

Compte Rendu

Maison des Liges

Introduction :

Lors d'un événement d'une manifestation quadriennale appelée "Les VIèmes assises nationales de l'Escrime» qui est composée par des chapiteaux disposent chacun d'une borne Wifi reliée à un commutateur dans l'espace Informatique de l'organisation.

*Un réseau wifi "public" sera proposé gratuitement aux 2500 visiteurs attendus, aux 50 groupes d'escrime artistique ainsi qu'aux équipementiers.

*Un réseau wifi "orga" non publié sera dédié aux organisateurs. Ce réseau permettra notamment d'imprimer sur une photocopieuse numérique connectée et sur un traceur à banderoles, également connecté.



La mission du Projet :

La mission consiste à mettre en place

*Un prototype de solution informatique qui doit comporter une séparation des deux réseaux wifi vlan.

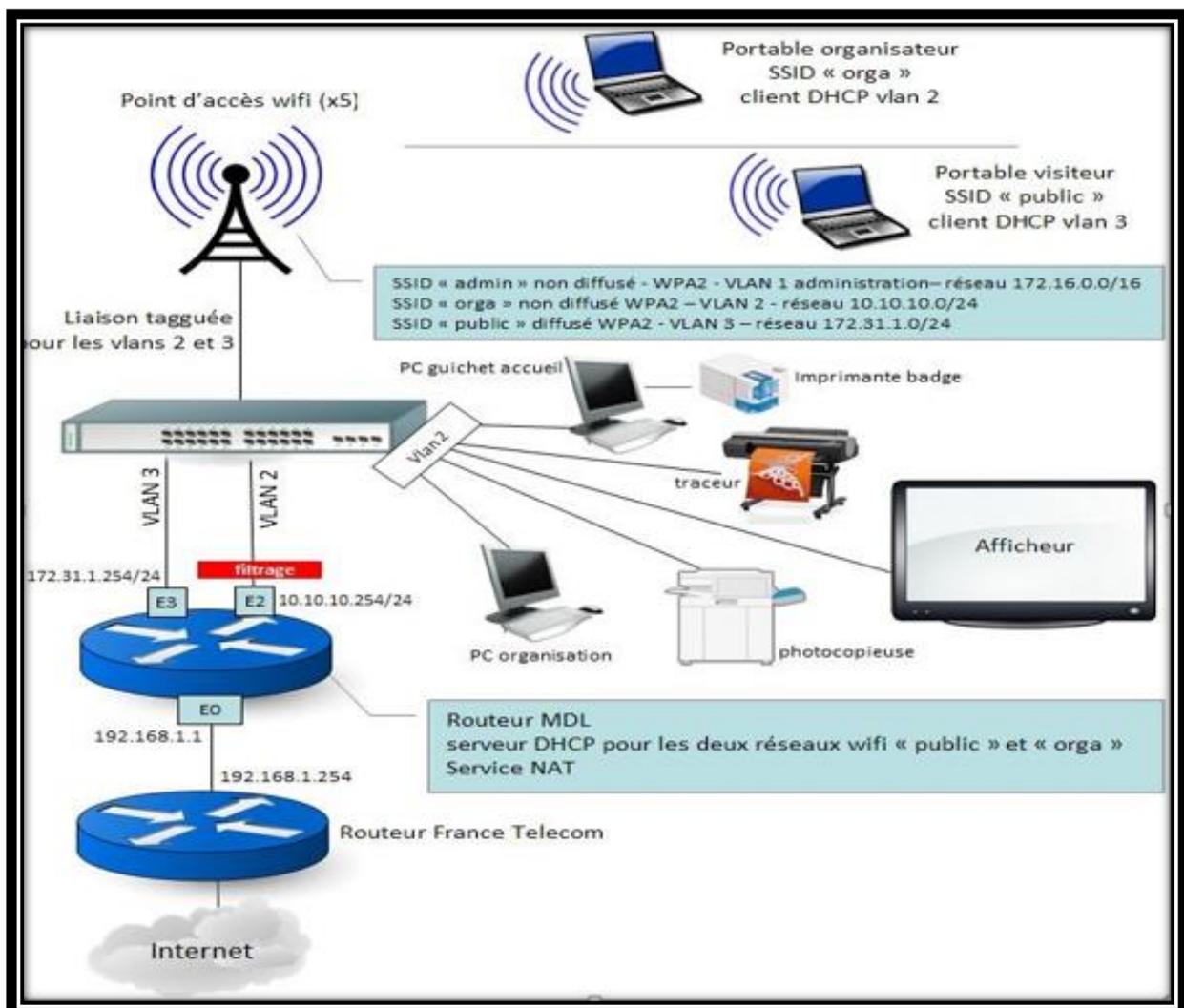
*SSID Public : La plage 172.31.1.0/16

*SSID Organisation : La plage 10.10.10.0/24

La solution proposée en /24 n'est pas adaptée pour les 2500 visiteurs attendus.

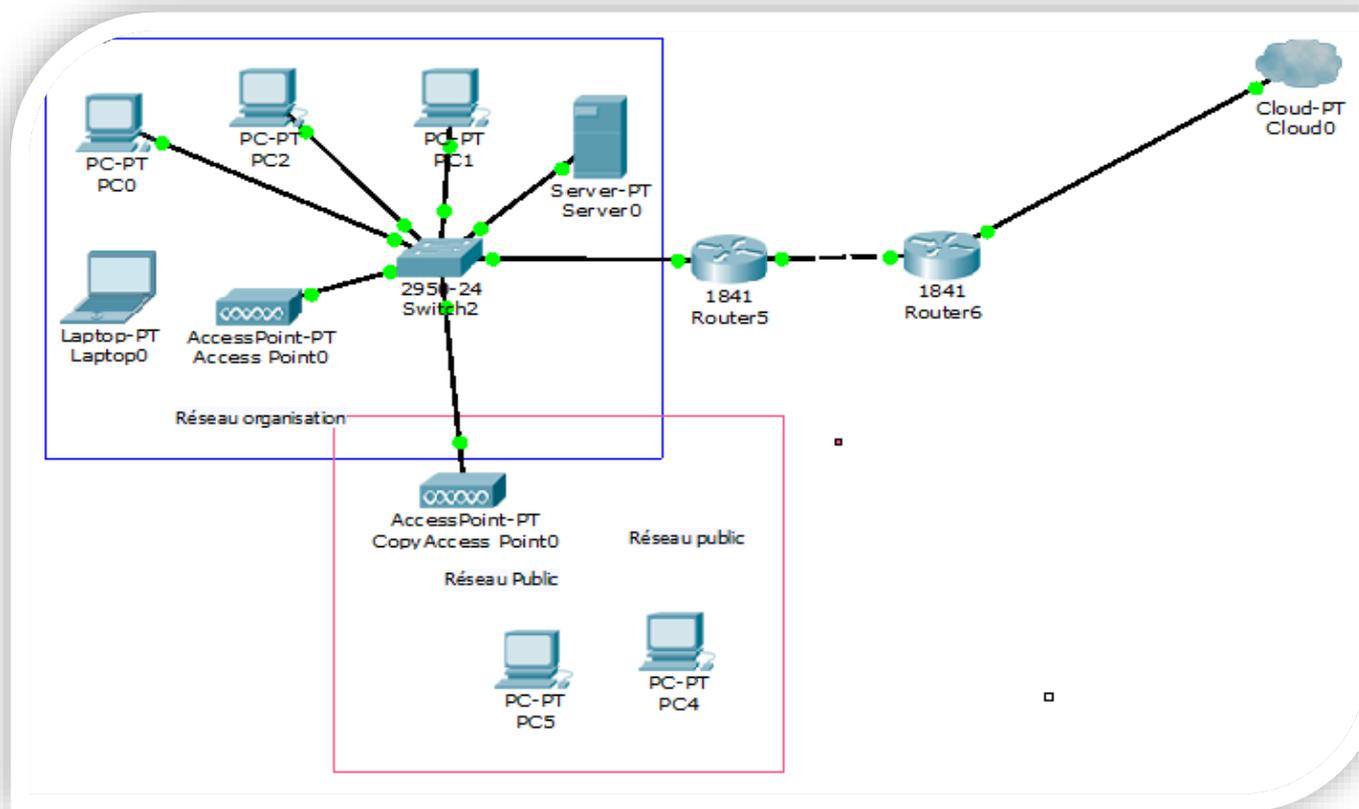
*L'établissement d'un périmètre de sécurité autour du réseau LAN et Wifi de l'organisation (filtrage).

Solution de Départ :



Mise en place de notre solution adaptée :

Nous avons étudié la solution de notre projet, qui se constitue d'un serveur DHCP se trouve dans la zone du réseau organisation est relié au Switch2 fait communiquer les différents réseaux et bornes wifi. Ceci permet aux utilisateurs présents sur le réseau d'obtenir une adresse IP automatiquement lors de la prochaine connexion à leurs sessions. Le réseau public peut distribuer jusqu'à 2500 adresses, car nous avons changé la notation CIDR /16.



Nous avons obtenu un prototype fonctionnel est organiser de façon compréhensible et de manière sécuriser.

Commande pour configurer la solution

Création des Vlans :

```
Switch>enable
Switch#conf t
Switch_1# VLAN database
Switch_1(vlan)# vlan 20 name Orga (on affecte le numéro et le nom au
vlan)
Switch_1(vlan)# vlan 30 name Public
Switch_1(vlan)# exit
Switch_1# show vlan
```

Supprimer des Vlans

```
Switch_1# VLAN database
Switch_1(vlan)# no vlan n° du VLAN à supprimer
Switch_1(vlan)# exit
```

Affecter les ports aux Vlans :

```
Switch_1# configure terminal
Switch_1 (config)# interface fa 0/1
Switch_1 (config-if)# switchport access vlan 20
Switch_1 (config-if)# no shutdown (active le port qui passe de l'état down
à up)
Switch_1 (config)# end
Switch_1# show vlan
```

Vérification des ports associés aux Vlans :

```
Switch_1# conf t
Switch_1(config)# interface fastethernet 0/ n° du port à configurer (ou int
fa 0/n)
Switch_1(config-if)# switchport access vlan 1 (ou sw a vl 1)
Switch_1(config-if)# no shutdown (ou no sh)
```

Switch_1(config)# end

Ajout d'une série de ports :

*Switch(config)#interface range fastethernet [fa 0/1 – fa 0/5]
Switch(config-if-range)#switchport access vlan vlan_number
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#no shutdown*

Attribution des adresses Ip :

*Router_md1(config)#interface FastEthernet0/0

Router_md1(config-if)#ip address 172.31.1.254 255.255.255.0

Router_md1(config-if)#exit

Router_md1(config)#interface FastEthernet0/1

Router_md1(config-if)#ip address 10.10.10.254 255.255.255.0

Router_md1(config-if)#exit

Router_md1(config)#exit

Router_md1(config)#interface FastEthernet1/0

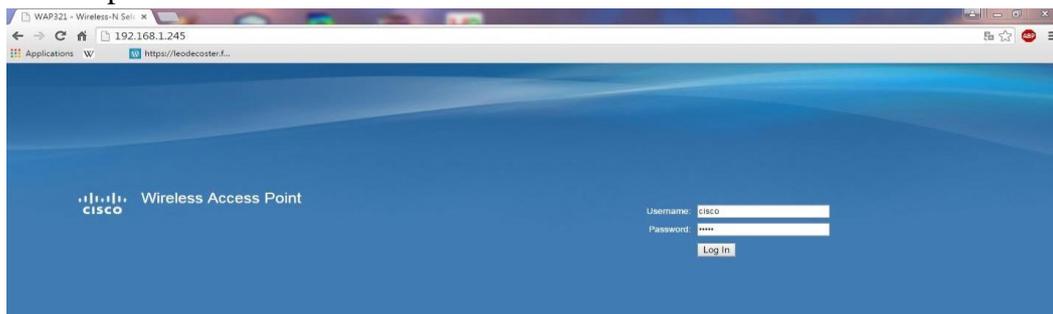
Router_md1(config-if)#ip address 192.168.1.1 255.255.255.0

Router_md1(config-if)#exit*

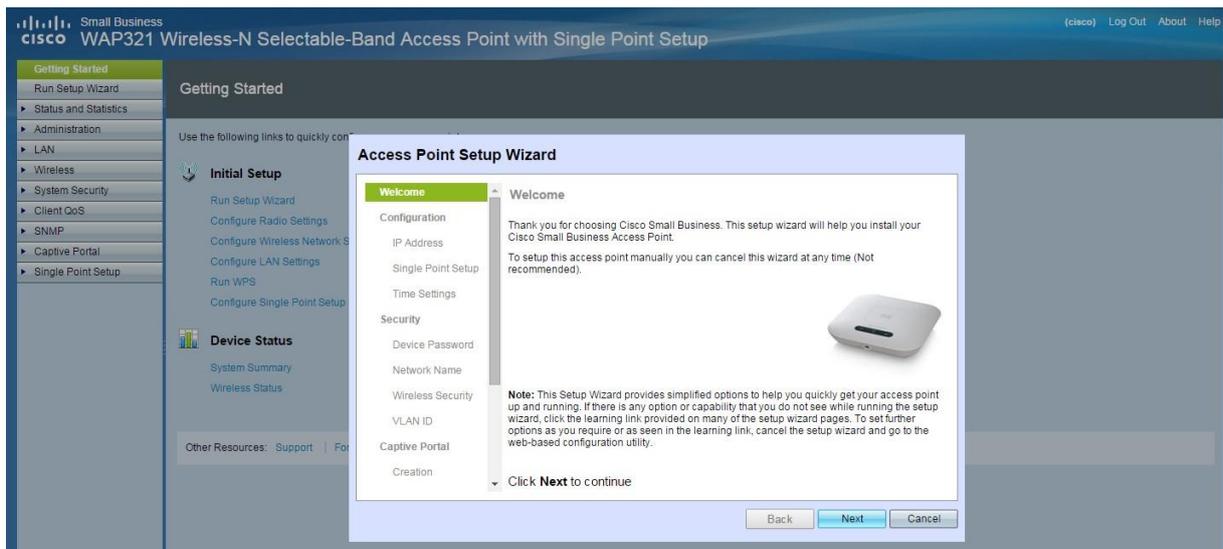
Configuration de la borne Wifi pour le technicien

Il faut tout d'abord se connecter :

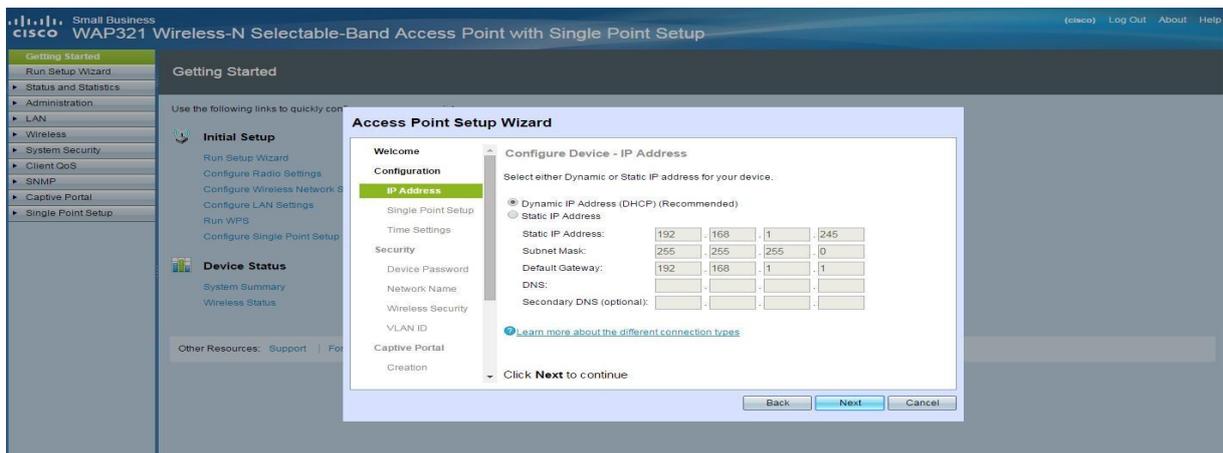
- Identifiant : cisco
- Mot de passe : root



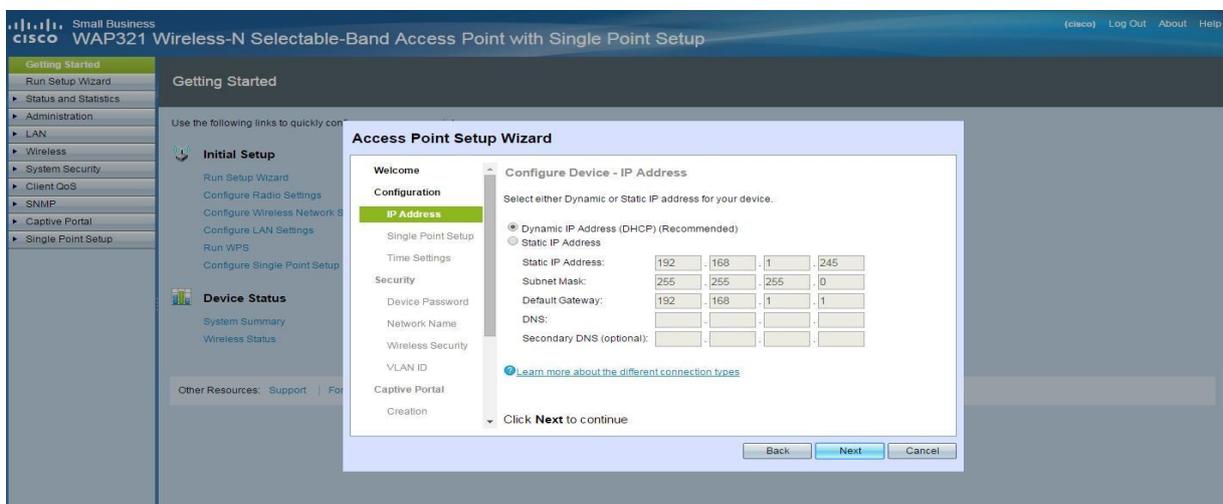
Next



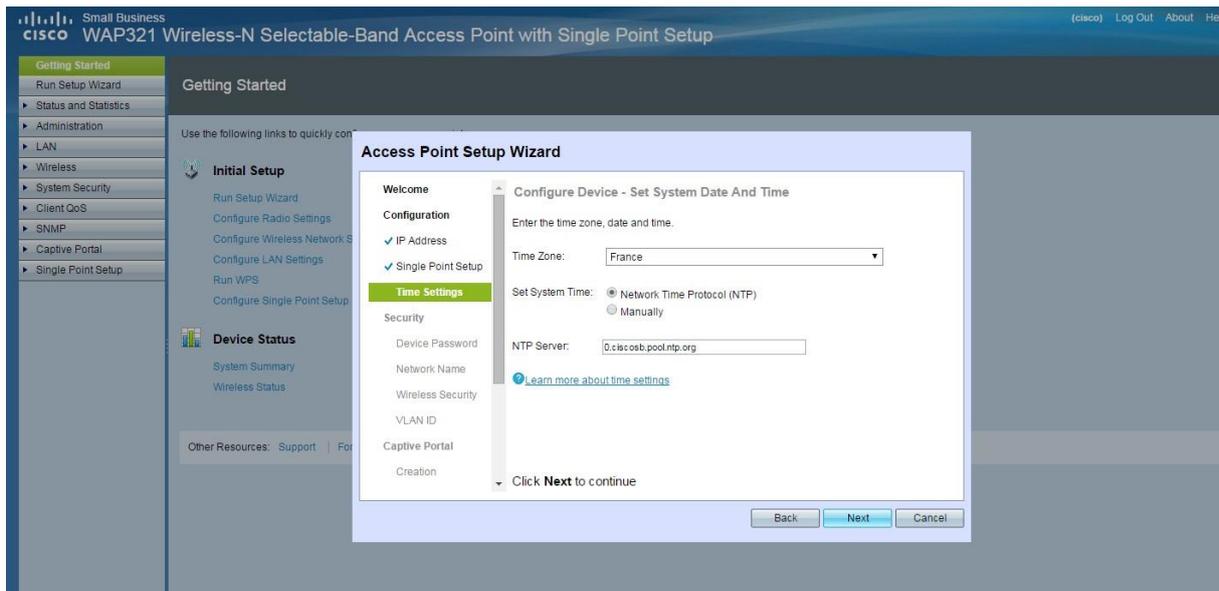
Configuration par défaut



Ne pas autoriser "Single point setup"



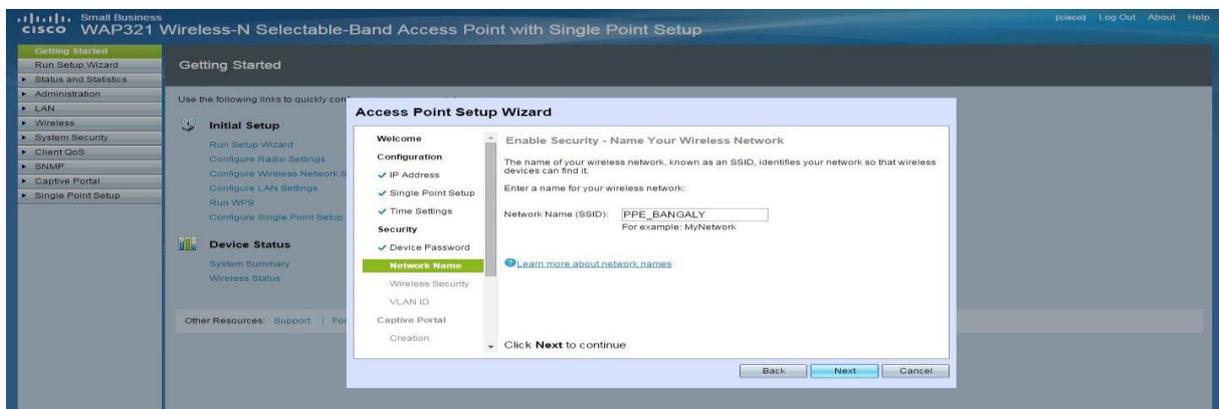
Appuyer sur suivant, remplissez les instructions demandées.

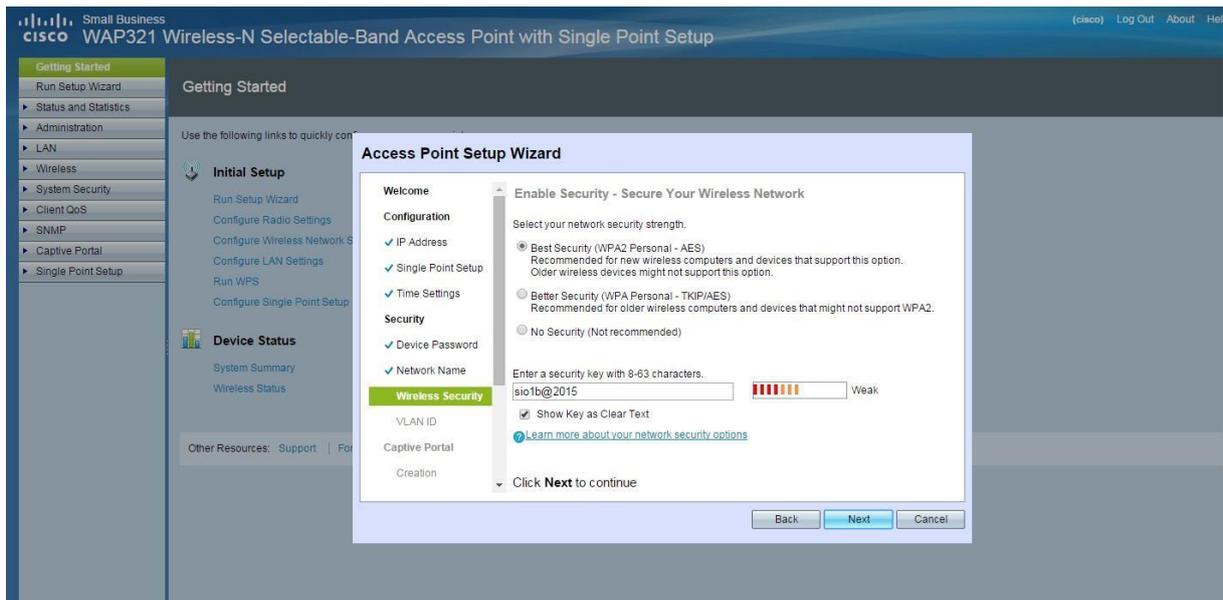


Etape suivante modification du mot de passe sio1b@2015

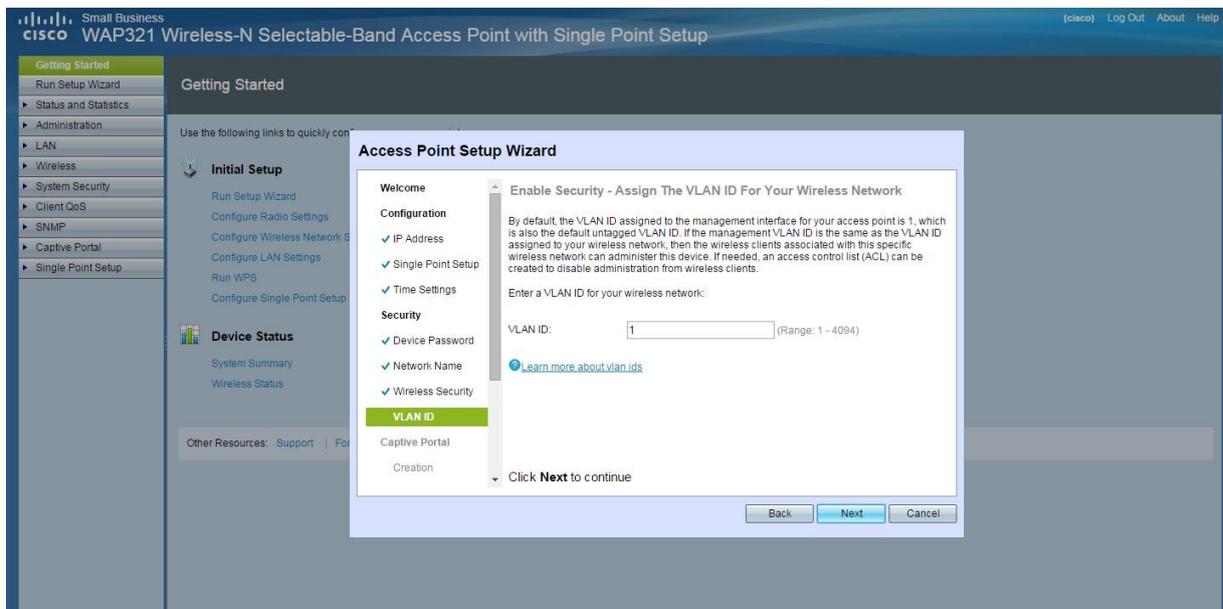


Mise en place SSID « Orga »

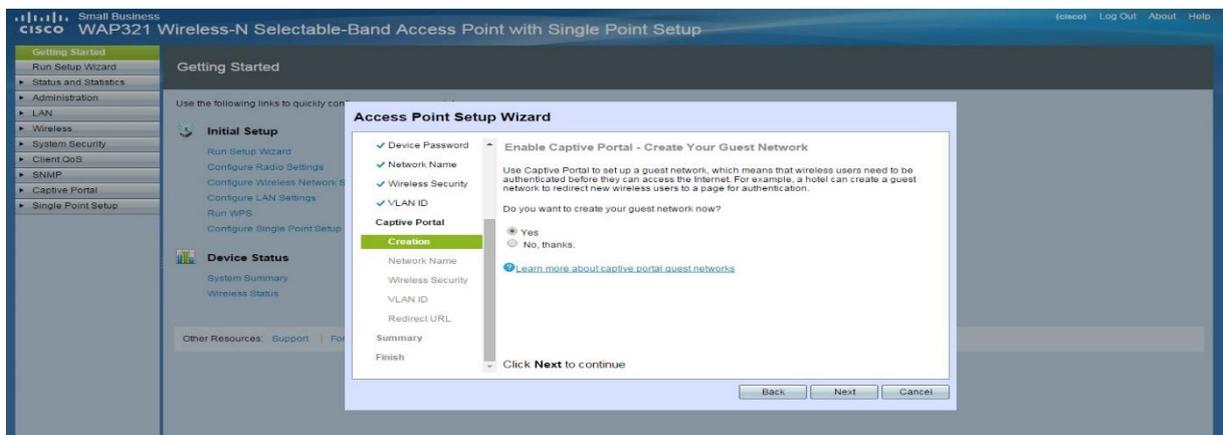




Définir les vlans : Vlan 2



Possibilité de configurer un nouveau point d'accès



Nommez ce point d'accès "invite"

The screenshot shows the Cisco WAP321 configuration interface. The main window is titled "Access Point Setup Wizard" and is currently on the "Network Name" step. The left sidebar shows a navigation menu with "Getting Started" selected. The main content area displays the following information:

- Device Password**:
- Network Name**: (Current step)
- Wireless Security**:
- VLAN ID**:
- Captive Portal**:
- Creation**:

The "Network Name" step is titled "Enable Captive Portal - Name Your Guest Network". It instructs the user to "Enter a name for your guest network:" and shows a text input field containing "invite". Below the field, it says "For example: MyGuestNetwork". There is a link "Learn more about network names" and a "Click Next to continue" instruction. Buttons for "Back", "Next", and "Cancel" are at the bottom.

Saisir le même mot de passe

The screenshot shows the Cisco WAP321 configuration interface, now on the "Wireless Security" step of the "Access Point Setup Wizard". The left sidebar remains the same. The main content area displays the following information:

- Device Password**:
- Network Name**:
- Wireless Security**: (Current step)
- VLAN ID**:
- Captive Portal**:
- Creation**:
- Network Name**:

The "Wireless Security" step is titled "Enable Captive Portal - Secure Your Guest Network". It asks the user to "Select your guest network security strength." and provides three radio button options:

- Best Security (WPA2 Personal - AES)
Recommended for new wireless computers and devices that support this option. Older wireless devices might not support this option.
- Better Security (WPA Personal - TKIP/AES)
Recommended for older wireless computers and devices that might not support WPA2.
- No Security (Not recommended)

Below these options, there is a text input field for a security key containing "sio1b@2015". To the right of the field is a strength indicator showing four red bars and the word "Weak". There is a checkbox for "Show Key as Clear Text" which is checked, and a link "Learn more about your network security options". A "Click Next to continue" instruction and "Back", "Next", and "Cancel" buttons are at the bottom.

Vérification de la totalité des saisies

Access Point Setup Wizard

- ✓ Device Password
- ✓ Network Name
- ✓ Wireless Security
- ✓ VLAN ID
- Captive Portal**
 - ✓ Creation
 - ✓ Network Name
 - ✓ Wireless Security
 - ✓ VLAN ID
 - ✓ Redirect URL
- Summary**
- Finish

Summary - Confirm Your Settings

Please review the following settings and ensure the data is correct.

Network Name (SSID):	Organisation
Network Security Type:	WPA2 Personal - AES
Security Key:	sio1b@2015
VLAN ID:	1

Captive Portal (Guest Network) Summary

Network Name (SSID):	Invité
Network Security Type:	WPA2 Personal - AES
Security Key:	sio1b@2015
Verification:	Guest
Redirect URL:	google.com
VLAN ID:	2

Note: The AP Radio will be enabled after clicking Submit.

Click **Submit** to enable settings on your Cisco Small Business Access Point

Back Submit Cancel

Conclusion

Pour conclure, nous avons modifié le masque réseau 255.255.0.0 du vlan public. De ce fait, le CIDR est passé de /24 à /16. Ainsi, le vlan installé peut héberger 2500 adresses, à la place des 254 adresses. De plus, le serveur DHCP est positionné sur le switch, ce qui lui permet d'avoir un accès direct aux bornes wifi. D'ailleurs, le serveur permet d'attribuer les adresses IP de façon dynamique aux différents postes. Enfin, nous avons obtenu un réseau sécurisé, partagé et de façons organisées.