***Formulaire des étapes à suivre***

**2e travail pratique du 2e semestre avec 15% d’influence sur la note de classe**

***Par TOKOBANZA EXAUCE***

**Matière : CRYPTOGRAPHIE Niveau : Dieux Durée : 03 jours**

* ***Pré – requis & calculs :***

On a déjà comme donnée l’adresse réseau principal (**192.178.12.0/24**) et le masque sou – réseau demandé est le /28.

* ***Calculs initiaux pour un sous – réseau /28 :***
* ***a. Le masque sous – réseau en notation décimale pointer pour un /28 :***

On a donc ceci : 255.255.255.240

* ***b. Nombre de bit allouer à la partie réseau et à la partie hôte :***

Pour la partie réseau on a **28 bits** qui y sont alloués et **4 bits** qui sont alloués à la partie hôte.

* ***C. Le nombre total d’adresse IP par sous – réseau :***

Par sous réseau on aura un total de **16** adresses.

* ***D. Le nombre d’hôtes utilisables :***

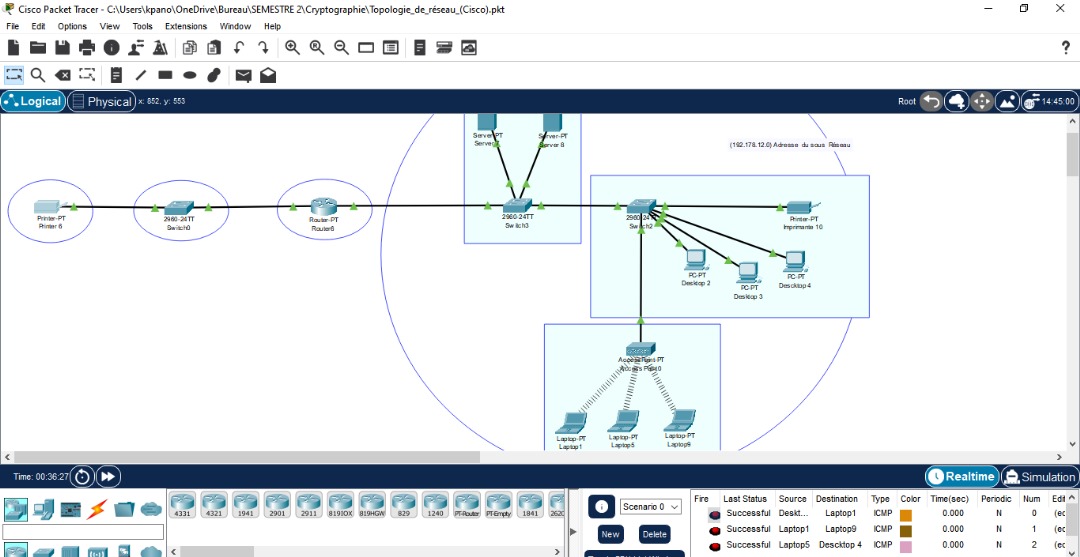
On a **14** hôtes utilisables d’une part on retient 1 pour l’adresse réseau et 1 pour le Broadcast.

* ***Les plages d’adresses pour les 4 premières sous – réseau :***

Avec l’adresse donnée 192.178.12.0/24, on va le couper en blocs de 16 adresses.

* ***Conception & implémentation du réseau :***
* ***Topologie du réseau :***
* ***Simulation du réseau :***

Avec l’utilisation du logiciel Cisco Packet Tracer.



* ***Indications des connexions entre les machines ou 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 des adressages :***

Des adressages statiques avec des adresses IP uniques et valides pour chacun des éléments.

* ***Test de connectivité :***

Vérification d’une connexion entre les machines.

* ***Détection et sécurit :***
* ***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**
* ***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.
* ***Message trouvé Suite du TP :***

Le message décrypter est la partie 03 du TP qui se trouve si dessous :

**Partie 3 - Questions stratégiques et Analyse**

**Répondez aux questions suivantes en vous basant sur vos calculs, votre configuration et votre compréhension des concepts réseau :**

**1. L’entreprise vient d’ajouter un nouveau département qui aura besoin de 20 hôtes uniques. Expliquez pourquoi un sous-réseau peut accueillir ces 20 hôtes. Pourquoi justifiez-vous votre choix en matière de masque de sous-réseau le plus approprié pour ce cas.**

**2. L’hôte actuel a pour adresse principale 192.178.0.2/24, quelle est l’adresse IP de réseau de ce sous-réseau et l’adresse de diffusion ? Expliquez comment vous pouvez retrouver ces informations.**

**3. Pourquoi l’adresse de diffusion ne peut-elle pas être assignée à un hôte ?**

**4. Dans un contexte de sécurité, pourquoi est-il important de ne pas divulguer l’adresse de diffusion d’un réseau ?**

**5. Deux ordinateurs (PC1 et PC2) ne parviennent pas à pinguer l’un l’autre, bien qu’ils soient dans le même sous-réseau. Donnez au moins deux raisons possibles à ce problème, en listant les commandes et les vérifications que vous effectueriez.**

**Le rapport PDF de l’équipe inclura :**

**• Les réponses argumentées à ces questions de la Partie 3.**

**• Les captures d’écran des tests de connectivité réussis.**

**• Les réponses également aux questions stratégiques de la Partie 1.**

****

* ***Résolution de la partie 03 :***

1. ***Le sous-réseau à choisir :***

L’entreprise à décider d’ajoute un nouveau département avec 20 hôtes uniques.

Alors pour accueillir les **20 hôtes**, on aura besoin d’un sous-réseau qui peut contenir au minim 20 adresses IP utilisables.

Un sous-réseau avec un /27 (c’est-à-dire un masque 255.255.255.224) offre :**2^ {32-27} - 2 =** **32 - 2 = 30 adresses utilisables.** Donc au final un /27 est parfaitement adapté pour un département de 20 hôtes car :

* + Il y a assez d’adresses (30) pour 20 machines.
  + Il évite le gaspillage d’adresses comparé à un /26 ou /24.

Utilisé plutôt ceux-là **/27 (255.255.255.224).**

1. ***L’adresse de réseau et l’adresse de diffusion :***

Avec comme adresse principale : **192.178.0.2/24** et avec un masque **/24 (255.255.255.0)**,

On a :

* + **Adresse de réseau :** la première adresse de la plage **192.178.0.0**
  + **Adresse de diffusion :** la dernière adresse **192.178.0.255**

Tout simplement car le masque /24 signifie que les 24 premiers bits sont réservés pour l’identifiant réseau, on garde les 8 derniers bits pour les hôtes : **(Tous à 0 → réseau → 192.178.0.0 ; tous à 1 → broadcast → 192.178.0.255)**

1. ***Pourquoi l’adresse de diffusion ne peut-elle pas être assignée à un hôte ?***

L’adresse de diffusion est réservée pour envoyer un message à tous les hôtes du réseau. Elle est réservée exclusivement aux communications de diffusion.

1. ***Pourquoi est-il important de ne pas divulguer l’adresse de diffusion dans un contexte de sécurité ?***

Parce que l’adresse de diffusion peut être utilisée pour :

* + Lancer des attaques de type broadcast Storm (inonder le réseau de messages inutiles).
  + Lancer des attaques DDoS (par amplification via le broadcast).
  + Découvrir tous les hôtes actifs du réseau facilement.

Donc, masquer ou protéger cette adresse est essentiel pour :

* + Réduire les surfaces d’attaque.
  + Protéger les hôtes contre les intrusions.
  + Maintenir une meilleure confidentialité du plan d’adressage.

***5. PC1 et PC2 dans le même sous-réseau ne se pinguent pas :***

Raisons possibles :

* **Pare-feu activé sur l’un des deux PC**

• Empêche les paquets ICMP (ping).

• ping PC3 depuis PC1 et inversement.

• Désactiver temporairement le pare-feu ou autoriser ICMP.

* **Adresse IP ou masque mal configuré**

• Si PC1 ou PC3 a une mauvaise IP ou un masque incorrect, ils ne se verront pas.

• Taper ipconfig (Windows) ou if config / ip a (Linux).

• Vérifier qu’ils ont la même adresse réseau et le même masque.