Implémentation d'une Infrastructure Réseau avec VLANs, OSPF et Services Serveur

Ce projet vise à concevoir et mettre en œuvre une infrastructure réseau robuste et sécurisée pour une organisation fictive, en utilisant des VLANs pour la segmentation, OSPF pour le routage dynamique et un serveur pour la distribution des adresses IP en dynamique.

NOTION VLANS

Les VLAN (Virtual Local Area Network) ou réseaux locaux virtuels, sont des réseaux informatiques logiques qui permettent de segmenter un réseau physique en plusieurs réseaux logiques indépendants. Cette segmentation présente plusieurs avantages :

1. Gestion du réseau améliorée : En regroupant des dispositifs similaires dans des VLAN distincts, la gestion du réseau devient plus efficace.
2. Optimisation de la bande passante : Les VLAN permettent de dédier des ressources réseau spécifiques à certains groupes d'utilisateurs, améliorant ainsi les performances globales.
3. Séparation des flux : En isolant le trafic entre les différents VLAN, il est possible d'éviter les interférences et les collisions.
4. Réduction du domaine de broadcast : En limitant la diffusion des paquets de diffusion (broadcast) à un seul VLAN, la charge sur le réseau est réduite.
5. Renforcement de la sécurité : Les VLAN permettent de créer des zones sécurisées, où le trafic est isolé des autres VLAN. Pour communiquer entre VLAN, les données doivent passer par un routeur, renforçant ainsi la sécurité du réseau.

Dans notre projet, nous avons utilisé différentes commandes pour configurer les ports des commutateurs :

1. **switchport mode access** : Définit un port comme un port d'accès, connecté à un seul VLAN.
2. **switchport access vlan ID** : Associe un port à un VLAN spécifique, comme le VLAN 10.
3. **switchport mode trunk** : Définit un port comme un port trunk, capable de transporter le trafic de plusieurs VLAN à travers un seul lien.

Ces commandes nous ont permis de configurer efficacement les ports des commutateurs pour répondre aux besoins spécifiques de notre projet, en garantissant une connectivité appropriée entre les VLAN et en permettant le passage du trafic entre eux au besoin.

NOTION OSPF

OSPF (Open Shortest Path First) est un protocole de routage à vecteur de liens utilisé dans les réseaux IP pour déterminer les meilleurs chemins entre les routeurs. Il utilise des informations sur la topologie du réseau pour calculer les chemins les plus courts vers toutes les destinations.
Dans ce projet, nous avons configuré OSPF en utilisant les commandes router ospf ID, network [adresse réseau] [wildcard mask] area ID pour attribuer un processus OSPF, annoncer les réseaux locaux et les placer dans la zone ID.

1. **Processus OSPF (router ospf ID)** : Chaque routeur OSPF doit être configuré avec un identifiant de processus OSPF unique. Cela permet de distinguer les processus OSPF sur différents routeurs et de les configurer individuellement.
2. **Annonce des réseaux (network)** : La commande "network" est utilisée pour annoncer les réseaux locaux dans le processus OSPF. Les réseaux spécifiés seront inclus dans le calcul des chemins de routage OSPF.
3. **Zones OSPF (area)** : Chaque réseau OSPF est divisé en zones logiques pour une gestion et une convergence efficaces. Dans notre configuration, tous les réseaux ont été placés dans la zone ID. Les routeurs OSPF échangent des informations de routage uniquement avec les routeurs de la même zone.

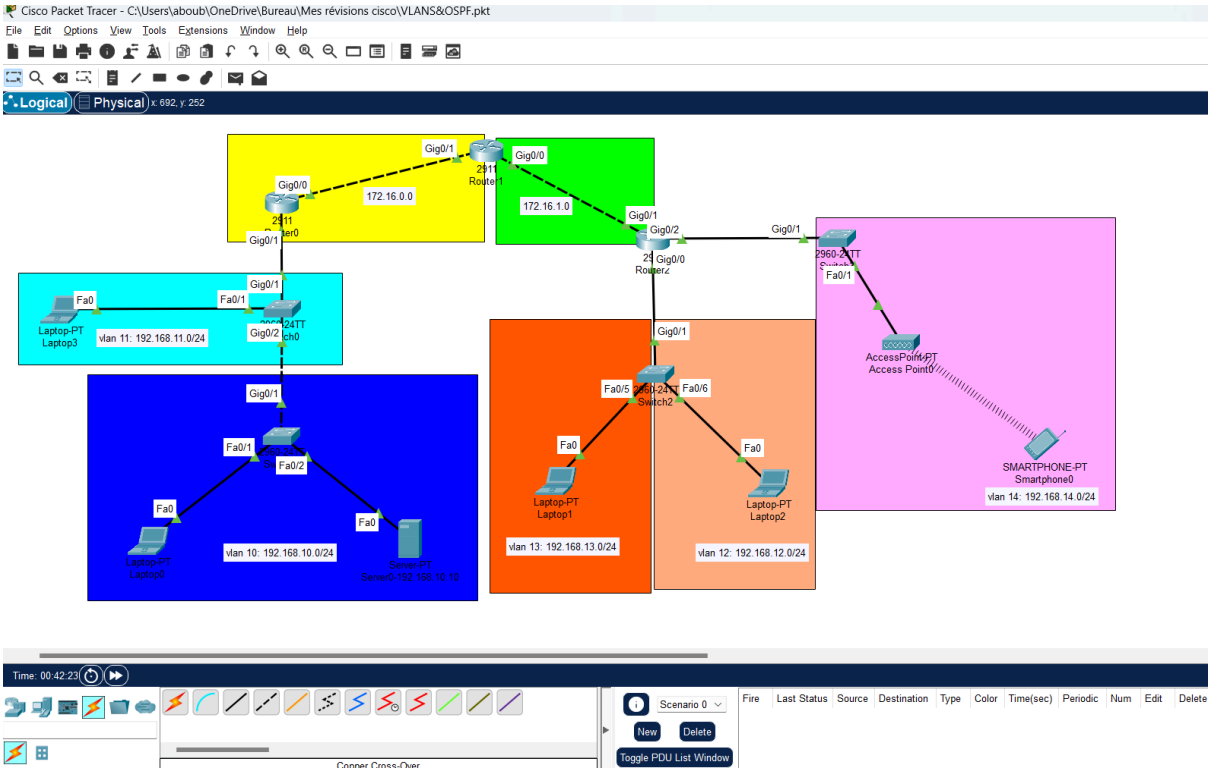
En résumé, OSPF est configuré sur chaque routeur avec un identifiant de processus OSPF unique. Les réseaux locaux sont annoncés dans le processus OSPF, et chaque réseau est placé dans une zone OSPF spécifique pour une gestion optimale du routage.

Dans ce projet, nous allons configurer une infrastructure réseau comprenant un total de 7 réseaux distincts. Parmi eux, 5 réseaux sont segmentés par des VLANs, et 2 réseaux sont utilisés pour la communication entre les routeurs. Le routage dynamique sera assuré par le protocole OSPF (Open Shortest Path First), et un serveur DHCP sera configuré pour la distribution d'adresses IP dynamiques. L'objectif est de permettre une communication efficace et sécurisée entre les différents segments du réseau tout en assurant une gestion automatisée des adresses IP.

- **Nombre de réseaux :** 7
    1. **Réseaux segmentés par des VLANs :** 5
        - VLAN 10
        - VLAN 11

        - VLAN 12
        - VLAN 13
        - VLAN 14
    2. **Réseaux de communication entre routeurs :** 2
        - Réseau de liaison entre le routeur 0 et le routeur 1
        - Réseau de liaison entre le routeur 1 et le routeur 2
- **But :**
    1. Segmenter le réseau en utilisant des VLANs pour améliorer la sécurité et la gestion.
    2. Utiliser OSPF pour le routage dynamique entre les VLANs et les réseaux de communication entre les routeurs.
    3. Configurer un serveur DHCP pour la distribution dynamique des adresses IP aux différents segments du réseau.

En guise de conclusion, ce projet vise à démontrer la mise en place d'une infrastructure réseau évolutive, sécurisée et bien gérée, essentielle pour toute organisation cherchant à optimiser ses ressources réseau et à assurer une communication fluide et sécurisée entre ses différents segments.



Code OSPF&VLAN

Nous allons configurer les switchs et les routeurs en utilisant les commandes suivantes.

Ces commandes configurent plusieurs VLANs et affectent des ports spécifiques sur un commutateur (switch) Cisco :

!sw0 : Commande fictive pour indiquer les instructions destinées à être appliquées sur le switch réseau nommé "sw0"

Enable : Accède au mode de configuration privilégié.

Configure terminal : Accède au mode de configuration globale.

vlan 10-14 : Créé cinq VLANs avec les identifiants 10 à 14.

interface range f0/1-10 : Accède aux interfaces de ports FastEthernet de 1 à 10.

switchport mode access : Configure les ports comme des ports d'accès, utilisés pour connecter des dispositifs finaux.

switchport access vlan 11 : Associe ces ports au VLAN 11.

interface range g0/1-2 : Accède aux interfaces de ports Gigabit Ethernet de 1 à 2.

switchport mode trunk : Configure les ports comme des trunks, permettant de transporter le trafic de plusieurs VLANs.

end : Retourne au mode d'exécution privilégié.

write memory : Enregistre la configuration dans la mémoire persistante.

En résumé, ces commandes créent cinq VLANs, assignent les ports FastEthernet 1 à 10 au VLAN 11 en tant que ports d'accès, et configurent les ports Gigabit Ethernet 1 et 2 en tant que trunks.

Nous répéterons les mêmes étapes pour les autres VLANs en affectant les ports appropriés à chaque VLAN sans reconfigurer le mode de port déjà défini, en tenant compte du fait que le switch précédent ne gère pas tous les VLANs, mais seulement ceux mentionnés dans ces commandes.

!sw1

```
enable
configure terminal
vlan 10
vlan 11
vlan 12
vlan 13
vlan 14
interface range f0/1-10
switchport mode access
switchport access vlan 10
interface g0/1
switchport mode trunk
end
write memory

!sw2
enable
configure terminal
vlan 10
vlan 11
vlan 12
vlan 13
vlan 14
interface range f0/1-5
switchport mode access
switchport access vlan 13
interface range f0/6-10
switchport mode access
switchport access vlan 12
interface g0/1
switchport mode trunk
end
write memory

!sw3
enable
configure terminal
vlan 10
vlan 11
vlan 12
vlan 13
vlan 14
interface range f0/1-10
switchport mode access
switchport access vlan 14
interface g0/1
switchport mode trunk
end
```

write memory

Avec les commandes suivantes, nous allons configurer les routeurs.

!R0 : Commande fictive pour indiquer les instructions destinées à être appliquées sur le routeur nommé "R0".

Enable : Accède au mode de configuration privilégié.

Configure terminal : Accède au mode de configuration globale.

interface g0/0 : Accède à l'interface GigabitEthernet 0/0.

no shutdown : Active l'interface GigabitEthernet 0/0.

ip address 172.16.0.254 255.255.255.0 : Configure l'adresse IP 172.16.0.254 avec un masque de sous-réseau de 255.255.255.0 sur l'interface GigabitEthernet 0/0.

interface g0/1 : Accède à l'interface GigabitEthernet 0/1.

no shutdown : Active l'interface GigabitEthernet 0/1.

interface g0/1.10 : Accède à la sous-interface GigabitEthernet 0/1.10.

encapsulation dot1q 10 : Configure l'encapsulation IEEE 802.1Q pour le VLAN 10 sur la sous-interface GigabitEthernet 0/1.10.

ip address 192.168.10.254 255.255.255.0 : Configure l'adresse IP 192.168.10.254 avec un masque de sous-réseau de 255.255.255.0 sur la sous-interface GigabitEthernet 0/1.10.

interface g0/1.11 : Accède à la sous-interface GigabitEthernet 0/1.11.

encapsulation dot1q 11 : Configure l'encapsulation IEEE 802.1Q pour le VLAN 11 sur la sous-interface GigabitEthernet 0/1.11.

ip address 192.168.11.254 255.255.255.0 : Configure l'adresse IP 192.168.11.254 avec un masque de sous-réseau de 255.255.255.0 sur la sous-interface GigabitEthernet 0/1.11.

ip helper-addr 192.168.10.10 : Configure l'adresse IP du serveur DHCP pour le VLAN 10.

router ospf 1 : Démarre le processus OSPF avec l'ID de processus 1.

network 192.168.0.0 0.0.255.255 area 0 : Inclut le réseau 192.168.0.0/16 dans le processus OSPF et le place dans la zone 0.

network 172.16.0.0 0.0.255.255 area 0 : Inclut le réseau 172.16.0.0/16 dans le processus OSPF et le place dans la zone 0.

end : Retourne au mode d'exécution privilégié.

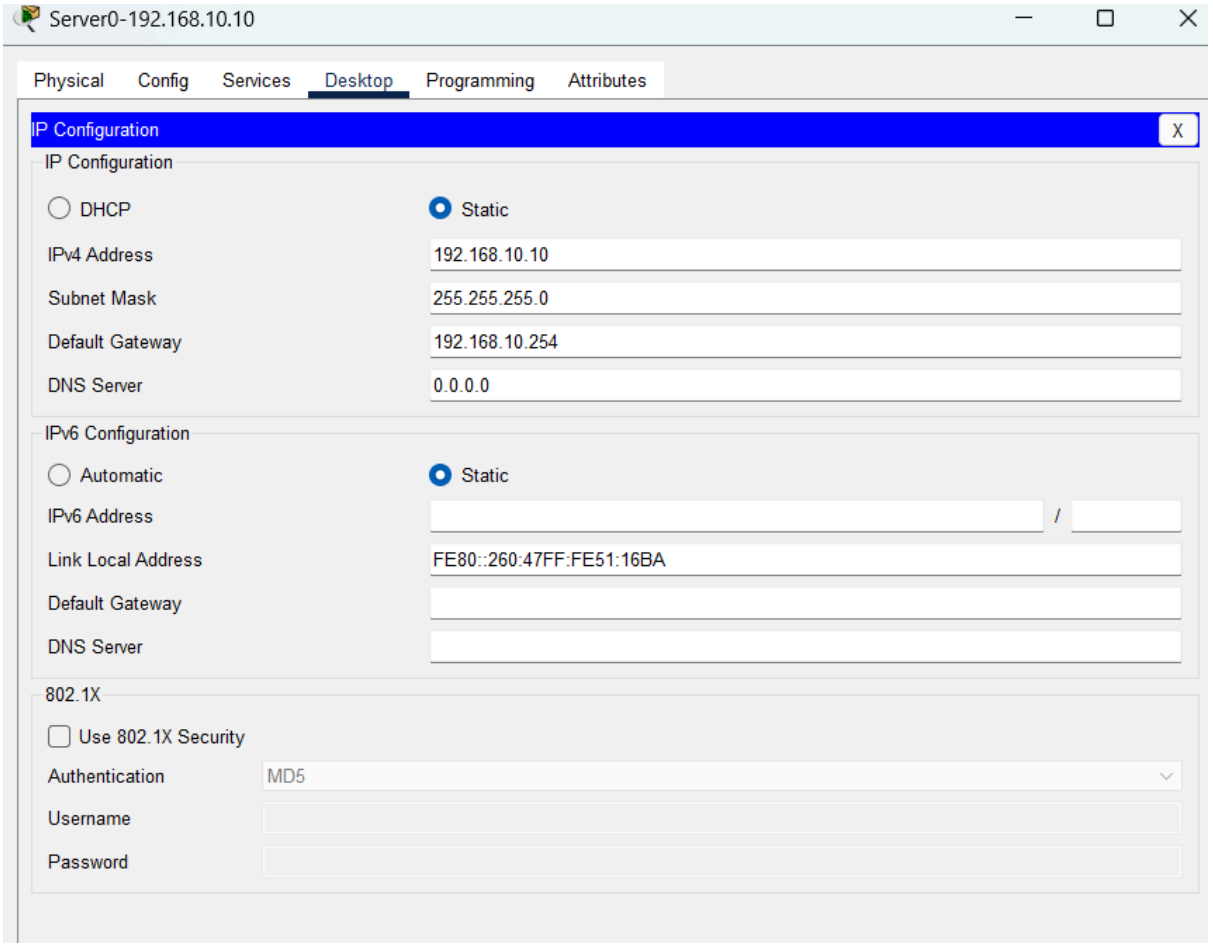
write memory : Enregistre la configuration dans la mémoire persistante.

La configuration attribuée au routeur 0 est fournie avec la prise en charge des VLANs. Par conséquent, le routeur 2 sera configuré de la même manière, mais avec les VLANs spécifiques qu'il gère. En revanche, le routeur 1, qui ne gère pas de VLAN, sera configuré de manière conventionnelle (classique).

```
!R1
enable
configure terminal
interface g0/1
no shutdown
ip address 172.16.0.253 255.255.255.0
interface g0/0
no shutdown
ip address 172.16.1.254 255.255.255.0
router ospf 2
network 192.168.0.0 0.0.255.255 area 0
network 172.16.0.0 0.0.255.255 area 0
end
write memory
```

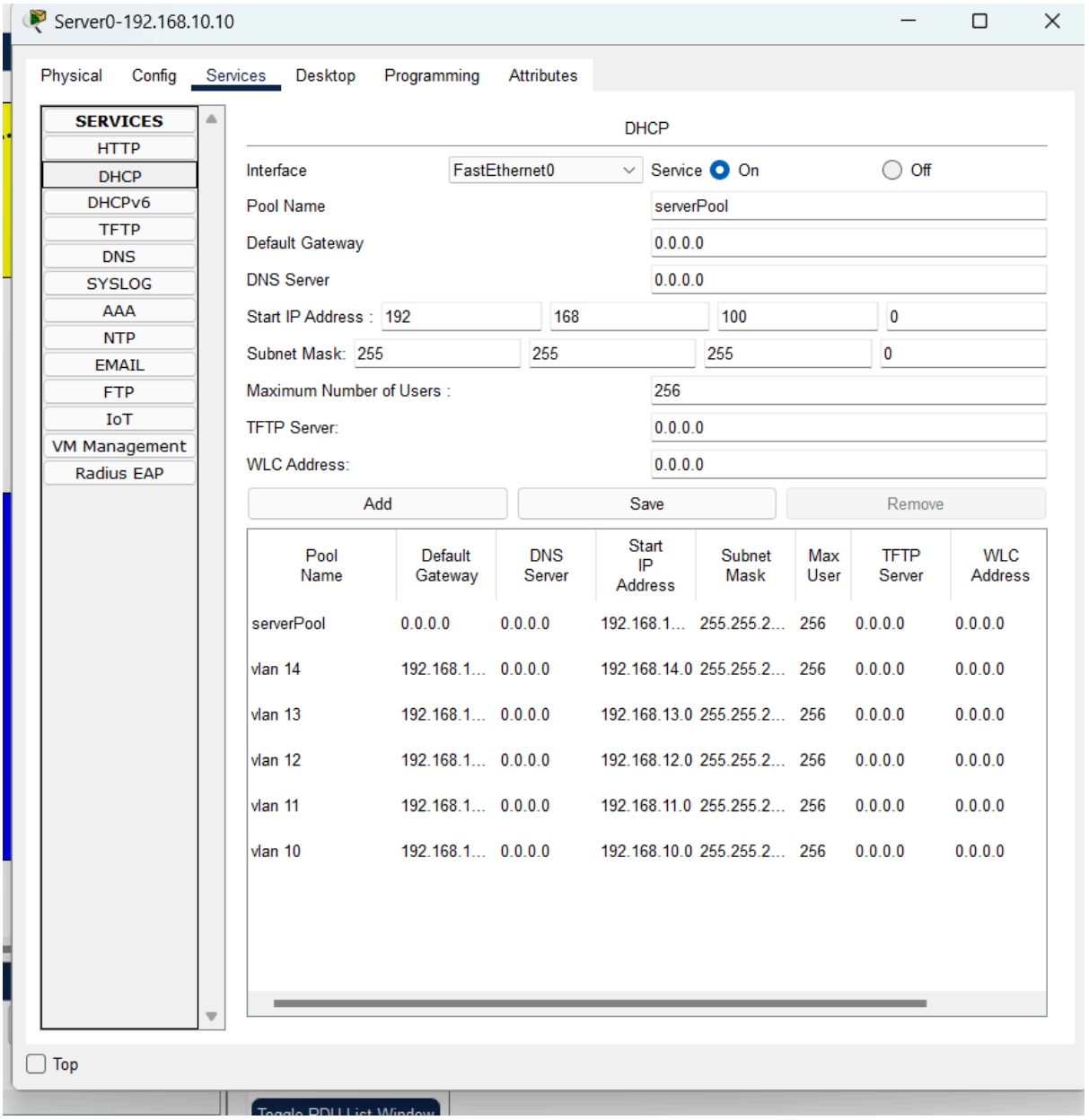
```
!R2
enable
configure terminal
interface g0/1
no shutdown
ip address 172.16.1.253 255.255.255.0
interface g0/0
no shutdown
interface g0/0.12
encapsulation dot1q 12
ip address 192.168.12.254 255.255.255.0
ip helper-addr 192.168.10.10
interface g0/0.13
encapsulation dot1q 13
ip address 192.168.13.254 255.255.255.0
ip helper-addr 192.168.10.10
interface g0/2
no shutdown
interface g0/2.14
encapsulation dot1q 14
ip address 192.168.14.254 255.255.255.0
ip helper-addr 192.168.10.10
router ospf 3
network 192.168.0.0 0.0.255.255 area 0
network 172.16.0.0 0.0.255.255 area 0
end
write memory
```

Après avoir configuré les routeurs ainsi que les switchs, nous allons procéder à la configuration du serveur. Tout d'abord, nous allons commencer par la Configuration de l'Interface Réseau du Serveur. Pour cela, accédez à l'interface desktop du serveur, puis Configurez l'adresse IP statique du serveur (en dehors des plages d'adresses DHCP pour éviter les conflits d'adresse), le masque de sous-réseau, et la passerelle par défaut appropriés pour votre réseau.



Ensuite nous allons passer à **l'Activation du Service DHCP**. Ouvrez donc l'onglet **Services** du serveur, puis activez le service DHCP pour gérer automatiquement l'attribution des adresses IP dans les VLANs.

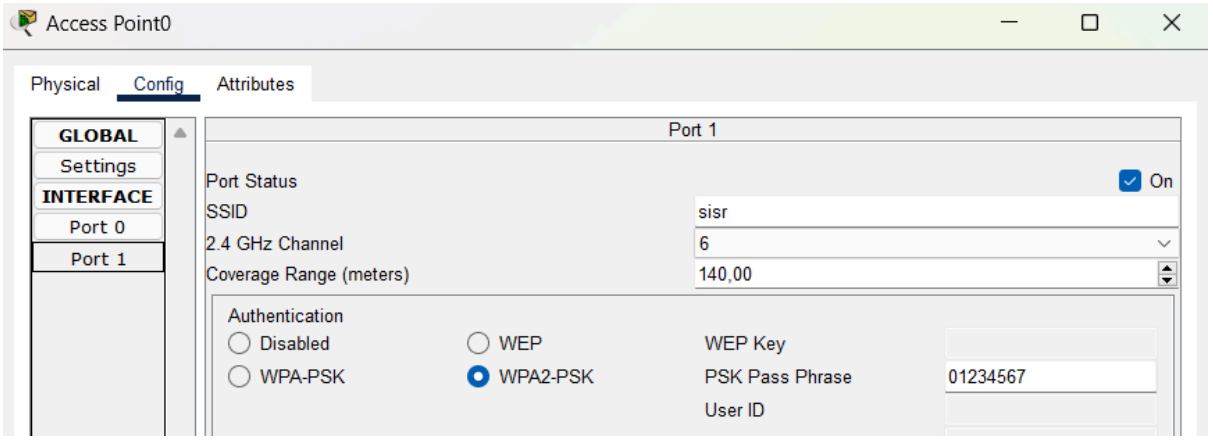
De surcroît, La configuration des plages d'adresses DHCP est à l'ordre du jour. Nous allons configurer les plages d'adresses IP (pools) pour les VLANs 10,11,12,13 et 14 puis définir également le pool d'adresses pour les clients DHCP du serveur.



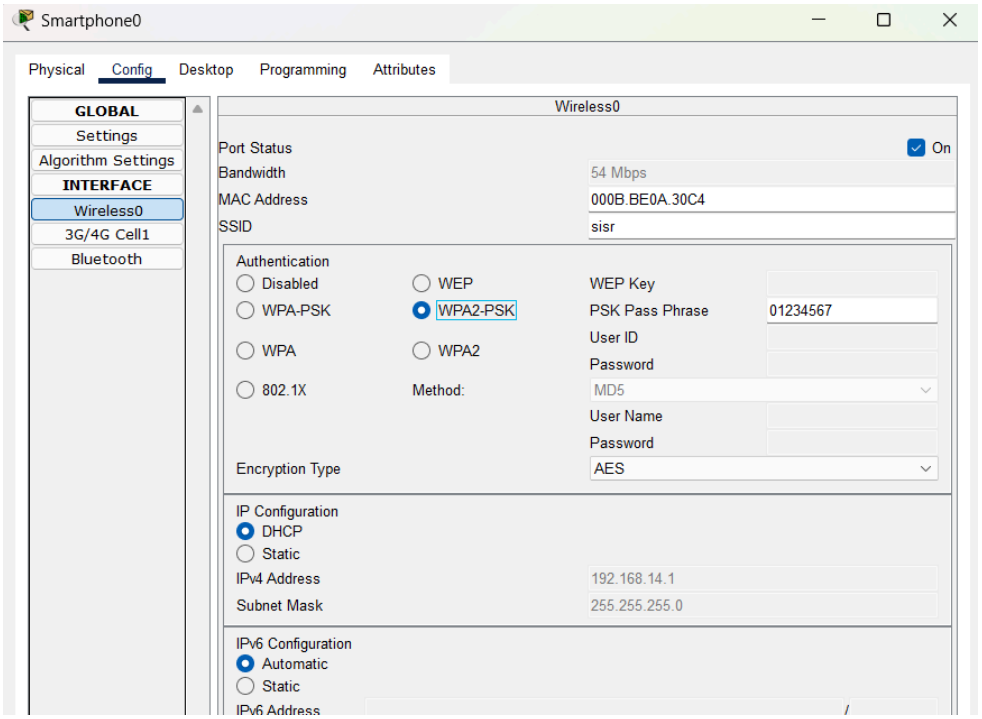
Il est important de mentionner que chaque VLAN doit avoir une plage d'adresses distinctes pour que les clients puissent recevoir une adresse IP unique et que le serveur doit être configuré pour répondre aux demandes DHCP des clients sur les différents VLANs.

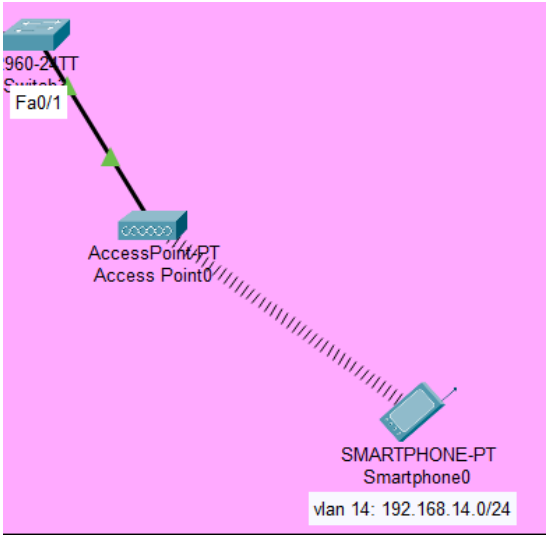
Nous allons également configurer le smartphone pour qu'il récupère automatiquement une adresse IP via DHCP et communique avec l'access point sur le port 1. Cela implique de configurer le mot de passe, le SSID et l'option WPA2-PSK dans l'interface de configuration (config/interface) de l'access point. Ensuite, nous ajusterons les paramètres sans fil du smartphone (wireless) pour établir la connexion.

Pour L’access Point



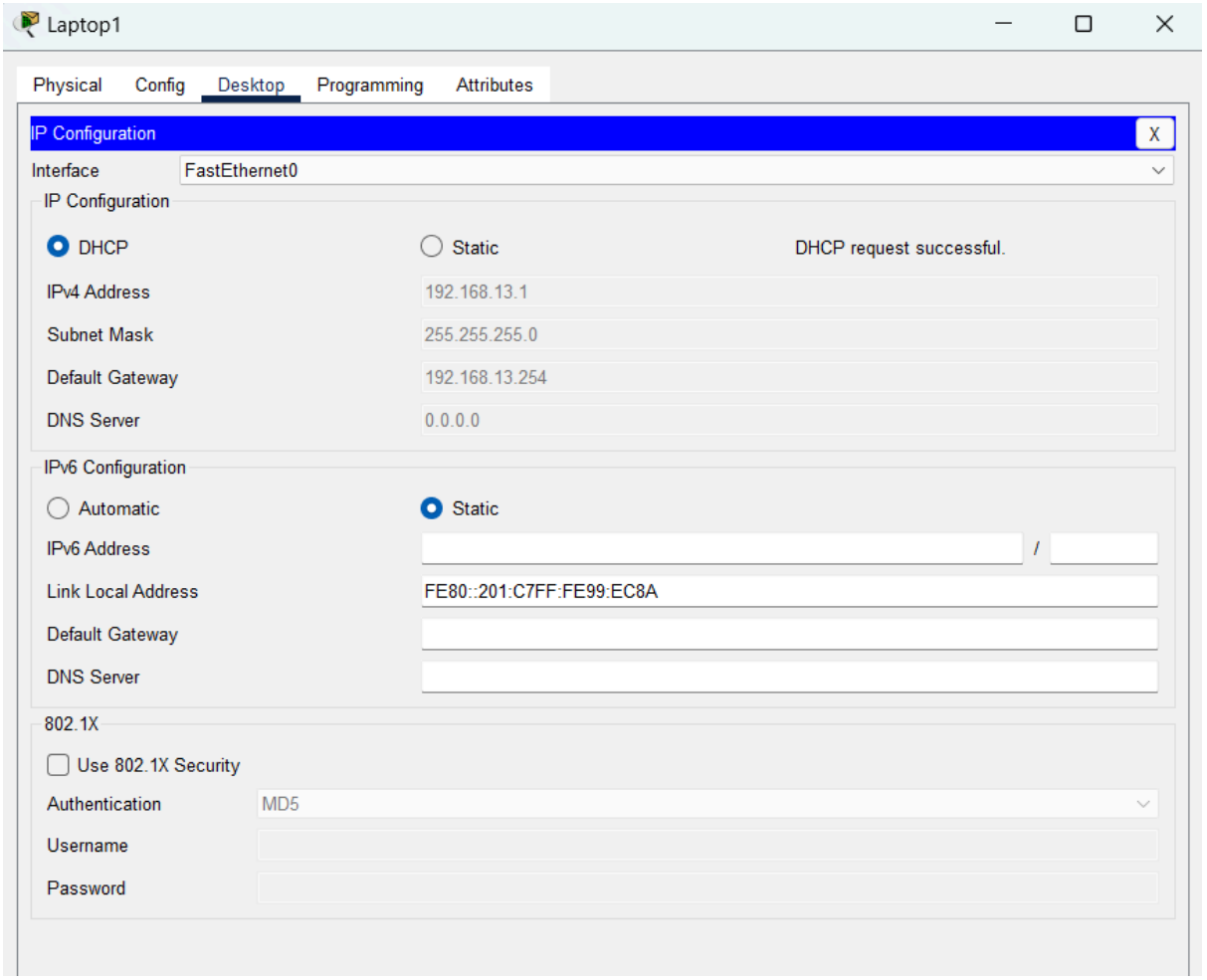
Pour le Smartphone





Ainsi les deux appareils communiquent

Le service DHCP fonctionne avec succès après la configuration complète de tous les équipements impliqués, permettant aux PC de recevoir automatiquement leurs adresses IP.



La connectivité est établie et fonctionnelle, confirmée par des pings réussis entre tous les équipements configurés.