**Nom** : LOUBAKI

**Prénom** : Amédée Genèse

**Classe** : GIIA L1

**Rapport du TP de cryptographie**

**Partie 1** : Prérequis et calculs

1. **Calculs initiaux pour un sous-réseau /28** :
2. Le masque de sous réseau en notation pointée est : **255 .255.255.240**
3. Le nombre de bits alloués :

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

1. Nombre total d’adresses IP :

2n = 24 = 16 d’où on a **16 adresses** IP par sous-réseau

1. Nombre maximal d’hôtes par sous-réseau :

2n – 2 = 24 – 2 = 14

Donc on a **14 hôtes** par sous-réseau

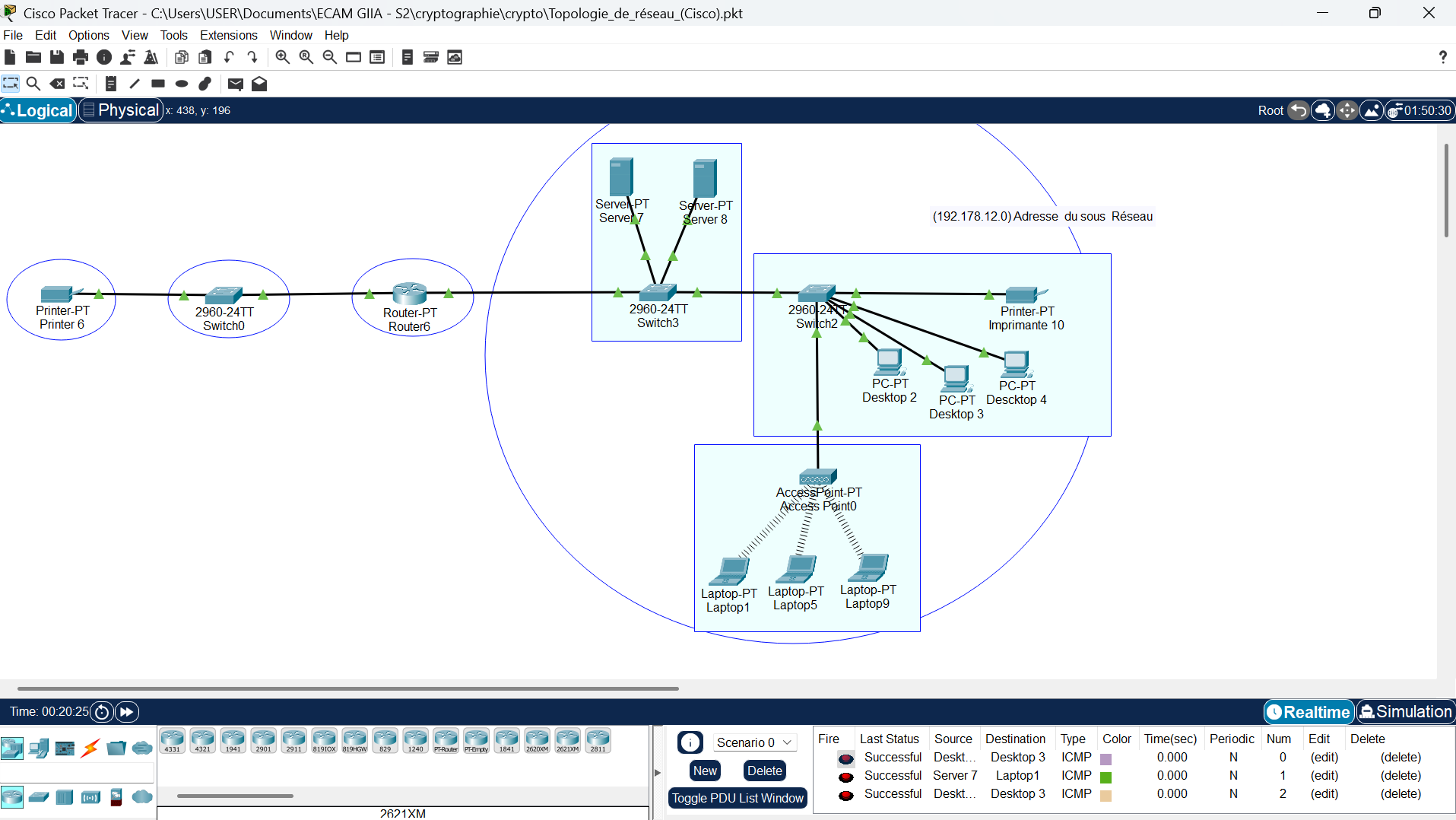
1. **Détermination des Plages d’Adresses IP** :
2. Tableau du découpage réseau

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| N° | Réseau | 1ere Adresse | Dernière Adresse | Broadcast |
| 1 | 192.178.12.0 | 192.178.12.1 | 192.178.12.14 | 192.178.12.15 |
| 2 | 192.178.12.16 | 192.178.12.17 | 192.178.12.30 | 192.178.12.31 |
| 3 | 192.178.12.32 | 192.178.12.33 | 192.178.12.46 | 192.178.12.47 |
| 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**

La topologie réseau a été dessinée et simulé en utilisant le logiciel **Cisco Packet Tracer**. Voir le fichier joint **Topologie.pkt**



1. **Plan d’adressage IP corrigé**

|  |  |  |  |
| --- | --- | --- | --- |
| N° | Type de machine | Adresse IP | Masque SR |
| 01 | Laptop | 192.178.12.2 | /28 |
| 02 | Desktop | 192.178.12.1 | /28 |
| 03 | Desktop | 192.178.12.3 | /28 |
| 04 | Desktop | 192.178.12.6 | /28 |
| 05 | Laptop | 192.178.12.12 | /28 |
| 06 | Imprimante | 192.178.12.17 | /28 |
| 07 | Serveur | 192.178.12.13 | /28 |
| 08 | Serveur | 192.178.12.11 | /28 |
| 09 | Laptop | 192.178.12.14 | /28 |
| 10 | Imprimante | 192.178.12.10 | /28 |

Légendes :

: Adresse inchangée

: : Adresse IP modifié en raison de validité

: : Intrus

1. **Test de connectivité**

Test de connectivité effectué avec succès. Les machines sont à présent capables de communiquer entre elles

1. **Détection et Sécurité**

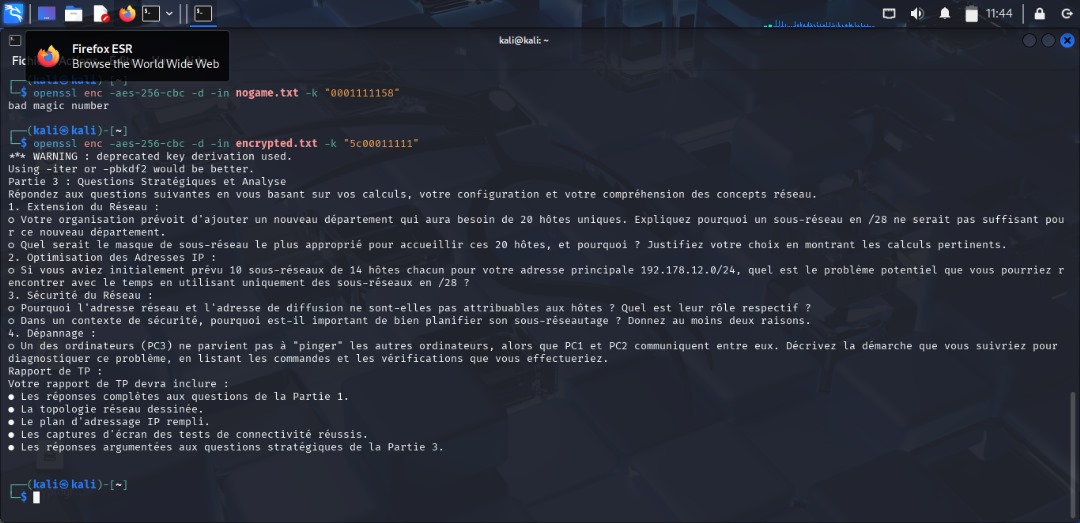
Au niveau du plan d’adressage de base, certaines erreurs ont été détectées à savoir :

* L’attribution de l’adresse non attribuable 192.178.12.0 au Laptop 1, pour résoudre ce problème cette adresse a été remplacée par 192.178.12.2
* La redondance de l’adresse 192.178.12.11 au niveau du Laptop 5 et du serveur 8, pour résoudre ce problème il a été attribué au Laptop 5 l’adresse unique 192.178.12.12
* La machine intruse dans ce plan d’adressage est l’Imprimante 6, elle n’est pas dans le bon sous-réseau et appartient au réseau 192.178.12.16/28 ayant pour adresse de broadcast 192.178.12.31/28

**Partie 3** : Cryptographie / Questions stratégiques et Analyse

**Prérequis de la partie 3** :

* Cryptage symétrique : une seule clé est utilisée pour crypter et décrypter
* Algorithmes d’encryptage : AES-256-CBC
* Clé : 5c00011111
* Résultat obtenu :



1. Extension du réseau

Il serait impossible d’étendre le réseau en y ajoutant un département de 20 hôtes uniques en utilisant le /28 car ce sous-réseau ne peut accueillir que 14 hôtes comme expliqué dans la partie 1.

1. **Optimisation des Adresses IP**

Les problèmes que l’on pourrait rencontrer en utilisation que des sous-réseaux /28 sont :

* Un nombre trop faible d’hôtes disponibles par sous-réseau
* Une configuration complexe en raison du grand nombre de sous-réseau

1. **Sécurité du réseau**

Les adresses du réseau et de broadcast ne peuvent pas être assignées aux machines hôtes car elles ont des rôles spécifiques au fonctionnement du réseau :

* **Adresse réseau** : elle identifie le sous-réseau lui-même et est utilisée pour le routage
* **Adresse de diffusion (broadcast) :** elle permet d’envoyer un message à tous les hôtes du sous-réseau.

**Planification du sous-réseautage**

Il est important de bien planifier son sous-réseautage pour plusieurs raisons, parmi lesquels :

* **Isolation du flux** : Le fait de segmenter les groupes utilisateurs/services permet de limiter la propagation de virus ou d’attaques internes.
* **Economie d’adresses :** Une planification efficace évite le gaspillage d’adresse IP et facilite l’évolutivité

1. **Dépannage**

Voici les étapes à suivre afin de dépanner le PC3 :

**Etape 1 : Vérification de l’adressage**

Ici on va tenter de vérifier si ce PC possède une adresse IP et le bon masque de sous réseau

**Commande**: ***IPCONFIG*** (Windows) ou ***ip addr*** (Linux)

Etape 2 : Vérification des connexions physiques

Ici, il s’agira de vérifier si le PC3 est bien relié au switch ou au point d’accès via le bon équipement d’interconnexion (câbles)