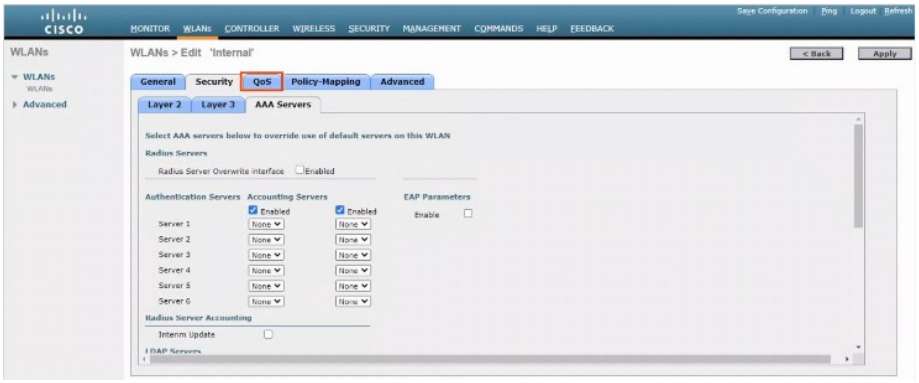


On sélectionne aussi le PSK format pour ASCII et on entre un mot de passe et on applique les modifications. Il est possible de modifier le Layer 3 et de modifier le mode d'authentification :

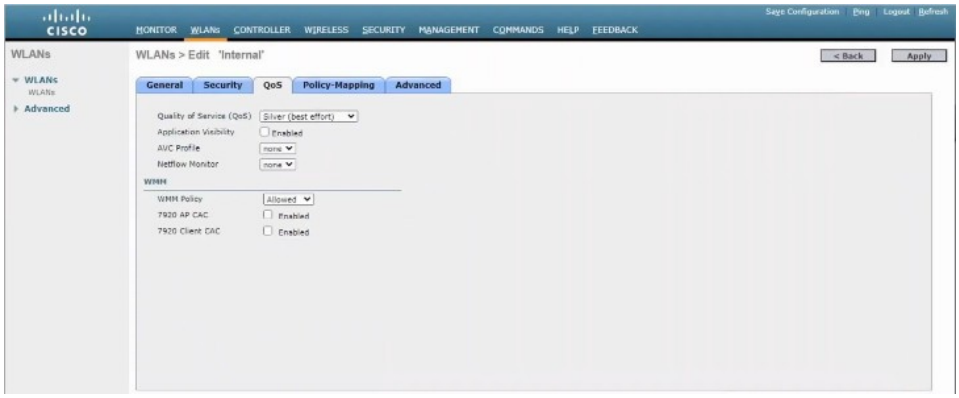


Plusieurs modes sont présents :
-Web Authentication : Après que les clients sans fil ont leurs adresse IP et essaient d'accéder à la page web, ils doivent entrer un nom d'utilisateur et un mode de passe pour s'authentifier.
- Web Passthrough : même chose que Web Authentication mais aucun nom d'utilisateur ou mot de passe n'est requis. Un signal ou déclaration apparaît et le client doit tout simplement accepter pour avoir accès à Internet.
- Conditional et Splash Page, sont des options de redirection web similaire mais qui requière de manière additionnel une authentification 802.1X couche 2.

Il y a aussi un mode AAA :

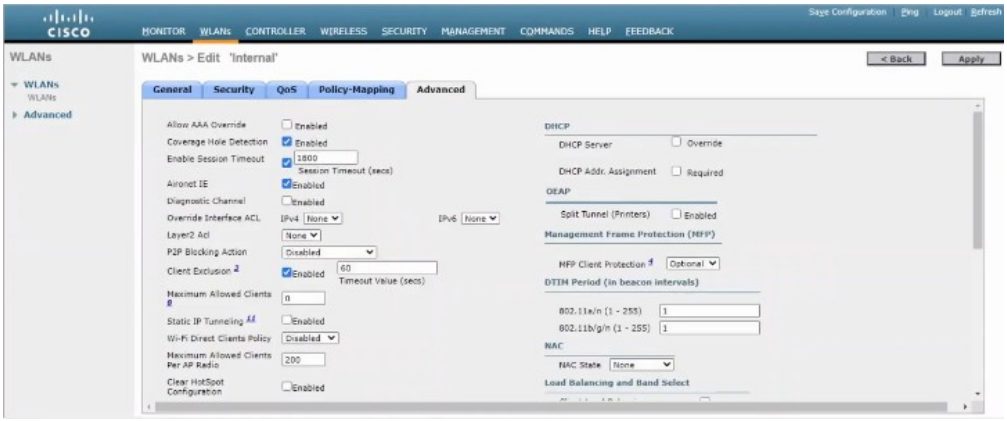


Voyons l'onglet QoS :

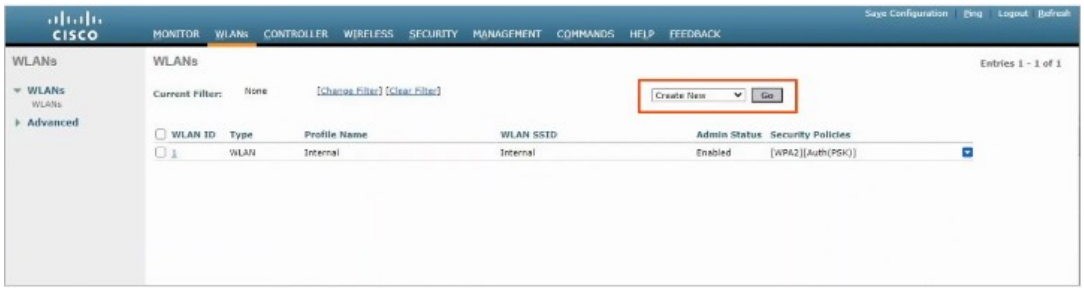


Il faut vérifier que le mode activé est bien le mode Silver (Best Effort).
Il existe d'autres modes comme Gold (Vidéo), Platinum (Voice), Bronze (Background)

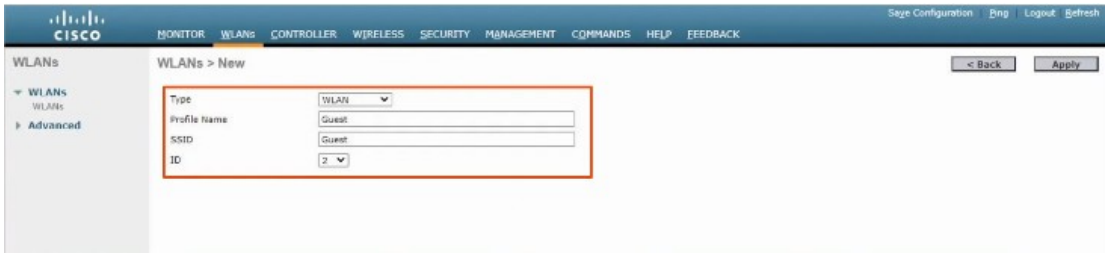
Dans l'onglet « advanced » on peut voir différents services :



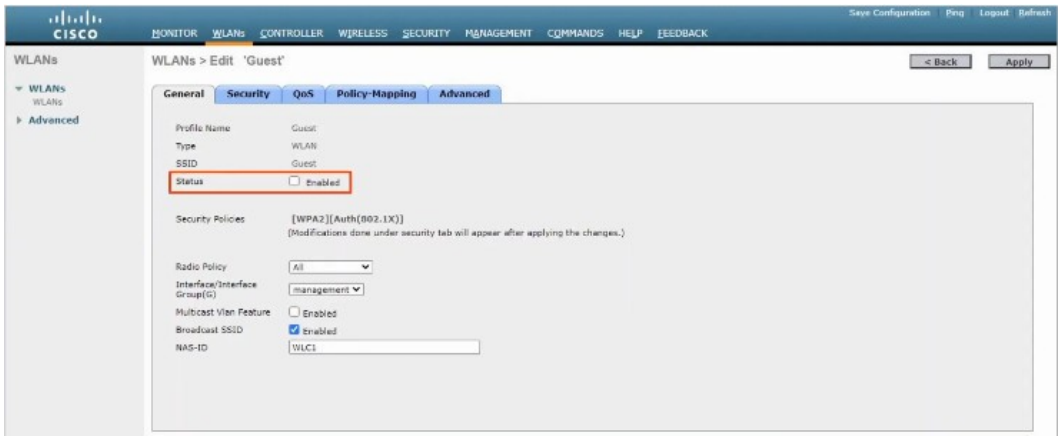
Pour créer un nouveau WLAN ou clique sur « Go », nous allons vréer le WLAN Guest.



On indique le Type, le Profile Name et le SSID, il n’est pas nécessaire qu’il soit identiques.



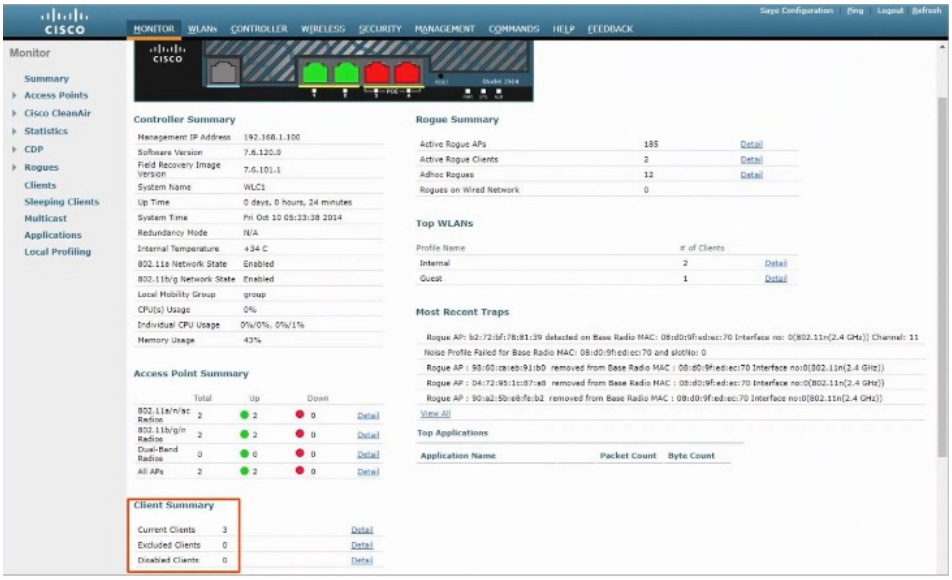
On arrive ensuite à cette page :



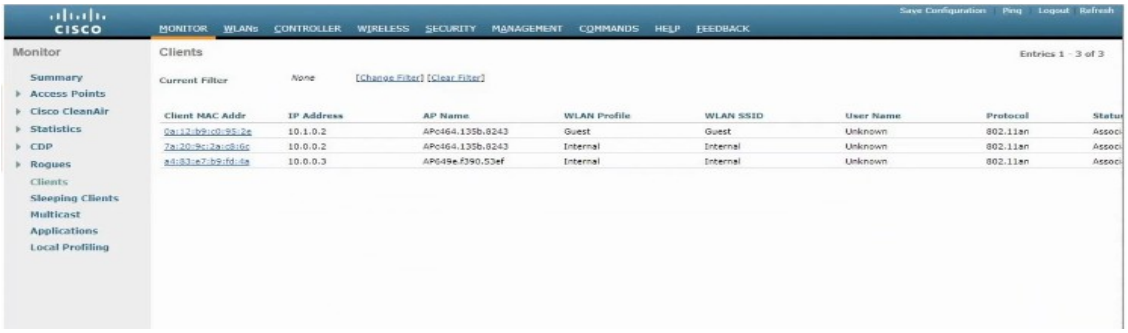
Il doit être changé différents paramètres. Le « status » doit être activé. Et le l’interface Group doit aussi être changé pour « Guest ». On change aussi le mode d’authentification pour PSK comme vu précédemment.

Les deux WLAN sont à présent bien présent comme on peut voir :

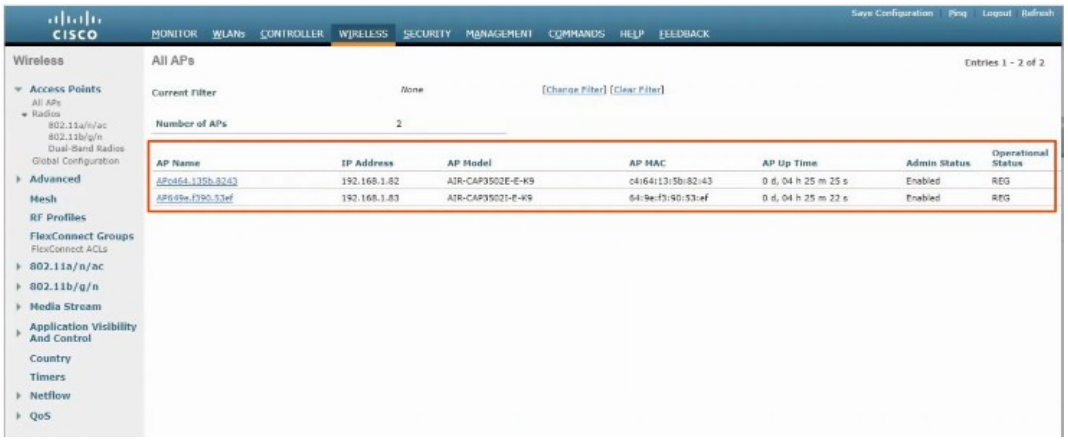
Lorsqu’un client se connecte aux point d’accès on peut voir que le nombre de client augmente.



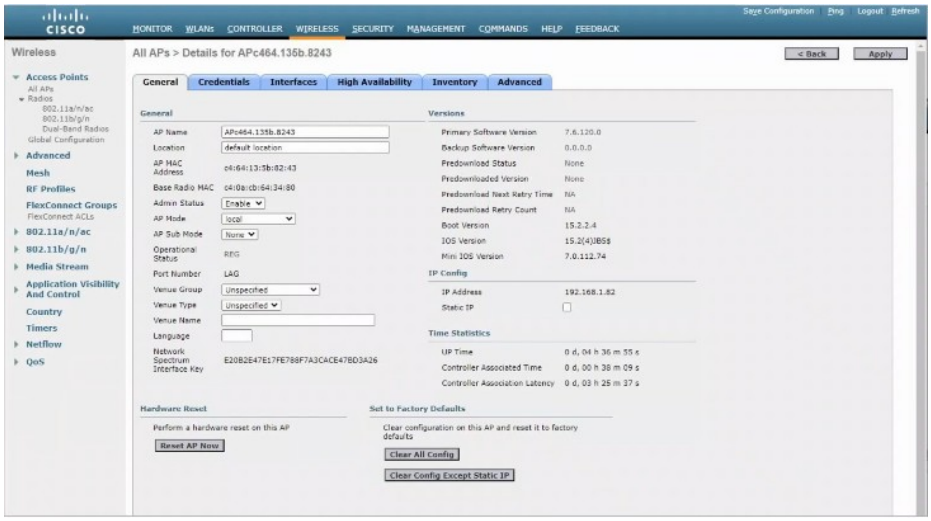
Pour afficher les clients ont clique sur l’onglet client on peut voir affiché leurs informations :



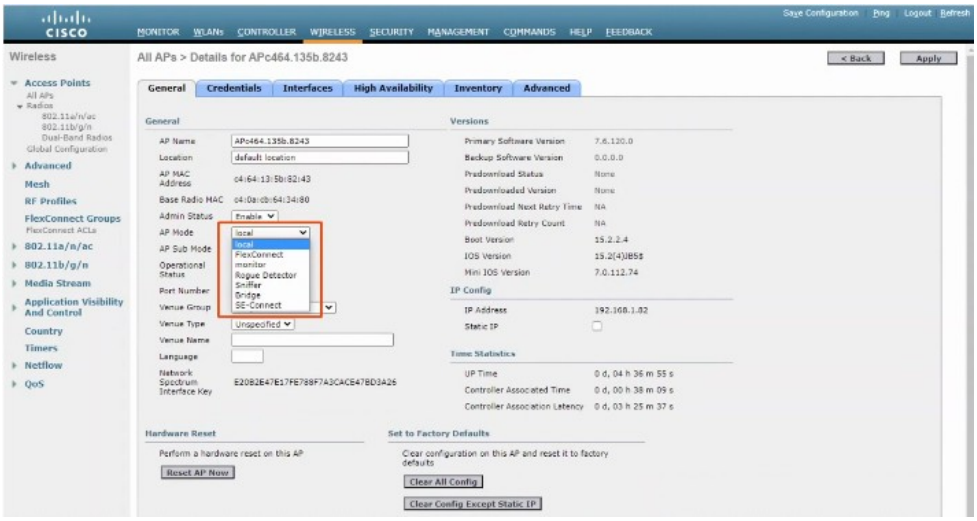
On peut aussi afficher les points d’accès avec leurs informations :



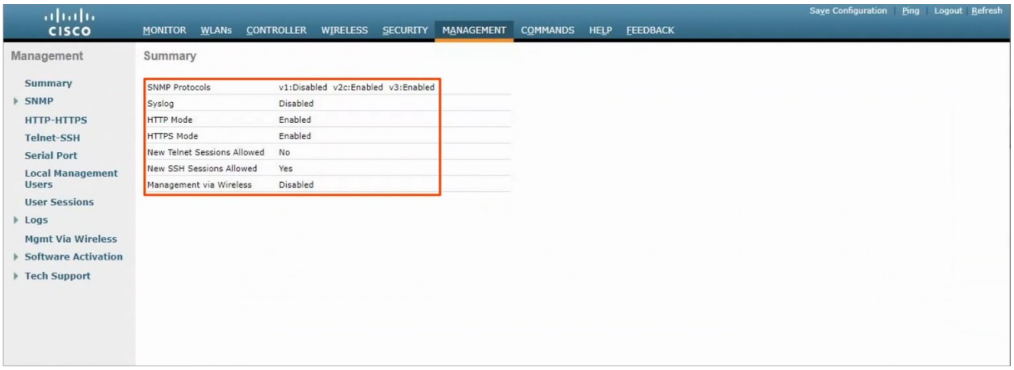
Pour modifier les paramètres de l’un des points d’accès on clique sur l’un d’eux :



Sur la partie AP Mode on peut changer le mode de configuration, flexconnect, RogueDetector, Sniffer, etc.. comme vu auparavant.

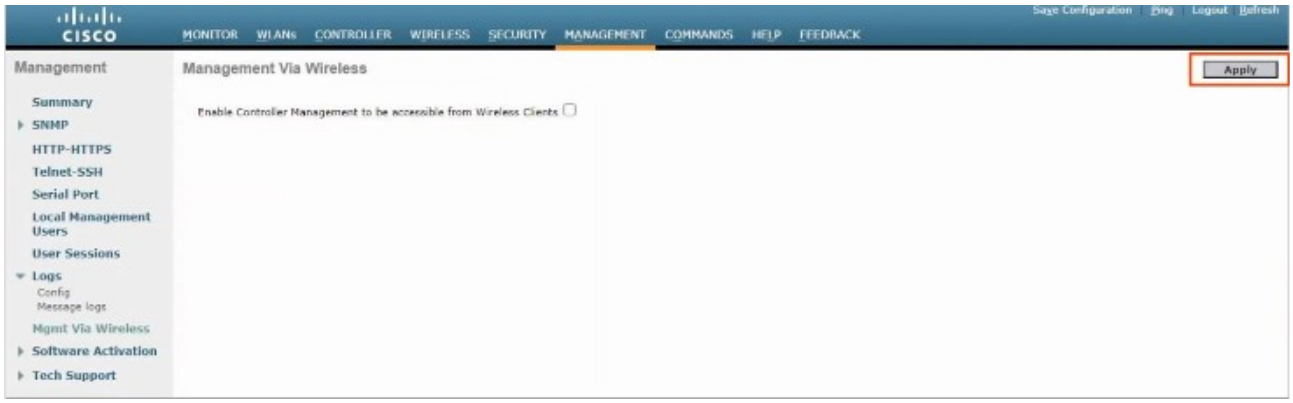


Sur l’onglet Management on peut voir différents paramètres, comme par exemple la version de SNMP activé, le mode HTTP activé, Syslog, SSH, etc.

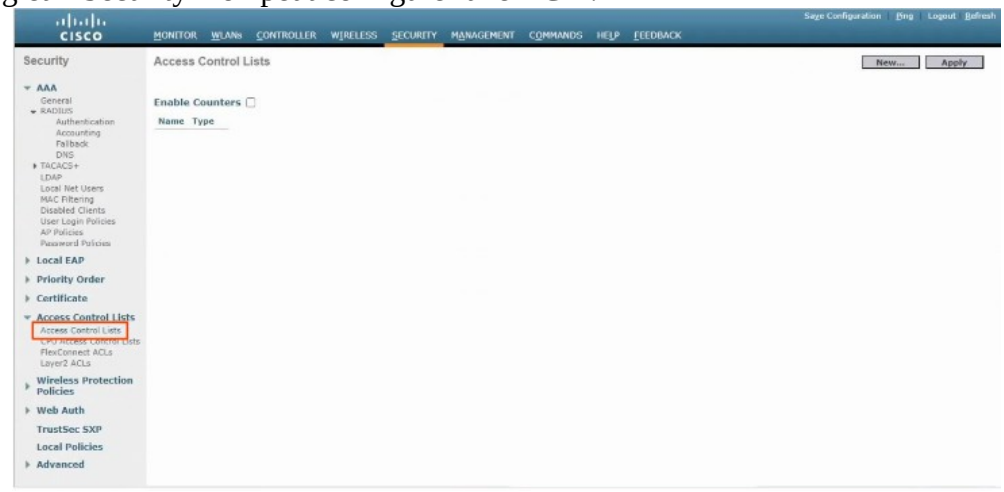


Telnet est ici désactivé comme on peut le voir :

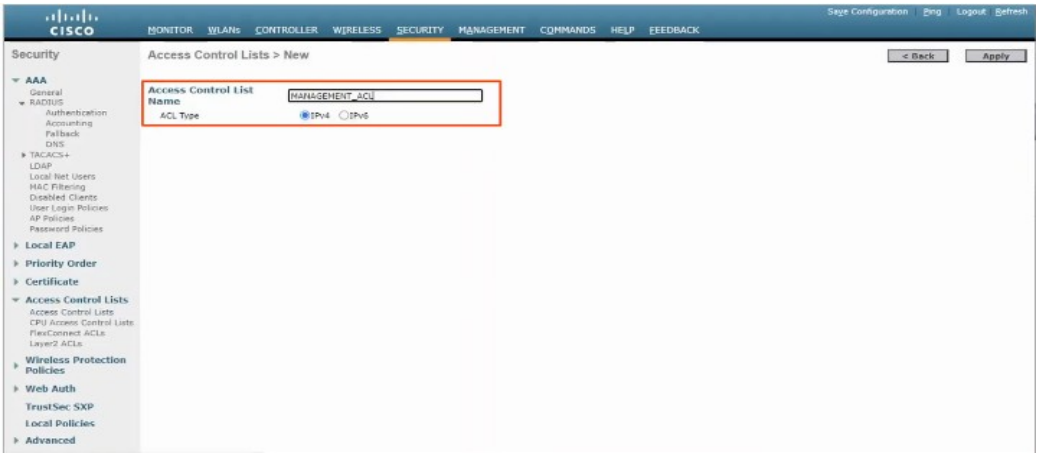
On peut activer un mode pour que les clients d’un point d’accès puisse avoir accès à la gestion du contrôleur.



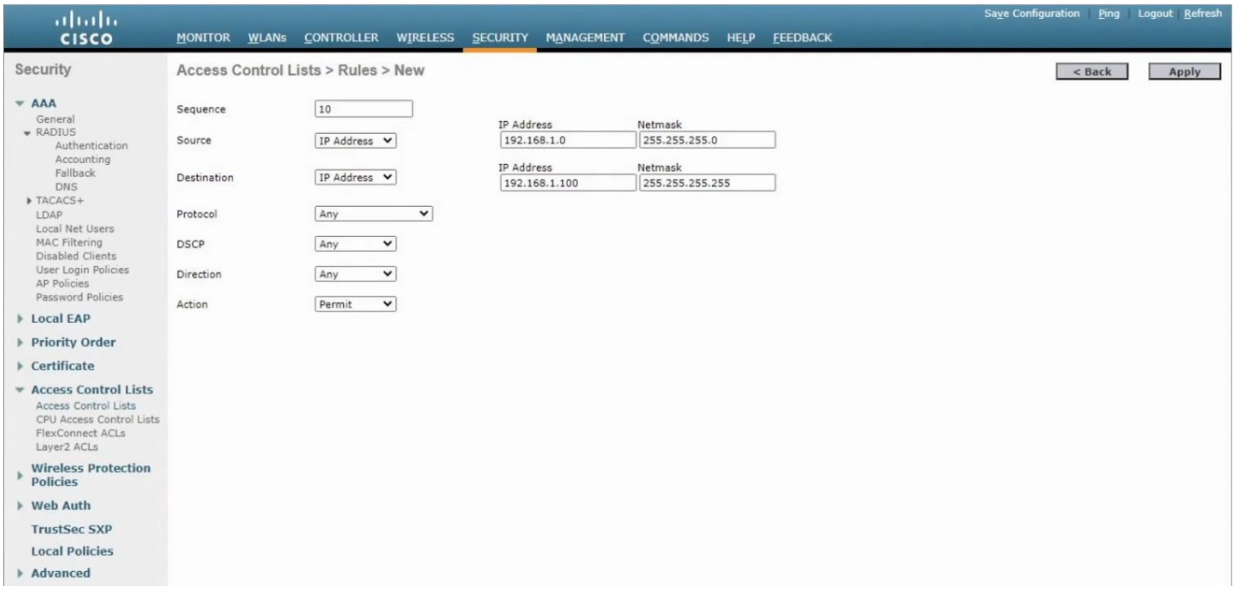
Dans l’onglet « Security » on peut configurer une ACL :



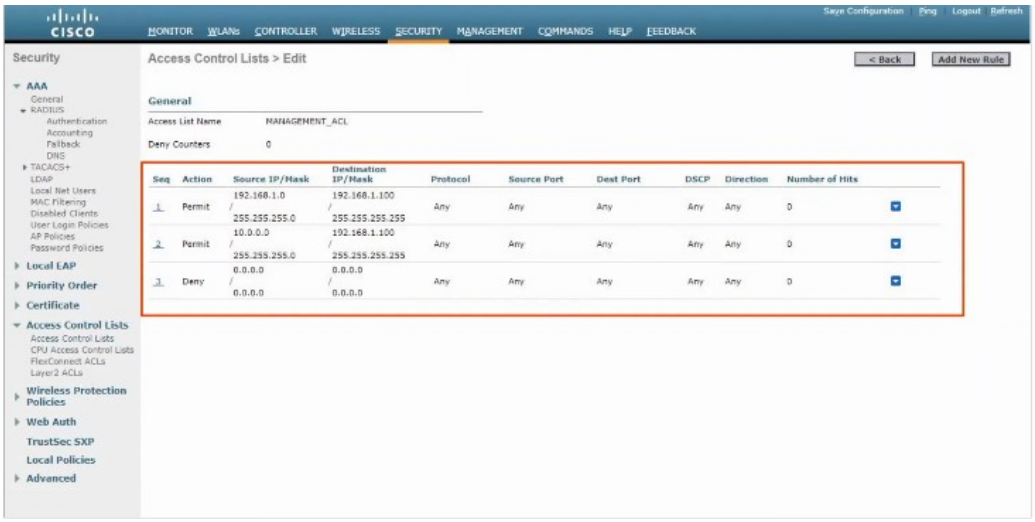
On donne un nom à l’ACL :



L’ACL est bien crée mais n’a pas de règle, on ajoute des règles en cliquant sur « add new rule »



On crée 3 règles comme suit :



Pour faire Appliquer ces ACL on clique sur : « CPU Access Control Lists »
Puis on sélectionne Enable CPU ACL et on clique sur Apply pour appliquer les modifications.