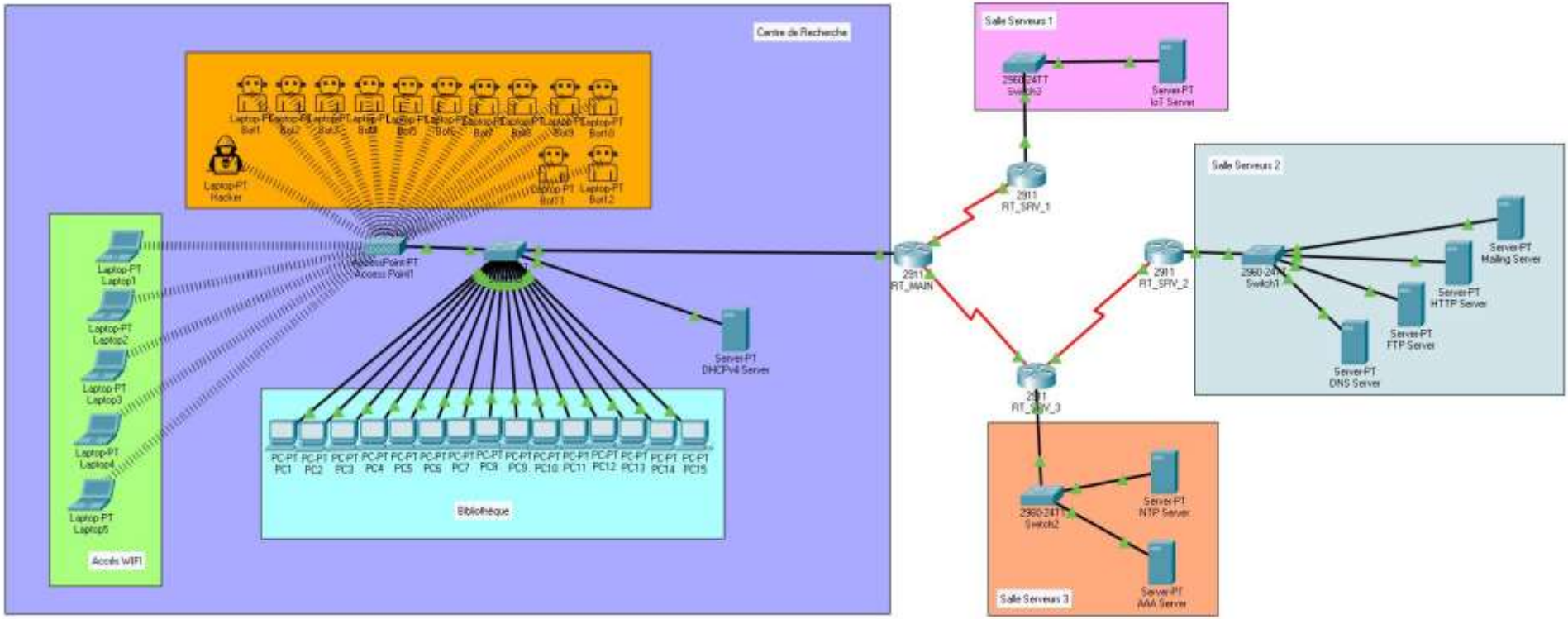

Centre de Recherche
Laptop-PT Hacker
Access Point-PT Access Point1
Laptop-PT Laptop1
Laptop-PT Laptop2
Laptop-PT Laptop3
Laptop-PT Laptop4
Laptop-PT Laptop5
Accès WIFI
Server-PT DHCPv6 Server
PC-PT PC1
PC-PT PC2
PC-PT PC3
PC-PT PC4
PC-PT PC5
PC-PT PC6
PC-PT PC7
PC-PT PC8
PC-PT PC9
PC-PT PC10
PC-PT PC11
PC-PT PC12
PC-PT PC13
PC-PT PC14
PC-PT PC15
Bibliothèque
Salle Serveurs 1
Server-PT IoT Server
2911 RT_SRV_1
2911 RT_MAIN
2911 RT_SRV_2
Salle Serveurs 2
Server-PT Mailing Server
Server-PT HTTP Server
Server-PT FTP Server
Server-PT DNS Server
Server-PT NTP Server
Server-PT AAA Server
Salle Serveurs 3

Observer

Nouvellement recruté, l'administrateur a décidé de cartographier les différents réseaux existants dans la topologie, pour que son plan de travail soit plus clair et exploitable pour d'éventuelles pannes réseau :

Les résultats obtenus par la commande « show ip interface brief » sur les différents routeurs sont les suivants :

Routeur « RT_MAIN »

```
RT_MAIN#show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
GigabitEthernet0/0     192.168.1.30    YES NVRAM  up                    up
GigabitEthernet0/1     unassigned      YES NVRAM  administratively down down
GigabitEthernet0/2     unassigned      YES NVRAM  administratively down down
Serial0/2/0            192.168.201.1   YES manual up                    up
Serial0/2/1            unassigned      YES unset  down                  down
Serial0/3/0            unassigned      YES NVRAM  administratively down down
Serial0/3/1            192.168.200.1   YES manual up                    up
Vlan1                  unassigned      YES unset  administratively down down
```

Routeur « RT_SRV1 »

```
RT_SRV_1#show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
GigabitEthernet0/0     192.168.50.6    YES manual up                    up
GigabitEthernet0/1     unassigned      YES unset  administratively down down
GigabitEthernet0/2     unassigned      YES unset  administratively down down
Serial0/2/0            unassigned      YES unset  administratively down down
Serial0/2/1            unassigned      YES unset  administratively down down
Serial0/3/0            192.168.200.2   YES manual up                    up
Serial0/3/1            unassigned      YES unset  administratively down down
Vlan1                  unassigned      YES unset  administratively down down
```

Routeur « RT_SRV2 »

```
RT_SRV_2#show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
GigabitEthernet0/0     192.168.100.6   YES NVRAM  up                    up
GigabitEthernet0/1     unassigned      YES NVRAM  administratively down down
GigabitEthernet0/2     unassigned      YES NVRAM  administratively down down
Serial0/2/0            unassigned      YES unset  down                  down
Serial0/2/1            unassigned      YES unset  down                  down
Serial0/3/0            unassigned      YES NVRAM  administratively down down
Serial0/3/1            192.168.202.2   YES manual up                    up
Vlan1                  unassigned      YES unset  administratively down down
```

Routeur « RT_SRV3 »

```
RT_SRV_3#show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
GigabitEthernet0/0     192.168.150.6   YES manual up                    up
GigabitEthernet0/1     unassigned      YES unset  administratively down down
GigabitEthernet0/2     unassigned      YES unset  administratively down down
Serial0/2/0            unassigned      YES unset  administratively down down
Serial0/2/1            unassigned      YES unset  administratively down down
Serial0/3/0            192.168.201.2   YES manual up                    up
Serial0/3/1            192.168.202.1   YES manual up                    up
Vlan1                  unassigned      YES unset  administratively down down
```

1- Remplir les deux tableaux ci-dessous avec les réseaux et leurs adresses correspondantes :

Réseau	Adresse Réseau	Masque CIDR	Adresse Passerelle
Centre de Recherche	192.168.1.0	/27	192.168.1.30
Salle Serveurs 1	192.168.50.0	/29	192.168.50.6
Salle Serveurs 2	192.168.100.0	/29	192.168.100.6
Salle Serveurs 3	192.168.150.0	/29	192.168.150.6

Réseau	Adresse Réseau	Masque CIDR	Routeur	Adresse Interface Réseau
RT_MAIN – RT_SRV1	192.168.200.0	/30	RT_MAIN	192.168.200.1
			RT_SRV1	192.168.200.2
RT_MAIN – RT_SRV3	192.168.101.0	/30	RT_MAIN	192.168.101.1
			RT_SRV3	192.168.201.2
RT_SRV2 – RT_SRV3	192.168.102.0	/30	RT_SRV2	192.168.202.1
			RT_SRV3	192.168.202.2

2- Utilisez la commande nécessaire pour vérifier s'il existe un réseau entre les deux équipements du tableau ci-dessous :

Equipement 1	Equipement 2	Oui/Non
NTP server	AAA server	Oui
PC1 Bibliothèque	PC9 Bibliothèque	Oui
DNS server	Iot server	Non
Laptop1	Laptop2	Non
Laptop3	PC4	Non
Laptop5	PC5	Non

3- Remplir les informations sur le Hacker :

IP v4 ou IP v6 ?	IPv4
IP adresse	192.168.1.28
Subnet Mask	255.255.255.224
Type de connection filaire ou wifi ?	wifi

4- Remplir les informations suivantes sur le serveur DHCP trouvé dans la bibliothèque :

Nom de la pool	Default Gateway	Le 1ere IP	Subnet Mask	Nombre maximum d'utilisateurs

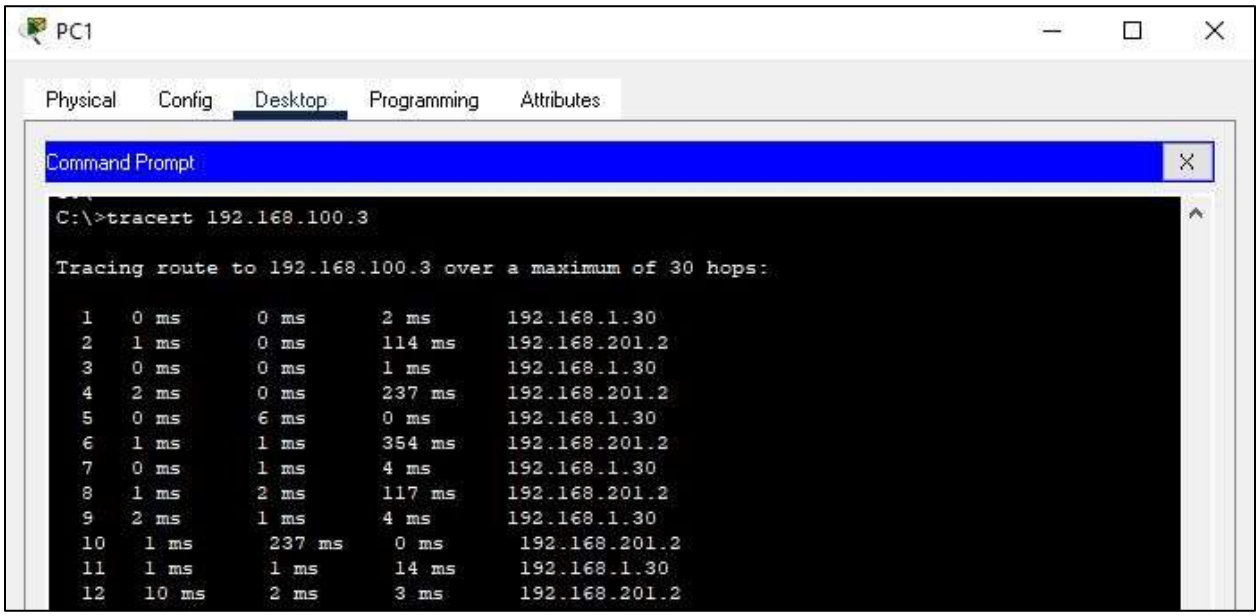
serverPool	192.168.1.30	192.168.1.16	255.255.255.224	13

Détecter et Agir

Le centre de recherche est composé de deux espaces, un dédié à la bibliothèque, un autre à l'accès Wifi. Les PCs de la bibliothèque sont configurés statiquement du .1 au .15, quant aux machines connectant au Wifi, se font attribuer dynamiquement une configuration réseau via le serveur DHCP du même réseau.

Partie 1 :

A un moment donné, Les PCs de la bibliothèque n'arrivent plus à accéder au serveur Web 192.168.100.3 de l'intranet, ni au serveur DNS 192.168.100.1, localisés dans la salle de serveurs 2. L'administrateur décide alors de lancer un tracert depuis le PC 1. Le résultat obtenu est ci-dessous :



1) D'où vient le problème ?

- ~~DNS mal configuré~~
- ~~Serveur Web inaccessible suite à un souci d'alimentation électrique.~~
- Problème de routage
- ~~Adressage mal configuré sur les routeurs~~
- ~~Interfaces réseau non allumées sur les routeurs~~

2) Très probablement un souci avec le routage ! les commandes « show ip route » sur les routeurs donnent les résultats suivant :

Routeur « RT_MAIN »

```
RT_MAIN#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.1.0/27 is directly connected, GigabitEthernet0/0
L       192.168.1.30/32 is directly connected, GigabitEthernet0/0
     192.168.50.0/29 is subnetted, 1 subnets
S       192.168.50.0/29 [1/0] via 192.168.200.2
     192.168.100.0/29 is subnetted, 1 subnets
S       192.168.100.0/29 [1/0] via 192.168.201.2
     192.168.150.0/29 is subnetted, 1 subnets
S       192.168.150.0/29 [1/0] via 192.168.201.2
     192.168.200.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.200.0/30 is directly connected, Serial0/3/1
L       192.168.200.1/32 is directly connected, Serial0/3/1
     192.168.201.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.201.0/30 is directly connected, Serial0/2/0
L       192.168.201.1/32 is directly connected, Serial0/2/0
     192.168.202.0/30 is subnetted, 1 subnets
S       192.168.202.0/30 [1/0] via 192.168.201.2
```

Routeur « RT_SRV1 »

```
RT_SRV_1#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     192.168.1.0/27 is subnetted, 1 subnets
S       192.168.1.0/27 [1/0] via 192.168.200.1
     192.168.50.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.50.0/29 is directly connected, GigabitEthernet0/0
L       192.168.50.6/32 is directly connected, GigabitEthernet0/0
     192.168.100.0/29 is subnetted, 1 subnets
S       192.168.100.0/29 [1/0] via 192.168.200.1
     192.168.150.0/29 is subnetted, 1 subnets
S       192.168.150.0/29 [1/0] via 192.168.200.1
     192.168.200.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.200.0/30 is directly connected, Serial0/3/0
L       192.168.200.2/32 is directly connected, Serial0/3/0
     192.168.201.0/30 is subnetted, 1 subnets
S       192.168.201.0/30 [1/0] via 192.168.200.1
     192.168.202.0/30 is subnetted, 1 subnets
S       192.168.202.0/30 [1/0] via 192.168.200.1
```

Routeur « RT_SRV2 »

```
RT_SRV_2#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     192.168.1.0/27 is subnetted, 1 subnets
S       192.168.1.0/27 [1/0] via 192.168.202.1
     192.168.50.0/29 is subnetted, 1 subnets
S       192.168.50.0/29 [1/0] via 192.168.202.1
     192.168.100.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.100.0/29 is directly connected, GigabitEthernet0/0
L       192.168.100.6/32 is directly connected, GigabitEthernet0/0
     192.168.150.0/29 is subnetted, 1 subnets
S       192.168.150.0/29 [1/0] via 192.168.202.1
     192.168.200.0/30 is subnetted, 1 subnets
S       192.168.200.0/30 [1/0] via 192.168.202.1
     192.168.201.0/30 is subnetted, 1 subnets
S       192.168.201.0/30 [1/0] via 192.168.202.1
     192.168.202.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.202.0/30 is directly connected, Serial0/3/1
L       192.168.202.2/32 is directly connected, Serial0/3/1
```

Routeur « RT_SRV3 »

```
RT_SRV_3#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     192.168.1.0/27 is subnetted, 1 subnets
S       192.168.1.0/27 [1/0] via 192.168.201.1
     192.168.10.0/29 is subnetted, 1 subnets
S       192.168.10.0/29 [1/0] via 192.168.202.2
     192.168.50.0/29 is subnetted, 1 subnets
S       192.168.50.0/29 [1/0] via 192.168.201.1
     192.168.100.0/29 is subnetted, 1 subnets
S       192.168.100.0/29 [1/0] via 192.168.201.1
     192.168.150.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.150.0/29 is directly connected, GigabitEthernet0/0
L       192.168.150.6/32 is directly connected, GigabitEthernet0/0
     192.168.200.0/30 is subnetted, 1 subnets
S       192.168.200.0/30 [1/0] via 192.168.201.1
     192.168.201.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.201.0/30 is directly connected, Serial0/3/0
L       192.168.201.2/32 is directly connected, Serial0/3/0
     192.168.202.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.202.0/30 is directly connected, Serial0/3/1
L       192.168.202.1/32 is directly connected, Serial0/3/1
```

Sur quel routeur le problème réside ?

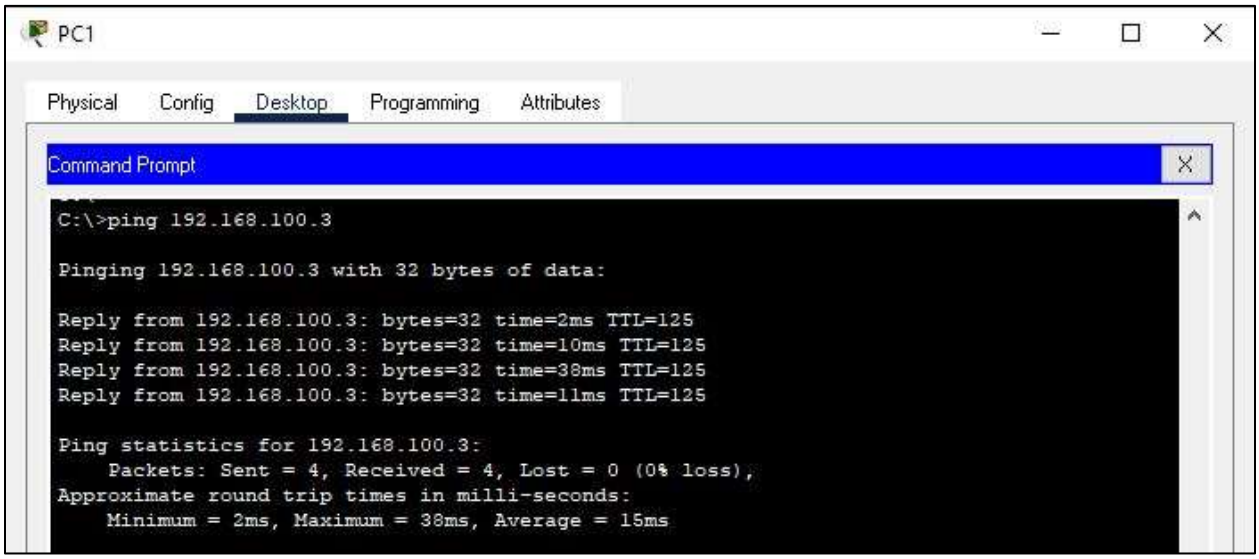
- RT_MAIN
- RT_SRV1
- RT_SRV2
- RT_SRV3

3) Quelle suite de configurations pourrait résoudre les soucis de routage ?

……

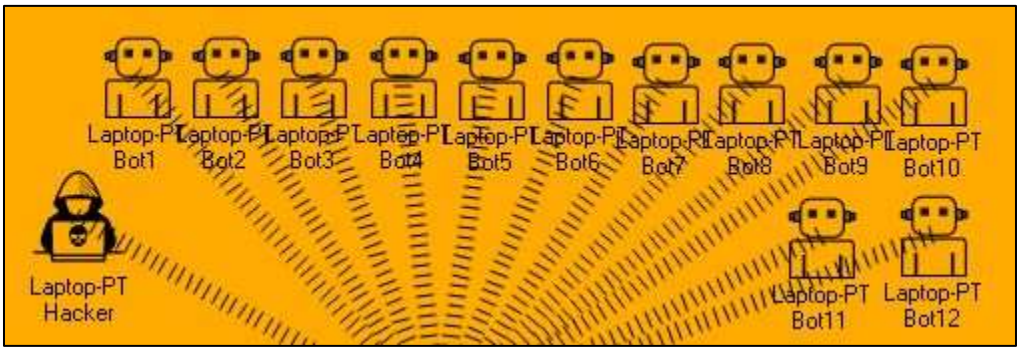
……

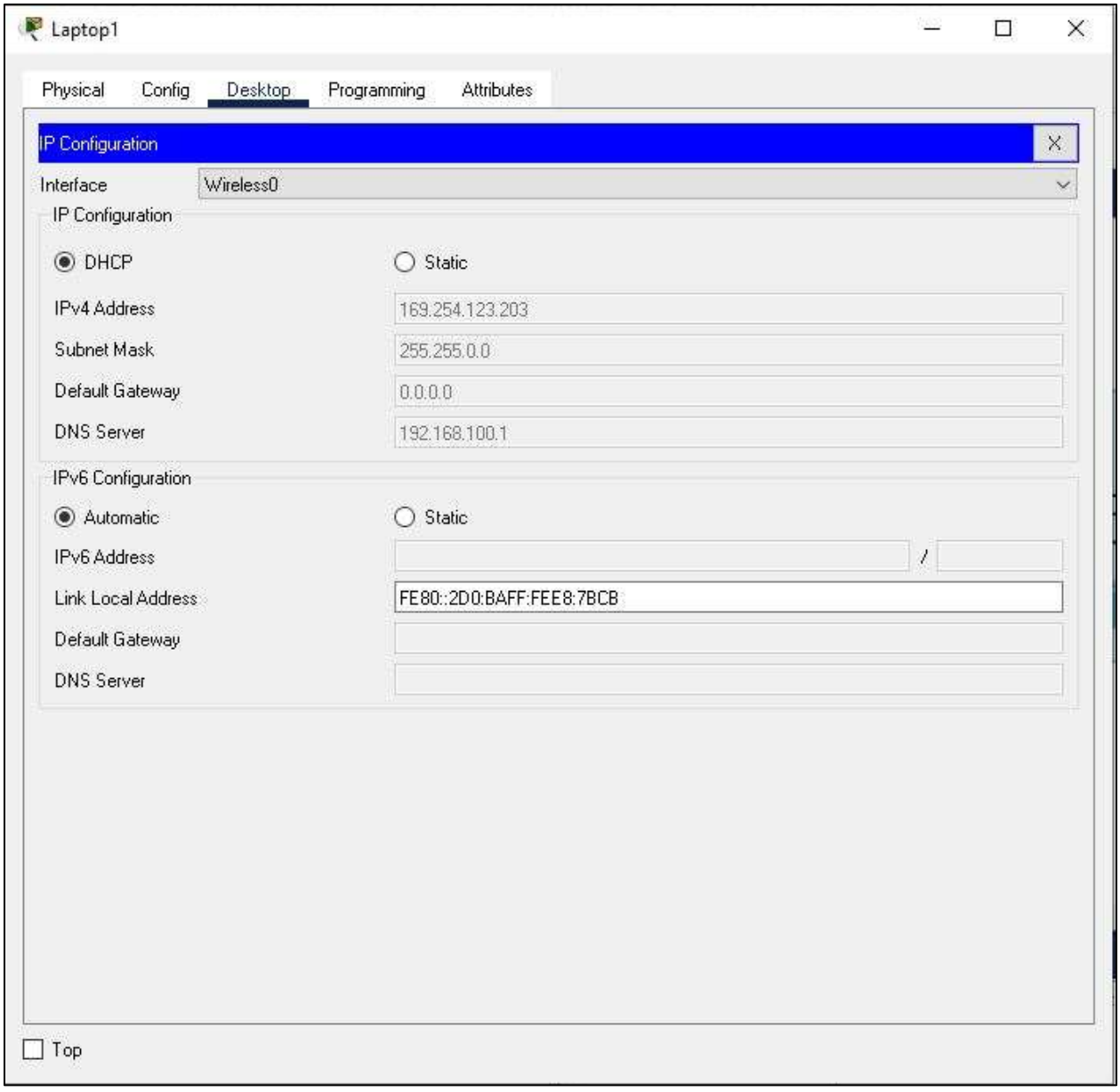
Bravo ! les PC du centre de recherche peuvent communiquer maintenant avec le serveur Web



Partie 2:

Un Hacker a pu s'introduire au réseau du centre de recherche via l'accès wifi. Il enchaine une attaque appelée « DHCP Starvation », en générant des Bots avec des interfaces réseau virtuelles configurées avec les adresses restantes du pool, configuré sur le serveur DHCP. Aucun accès n'est disponible sur la Wifi maintenant, il faut agir rapidement.





Très rapidement, l'administrateur décide d'autoconfigurer le réseau du centre de recherche en IPv6 via le routeur « RT_MAIN » (EUI-64 stateless autoconfiguration), et cela temporairement pour faire face à la capacité maximale du hacker à générer des bots, et garantir une disponibilité de services immédiate.

1) Quelles sont les configurations à réaliser sur le routeur principal « RT_MAIN » ainsi que son interface GigabitEthernet 0/0 pour attribuer automatiquement des adresses IPv6 en EUI-64 aux machines du centre de recherche ?

(Remarque : le préfixe EUI-64 utilisé est : 2001 ::/64)

Sur le routeur :

RT_MAIN(config)# _____

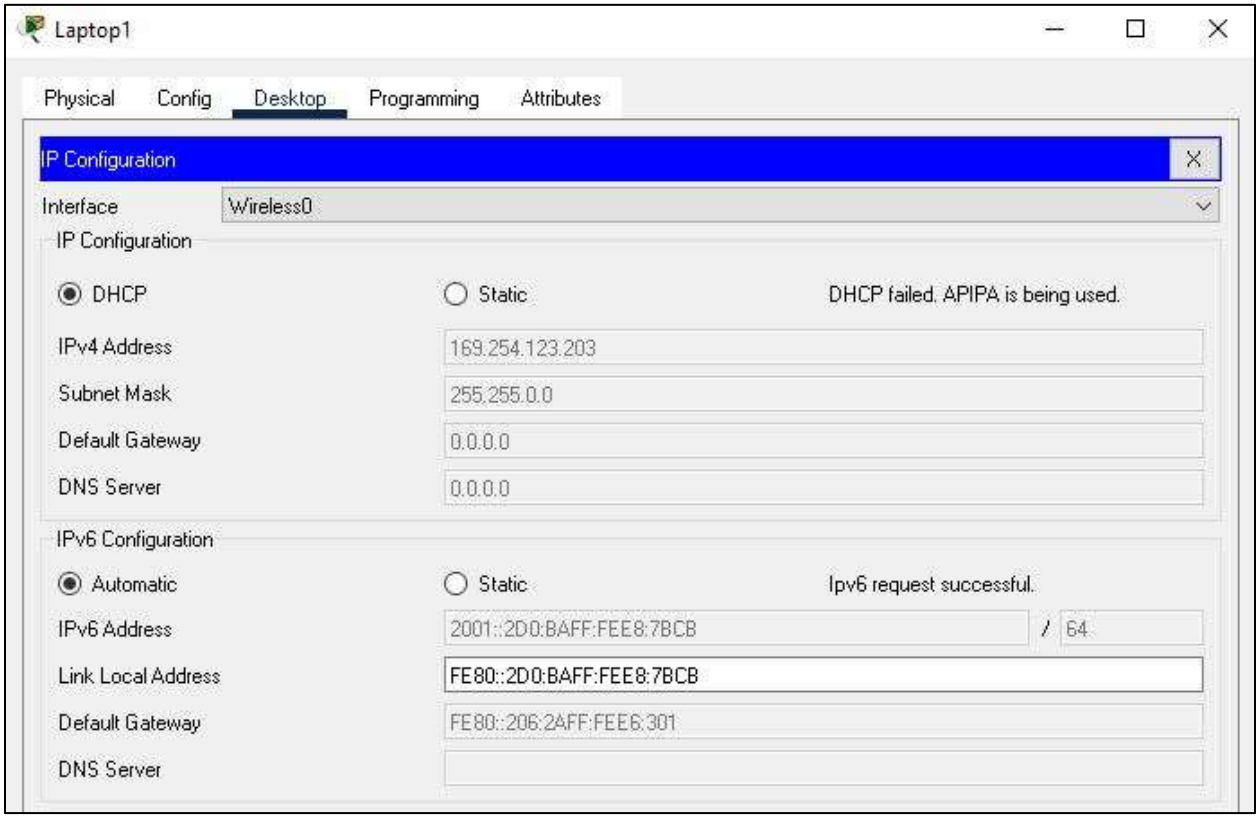
Sur l'interface GigabitEthernet 0/0 :

RT_MAIN(config-if)#_____

RT_MAIN(config-if)#_____

RT_MAIN(config-if)#_____

Excellent ! les laptops arrivent à obtenir une adresses IPv6 depuis le routeur « RT_MAIN ».



2) Nous sommes face à un autre souci. Tous les autres réseaux sont en IPv4, il faut que les machines du centre de recherche adressées maintenant en IPv6 puissent communiquer avec les serveurs de la salle 2, adressés en IPv4. Le NAT-PT permet de faire cette translation. En se basant sur le manuel fourni ci-dessous, compléter la configuration à déployer sur le routeur « RT_MAIN ».

Manuel d'utilisation :

1 - Sur le routeur :

Router(config)# ipv6 nat v6v4 source list {nom_acl} pool {nom_pool_ipv4}

Router(config)# ipv6 nat v6v4 pool {nom_pool_ipv4} {première_adresse} {dernière_adresse} prefix-length {masque_CIDR}

Router(config)# ipv6 nat prefix {prefixe_attribué_aux_adresses_IPv4}

Router(config)# ipv6 access-list {nom_acl}

Router(config-ipv6-acl)# permit ipv6 {reseau_IPv6} { prefixe_attribué_aux_adresses_IPv4}

2- Sur l'interface face au réseau IPv6 :

Router(config-if)# ipv6 nat

Router(config-if)# ipv6 nat prefix { prefixe_attribué_aux_adresses_IPv4} v4-mapped {nom_acl}

3- Sur l'interface face au réseau IPv4 :

Router(config-if)# ipv6 nat

En attribuant les dénominations suivantes, compléter les champs vides pour obtenir la configuration finale :

{nom_acl} = v4mapacl

{nom_pool_ipv4} = v4pool

{prefixe_attribué_aux_adresses_IPv4} = 2002::/96

1 - Sur le routeur « RT_MAIN » :

Router(config)# ipv6 nat v6v4 source list **v4mapacl** pool **v4pool**

Router(config)# ipv6 nat v6v4 pool **v4pool** _____ _____ prefix-length _____

Router(config)# ipv6 nat prefix **2002::/96**

Router(config)# ipv6 access-list **v4mapacl**

Router(config-ipv6-acl)# permit ipv6 _____ **2002::/96**

2- Sur l'interface GigabitEthernet 0/0

Router(config-if)# ipv6 nat

Router(config-if)# ipv6 nat prefix **2002::/96** v4-mapped **v4mapacl**

3- Sur l'interface Serial 0/2/0

Router(config-if)# ipv6 nat