

## PARTIE1 : REPONSES AUX QUESTIONS

1-a) le masque de sous réseau en /28 est 255.255.255.240

b) les nombres de bits alloués sont :

-pour la partie réseau : 28 bits

-pour la partie hôte : 4 bits

c) pour le nombre total d'adresses IP on a

$2^n$  avec  $n = 4$  donc on a 16 adresses IP par sous réseau.

d) pour le nombre maximal d'hôte par sous réseau on a :  $2^n - 2$  avec  $n=2$  donc on a 14 hôtes par sous réseau.

## 2-détermination des plages d'adresses IP sous forme de tableau

Sous réseau	Adresse du réseau	Première adresse utilisable	Dernière adresse utilisable	Adresse de broadcast
SR1	192.178.12.0	192.178.12.1	192.178.12.14	192.178.12.15
SR2	192.178.12.16	192.178.12.17	192.178.12.30	192.178.12.31
SR3	192.178.12.32	192.178.12.33	192.178.12.46	192.178.12.47
SR4	192.178.12.48	192.178.12.49	192.178.12.62	192.178.12.63

## 1-TOPOLOGIE Réseau

Nous avons :

-Une simulation du réseau avec tous les équipements cités en se servant du logiciel Cisco

- Des indications des connexions entre les appareils

-liaison entre le point d'accès et les trois laptops (1, 5, 9) ensuite une liaison entre le point d'accès, puis la liaison entre le switch 2 et le switch 3, la liaison entre le switch 3 et les deux serveurs A et B, une autre liaison entre le switch 3 et le routeur, puis également une liaison entre le ROUTEUR ET LE SWITCH0 pour finir, il y'a une liaison entre le switch3 et l'imprimante.

## 2-plan d'adressage IP

L'adressage statique a des adresses IP uniques et validés pour chaque élément.

## 3-detection des erreurs de configuration

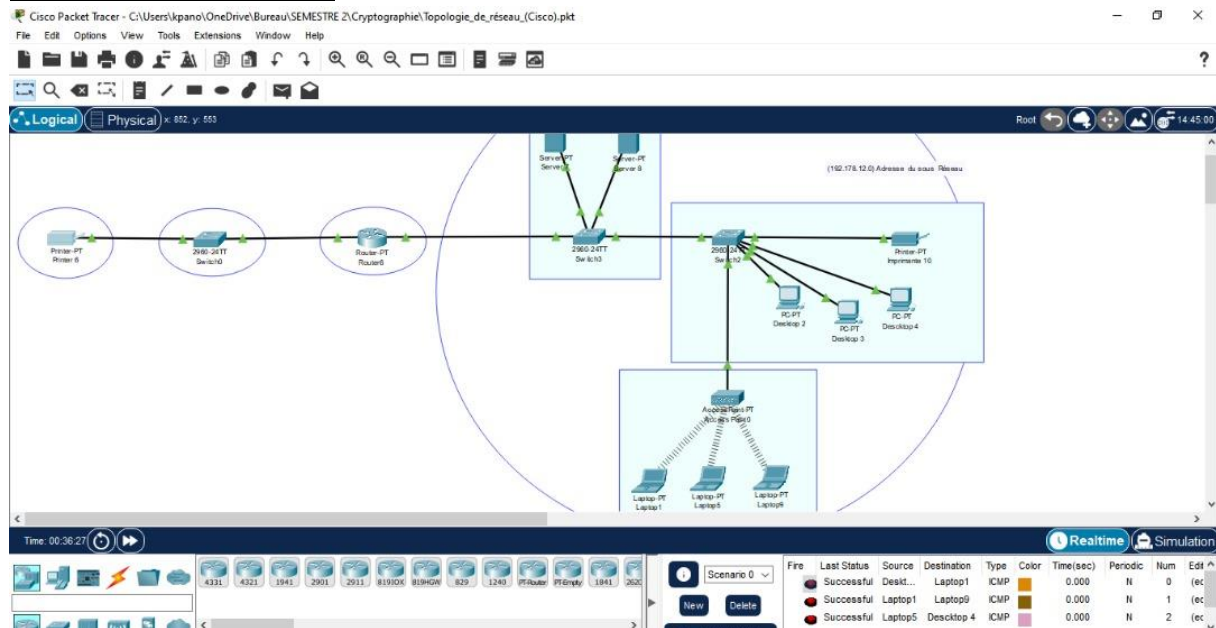
-192.178.12.0 : adresse du réseau attribué au laptop1 qui est remplacé de l'adresse IP du laptop 1 par 102.178.12.2

-192.178.12.12 : adresse IP appartenant au laptop5 et au serveur S alors il y'a conservation de l'adresse pour le serveur B et remplacement de l'adresse IP du laptop 5 par 192.178.12.12.

FINALISATION DU RESEAU : LA machine qui ne se trouve pas dans le bon réseau est l'imprimante. Cette machine appartient au sous réseau 2 dont l'adresse est 192.178.12.16 et l'adresse broadcast est 192.178.12.31.

## RESOLUTION DE L'EXO DE CRYPTOGRAPHIE

### IMAGE DU RESEAU SIMULE



PARTIE3 :

## EXPLOITATION DES INDICES FOURNIS

Le chiffrement utilisé est un cryptage asymétrique ayant un mode d'opération CBC avec une clé de 256bits.

La clé de déchiffrement est construite à partir du dernier octet en binaire de l'adresse broadcast de la machine infiltrée dans le réseau et des deux premiers octets de l'adresse MAC de l'ordinateur dont l'IP est 183.216.58.64 selon les données du fichier de capture wireshark transmis :

Le dernier octet de l'adresse est 31, soit 000011111 en binaire, l'adresse MAC de la machine cible est 5C:8C:30:5E:77:BC.

Donc la clé se forme comme suit : 5C8C00011111 ou CC00011111 (pour anonymiser les vraies valeurs).

## DECHIFFREMENT DU FICHIER

Pour déchiffrer le fichier, nous avons tout d'abord importé le fichier depuis la machine hôte vers la machine virtuelle, ensuite nous avons déchiffré le fichier à l'aide de la clé obtenue pour pouvoir extraire et lire le message caché.