RESOLUTION DE L’EXERCICE DE CRYPTOGRAPHIE

**PARTIE 1 :**  Prérequis et calcul

1. Le masque de sous-réseau en /28 est : 255.255.255.240
2. Les nombres de bits alloués sont :

* Pour la partie réseau : 28 bits
* Pour la partie hôte : 4 bits

1. Pour le nombre total d’adresses IP on a : 2n avec n = 4 donc on a 16 adresses IP par sous-réseau.
2. Pour le nombre maximal d’hôte par sous-réseau on a : 2n -2 avec n = 4 donc on a 14 hôtes par sous-réseau.
3. Présentons les informations sous forme de tableau

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Sous-réseau** | **Adresse du réseau** | **Première adresse utilisable** | **Dernière adresse utilisable** | **Adresse du**  **broadcast** |
| SR 1 | 192.178.12.0 | 192.178.12.1 | 192.178.12.14 | 192.178.12.15 |
| SR 2 | 192.178.12.16 | 192.178.12.17 | 192.178.12.30 | 192.178.12.31 |
| SR 3 | 192.178.12.32 | 192.178.12.33 | 192.178.12.46 | 192.178.12.47 |
| SR 4 | 192.178.12.48 | 192.178.12.49 | 192.178.12.62 | 192.178.12.63 |

**Partie 2 :** Conception et implémentation du réseau

1. **Topologie réseau**

* Simulation du réseau avec tous les équipements cités en se servant du logiciel Cisco Packet Tracer
* Indications des connexions entre les appareils
* Liaisons entre le switch2 et les trois desktops (2 ; 3 ; 4) ainsi que l’imprimante10
* Liaison entre le switch2 et un point d’accès
* Liaisons entre le point d’accès et les trois laptops (1 ; 5 ; 9)
* Liaison entre le switch2 et le switch3
* Liaisons entre le switch3 et les deux serveurs (Serveur A et Serveur B)
* Liaison entre le switch3 et un routeur (Routeur0)
* Liaison entre le routeur et le switch0
* Liaison entre le switch3 et l’imprimante6

1. **Plan d’adressage IP**

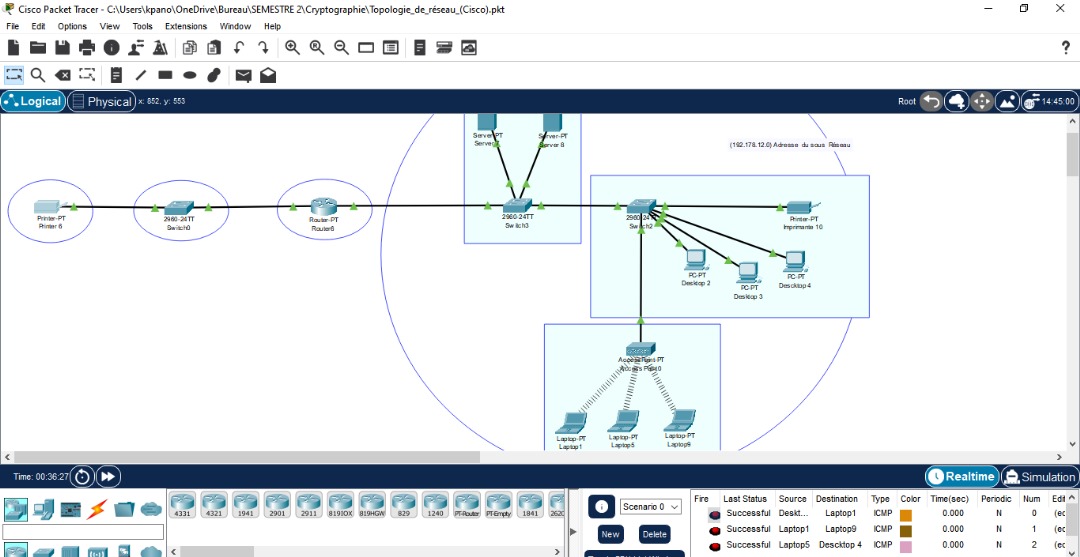
Adressage statique avec des adresses IP uniques et valides pour chaque élément

1. **Tests de connectivité**

Test de connectivité entre les machines

1. **Détection et sécurité**

* **Détection des erreurs de configuration**
* 192.178.12.0 : Adresse du réseau attribué au Laptop1 alors remplacement de l’adresse IP du Laptop1 par **192.178.12.2**
* 192.178.12.11 : Adresse IP appartenant au Laptop5 et au serveur B alors conservation de l’adresse pour le serveur B et remplacement de l’adresse IP du Laptop5 par **192.178.12.12**
* **Finalisation du réseau**
* La machine ne se trouvant pas dans le bon réseau est l’imprimante6
* Cette machine appartient au sous-réseau 2 dont l’adresse est **192.178.12.16** et l’adresse de broadcast est **192.178.12.31**
* **Image du réseau simulé**



**PARTIE 3 :** TP Cryptographie

1. **Mise au point des indices donnés**

* Cryptage asymétrique
* Mode d’opération CBC en 256
* Clé : Le dernier octet en binaire de l’adresse broadcast de la machine infiltré du réseau avec **le préfix des deux premières lettres de l’adresse mac de l’ordinateur ayant pour adresse IP 182.216.58.64** du fichier de capture de wireshark transmis
* 31 en binaire donne : **00011111**
* Adresse MAC de l’ordinateur : **5c : 8c : 30 : 5e :77 : bc**
* La clé est donc : **cc00011111**

1. **Décryptage du fichier**

* Importation du fichier crypté de la machine hôte vers la machine virtuelle
* Décryptage du fichier et obtention du message caché.