RESOLUTION DE L’EXERCICE DE CRYPTOGRAPHIE

**PARTIE 1 :**  Prérequis et calcul

* Le masque de sous-réseau en /28 est : 255.255.255.240
* Les nombres de bits alloués sont :
* Pour la partie réseau : 28 bits
* Pour la partie hôte : 4 bits
* Pour le nombre total d’adresses IP on a : 2n avec n = 4 donc on a 16 adresses IP par sous-réseau.
* Pour le nombre maximal d’hôte par sous-réseau on a : 2n -2 avec n = 4 donc on a 14 hôtes par sous-réseau.

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

**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

**Plan d’adressage IP**

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

**Tests de connectivité**

Test de connectivité entre les machines

**Détection et sécurité**

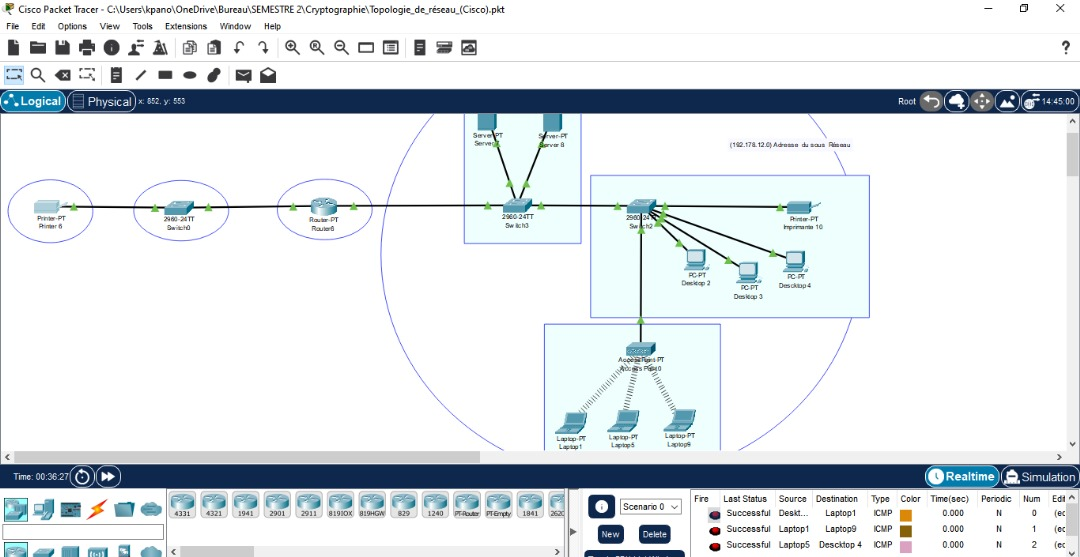
**Analyse des erreurs de configuration :**

* Le **Laptop1** utilisait l'adresse IP **192.178.12.0**, ce qui correspond à l'adresse du **réseau**. Cette adresse a donc été corrigée et remplacée par **192.178.12.2**, une adresse utilisable.
* Un **conflit d’adresse IP** a été détecté entre le **Laptop5** et le **Serveur B**, tous deux configurés avec l'adresse **192.178.12.11**. Pour résoudre ce conflit, l'adresse du Laptop5 a été modifiée en **192.178.12.12**.

**Appareil identifié en dehors de son réseau :**

* L’**imprimante6** ne faisait pas partie du sous-réseau auquel elle était censée appartenir.
* Elle est en réalité rattachée au **sous-réseau SR2 (192.178.12.16/28)**.
  + **Adresse du réseau** : 192.178.12.16
  + **Adresse de broadcast** : 192.178.12.31

**Image du réseau simulé**



**PARTIE 3 :** TP Cryptographie

**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**

**Décryptage du fichier**

Importation du fichier crypté de la machine hôte vers la machine virtuelle

Décryptage du fichier et obtention du message caché.

**apperçu**

