NOM :BATANTOU

Prenom :Messie

Niveau : L1

Filière :GIIA

*RESOLUTION DU TRAVAIL PRATIQUE de CRYPTOGRAPHIE*

**PARTIE 1 :**  Prérequis et calcul

1. **Calculs initiaux pour un sous réseau /28**
2. Le masque de sous-réseau en notation décimale pour un /28 est : 255.255.255.240
3. Le nombres de bits alloués a la partie réseau et a la partie hôte sont :

* La partie réseau : 28 bits
* La partie hôte : 4 bits

1. Le nombre total d’adresses IP par sous réseau :

2n avec n = 4 ↔24 =16 adresses IP par sous-réseau.

1. Le nombre maximal d’hôtes par sous-réseau :

2n – 2 avec n = 4 = 24 – 2 = 14 donc 14 hôtes par sous réseau.

1. Détermination des plages d’adresses IP :
2. Tableau

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Sous-réseau | Adresse du réseau | 1 ère Adresse | Dernière Adresse | Adresse du broadcast |
| N°1 | 192.178.12.0 | 192.178.12.1 | 192.178.12.14 | 192.178.12.15 |
| N°2 | 192.178.12.16 | 192.178.12.17 | 192.178.12.30 | 192.178.12.31 |
| N°3 | 192.178.12.32 | 192.178.12.33 | 192.178.12.46 | 192.178.12.47 |
| N° 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 ainsi que les équipements cités en utilisant le logiciel Cisco Packet Tracer
* Les connexions entre les appareils
* 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**

Un adressage statique avec des adresses IP uniques et valides pour chaque élément

|  |  |  |  |
| --- | --- | --- | --- |
| 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 |

**Légende**

: Adresse inchangée :Adresse IP modifié en raison de validité

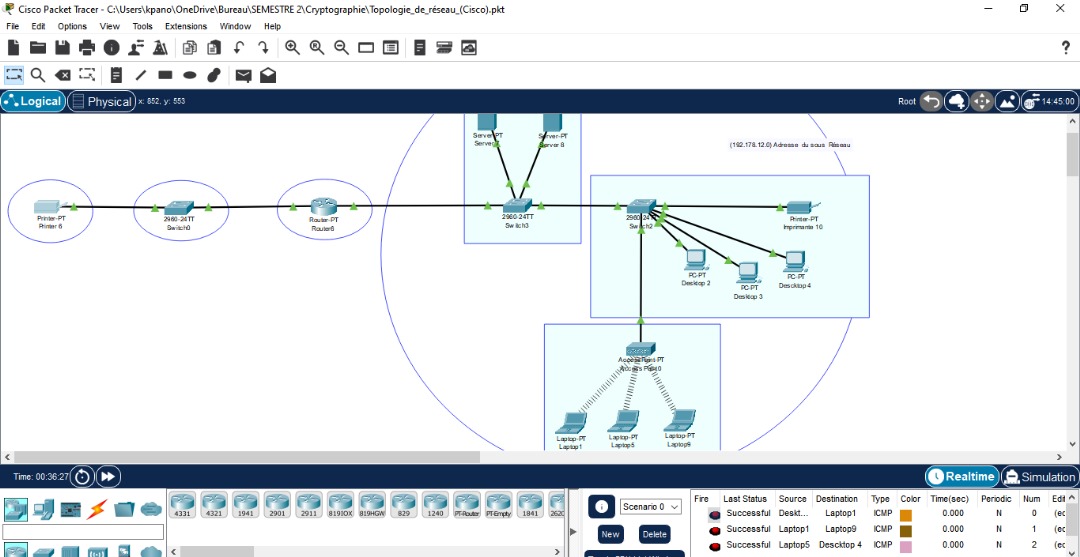
: intrus

1. **Test de connectivité**

Test de connectivité effectué avec succès

**4.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 :**

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

* Cryptage asymétrique : une seule clé est utilisée pour crypter et décrypter
* 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 deuxpremières lettres de l’adresse mac de l’ordinateurayant pour adresse IP 182.216.58.64 du fichier de capture de wireshark transmis
* Adresse MAC de l’ordinateur : **5c : 8c : 30 : 5e :77 : bc**
* La clé est donc : **5c00011111**

1. **Décryptage du fichier**

* Importation du fichier crypté de la machine hôte vers la machine virtuelle.
* On obtient comme message une partie 3 dont voici l’image :

****

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
2. Rôles des deux types d’adresse

* 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.

1. Planification du sous-réseautage

Il est important de planifier un sous-réseautage pour plusieurs raisons parmi lesquelles :

* Isolation des 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 le diagnostic :

* Etape 1 : Vérification de l’adresse IP du PC3

Commande : PC3 > Desktop > ip configuration

A ce stade il faut vérifier :

* **L’adresse IP (doit appartenir au bon sous-réseau)**
* **Le masque de sous-réseau**
* **La passerelle (si utilisée)**
* Etape 2 : Vérification des connexions physiques

Ici, il s’agit de vérifier si le PC3 est bien relié au switch ou au routeur via le bon câble avec inspection des ports actifs.