

RAPPORT TP3 : VPN



SENECHAL Morgan

SAVORY Edwin

SEBBANE Ryan

PIMENTA SILVA Lionel

Professeur : AHMADI Laifa

Module : TI630

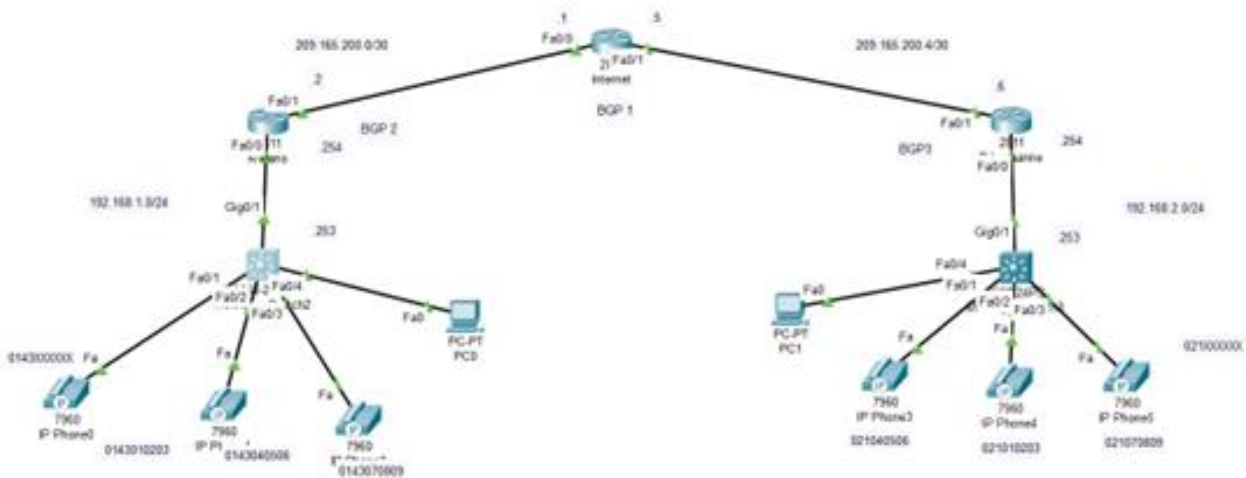
Introduction

Le réseau privé virtuel (VPN) est un type de réseau informatique qui permet à des utilisateurs distants de se connecter à un réseau privé via une connexion Internet publique. Cisco Packet Tracer est un outil de simulation de réseau qui permet de créer et de configurer des réseaux informatiques.

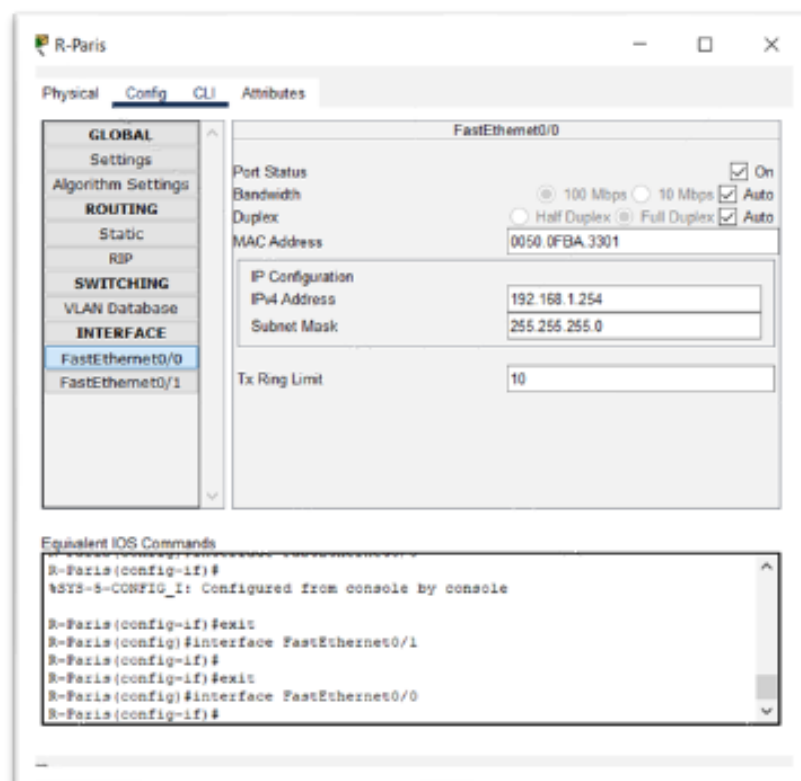
Ce TP a pour but de nous faire comprendre le fonctionnement d'un VPN en passant par sa création à l'aide de Cisco Packet Tracer afin de saisir les concepts de base des VPN et de se familiariser avec les outils nécessaires à leur création.

Ainsi, nous allons donc voir les différents paramètres réseaux et sécurité que nous avons fait pour élaborer notre VPN.

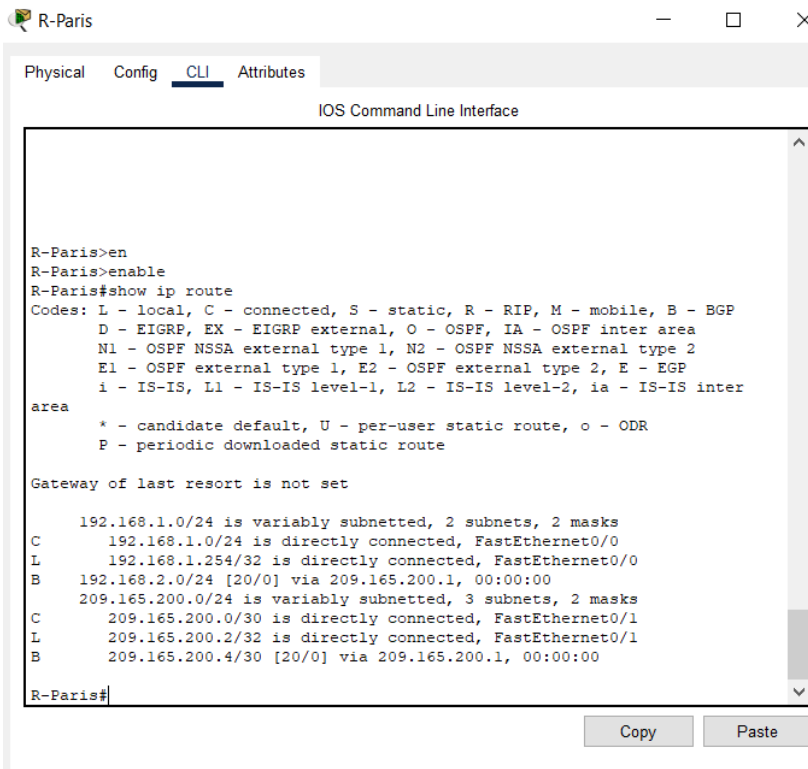
Réalisation TP3



Ici nous avons une capture d'écran du circuit où l'on va configurer le VPN. Nous avons premièrement pris 2 switch 3560, 3 routeurs et des téléphones IP qui vont être utilisés pour passer des coups de fils d'un réseau à un autre réseau. Ici dans ce cas de figure nous avons une entreprise qui possède un siège en Lausanne et un autre à Paris et l'on aimerait configurer les téléphones IP de tel sorte qu'ils puissent communiquer. Nous allons ainsi configurer les adresses des différents réseaux et les Gateway des routeurs afin de pouvoir créer plus tard les routes IP.



IP route sur le routeur de Paris :



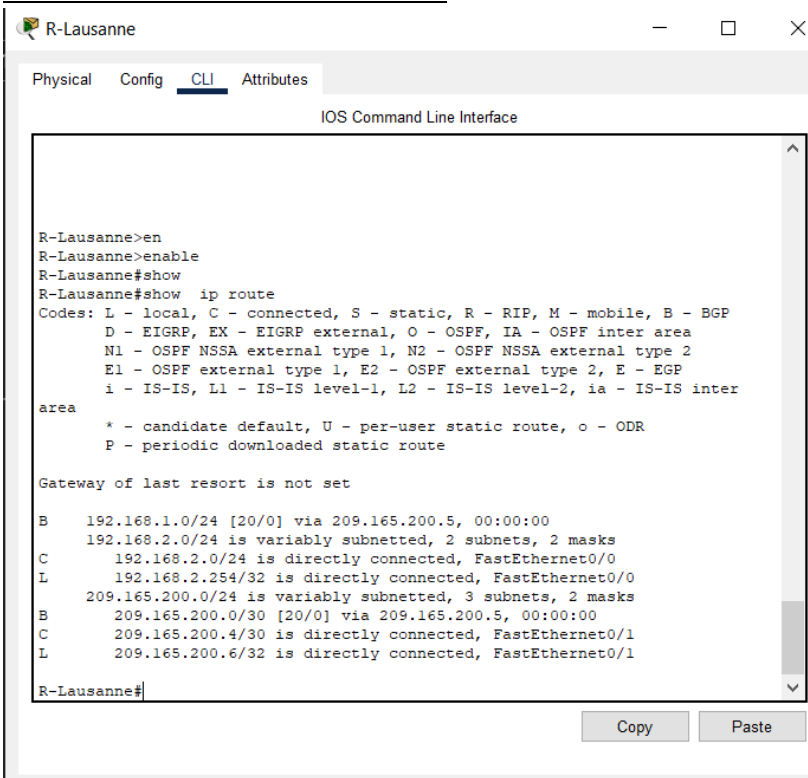
The screenshot shows the CLI of the R-Paris router. The user has entered 'en' to enter enable mode and 'show ip route' to display the routing table. The output lists several routes, including 192.168.1.0/24, 192.168.1.254/32, 192.168.2.0/24, and 209.165.200.0/24, along with their respective interfaces and metrics. The CLI also displays a legend for route codes and a message about the gateway of last resort.

```
R-Paris>en
R-Paris>enable
R-Paris#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       192.168.1.0/24 is directly connected, FastEthernet0/0
L       192.168.1.254/32 is directly connected, FastEthernet0/0
B       192.168.2.0/24 [20/0] via 209.165.200.1, 00:00:00
      209.165.200.0/24 is variably subnetted, 3 subnets, 2 masks
C       209.165.200.0/30 is directly connected, FastEthernet0/1
L       209.165.200.2/32 is directly connected, FastEthernet0/1
B       209.165.200.4/30 [20/0] via 209.165.200.1, 00:00:00
R-Paris#
```

IP route sur le routeur de Lausanne :

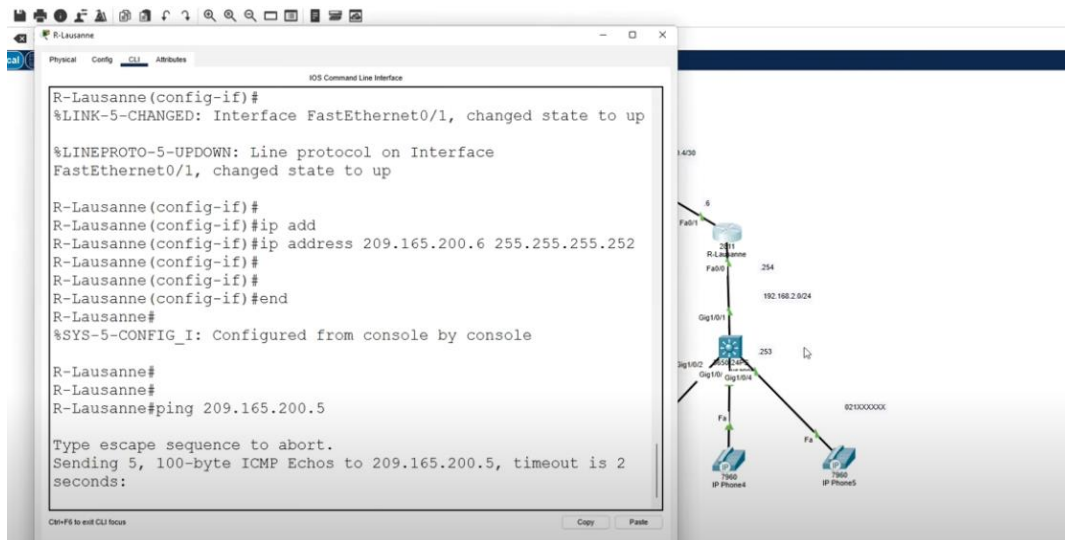


The screenshot shows the CLI of the R-Lausanne router. The user has entered 'en' to enter enable mode and 'show ip route' to display the routing table. The output lists several routes, including 192.168.1.0/24, 192.168.2.0/24, 192.168.2.254/32, and 209.165.200.0/24, along with their respective interfaces and metrics. The CLI also displays a legend for route codes and a message about the gateway of last resort.

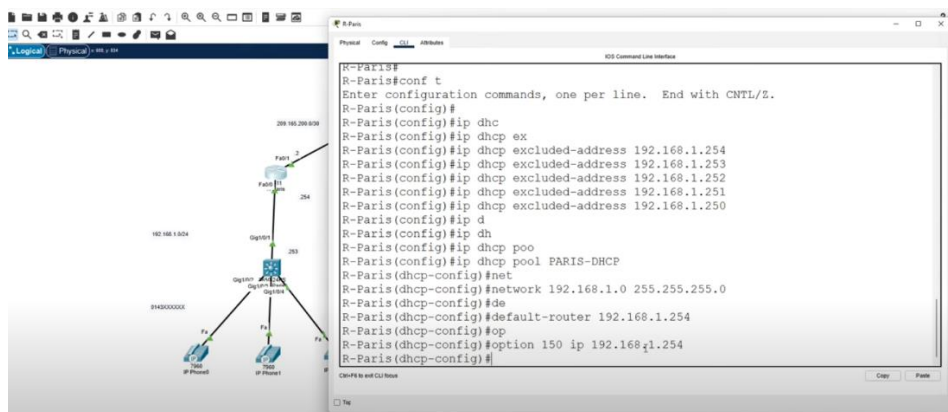
```
R-Lausanne>en
R-Lausanne>enable
R-Lausanne#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external 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

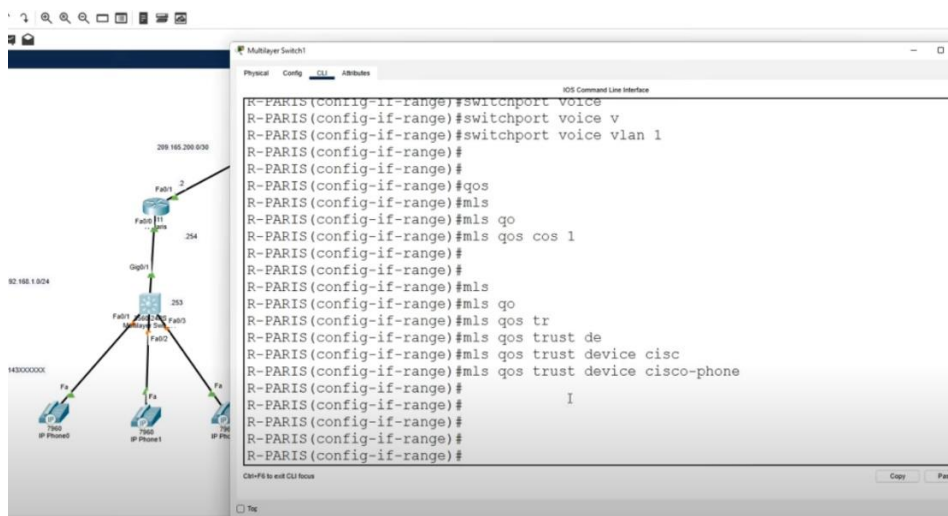
B       192.168.1.0/24 [20/0] via 209.165.200.5, 00:00:00
      192.168.2.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.2.0/24 is directly connected, FastEthernet0/0
L       192.168.2.254/32 is directly connected, FastEthernet0/0
      209.165.200.0/24 is variably subnetted, 3 subnets, 2 masks
B       209.165.200.0/30 [20/0] via 209.165.200.5, 00:00:00
C       209.165.200.4/30 is directly connected, FastEthernet0/1
L       209.165.200.6/32 is directly connected, FastEthernet0/1
R-Lausanne#
```

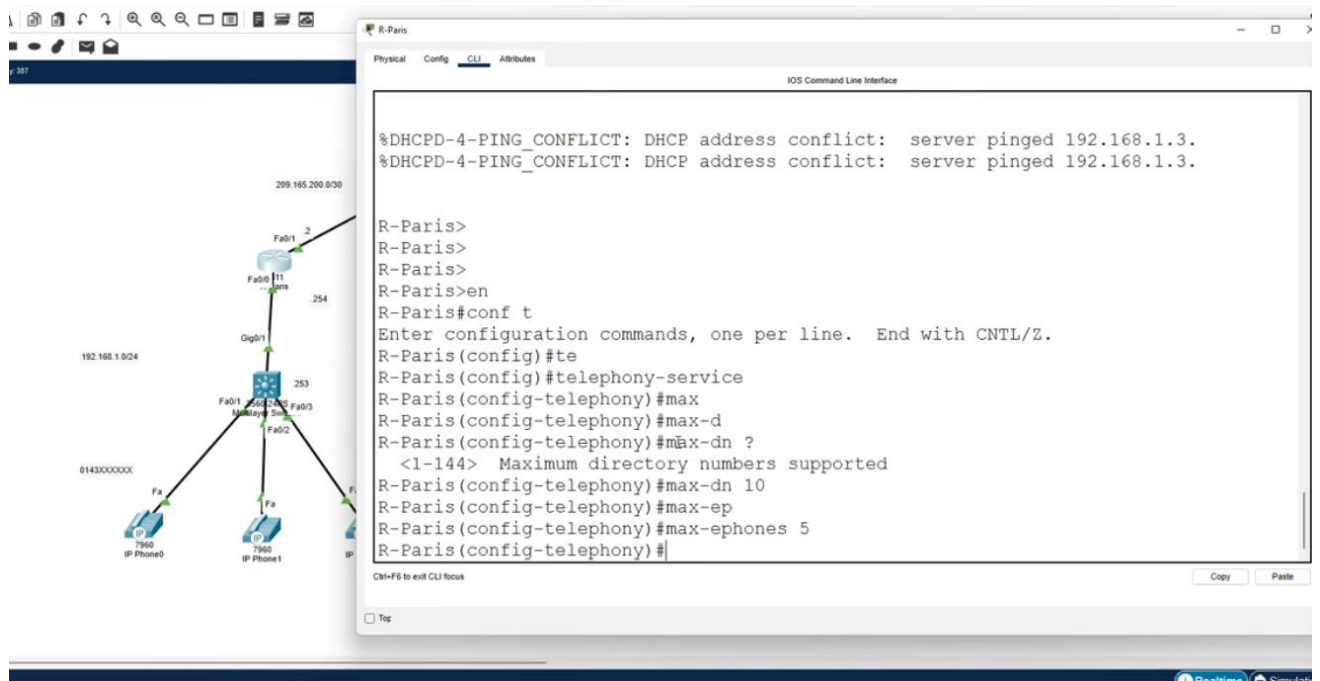
Ensuite nous avons configuré les adresses IP des téléphones en DHCP comme ça leur IP sont automatiquement attribuées lors du démarrage de Cisco. Le DHCP est pratique lorsque le réseau est composé de nombreux end devices. En effet cela nous évite de configurer manuellement 1 par 1 les IP des différents hosts et ainsi de gagner du temps dans la configuration.



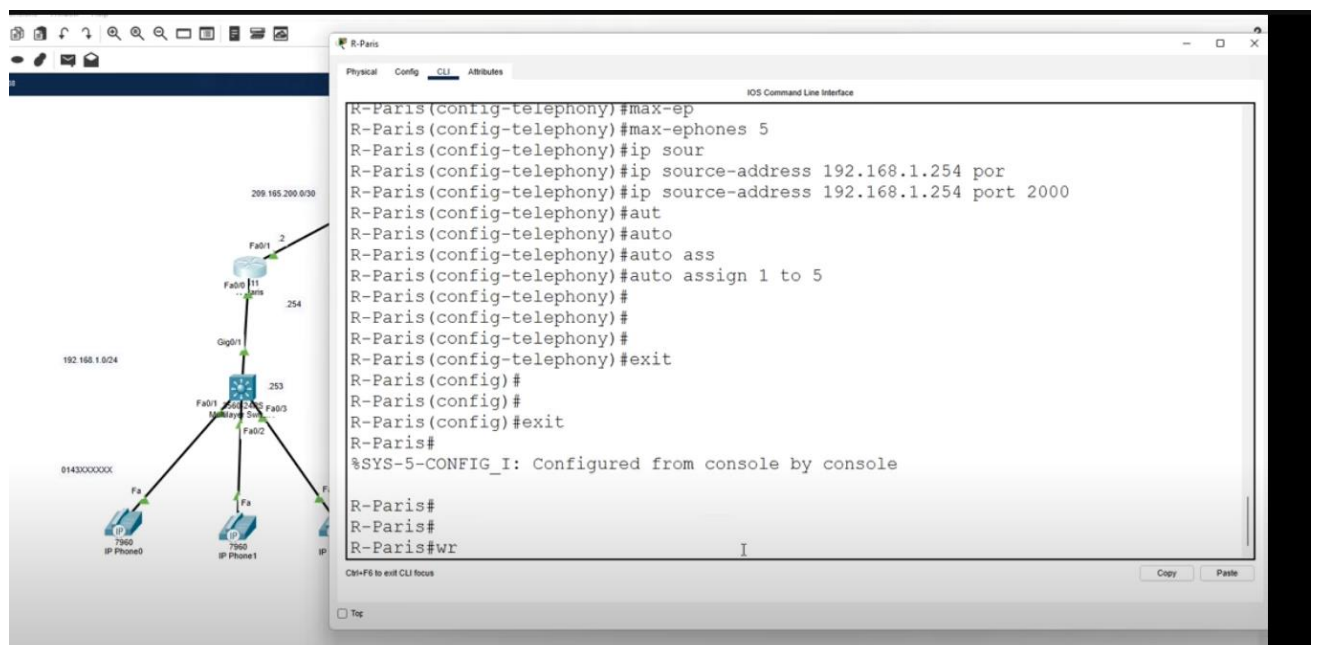
Nous avons ensuite fait la même sur le routeur de Lausanne pour configurer le DHCP.



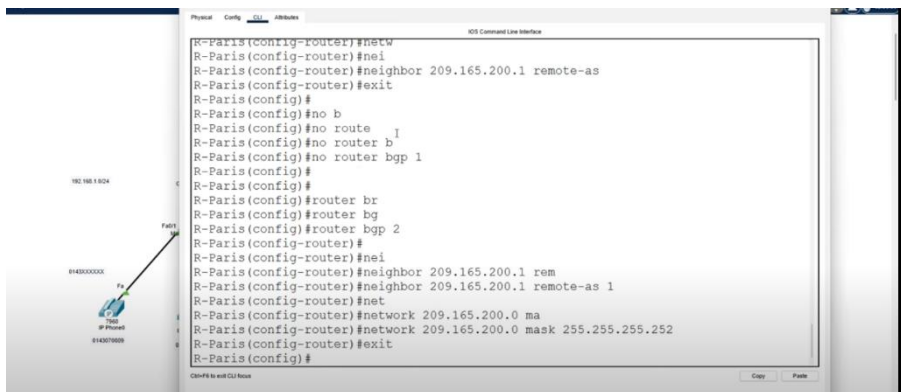
Ensuite sur le switch nous avons configuré la quality of service ainsi les switch trust les téléphones cisco IP pour leur donner une bande passante suffisante.



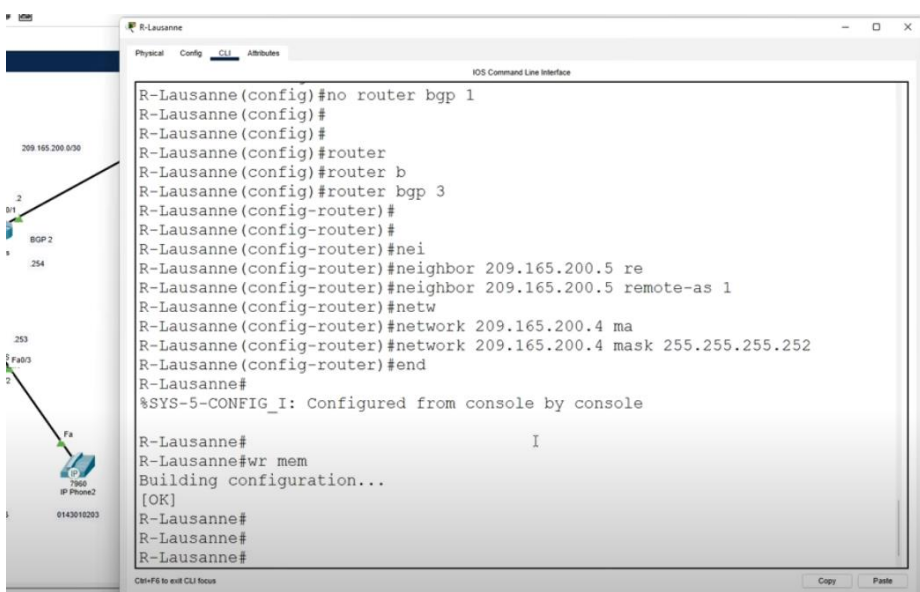
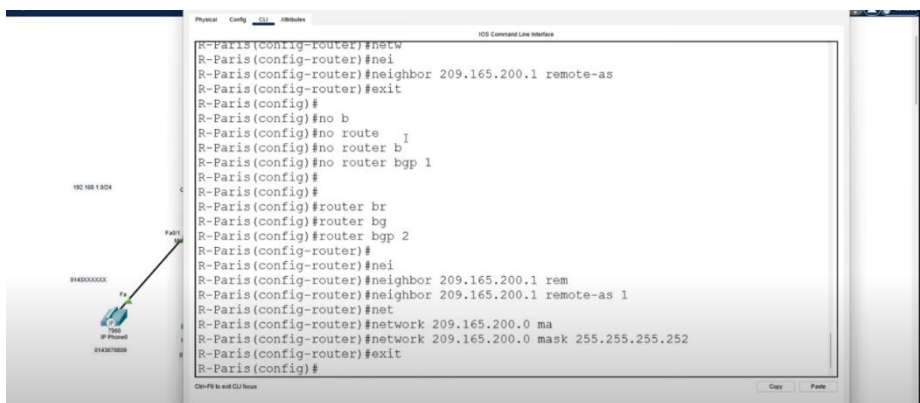
Sur le routeur nous avons pu attribuer 5 places pour des téléphones ip. De plus chacun peut avoir 2 numéros car 10 numéros sont disponibles.

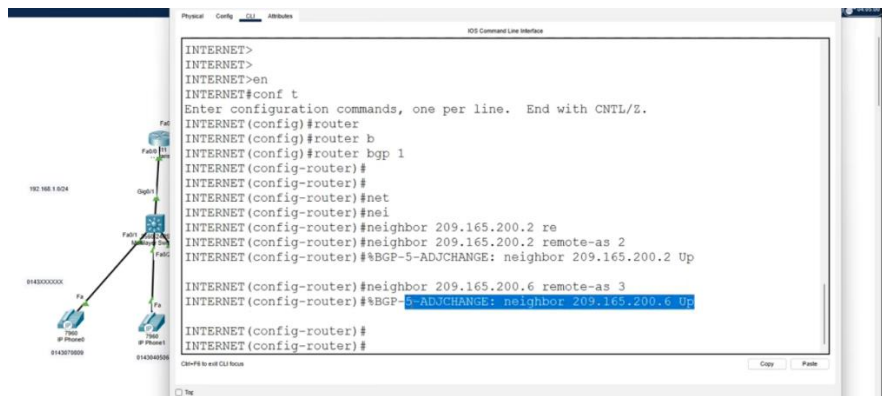


On attribue automatiquement les numéros de téléphones aux téléphones IP.

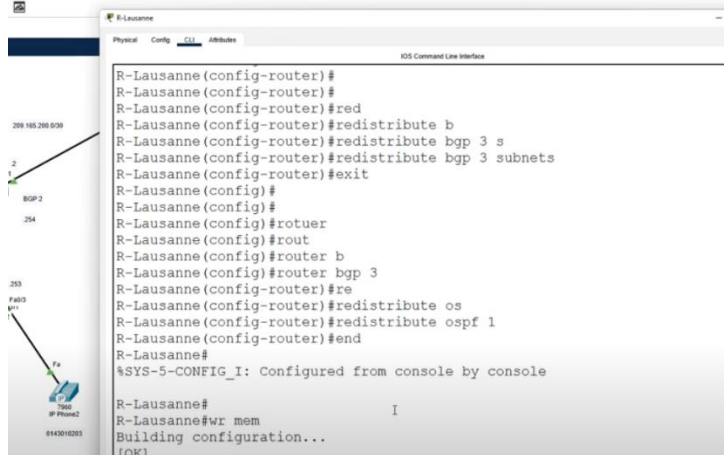
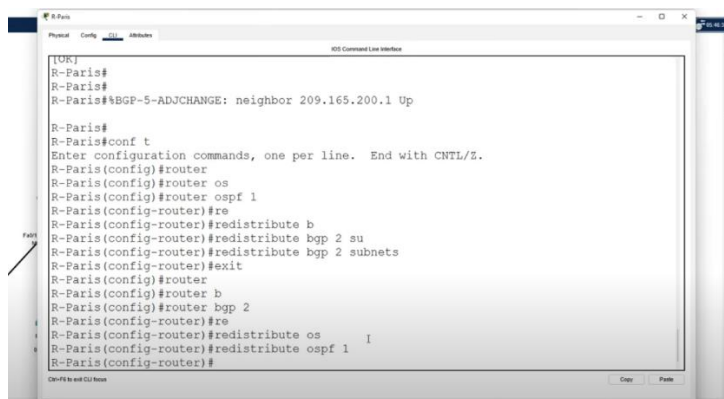
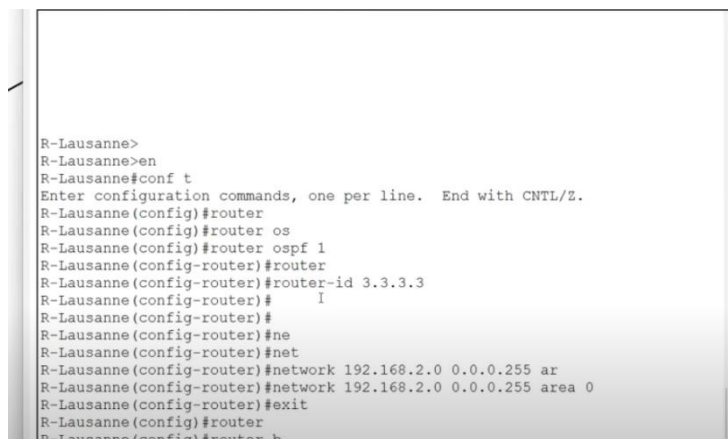


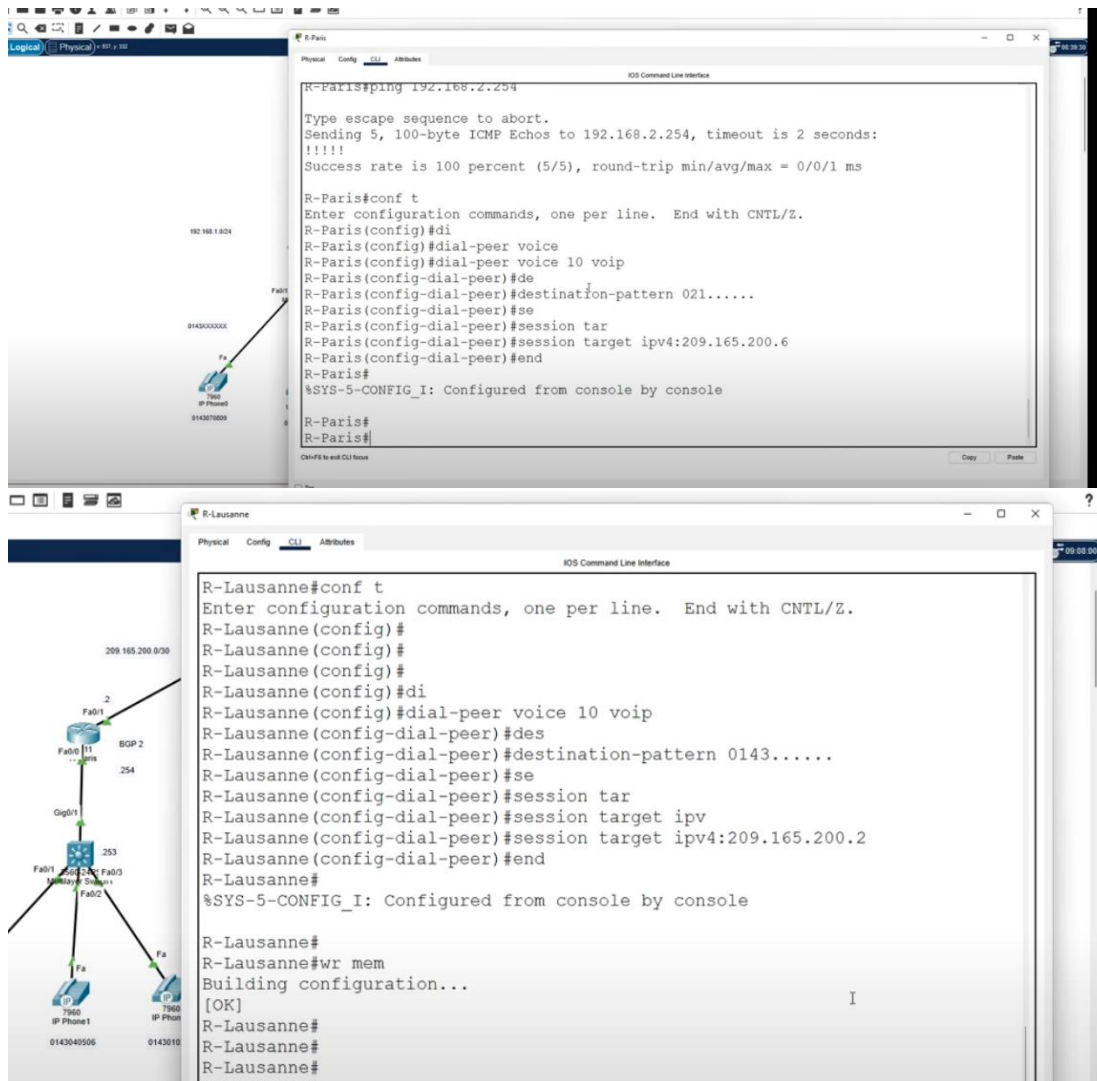
Enfin pour pouvoir appeler de Lausanne à Paris et inversement nous devons configurer une route dynamique entre Paris et Lausanne. Pour cela on utilise bgp et ospf pour créer un routing dynamique entre les différents réseaux. Premièrement on fait le bgp sur les routeurs :



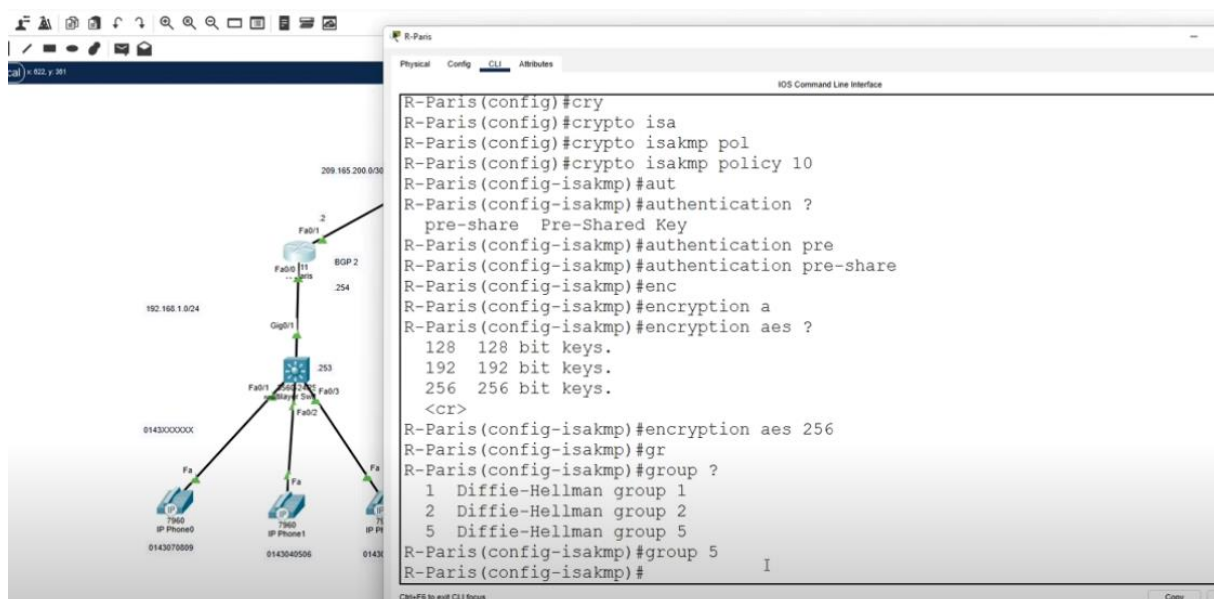


Puis on fait le ospf : Sur Lausanne et Paris.

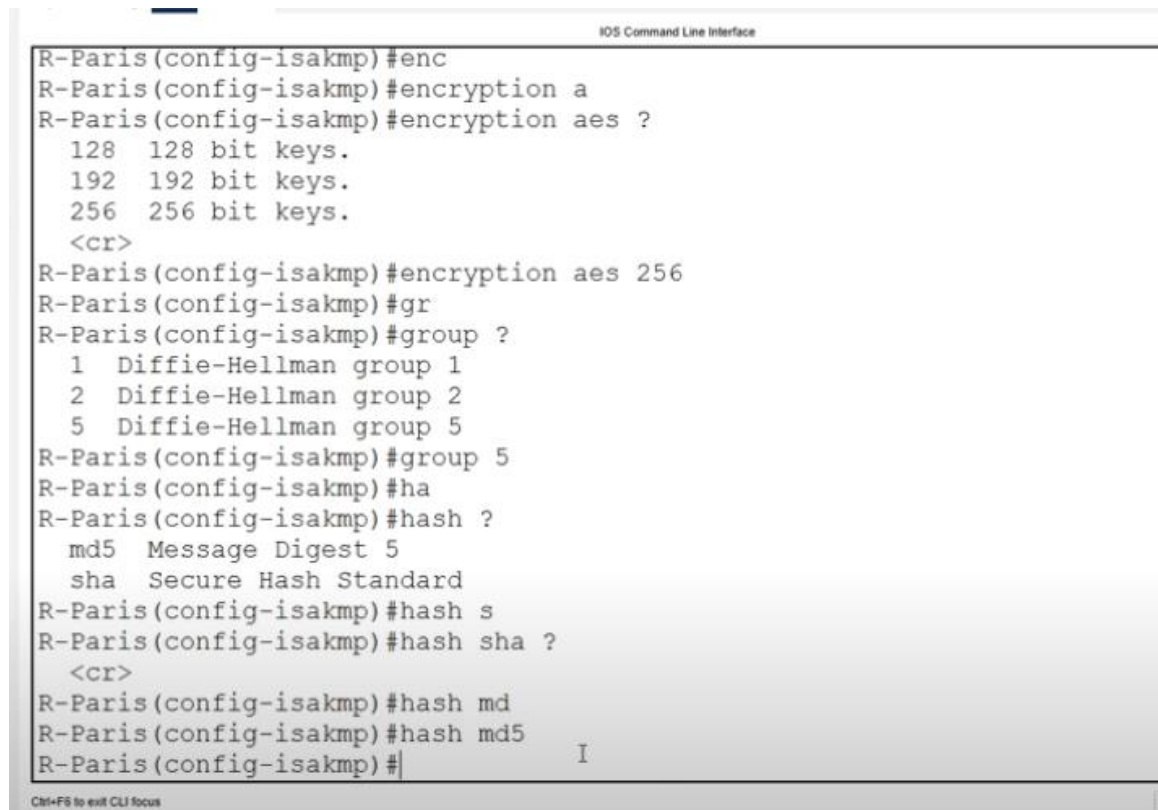




Puis on va créer le tunnel VPN et on va le configurer :



Ici nous commençons à configurer le protocole VPN utilisé sur le routeur et le chiffrement. Ici nous avons mis pre share qui consiste à partager un tunnel VPN avec seulement les routeurs qui connaissent la clé de chiffrement car cela est forcément la même personne qui a créé la clé qui va la partager.



```
R-Paris(config-isakmp)#enc
R-Paris(config-isakmp)#encryption a
R-Paris(config-isakmp)#encryption aes ?
  128 128 bit keys.
  192 192 bit keys.
  256 256 bit keys.
<cr>
R-Paris(config-isakmp)#encryption aes 256
R-Paris(config-isakmp)#gr
R-Paris(config-isakmp)#group ?
  1 Diffie-Hellman group 1
  2 Diffie-Hellman group 2
  5 Diffie-Hellman group 5
R-Paris(config-isakmp)#group 5
R-Paris(config-isakmp)#ha
R-Paris(config-isakmp)#hash ?
  md5 Message Digest 5
  sha Secure Hash Standard
R-Paris(config-isakmp)#hash s
R-Paris(config-isakmp)#hash sha ?
<cr>
R-Paris(config-isakmp)#hash md
R-Paris(config-isakmp)#hash md5
R-Paris(config-isakmp)#
```

Puis on applique du hash pour crypter les données que l'on a préalablement mis sur le groupe 5 de Diffie Hellman. Cela est pour éviter l'attaque du Man in the middle.

```
R-Paris(config)#crypt
R-Paris(config)#crypto isa
R-Paris(config)#crypto isakmp key oKiTasouji-cisc0
% Incomplete command.
R-Paris(config)#crypto isakmp key oKiTasouji-cisc0 address 209.165.200.6
R-Paris(config)#
R-Paris#
%SYS-5-CONFIG_I: Configured from console by console

R-Paris#config t
Enter configuration commands, one per line. End with CNTL/Z.
R-Paris(config)#cr
R-Paris(config)#crypto ipse
R-Paris(config)#crypto ipsec tr
R-Paris(config)#crypto ipsec transform-set EASI-SET es
R-Paris(config)#crypto ipsec transform-set EASI-SET esp-a
R-Paris(config)#crypto ipsec transform-set EASI-SET esp-aes esp-m
R-Paris(config)#crypto ipsec transform-set EASI-SET esp-aes esp-md5-hmac
R-Paris(config)#ip acc
R-Paris(config)#ip access-list ex
R-Paris(config)#ip access-list extended ACL-EASI
R-Paris(config-ext-nacl)#per
R-Paris(config-ext-nacl)#permit ip 193.168.1.0 0.0.0.255 192.168.2.0 0.0.0.255
R-Paris(config-ext-nacl)#exit
R-Paris(config)#cry
R-Paris(config)#crypto map OKITA-VPN 1 ipse
R-Paris(config)#crypto map OKITA-VPN 1 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
and a valid access list have been configured.
```

Ensuite on crée la clé qui va être utilisée pour partager le tunnel VPN sur d’autres réseaux. On crée un transform set qui sont les protocoles qui vont chiffrer nos données. On a aussi créé une ACL comme lors du TP 1 Proxy en Linux qui vont être une liste d’instructions de connexions pour notre VPN.

```

ROUTERLAUSANNE(config)#crypto isakmp key OKITA-souji-cisco address 209.165.200.2
ROUTERLAUSANNE(config)#cry
ROUTERLAUSANNE(config)#crypto ipsec transform-set EASI-SET esp-aes esp-md5-hmac
ROUTERLAUSANNE(config)#ip acc
ROUTERLAUSANNE(config)#ip access-list ex
ROUTERLAUSANNE(config)#ip access-list extended ACL-EASI
ROUTERLAUSANNE(config-ext-nacl)#perm
ROUTERLAUSANNE(config-ext-nacl)#permit ip 192.168.2.0 0.0.0.255 192.168.1.0 0.0.0.255
ROUTERLAUSANNE(config-ext-nacl)#exit
ROUTERLAUSANNE(config)#crypt
ROUTERLAUSANNE(config)#crypto map OKITA-VPN 1 ipse
ROUTERLAUSANNE(config)#crypto map OKITA-VPN 1 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
and a valid access list have been configured.
ROUTERLAUSANNE(config-crypto-map)#set pe
ROUTERLAUSANNE(config-crypto-map)#set peer 209.165.200.2
ROUTERLAUSANNE(config-crypto-map)#se
ROUTERLAUSANNE(config-crypto-map)#set trans
ROUTERLAUSANNE(config-crypto-map)#set transform-set EASI-SET
ROUTERLAUSANNE(config-crypto-map)#match address ACL-EASI
ROUTERLAUSANNE(config-crypto-map)#exit
ROUTERLAUSANNE(config)#inter
ROUTERLAUSANNE(config)#interface fa
ROUTERLAUSANNE(config)#interface fastEthernet 0/1
ROUTERLAUSANNE(config-if)#cry
ROUTERLAUSANNE(config-if)#crypto map OKITA-VPN
*Jan 3 07:16:26.785: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
ROUTERLAUSANNE(config-if)#end

```

Puis on fait la même sur le routeur de Lausanne et on a créé le tunnel VPN qui se tient entre le routeur de Paris et celui de Lausanne.

On teste si le VPN est fonctionnel grâce à un ping du PC0 au PC1 qui se trouve chacun dans des réseaux différents. Grâce à la route que l’on a configuré dynamiquement grâce au bgp . Si le ping passe avec succès, c’est que le vpn est bien configuré mais surtout que la route l’est aussi. Si le ping ne passe pas bien d’une machine à l’autre, alors la route est mal configurée. Enfin on teste si l’on arrive à passer des appels entre Paris et Lausanne et on peut voir sur le screen que cela fonctionne donc le VPN et le routage est bien configuré.



Conclusion

La réalisation de ce TP sur la création d'un VPN avec Cisco Packet Tracer aura été une excellente occasion pour apprendre à développer nos compétences en matière de configuration et de sécurité réseaux. De plus, cela nous aura aussi permis d'appliquer les différentes connaissances théoriques reçues lors des cours magistraux d'introduction à la cybersécurité. Ainsi, ce TP aura été une expérience pratique très enrichissante nous permettant de bien conclure notre introduction à la cybersécurité.