NOM :MAÏDOU

PRÉNOM :Jude

**TP de cryptographie**

**Partie 1 : Bases et Calculs Préliminaires**

**1. Paramètres initiaux pour un sous-réseau en /28**

a. Masque de sous-réseau (notation décimale pointée) :

        255.255.255.240

b. Répartition des bits :

* Bits réservés à la partie réseau : 28
* Bits réservés à la partie hôte : 4

c. Nombre total d’adresses IP disponibles :

* Calcul : 2^4 = 16
* Résultat : 16 adresses IP par sous-réseau

d. Nombre d’hôtes utilisables dans un sous-réseau :

* Calcul : 2^4 - 2 = 14
* Résultat : 14 adresses valides attribuables aux équipements

1. **Détermination des Plages d’Adresses IP** :

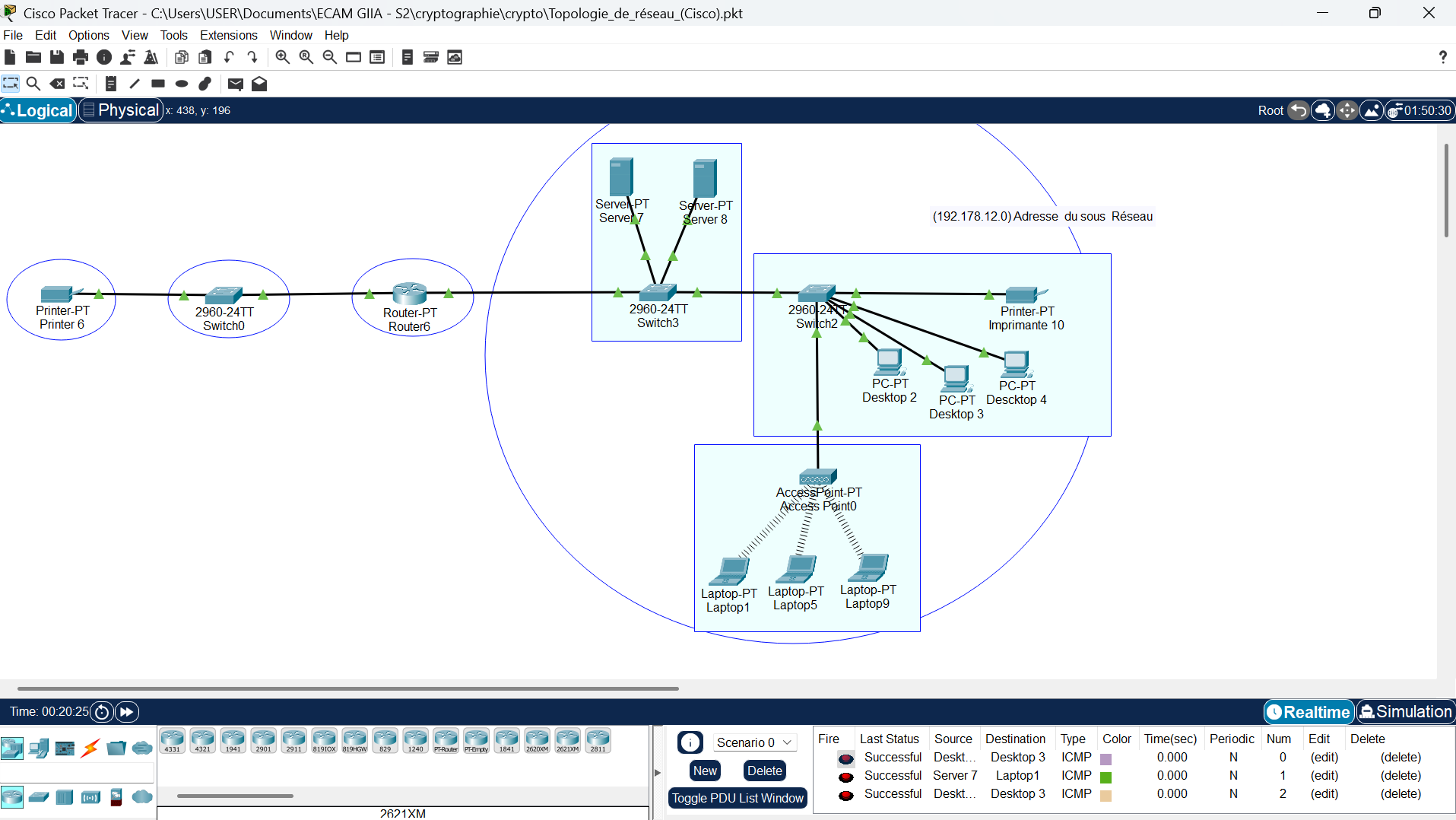
|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| N° | Réseau | 1ere Adresse | Dernière Adresse | Broadcast |
| 1 | 192.178.12.0 | 192.178.12.1 | 192.178.12.14 | 192.178.12.15 |
| 2 | 192.178.12.16 | 192.178.12.17 | 192.178.12.30 | 192.178.12.31 |
| 3 | 192.178.12.32 | 192.178.12.33 | 192.178.12.46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

**1. Schéma de la topologie**

Le réseau a été modélisé et testé à l’aide du logiciel Cisco Packet Tracer.

* La simulation intègre l’ensemble des équipements mentionnés dans le cahier des charges.
* Les interconnexions entre les différents dispositifs ont été définies avec précision.
* Le switch2 est relié aux trois ordinateurs de bureau (Desktop 2, 3 et 4) ainsi qu’à l’imprimante 10.
* Une liaison est établie entre switch2 et un point d’accès sans fil.
* Le point d’accès dessert les trois ordinateurs portables (Laptop 1, 5 et 9).
* Une connexion est également mise en place entre le switch2 et le switch3.
* Le switch3 est connecté aux deux serveurs (Serveur A et Serveur B).
* Une liaison directe est configurée entre le switch3 et le routeur principal (Routeur0).
* Ce routeur est ensuite connecté au switch0, assurant la liaison inter-réseaux.
* Enfin, l’imprimante 6 est reliée au switch3 pour une impression réseau centralisée.



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. Vérification de la connectivité**

La connectivité entre les équipements a été testée avec succès. Toutes les machines sont désormais en mesure d’échanger des données sans problème.

**2. Analyse et Sécurisation**

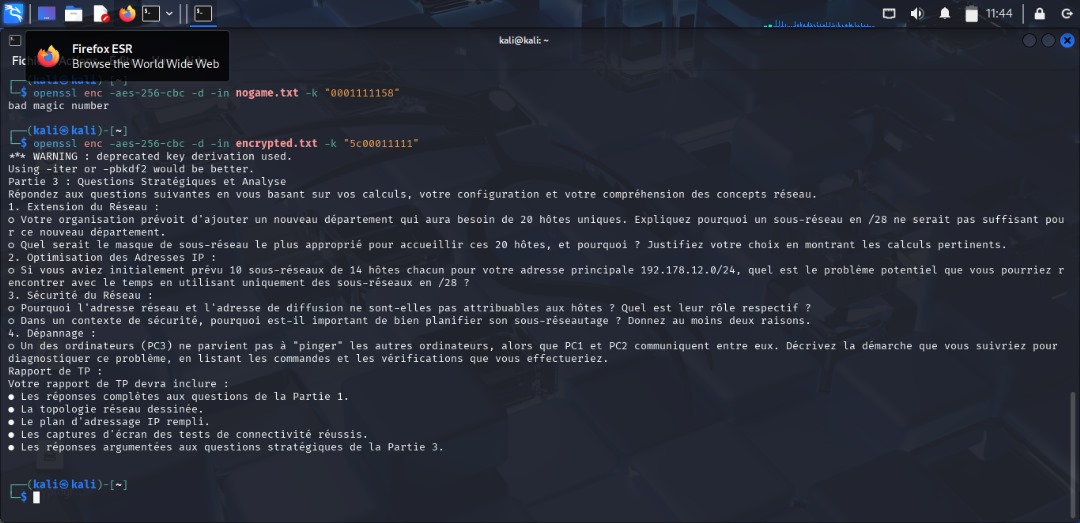
Lors de l’examen du plan d’adressage initial, plusieurs anomalies ont été relevées, notamment :

* L’utilisation incorrecte de l’adresse 192.178.12.0 pour le Laptop 1. Cette adresse étant réservée, elle a été remplacée par 192.178.12.2.
* Une duplication de l’adresse IP 192.178.12.11 entre le Laptop 5 et le Serveur 8. Ce conflit a été résolu en attribuant une nouvelle adresse (192.178.12.12) au Laptop 5.
* L’Imprimante 6 a été identifiée comme étant hors du sous-réseau prévu. Elle dépend en réalité du réseau 192.178.12.16/28, dont l’adresse de broadcast est 192.178.12.31.

**Partie 3 : Cryptographie / Analyse stratégique**

Notions de base :

* Chiffrement symétrique : une même clé est utilisée à la fois pour le chiffrement et le déchiffrement des données
* Algorithme utilisé : AES-256-CBC
* Clé de chiffrement : 5c00011111



**1. Possibilité d’agrandissement du réseau**

Il n’est pas envisageable d’ajouter un département comprenant 20 postes dans un sous-réseau en /28, car celui-ci ne permet que l’hébergement de 14 hôtes maximum, comme présenté précédemment.

**2. Gestion optimisée des adresses IP**

Les inconvénients liés à l’usage exclusif de sous-réseaux en /28 incluent :

* Une capacité d’accueil limitée pour les hôtes dans chaque segment
* Une complexité accrue de la configuration en raison de la multiplication des sous-réseaux

**3. Aspects sécuritaires du réseau**

Les adresses réservées telles que l’adresse réseau et celle de diffusion (broadcast) ne doivent pas être affectées à des machines, car elles ont des fonctions particulières dans l’organisation du réseau :

* Adresse réseau : identifie le sous-réseau et sert à son identification dans les tables de routage
* Adresse de broadcast : permet d’émettre un message à l’ensemble des hôtes d’un même sous-réseau

**4. Planification du découpage réseau**

Une bonne stratégie de sous-réseautage est essentielle pour :

* Isoler les flux : en cloisonnant les services ou groupes utilisateurs, on limite la propagation d’éventuelles menaces internes
* Optimiser l’allocation d’adresses : une organisation rigoureuse prévient le gaspillage d’adresses IP et favorise l’évolutivité du réseau

**5. Dépannage**

Les étapes suivantes permettent de corriger un dysfonctionnement observé sur la machine PC3 :

**Étape 1 : Contrôle de l’adressage**

Dans cette étape, il s’agit de s’assurer que l’ordinateur concerné dispose bien d’une adresse IP valide ainsi que du masque de sous-réseau adéquat.

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

**Étape 2 : Vérification des liaisons physiques**

On vérifie ici que le PC3 est correctement connecté au commutateur ou au point d’accès à l’aide du bon câble ou du matériel réseau approprié.