

COMPTE RENDU 2

Hossam Nazih

IIR G3

Introduction

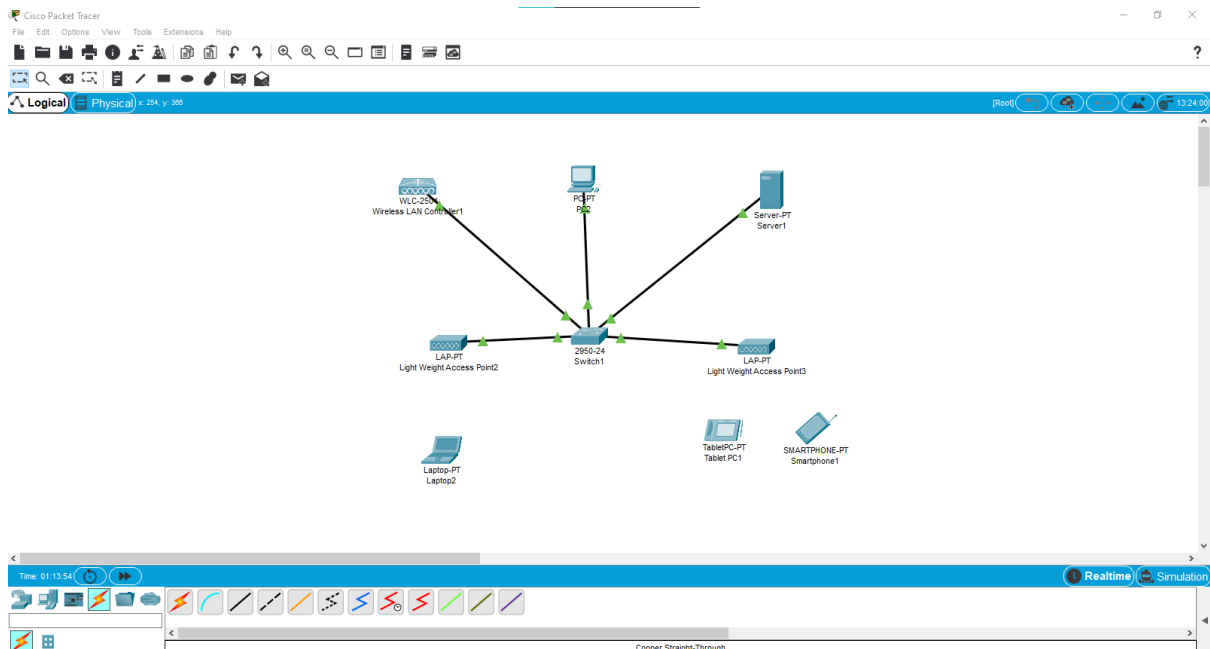
Ce rapport décrit les étapes détaillées pour la simulation d'un réseau Wi-Fi en utilisant un contrôleur Cisco Wireless LAN Controller (WLC). L'objectif est de configurer un réseau Wi-Fi fonctionnel, permettant de gérer des points d'accès (APs) et d'assurer une connexion fluide pour les utilisateurs.

Étape 2 : Création de l'Infrastructure Réseau

Topologie :

Une infrastructure typique inclut :

- Un routeur pour fournir la connectivité au réseau externe.
- Un switch pour relier les points d'accès (APs) au contrôleur.
- Le contrôleur Cisco WLC pour gérer les APs.
- Des points d'accès (Access Points, APs) pour diffuser le réseau Wi-Fi.
- Des dispositifs clients (ordinateurs, smartphones) pour tester la connectivité.



Configuration :

1. Ajout des appareils :

a. Glissez et déposez les appareils nécessaires dans la zone de simulation de votre émulateur.

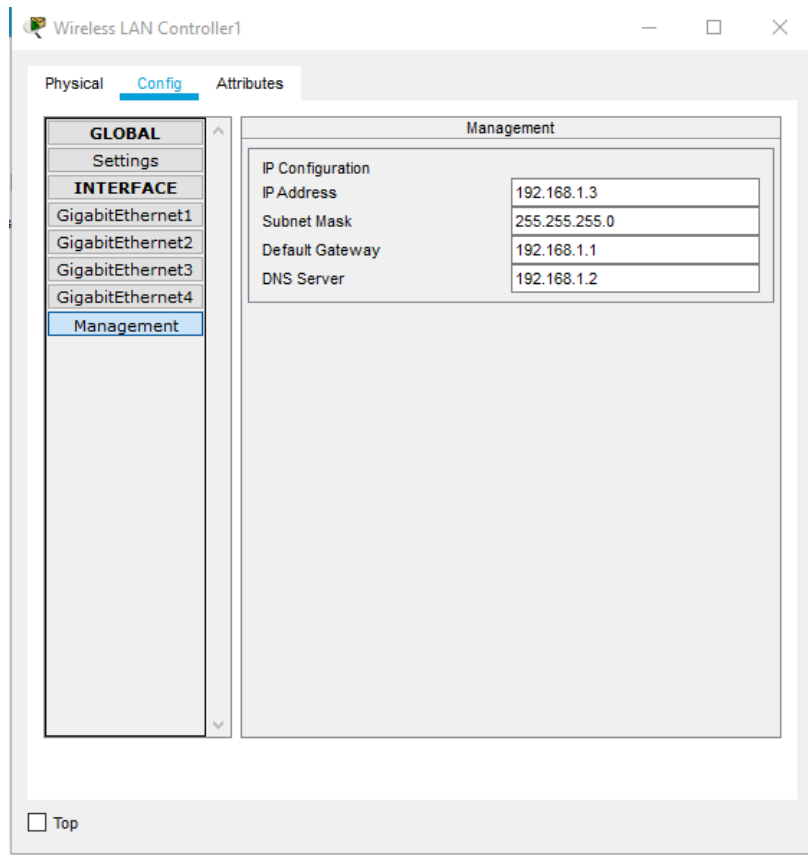
2. Connexion des appareils :

a. Utilisez des câbles Ethernet pour relier les points d'accès au switch.

b. Connectez le switch au contrôleur WLC.

1.2 Configuration des adresses IP

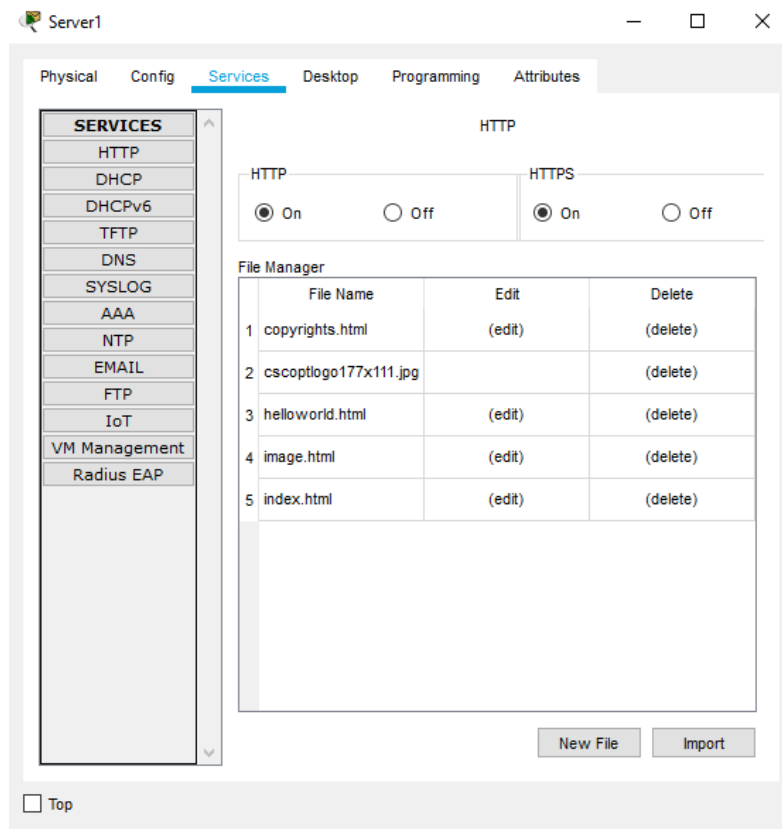
- Serveur DHCP : 192.168.1.2
- Interface de gestion du WLC : 192.168.1.3
- Passerelle par défaut : 192.168.1.1
- Plage d'adresses DHCP attribuées : 192.168.1.3 - 192.168.1.103



1.3 Configuration du DHCP

Les paramètres configurés sur le serveur DHCP sont :

- Plage IP : 192.168.1.3 - 192.168.1.103
- Masque de sous-réseau : 255.255.255.0
- Passerelle : 192.168.1.1
- Serveur DNS : 192.168.1.2



Explication : Cette topologie illustre comment les appareils sont connectés dans la simulation. Chaque élément doit être correctement configuré pour une communication fluide.

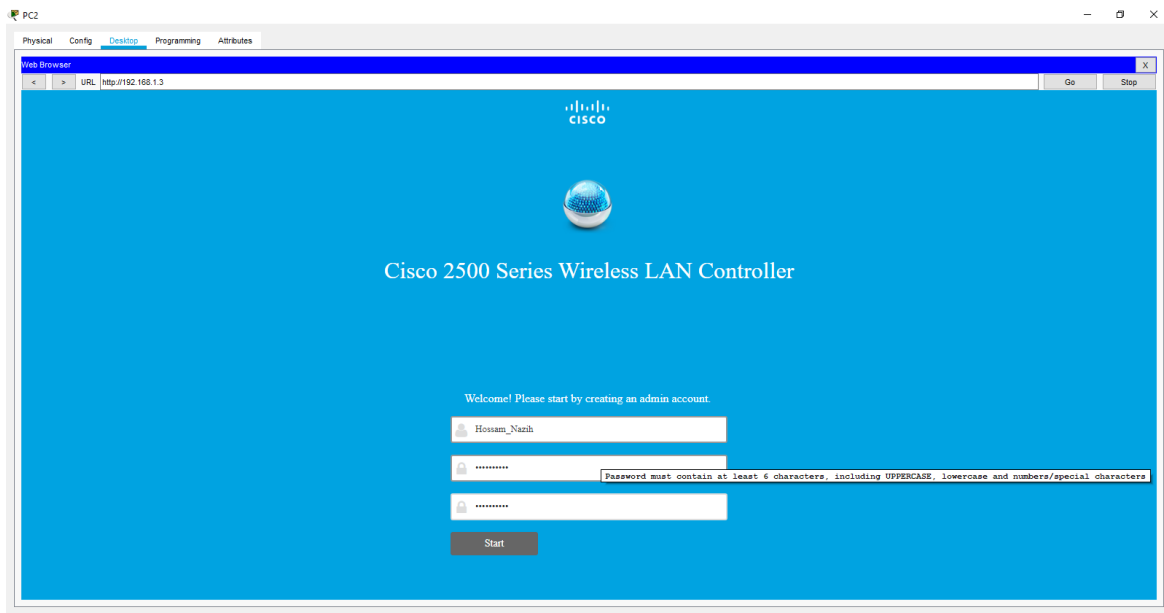
Étape 3 : Configuration Initiale du Cisco WLC

Connexion initiale : Accès via HTTP à l'adresse 192.168.1.3. Configuration d'un nom (admin) d'utilisateur et mot de passe administrateur (Admin@1).

2. Paramètres de base : Configuration de l'adresse IP de gestion, de l'emplacement et de l'heure. 3. Création du réseau WiFi sécurisé :

- SSID :HOSSAM
- Sécurité : WPA2 Personnel
- Clé : Hossam2003

Une fois la configuration terminée, le WLC redémarre, et l'accès se fait ensuite via HTTPS.



Accès au WLC :

1. Ouvrez un navigateur Web et entrez l'adresse IP du contrôleur pour accéder à son interface de gestion.
2. Utilisez les identifiants administratifs fournis pour vous connecter.

Assurez-vous d'utiliser les bonnes informations d'identification pour accéder à l'interface de gestion.

Paramètres de base :

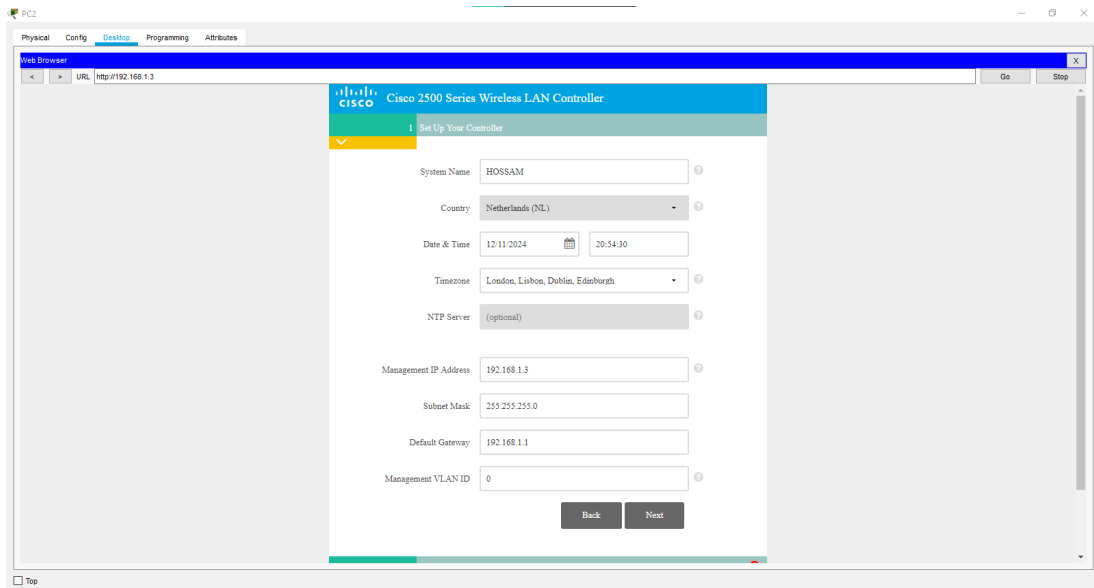
1. Configurez les paramètres IP (adresse IP, masque de sous-réseau, passerelle).
2. Activez le serveur DHCP sur le WLC pour attribuer des adresses IP aux points d'accès.

Étape 4 : Configuration des Points d'Accès (APs)

Association des APs au WLC :

1. **Connectez les APs au switch.**
2. **Les APs obtiennent automatiquement une adresse IP du serveur DHCP configuré sur le WLC.**

3. Une fois connectés, les APs apparaissent dans la liste des appareils du WLC.



Etape 5 : Création d'un SSID

Configuration :

1. Accédez à l'onglet **WLANS** et cliquez sur **Create**.
2. Renseignez les informations suivantes :
 - a. Nom du SSID.
 - b. Type de sécurité souhaité (WPA2, WPA3, etc.).
3. Associez le SSID à une interface VLAN préalablement configurée sur le WLC.

PC2

Physical Config Desktop Programming Attributes

Web Browser

URL: http://192.168.1.3

Cisco 2500 Series Wireless LAN Controller

1 Set Up Your Controller

System Name: HOSSAM

Country: Netherlands (NL)

Date & Time: 12/11/2024 20:54:30

Timezone: London, Lisbon, Dublin, Edinburgh

NTP Server: (optional)

Management IP Address: 192.168.1.3

Subnet Mask: 255.255.255.0

Default Gateway: 192.168.1.1

Management VLAN ID: 0

Back Next

Top

Remplissez les champs requis pour créer un SSID sécurisé et fonctionnel.

PC2

Physical Config Desktop Programming Attributes

Web Browser

URL: http://192.168.1.3

Cisco 2500 Series Wireless LAN Controller

1 Set Up Your Controller

2 Create Your Wireless Networks

3 Advanced Setting

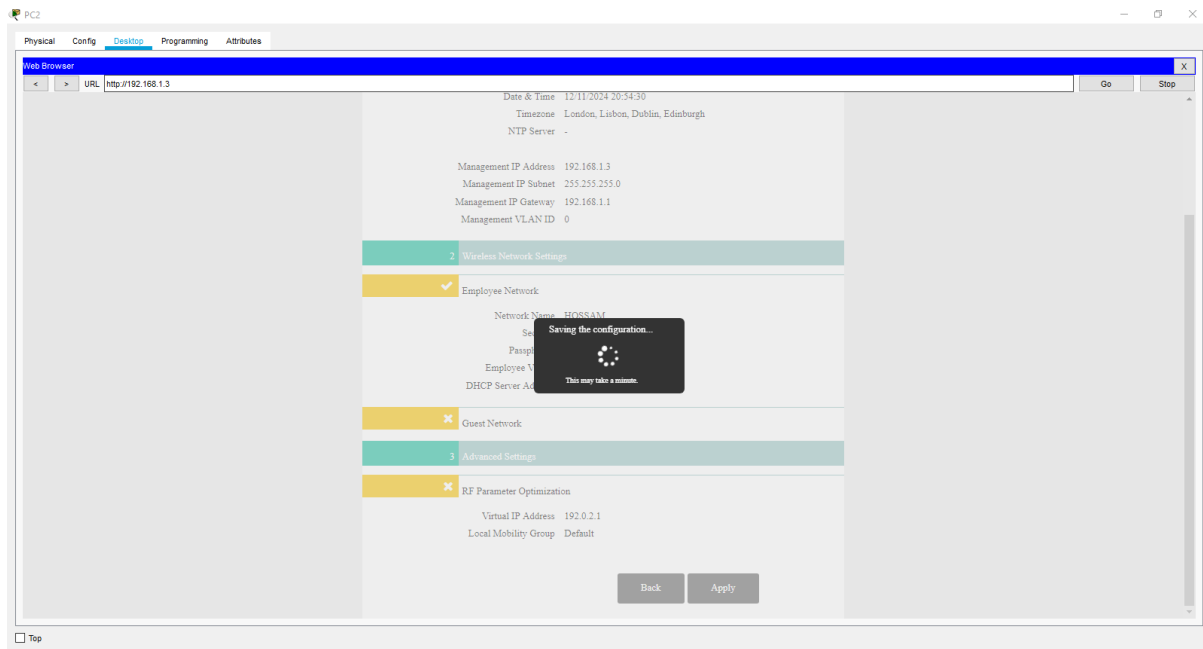
RF Parameter Optimization

Virtual IP Address: 192.0.2.1

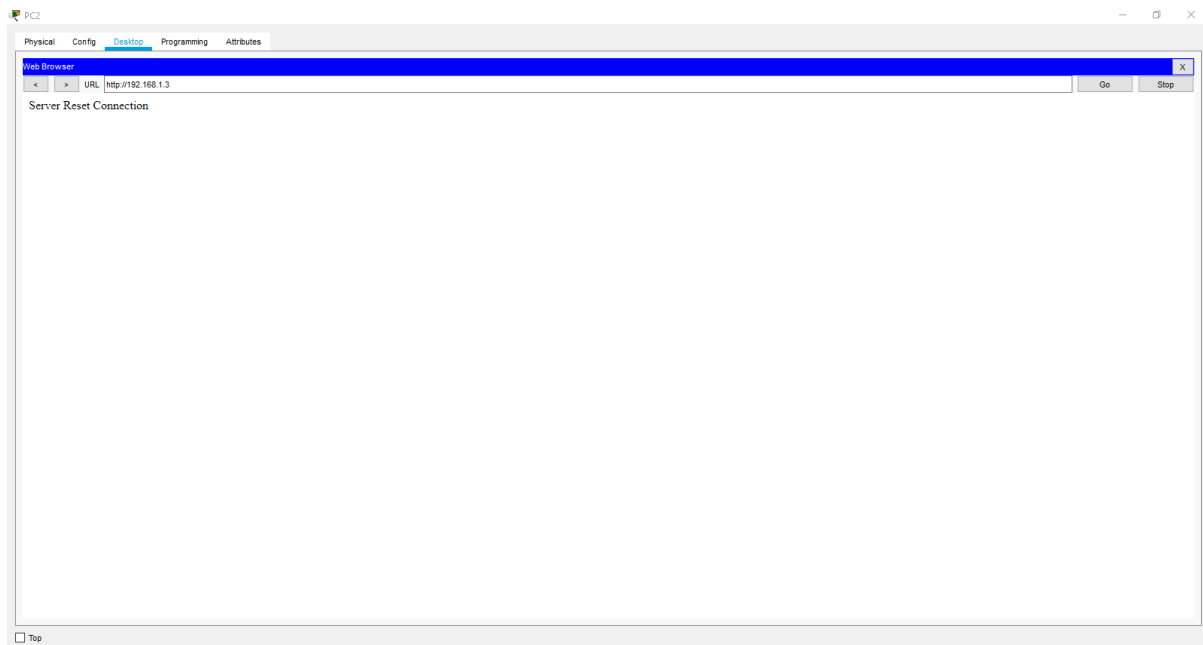
Local Mobility Group: Default

Back Next

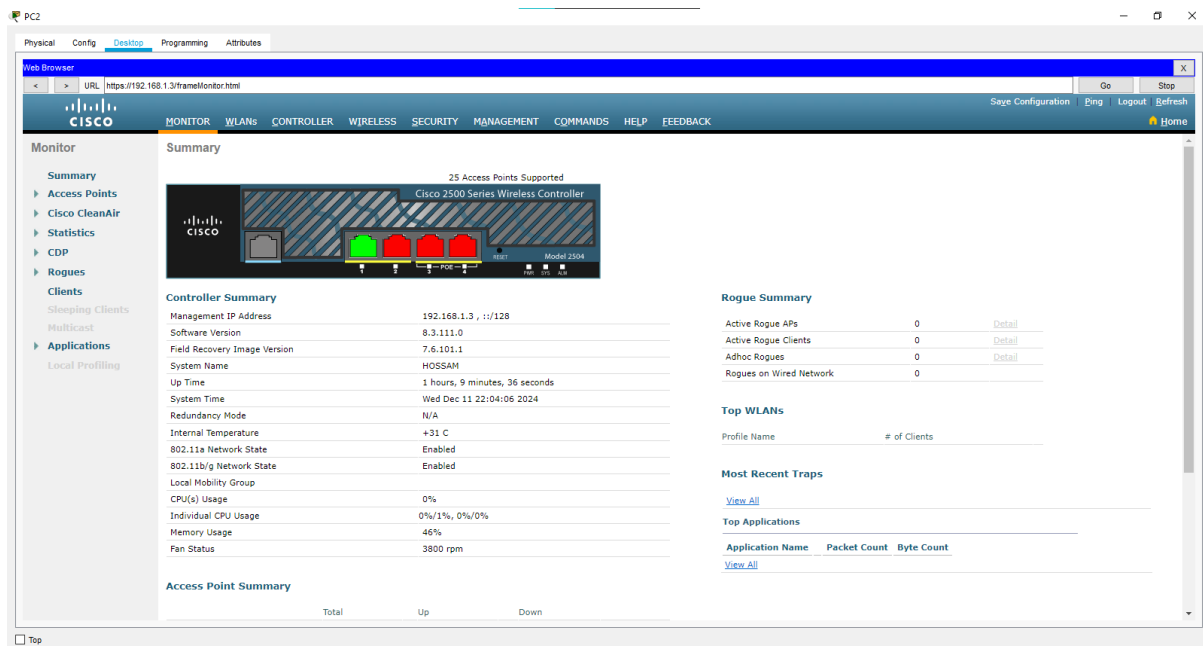
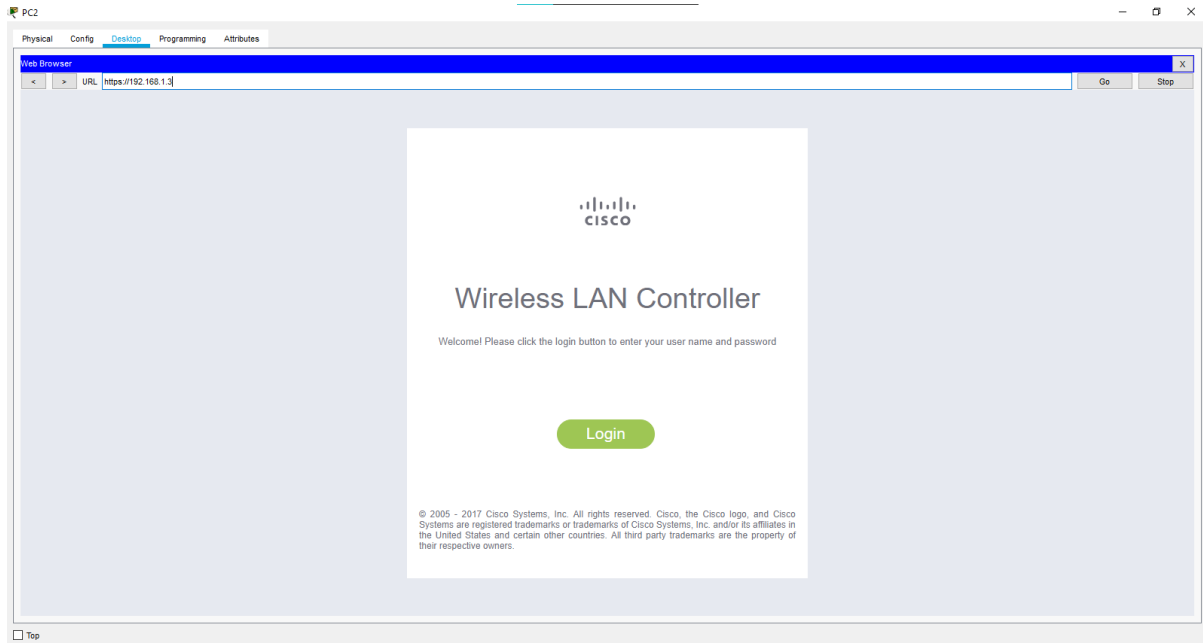
Top



Après remplissage cliquer sur le Bouton apply ça va enregistrer les configurations et les ssid tu donnes pour la sécurisation après cette étape pour login on utilise https.



Http ne travaille pas car les points d'accès sont sécuriser il obligatoire d'un username et motpass.



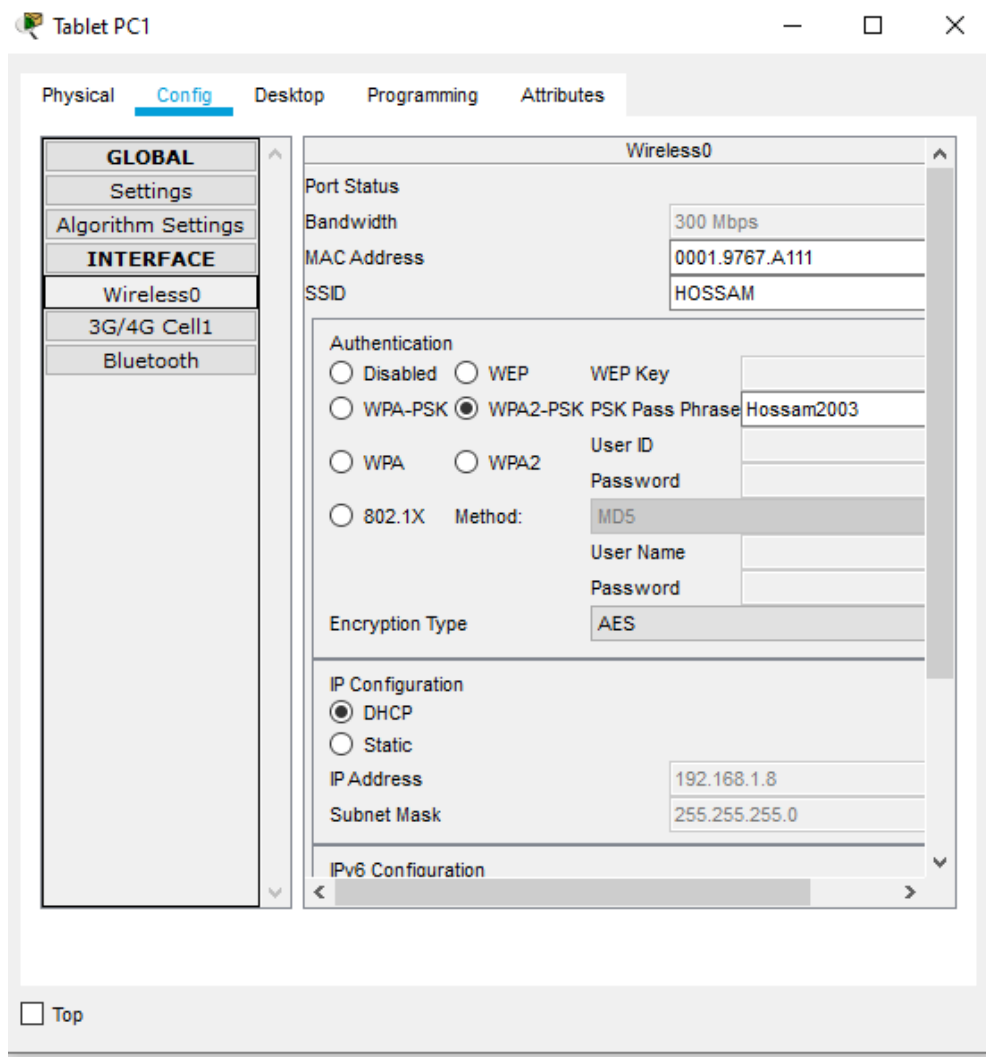
The screenshot shows the Cisco WLC GUI with the 'All APs' page. The table below represents the data shown in the interface:

AP Name	IP Address(Ipv4/Ipv6)	AP Model	AP MAC	AP Up Time	Admin Status	Operational Status
Light Weight Access Point2	192.168.1.5	PT-AIR-CAP1000I-A-K9	00:90:21:3E:07:01	0 d, 0 h 3 m 29 s	Enabled	REG
Light Weight Access Point3	192.168.1.4	PT-AIR-CAP1000I-A-K9	00:06:2A:25:BE:01	0 d, 1 h 44 m 40 s	Enabled	REG

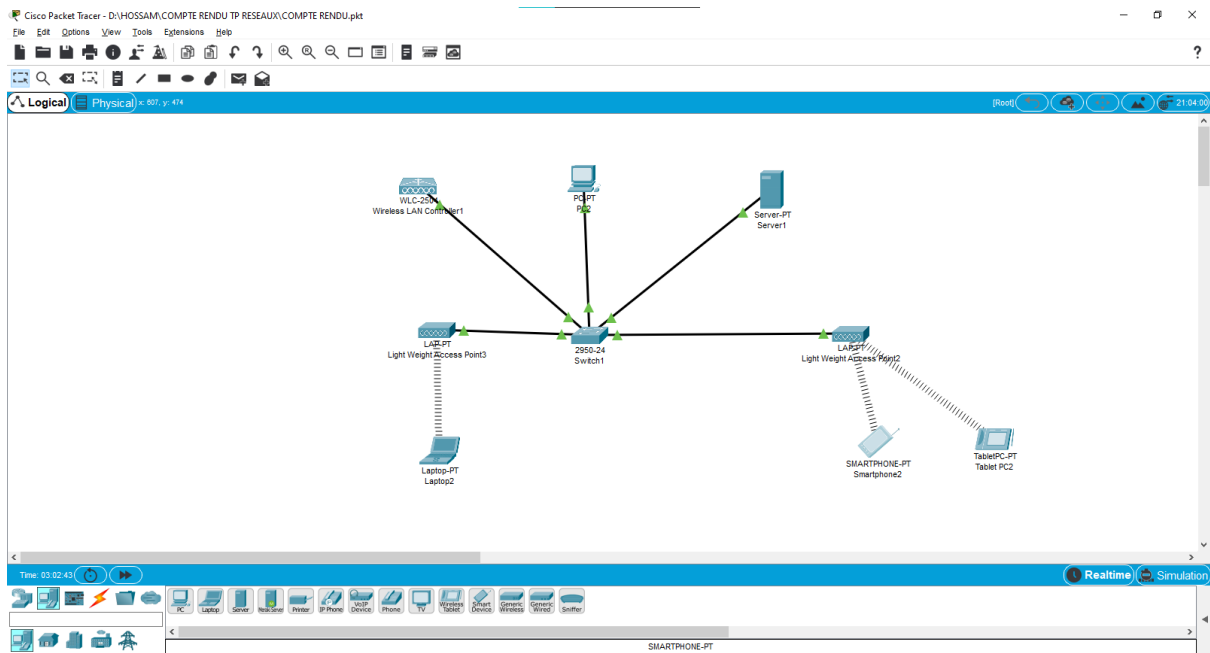
Étape 6 : Test de Connectivité

Vérification :

1. Connectez un dispositif client au SSID configuré.
2. Vérifiez que le client reçoit une adresse IP correcte.
3. Testez la connectivité à Internet ou à un serveur local.



POUR CONNECTER AVEC LE POINT ACCES TU ES OBLIGATOIRE DENTRER LE SSID ET LE MOT PASS SOIT POUR LE PC PORTABLE OU BIEN SMARTPHONE



cette capture montre qu'un client est connecté avec succès au réseau et que la connectivité est fonctionnelle.

Test du fonctionnement :

Smartphone0

Physical Config **Desktop** Programming Attributes

IP Configuration X

Interface: Wireless0

IP Configuration

☒ DHCP ☐ Static

IP Address: 192.168.1.25

Subnet Mask: 255.255.255.0

Default Gateway: 192.168.1.1

DNS Server: 192.168.1.2

IPv6 Configuration

☒ DHCP ☐ Auto Config ☐ Static

IPv6 Address: /

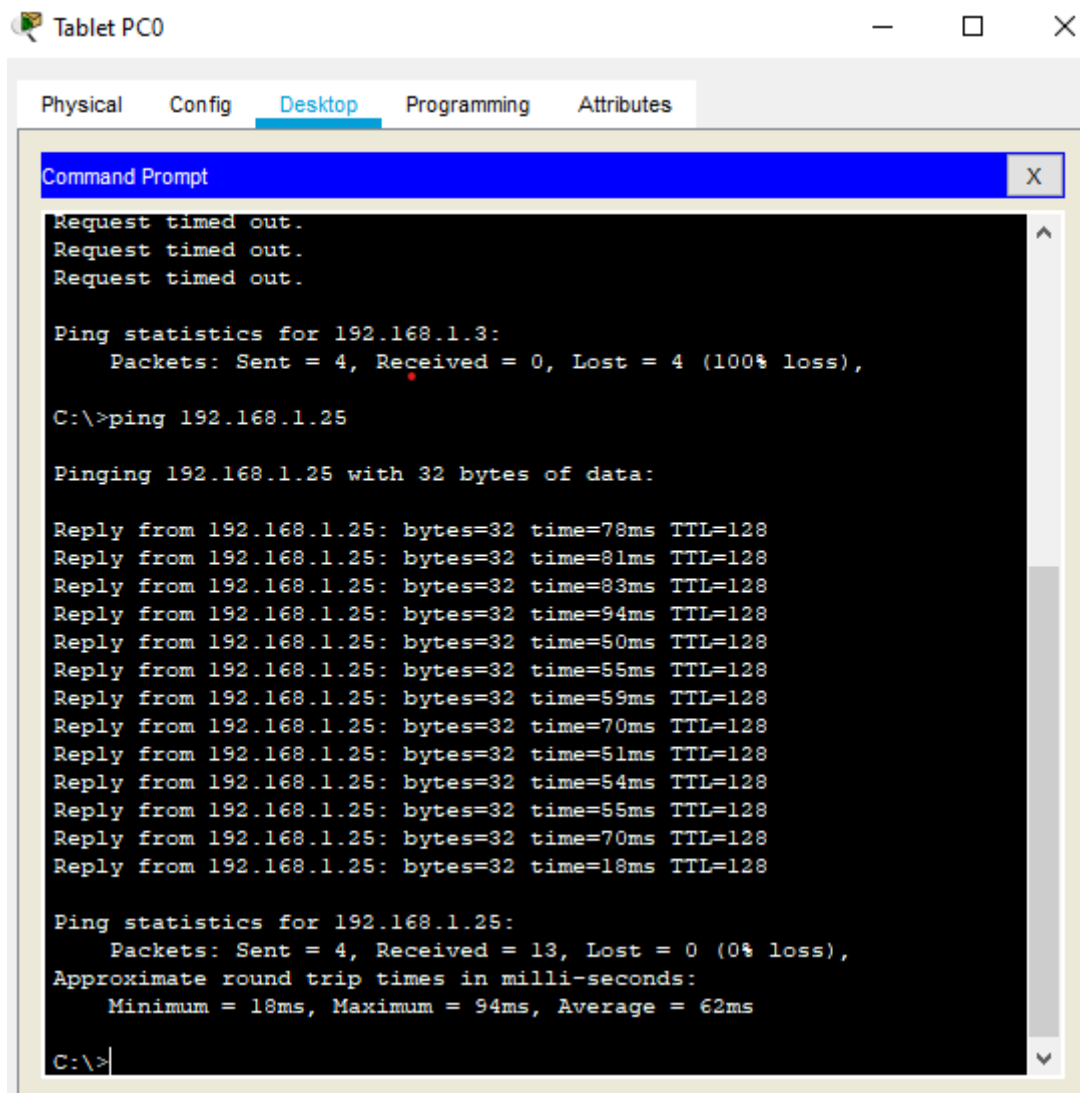
Link Local Address: FE80::240:BFF:FE5D:8624

IPv6 Gateway:

IPv6 DNS Server:

☐ Top

VOILA LA CONFIGURATION DU SMARTPHONE



The screenshot shows a window titled "Tablet PC0" with standard Windows window controls. Inside the window, there are tabs for "Physical", "Config", "Desktop", "Programming", and "Attributes". The "Desktop" tab is active, displaying a "Command Prompt" window. The Command Prompt shows the results of a ping command to 192.168.1.25. It indicates that the first three ping attempts to 192.168.1.3 timed out, and then a series of successful pings to 192.168.1.25 were received with varying response times.

```
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.1.3:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>ping 192.168.1.25

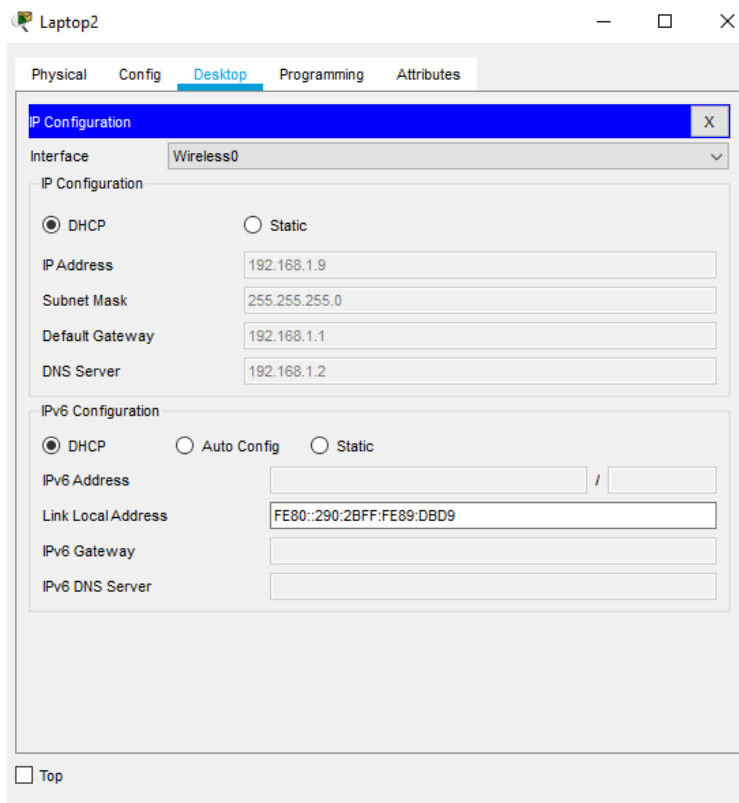
Pinging 192.168.1.25 with 32 bytes of data:

Reply from 192.168.1.25: bytes=32 time=78ms TTL=128
Reply from 192.168.1.25: bytes=32 time=81ms TTL=128
Reply from 192.168.1.25: bytes=32 time=83ms TTL=128
Reply from 192.168.1.25: bytes=32 time=94ms TTL=128
Reply from 192.168.1.25: bytes=32 time=50ms TTL=128
Reply from 192.168.1.25: bytes=32 time=55ms TTL=128
Reply from 192.168.1.25: bytes=32 time=59ms TTL=128
Reply from 192.168.1.25: bytes=32 time=70ms TTL=128
Reply from 192.168.1.25: bytes=32 time=51ms TTL=128
Reply from 192.168.1.25: bytes=32 time=54ms TTL=128
Reply from 192.168.1.25: bytes=32 time=55ms TTL=128
Reply from 192.168.1.25: bytes=32 time=70ms TTL=128
Reply from 192.168.1.25: bytes=32 time=18ms TTL=128

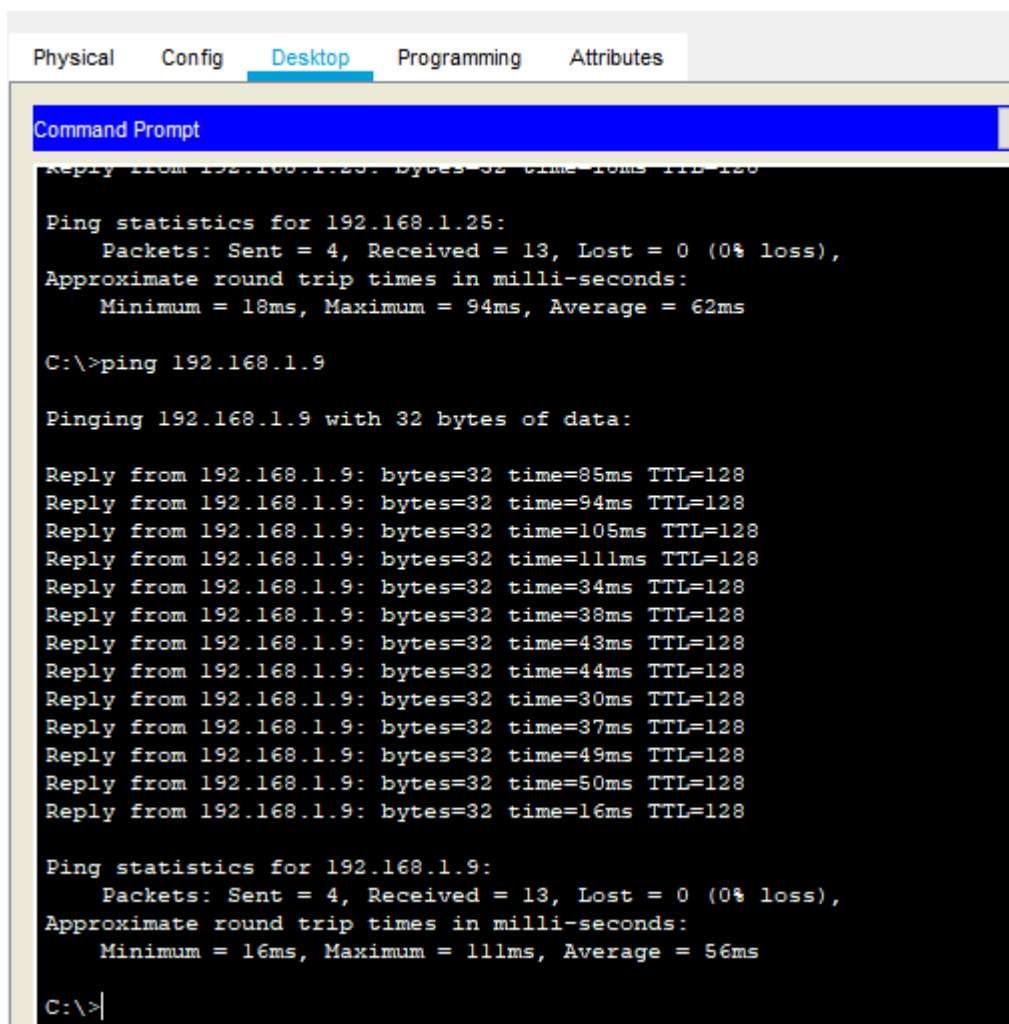
Ping statistics for 192.168.1.25:
    Packets: Sent = 4, Received = 13, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 18ms, Maximum = 94ms, Average = 62ms

C:\>
```

Vérification de la connectivité entre deux équipements connectés au même point d'accès.



Le configuration du laptop



The screenshot shows a Tablet PC interface with a window titled 'Tablet PC0'. The window has a menu bar with 'Physical', 'Config', 'Desktop', 'Programming', and 'Attributes'. The 'Desktop' tab is selected. Below the menu bar is a 'Command Prompt' window. The Command Prompt displays the following text:

```
Reply from 192.168.1.25: bytes=32 time=10ms TTL=128

Ping statistics for 192.168.1.25:
    Packets: Sent = 4, Received = 13, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 18ms, Maximum = 94ms, Average = 62ms

C:\>ping 192.168.1.9

Pinging 192.168.1.9 with 32 bytes of data:

Reply from 192.168.1.9: bytes=32 time=85ms TTL=128
Reply from 192.168.1.9: bytes=32 time=94ms TTL=128
Reply from 192.168.1.9: bytes=32 time=105ms TTL=128
Reply from 192.168.1.9: bytes=32 time=111ms TTL=128
Reply from 192.168.1.9: bytes=32 time=34ms TTL=128
Reply from 192.168.1.9: bytes=32 time=38ms TTL=128
Reply from 192.168.1.9: bytes=32 time=43ms TTL=128
Reply from 192.168.1.9: bytes=32 time=44ms TTL=128
Reply from 192.168.1.9: bytes=32 time=30ms TTL=128
Reply from 192.168.1.9: bytes=32 time=37ms TTL=128
Reply from 192.168.1.9: bytes=32 time=49ms TTL=128
Reply from 192.168.1.9: bytes=32 time=50ms TTL=128
Reply from 192.168.1.9: bytes=32 time=16ms TTL=128

Ping statistics for 192.168.1.9:
    Packets: Sent = 4, Received = 13, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 16ms, Maximum = 111ms, Average = 56ms

C:\>|
```

Ping inter-points d'accès : Vérification de la connectivité entre deux équipements connectés à des points d'accès différents.

PC2

Physical Config **Desktop** Programming Attributes

IP Configuration X

Interface FastEthernet0

IP Configuration

☒ DHCP ☐ Static

IP Address 192.168.1.1

Subnet Mask 255.255.255.0

Default Gateway 192.168.1.1

DNS Server 192.168.1.2

IPv6 Configuration

☐ DHCP ☐ Auto Config ☒ Static

IPv6 Address /

Link Local Address FE80::20C:CFFF:FE47:123

IPv6 Gateway

IPv6 DNS Server

802.1X

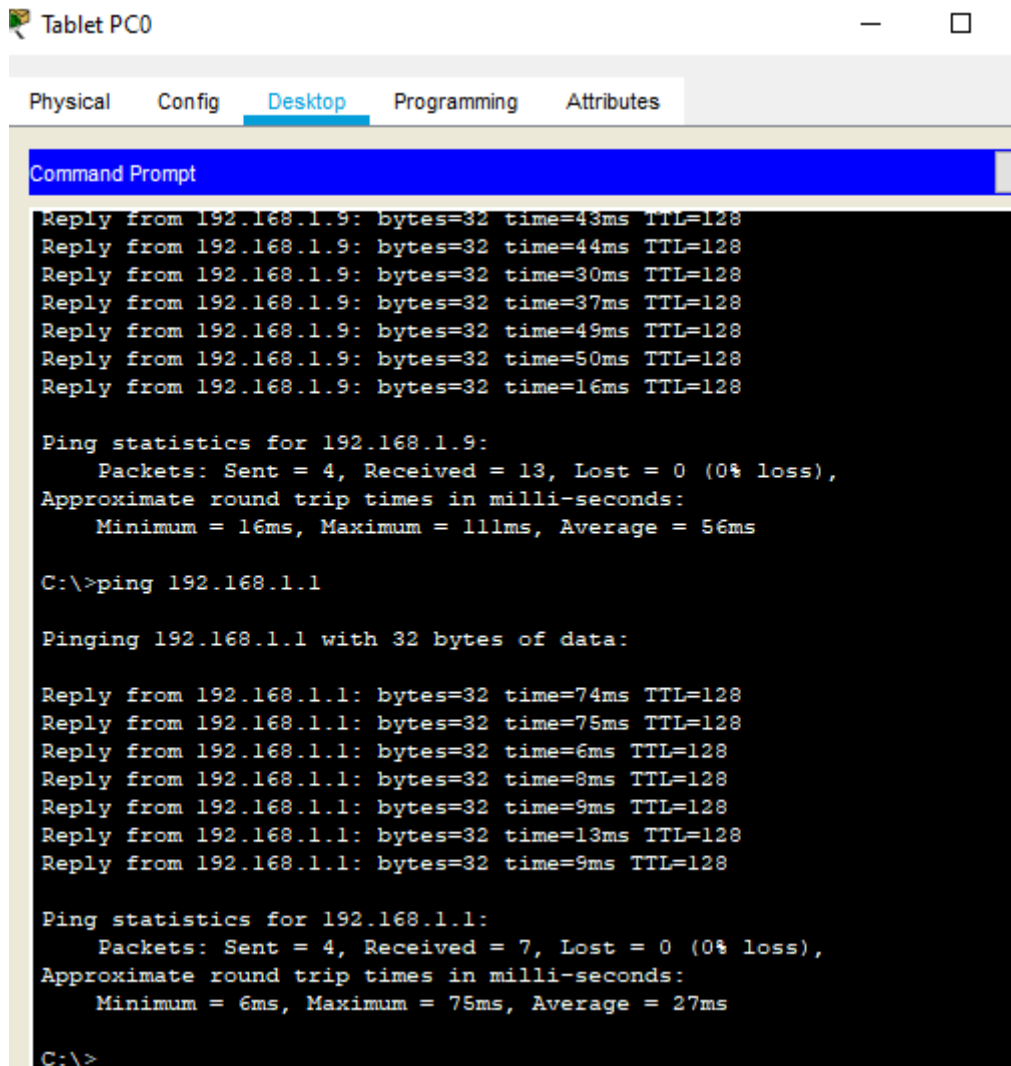
☐ Use 802.1X Security

Authentication MD5

Username

☐ Top

La configuration du pc administratif



The screenshot shows a Tablet PC0 interface with a Command Prompt window open. The window displays the results of two ping commands. The first command is 'ping 192.168.1.9', which shows 6 successful replies with varying round trip times (16ms to 50ms) and a statistics summary: 4 packets sent, 13 received, 0% loss, average 56ms. The second command is 'ping 192.168.1.1', which shows 7 successful replies with round trip times (6ms to 75ms) and a statistics summary: 4 packets sent, 7 received, 0% loss, average 27ms.

```
Tablet PC0
Physical Config Desktop Programming Attributes
Command Prompt
Reply from 192.168.1.9: bytes=32 time=43ms TTL=128
Reply from 192.168.1.9: bytes=32 time=44ms TTL=128
Reply from 192.168.1.9: bytes=32 time=30ms TTL=128
Reply from 192.168.1.9: bytes=32 time=37ms TTL=128
Reply from 192.168.1.9: bytes=32 time=49ms TTL=128
Reply from 192.168.1.9: bytes=32 time=50ms TTL=128
Reply from 192.168.1.9: bytes=32 time=16ms TTL=128

Ping statistics for 192.168.1.9:
    Packets: Sent = 4, Received = 13, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 16ms, Maximum = 111ms, Average = 56ms

C:\>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:

Reply from 192.168.1.1: bytes=32 time=74ms TTL=128
Reply from 192.168.1.1: bytes=32 time=75ms TTL=128
Reply from 192.168.1.1: bytes=32 time=6ms TTL=128
Reply from 192.168.1.1: bytes=32 time=8ms TTL=128
Reply from 192.168.1.1: bytes=32 time=9ms TTL=128
Reply from 192.168.1.1: bytes=32 time=13ms TTL=128
Reply from 192.168.1.1: bytes=32 time=9ms TTL=128

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 7, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 6ms, Maximum = 75ms, Average = 27ms

C:\>
```

Ping Ethernet-WiFi : Vérification de la connectivité entre un équipement Ethernet et un équipement WiFi.

Équipements connectés au même point d'accès :

1. Ping entre deux équipements :

- Depuis l'équipement A (Tablet pc0), un ping est envoyé vers l'équipement B (Smartphone0), tous deux connectés au même point d'accès.

2. Mode Simulation :

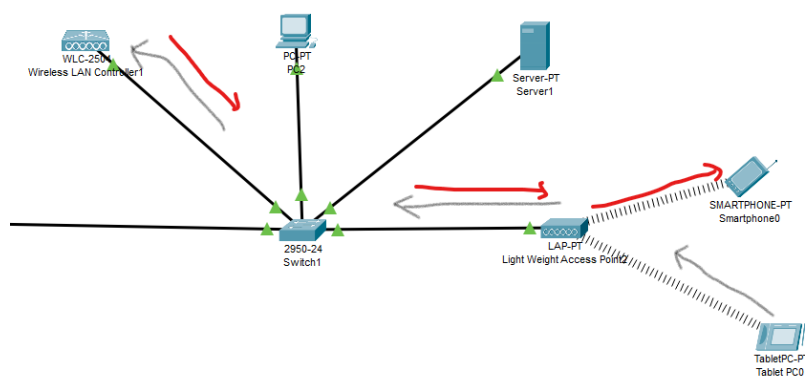
- a. Les étapes du message (encapsulation, transmission, décapsulation) sont suivies pour observer son acheminement.

Étapes d'encapsulation des messages

1. **Niveau Application** : Création du message ICMP (ping).
2. **Niveau Transport** : Encapsulation du message ICMP dans un paquet IP (avec adresses IP source et destination).
3. **Niveau Réseau** : Encapsulation du paquet dans une trame Wi-Fi (avec adresses MAC source et celle du point d'accès).
4. **Niveau Liaison** : Le point d'accès reçoit la trame et la redirige vers l'équipement cible.

Adresses IP et MAC

- **Adresse IP source** : Émetteur (ex. 192.168.1.22).
- **Adresse IP destination** : Récepteur (ex. 192.168.1.25).
- **Adresse MAC source** : MAC de l'équipement émetteur.
- **Adresse MAC destination** : MAC du point d'accès.



Type d'infrastructure

- Ici, nous sommes dans une infrastructure BSS (Basic Service Set) : les équipements communiquent via un point d'accès unique. 3.1.5 Protocole et objectif

- Protocole utilisé : ICMP, utilisé pour tester la connectivité.

- Objectif : Vérifier que les deux équipements peuvent échanger des paquets au niveau IP.

Équipements connectés à différents points d'accès

Processus simulé

1. Ping entre deux équipements :

- a. Un ping est envoyé depuis un équipement A connecté à un point d'accès 1 vers un équipement B connecté à un point d'accès 2.

2. Transmission via WLC :

- a. Le message passe par le contrôleur WLC, qui gère la communication entre les points d'accès.

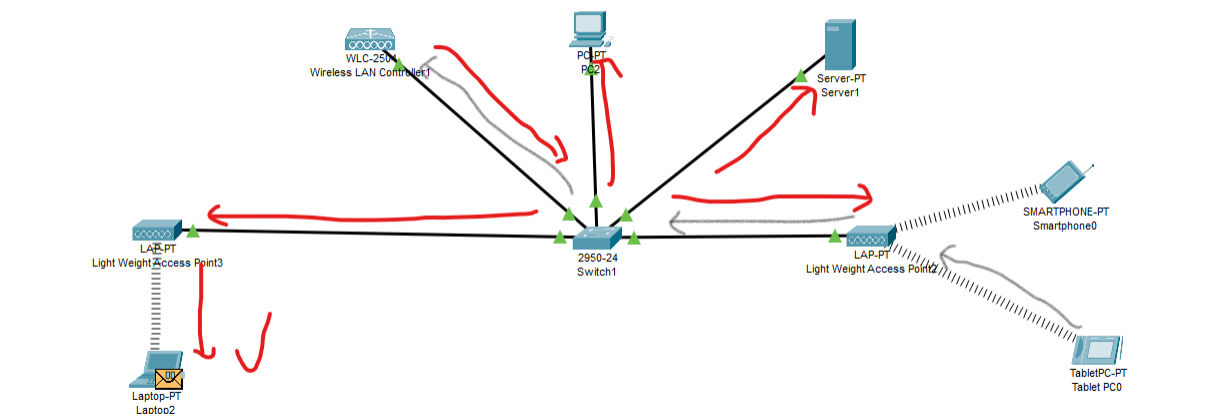
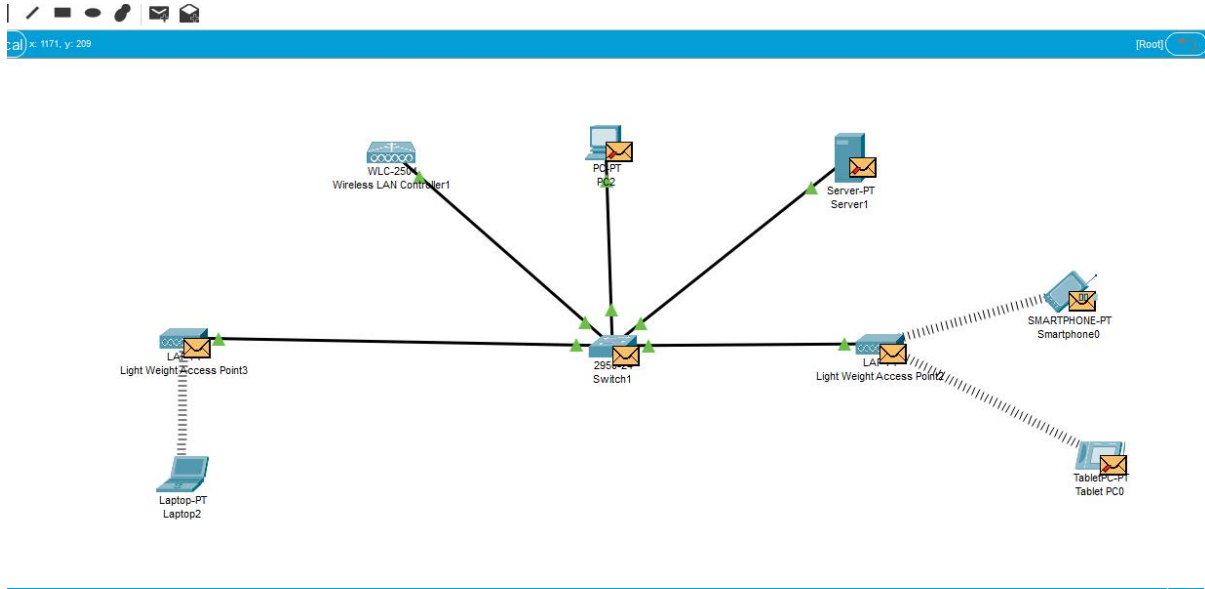
Étapes d'encapsulation des messages

1. **Niveau Liaison** : Le message est encapsulé dans une trame Wi-Fi et envoyé au premier point d'accès.
2. **Niveau Réseau** : Le point d'accès encapsule le paquet dans un message CAPWAP, transmis au WLC.
3. **Traitement par le WLC** : Le WLC analyse le paquet et le transmet au second point d'accès via CAPWAP.
4. **Liaison et Réseau** : Le second point d'accès décapsule le paquet et l'envoie à l'équipement cible.

Adresses IP et MAC

- **Adresse IP source** : Émetteur (ex. 192.168.1.22).
- **Adresse IP destination** : Récepteur (ex. 192.168.1.9).

- **Adresse MAC source** : MAC de l'équipement émetteur.
- **Adresse MAC intermédiaire** : MAC du premier point d'accès.
- **Adresse MAC destination** : MAC de l'équipement récepteur.



Type d'infrastructure

- **Infrastructure ESS (Extended Service Set)** :
- Plusieurs points d'accès sont interconnectés et centralisés via un WLC.

Protocole et Objectif

- **Protocole utilisé** : CAPWAP, utilisé pour transporter les données entre le WLC et les points d'accès.

- **Objectif** : Assurer la transmission des paquets entre équipements connectés à différents points d'accès.

Équipements connectés à différentes technologies

Processus simulé

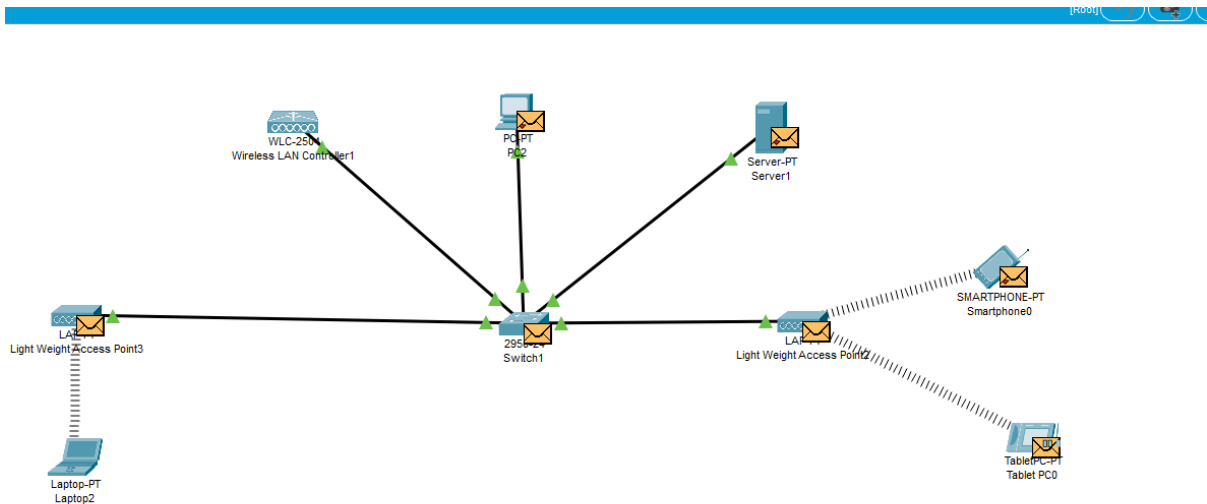
1. **Ping entre Ethernet et WiFi** :
 - a. Un équipement connecté au réseau via Ethernet envoie un ping à un équipement connecté au WiFi.
2. **Transmission via passerelle ou WLC** :
 - a. Le message est routé par une passerelle ou le contrôleur WLC.

Étapes d'encapsulation des messages

1. **Niveau Réseau** : Un paquet IP est généré par l'équipement Ethernet.
2. **Niveau Liaison Ethernet** : Le paquet est encapsulé dans une trame Ethernet pour la transmission via le câble réseau.
3. **Traitement par le WLC** : Le message est reçu, analysé, puis transmis au point d'accès via le protocole CAPWAP.
4. **Niveau Liaison WiFi** : Le point d'accès décapsule la trame et la transmet à l'équipement WiFi via une trame WiFi.

Adresses IP et MAC

- **Adresse IP source** : IP de l'équipement connecté via Ethernet.
- **Adresse IP destination** : IP de l'équipement connecté via WiFi.
- **Adresse MAC source** : MAC de l'équipement Ethernet.
- **Adresse MAC intermédiaire** : MAC du point d'accès.
- **Adresse MAC destination** : MAC de l'équipement WiFi.



Type d'infrastructure

- **Infrastructure ESS (Extended Service Set) :**
Ce scénario repose sur un WLC permettant l'interconnexion entre différentes technologies (Ethernet et WiFi).

Protocole et Objectif

- **Protocole utilisé :** ICMP pour tester la connectivité et CAPWAP pour gérer la communication entre Ethernet et WiFi.
- **Objectif :** Assurer l'interopérabilité et la connectivité entre des équipements utilisant des technologies différentes.

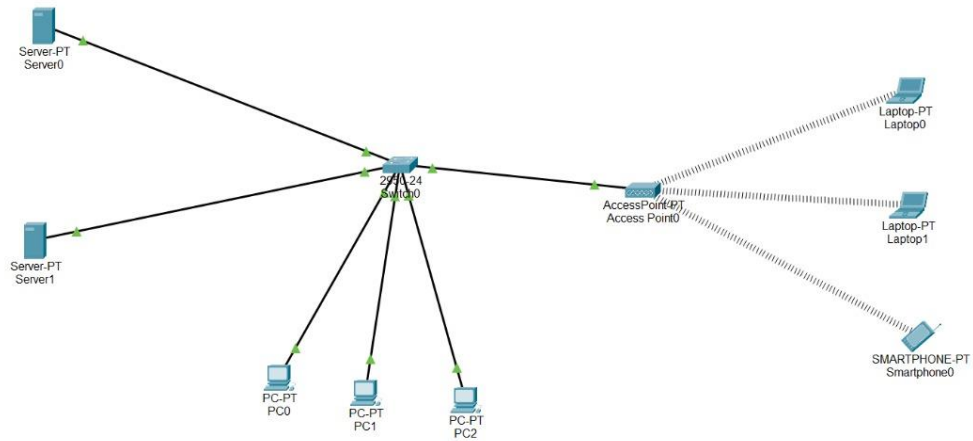
Conclusion

En suivant ces étapes, vous avez simulé avec succès un réseau Wi-Fi fonctionnel en utilisant un contrôleur Cisco WLC. Ce processus fournit une base solide pour comprendre la gestion centralisée des réseaux sans fil.

TP2

Partie Dynamique :

Schema:



Le schéma représente la topologie réseau mise en place pour les travaux pratiques. Il inclut les différents équipements tels que les serveurs, ordinateurs, et appareils mobiles connectés via des interfaces Ethernet ou sans fil.

Server0

Physical Config **Services** Desktop Programming Attributes

SERVICES

- HTTP
- DHCP**
- DHCPv6
- TFTP
- DNS
- SYSLOG
- AAA
- NTP
- EMAIL
- FTP
- IoT
- VM Management
- Radius EAP

DHCP

Interface: FastEthernet0 Service: ☒ On ☐ Off

Pool Name: serverPool

Default Gateway: 192.168.1.1

DNS Server: 192.168.1.2

Start IP Address: 192.168.1.1

Subnet Mask: 255.255.255.0

Maximum Number of Users: 100

TFTP Server: 0.0.0.0

WLC Address: 0.0.0.0

Add Save Remove

Pool Name	Default Gateway	DNS Server	Start IP Address	Subnet Mask	Max User	TFTP Server	WLC Address
serverPool	192.168.1.1	192.168.1.2	192.168.1.1	255.255.255.0	100	0.0.0.0	0.0.0.0

Top

Server0

Physical Config Services **Desktop** Programming Attributes

IP Configuration

IP Configuration

☐ DHCP ☒ Static

IPv4 Address: 192.168.1.3

Subnet Mask: 255.255.255.0

Default Gateway: 192.168.1.1

DNS Server: 192.168.1.2

IPv6 Configuration

☐ Automatic ☒ Static

IPv6 Address: /

Link Local Address: FE80::206:2AFF:FEE4:8651

Default Gateway:

DNS Server:

802.1X

☐ Use 802.1X Security

Authentication: MD5

Username:

Password:

Serveur 0 : Ce serveur est configuré pour fournir des services spécifiques (précisez lesquels, par exemple DHCP, HTTP, etc.) au réseau. Il joue un rôle crucial dans la gestion des connexions.

Server1

Physical Config Services **Desktop** Programming Attributes

IP Configuration

IP Configuration

☐ DHCP ☒ Static

IPv4 Address 192.168.1.104

Subnet Mask 255.255.255.0

Default Gateway 192.168.1.1

DNS Server 192.168.1.2

IPv6 Configuration

☐ Automatic ☒ Static

IPv6 Address /

Link Local Address FE80::260:5CFF:FE82:862A

Default Gateway

DNS Server

802.1X

☐ Use 802.1X Security

Authentication MD5

Username

Password

Server1

Physical Config **Services** Desktop Programming Attributes

SERVICES

- HTTP
- DHCP**
- DHCPv6
- TFTP
- DNS
- SYSLOG
- AAA
- NTP
- EMAIL
- FTP
- IoT
- VM Management
- Radius EAP

DHCP

Interface FastEthernet0 Service ☒ On ☐ Off

Pool Name serverPool

Default Gateway 192.168.1.1

DNS Server 192.168.1.2

Start IP Address : 192 168 1 104

Subnet Mask: 255 255 255 0

Maximum Number of Users : 100

TFTP Server: 0.0.0.0

WLC Address: 0.0.0.0

Add Save Remove

Pool Name	Default Gateway	DNS Server	Start IP Address	Subnet Mask	Max User	TFTP Server	WLC Address
serverPool	192.168.1.1	192.168.1.2	192.168.1...	255.255.2...	100	0.0.0.0	0.0.0.0

Serveur 1 : Ce serveur assure une redondance ou des services complémentaires (exemple : serveur DNS ou sauvegarde). Il est éteint dans certains tests pour évaluer la résilience du réseau.

The image shows a screenshot of a network configuration window for a device labeled 'PC1'. The window has a title bar with standard minimize, maximize, and close buttons. Below the title bar, there are tabs for 'Physical', 'Config', 'Desktop', 'Programming', and 'Attributes'. The 'Config' tab is active, and within it, the 'IP Configuration' section is highlighted in blue. The 'Interface' dropdown menu is set to 'FastEthernet0'. The 'IP Configuration' section contains two radio buttons: 'DHCP' (selected) and 'Static'. Below these are input fields for 'IPv4 Address' (192.168.1.104), 'Subnet Mask' (255.255.255.0), 'Default Gateway' (192.168.1.1), and 'DNS Server' (192.168.1.2). The 'IPv6 Configuration' section has two radio buttons: 'Automatic' and 'Static' (selected). Below these are input fields for 'IPv6 Address' (empty), 'Link Local Address' (FE80::204:9AFF:FED8:9E7D), 'Default Gateway' (empty), and 'DNS Server' (empty). The '802.1X' section has a checkbox for 'Use 802.1X Security' (unchecked), a dropdown for 'Authentication' (MD5), and input fields for 'Username' and 'Password'.

Section	Option	Value
IP Configuration	<input checked="" type="radio"/> DHCP	
	<input type="radio"/> Static	
	IPv4 Address	192.168.1.104
	Subnet Mask	255.255.255.0
	Default Gateway	192.168.1.1
DNS Server	192.168.1.2	
IPv6 Configuration	<input type="radio"/> Automatic	
	<input checked="" type="radio"/> Static	
	IPv6 Address	
	Link Local Address	FE80::204:9AFF:FED8:9E7D
	Default Gateway	
DNS Server		
802.1X	<input type="checkbox"/> Use 802.1X Security	
	Authentication	MD5
	Username	
	Password	

PC0 : PC0 est un poste client utilisé pour tester la connectivité avec les serveurs et d'autres machines sur le réseau.

PC1

Physical Config Desktop Programming Attributes

IP Configuration

Interface FastEthernet0

IP Configuration

☒ DHCP ☐ Static

IPv4 Address 192.168.1.104

Subnet Mask 255.255.255.0

Default Gateway 192.168.1.1

DNS Server 192.168.1.2

IPv6 Configuration

☐ Automatic ☒ Static

IPv6 Address /

Link Local Address FE80::204:9AFF:FED8:9E7D

Default Gateway

DNS Server

802.1X

☐ Use 802.1X Security

Authentication MD5

Username

Password

PC1 : Similaire à PC0, il est utilisé pour vérifier les paramètres du réseau et évaluer les performances de la configuration.

PC2

Physical Config Desktop Programming Attributes

IP Configuration [X]

Interface FastEthernet0

IP Configuration

☒ DHCP ☐ Static DHCP request successful.

IPv4 Address 192.168.1.9

Subnet Mask 255.255.255.0

Default Gateway 192.168.1.1

DNS Server 192.168.1.2

IPv6 Configuration

☐ Automatic ☒ Static

IPv6 Address /

Link Local Address FE80::240:BFF:FE6B:B0A4

Default Gateway

DNS Server

802.1X

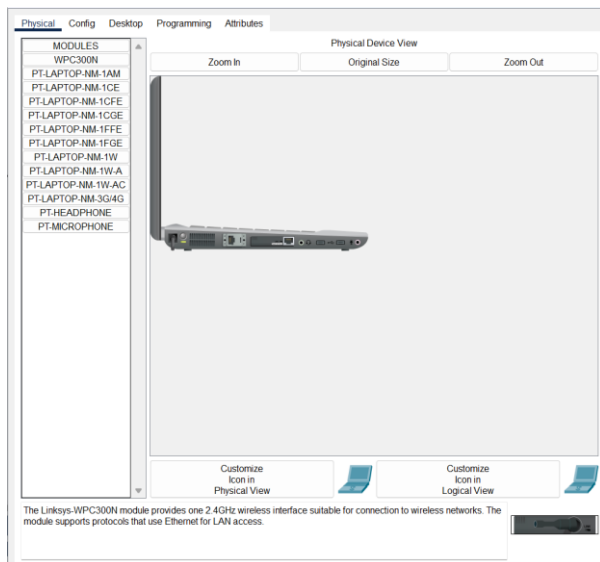
☐ Use 802.1X Security

Authentication MD5

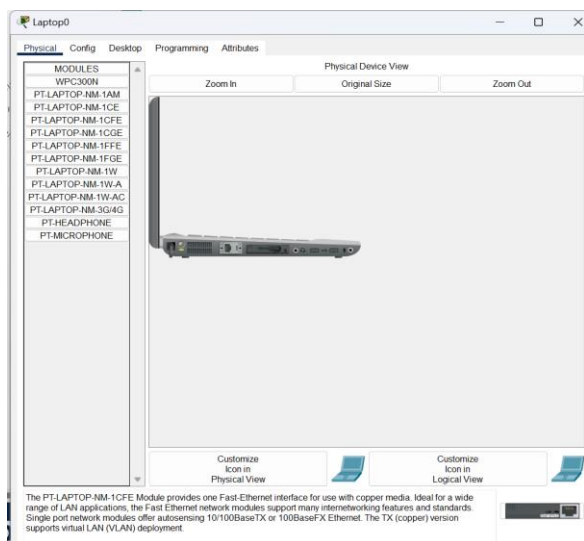
Username

Password

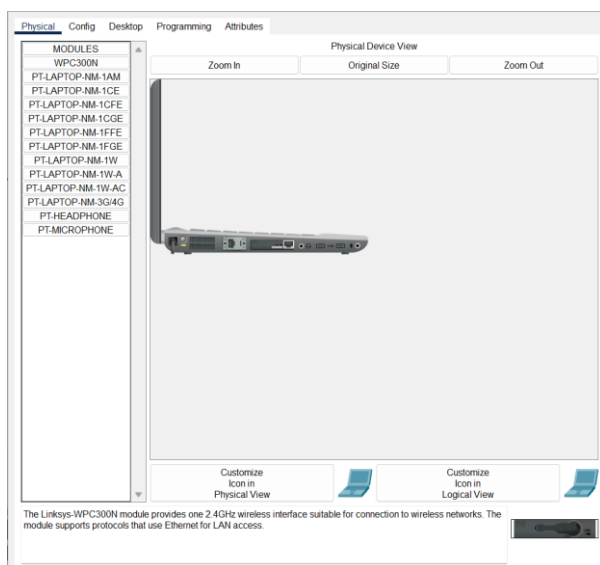
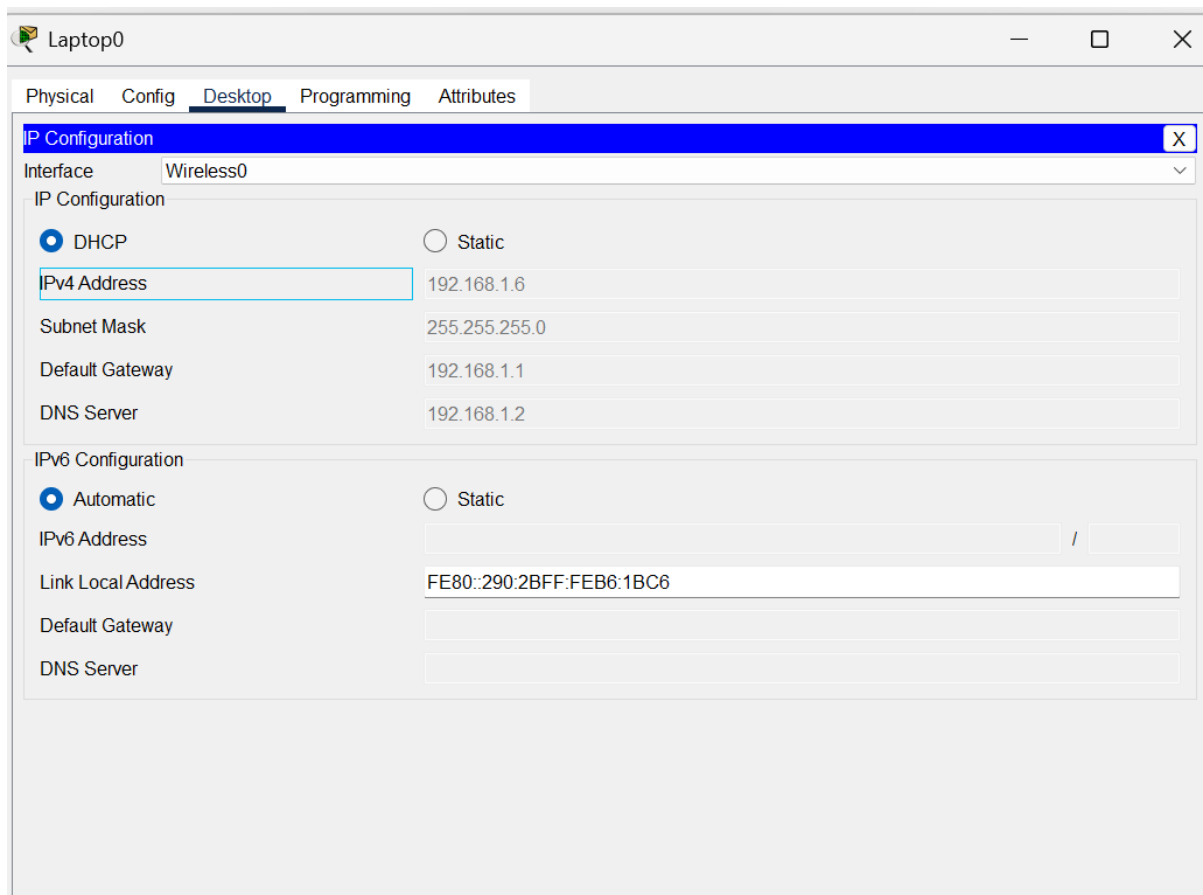
PC2 : Ce poste représente un utilisateur additionnel et permet de simuler une charge supplémentaire sur le réseau.



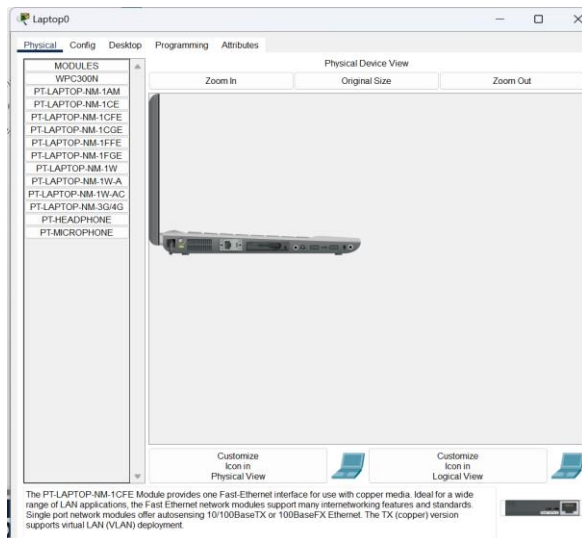
Laptop 0 : Laptop 0 est connecté via le port Wireless pour tester la configuration sans fil et comparer les performances par rapport à une connexion Ethernet.



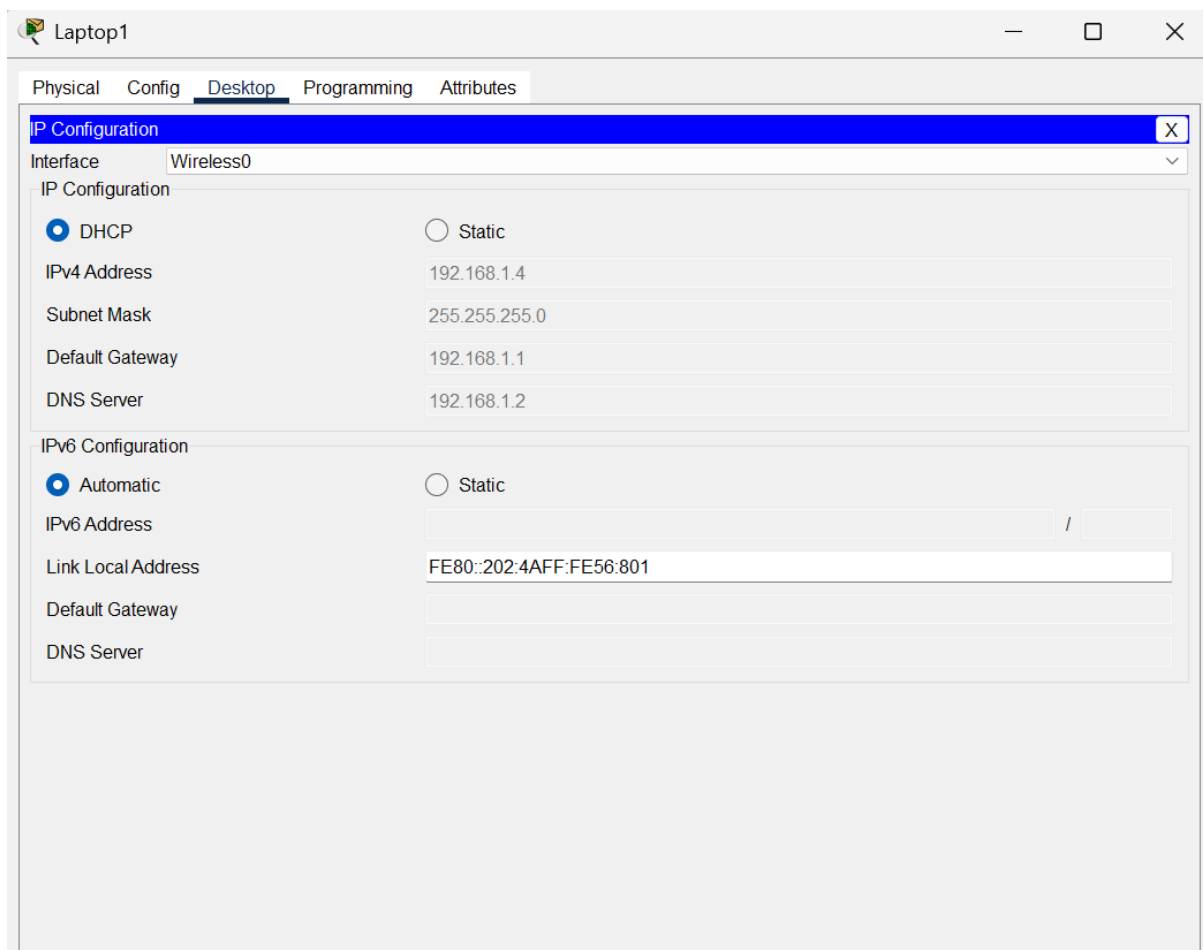
Changement du port Ethernet par le port Wireless



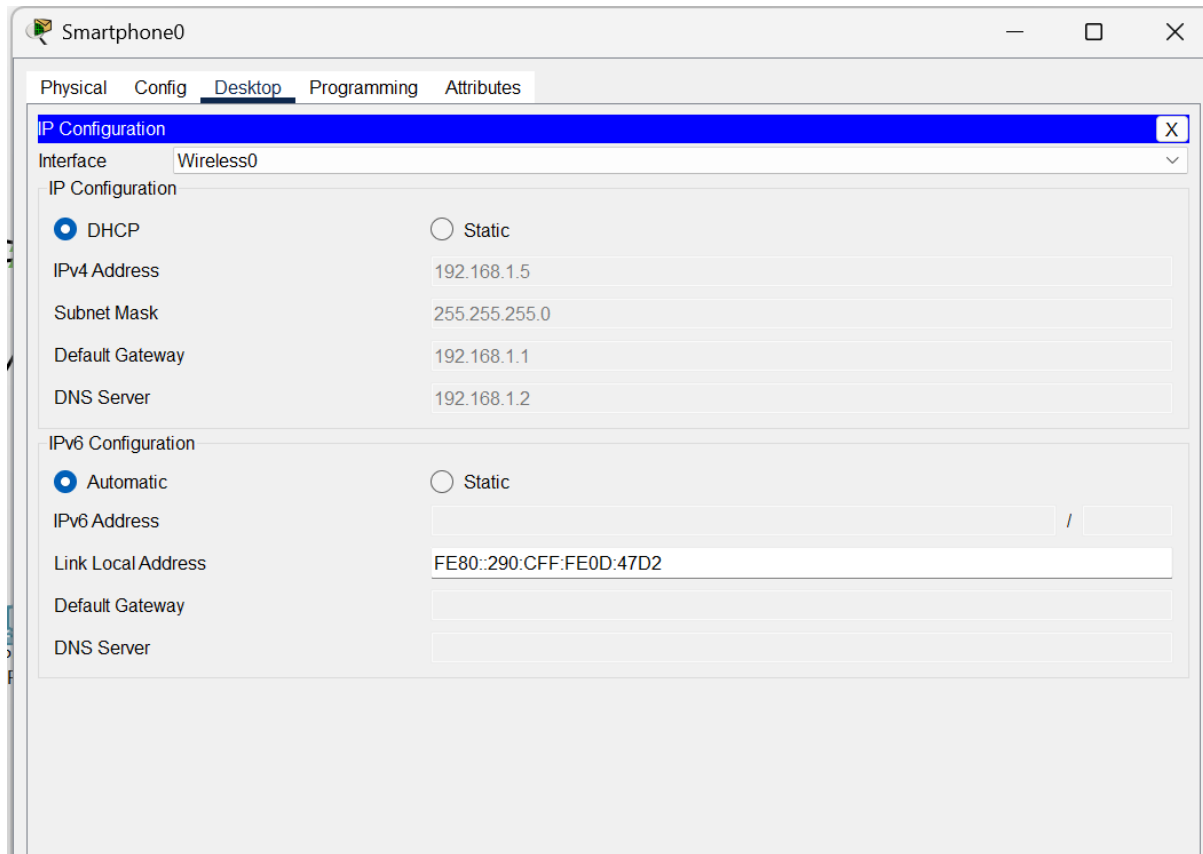
Laptop 1 : xplication : Tout comme Laptop 0, il permet d'évaluer la connectivité sans fil et de comparer les résultats avec d'autres appareils.



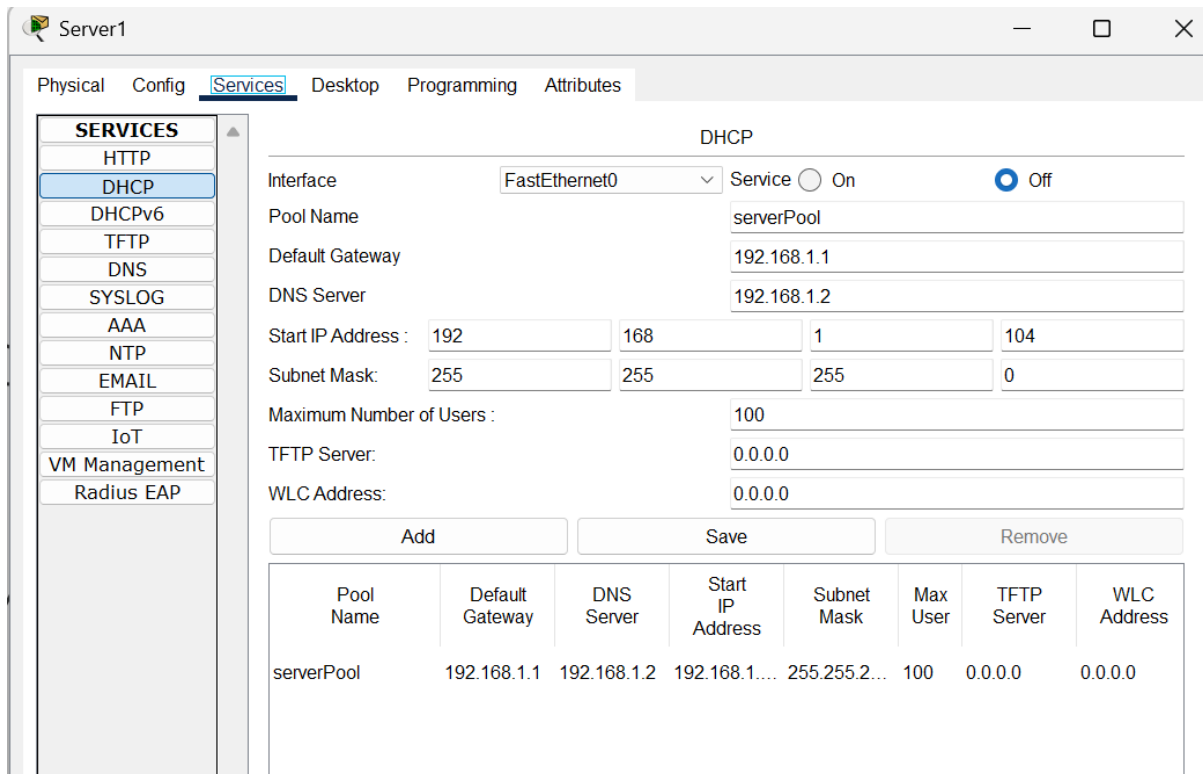
Cette expérience consiste à déconnecter un appareil d'une connexion filaire pour le connecter sans fil, permettant d'évaluer les performances et la stabilité de la connexion sans fil.



Smartphone0 : Smartphone0 est utilisé pour tester la compatibilité mobile du réseau et s'assurer que les services sont accessibles via des appareils portables.



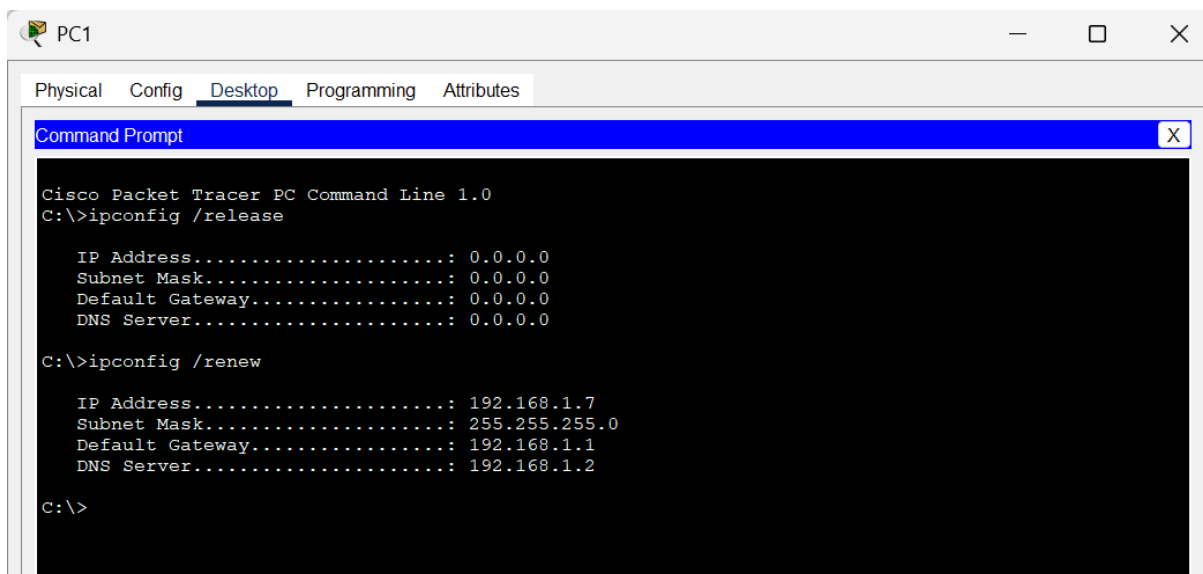
Smartphone0 : Smartphone0 est utilisé pour tester la compatibilité mobile du réseau et s'assurer que les services sont accessibles via des appareils portables.



On éteint le serveur 1

Cet exercice vise à tester la capacité du réseau à fonctionner avec un serveur principal inactif, en vérifiant si le serveur restant prend en charge les besoins du réseau.

PC1 :



PC1 est de nouveau évalué pour tester la connectivité et la réponse du réseau après avoir effectué des modifications (comme l'arrêt du serveur 1).

Conclusion :

En conclusion, ces travaux pratiques ont permis de tester et d'évaluer différents aspects de la configuration et de la gestion d'un réseau informatique. Nous avons pu observer les performances du réseau dans des scénarios variés, tels que l'utilisation de connexions filaires et sans fil, ainsi que la résilience en cas d'arrêt d'un serveur. Ces expériences fournissent une base solide pour comprendre les principes fondamentaux du fonctionnement des réseaux.
