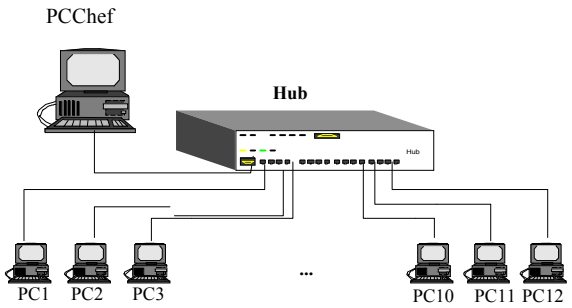
TD 1 – Outil de base

Documentation : lire les pages de manuel suivantes : ping, arp, tcpdump, netstat, ifconfig

Exercice 1 :

Installez la configuration suivante :



Solution :

Exercice 2 :

A l'aide de l'utilitaire ***ifconfig,*** initialisez votre IP à 192.168.42.*num_pc.*
Faites quelques connexions (telnet, ping ou autre) avec d'autres machines afin de vérifier les connexions.
Vérifiez la liste des interfaces avec ***netstat –in***. A quoi sert chaque interface? Donner pour chacune d'elles le taux d'erreurs en entrée, en sortie, et le nombre de collisions.

Solution :

Exercice 3 :

On peut vouloir ne pas avoir à reconfigurer le réseau à chaque démarrage de la machine. Pour cela, on édite habituellement un fichier de configuration qui sera lu au démarrage de la machine. L'emplacement de ce fichier peut varier d'un système d'exploitation à un autre :

- sur **FreeBSD,** il s'agit du fichier /etc/rc.conf ;
- sur **HP-UX,** il s'agit du fichier /etc/rc.config.d/netconf ;
- sur **Linux** avec une distribution **Redhat**, il s'agit du fichier /etc/sysconfig/network ;
- …

Fixez de cette manière votre adresse IP, redémarrez et vérifiez que votre configuration a bien été prise en compte.

Solution :

Exercice 4 :

Avec l'utilitaire ***ping***, vérifiez que la machine de votre voisin et bien accessible. Après une dizaine de secondes d'activité, donnez le nombre de paquets perdus et le temps moyen d'aller/retour (round trip time) d'un paquet sur le réseau local.

Solution :

Exercice 5 :

L'utilitaire ***arp*** permet de consulter et de modifier la table ARP du système local.

1. affichez le contenu de la table ARP ;
2. videz le contenu de la table ARP, vérifiez en affichant de nouveau le contenu ;
3. cette table se remplit à l'initiative d'autres machines (qui trafiquent avec la vôtre) ou à l'initiative de votre machine. Initiez un trafic avec ping et vérifiez qu'une nouvelle entrée a été ajoutée dans la table.

Solution :

Exercice 6 :

L'utilitaire ***tcpdump*** a pour but de capturer tous les paquets qui passent sur le réseau local. Pour cela, il place l'interface Ethernet dans le mode promiscuous, ce qui permet à l'interface de capturer effectivement tous les paquets, même ceux qui ne sont pas destinés à cette machine.
Lancez ***tcpdump*** et vérifiez avec ifconfig que l'interface est bien en mode promiscuous. Analysez quelques paquets reçus par tcpdump.
Une caractéristique intéressante de tcpdump est la possibilité de filtrer les paquets reçus suivant des critères. Par exemple,

Tcpdump host pc1and host pc2

Permet d'afficher le trafic entre les machines pc1 et pc2. Affichez tous les paquets de type ARP circulant sur le réseau.

Solution :

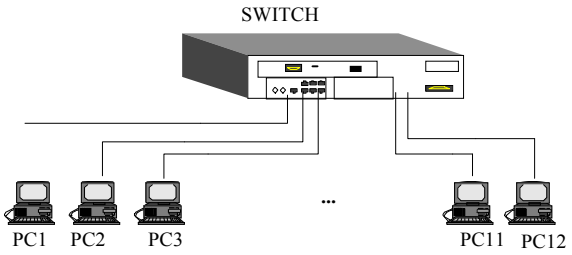
Exercice 7 :

Utilisez le programme ethereal. Pour cela, vous aurez besoin de démarrer X-Window.

Solution :

Exercice 8 :

Remplacez l'accès au réseau via le concentrateur (ou hub) par un accès .via le commutateur (ou switch) comme indiqué dans sur la figure ci-dessous. Quels paquets pouvez-vous voir avec tcpdump ou ethereal ?



Solution :

Exercice 9 :

Une diffusion IP (ou broadcast IP) consiste à envoyer un ou plusieurs paquets IP à destination de toutes les stations du réseau logique.
L'adresse de diffusion IP de votre réseau est 192.168.42.255.
A l'aide d'un ping sur l'adresse de diffusion, déterminez les adresses IP des machines de votre réseau
Solution :