Travaux Pratiques n°1
Principes et Normes des réseaux.

Objectifs

- Connaitre le matériel de base (switch, hub et routeur)
- Savoir configurer une machine windows et linux en statique et dynamique.
- Connaitre les commandes de base pour vérifier que la connexion est opérationnelle.
- Prise en main d'un outil d'analyse de trafic réseau (wireshark).

1. Le matériel

- Donnez la liste du matériel réseau nécessaire pour constituer un réseau local.
- Précisez les caractéristiques et leur rôle. Donnez aussi le niveau de la couche OSI dans lequel ils interviennent.
- Quel type de câble (droit ou croisé) est à utiliser pour relier deux PC ? deux switch ? un PC et un switch ? Expliquez.
- Au niveau matériel (carte réseau, switch et hub), qu'est-ce qui indique qu'il y a un trafic réseau ?
- Donnez et utilisez la commande permettant de trouver l'adresse MAC de votre machine.
- Branchez vos machines sur les switchs de la salle.

2. Adresse IP

Afin de pouvoir communiquer dans un réseau il faut choisir une adresse IP adéquate :

- Rappelez les adresses IP utilisables au sein d'un réseau privé. Qu'ont-elles de particulier aux adresses publiques ?
- Au niveau du masque de réseau et de l'adresse IP, quelle est la condition nécessaire pour que les machines puissent communiquer entre elles sur un même réseau ethernet (pas de routeur entre les machines comme dans le cas de la salle de TP) ?
- En conséquence vous devrez tous vous consultez afin de choisir une adresse IP pour votre machine afin qu'elles puissent communiquer ensemble.

3. Configuration statique

- Indiquez la méthode que vous aurez utilisée pour configurer statiquement une machine windows (en ligne de commande ou bien par clic).
- Idem pour la distribution Ubuntu que vous utiliserez (voir la page de manuel **man ifconfig** à taper dans un terminal. Ici la configuration par le biais du terminal est préférée à la configuration graphique car elle est valable sur toutes les distributions linux. Vous donnerez donc la commande que vous aurez tapée).
- Outre l'adresse IP et le masque de réseau, quelles sont les 2 autres informations réseaux importantes à paramétrer pour une station ? Sont-elles absolument indispensables ? Expliquez.

4. Commandes de base

- Une fois l'adresse IP configurée, quelle est la commande vous permettant de vérifier qu'une route existe entre une machine de votre voisinage et la vôtre ? Expliquez ce qui s'affiche. Si vous n'obtenez pas de réponse, quelles peuvent être les causes du dysfonctionnement.
- Examinez la commande **nslookup** sous windows et **host** sous linux. A quoi sert-elle précisément ?
- En quoi les deux commandes ci-dessus sont-elles importantes d'un point de vue pratique dans la résolution des problèmes réseaux sur une station ?

5. Utilisation de Wireshark

Wireshark est l'outil qui nous permet de visualiser tous les échanges sur le réseau. Comme avec tous logiciels d'analyse de trafic, le principe est simple : vous lancez une session de capture à l'aide du menu **Capture**. Cette session peut être interactive ou pas. En d'autres termes, les paquets capturés peuvent être affichés au fur et à mesure ou à la fin de la capture.

Réalisez les exercices suivants :

1. Lancez une capture de 60 trames.

2. Lancez une capture pendant 1 minute. Quel est le nombre de trames capturées ?

3. Lancez une capture en ne capturant que le protocole ARP (mettre en place le bon filtre). Tentez de pinguer une adresse non présente sur le réseau de la salle mais avec la même adresse réseau de base. Tentez ensuite de pinquer une machine présente dans la salle. Expliquez le rôle de ce protocole en décrivant les paquets que vous apercevez. Comparez avec la commande **arp –a** (qu'affiche-t-elle ?). Expliquez aussi comment connaitre l'adresse MAC d'une machine à l'aide de cette outil.

4. Générez du trafic à capturer (ex : navigation web, ping, ...) vers une machine bien connue : www.google.fr, www.yahoo.fr, etc.
   Capturez le trafic émis par votre machine vers cette machine (et pas l'inverse).
   Pour connaître l'adresse IP de la machine destination, utilisez la commande :
   host <nom_de_la_machine> sous linux ou **nslookup <nom de la machine>** sous windows.

5. Dans un terminal, lancez la commande suivante, et laissez la tourner : **ping www.google.fr**
   Capturez uniquement le trafic généré par cette commande, entre votre machine et celle donnée. Utilisez le manuel de la commande ping pour savoir quel est le protocole utilisé.

6. Capturez uniquement le trafic http (navigation web) circulant sur le réseau. Pour faire ceci, vous devez trouver le protocole et le port concerné afin d'appliquer un filtre : une petite recherche sur internet pourra surement vous dépanner...

6. Configuration dynamique

- Comment fonctionne grossièrement l'allocation dynamique d'une machine ?
- Mettez-le en place avec votre machine sachant qu'il y a sur le réseau un serveur DHCP (Vous utiliserez wireshark pour visualiser les échanges qui s'opèrent entre la machine et le serveur DHCP).
- Quels sont les avantages et les inconvénients de cette méthode.

Commandes utiles pour paramétrer et vérifier votre station

Windows

ipconfig : configuration des interfaces réseaux.
ping : vérifie l'accessibilité d'une machine.
hostname : affiche le nom d'hôte local
nslookup : effectue une résolution DNS.
netstat : fournit des informations sur l'utilisation du réseau.
tracert : permet de connaître le chemin IP complet vers une autre machine
nbtstat : Nbtstat affiche les statistiques du protocole et les connexions TCP/IP actuelles utilisant NBT (NetBIOS sur TCP/IP).

Linux

man : consultation des pages de manuel.
ifconfig : configuration des interfaces réseaux.
ifup - ifdown : Démarrage - Arrêt d'une interface réseau
/etc/init.d/networking start/stop/restart : redémarrage de la couche réseau.
ping : vérifie l'accessibilité d'une machine.
hostname : configure le nom d'hôte local
nslookup : effectue une résolution DNS.
whois : récupère des information sur une adresse ou un réseau IP.
netstat : fournit des informations sur l'utilisation du réseau.
traceroute : permet de connaître le chemin IP complet vers une autre machine

Quelques fichiers utiles sous Linux :
/etc/network/interfaces : contient la configuration initiale des interfaces réseaux
/etc/hosts : contient la table statique de résolution de nom
/etc/resolv.conf : contient les mécanismes utilisés par le système pour résoudre les noms

Présentation de WireShark

Prenez le temps de découvrir chaque fenêtre, option, barre, etc ... L'interface de l'analyseur se décompose en plusieurs barres ou fenêtres :

Barre de menus
On y retrouve la liste classique de menus. Voici une liste des fonctions accessibles à partir de ces menus.

- Le menu File sert à sauvegarder ou charger un fichier de capture réseau. Une capture peut très bien avoir été réalisée sur une sonde distante ou avec un autre outil et être analysée avec *Wireshark* à postériori.
- Le menu Capture sert à fixer les paramètres d'une nouvelle capture réseau.

Barre des icônes
Cette barre regroupe tous les raccourcis sur les manipulations d'une capture.

Barre de filtrage
Cette barre sert à saisir l'expression de filtrage à postériori d'une capture pour isoler tout ou partie d'un échange réseau.

Fenêtre contenant la liste des trames capturées
Sur chaque ligne on retrouve :

- le numéro du paquet,
- son temps de capture,
- sa source,

- sa destination,
- le protocole de plus haut niveau décodé,
- le résumé des champs caractéristiques de ce protocole.

Fenêtre d'affichage de la pile des protocoles décodés pour la trame sélectionnée

Avant toute opération de développement des champs d'un ou plusieurs protocoles, cette fenêtre donne la liste la pile de protocoles décodés allant du niveau physique (en haut) jusqu'au niveau le plus haut reconnu (en bas). Le protocole de niveau le plus haut reconnu apparaît est celui qui apparaît dans la colonne protocole de la **Fenêtre contenant la liste des trames capturées.**

- La première ligne ou niveau Frame correspond à une pseudo couche physique. Comme il n'est pas possible de réaliser la capture directement à partir des composants électroniques qui pilotent l'interface réseau sans perturber le fonctionnement du système, l'opération a lieu au niveau liaison à l'aide de la bibliothèque *libpcap*.
  A ce niveau, les informations disponibles sont : la quantité de bits capturés et la date de capture.
- La deuxième ligne correspond au niveau liaison. On y détaille le type et les champs de la trame et les adresses physiques.
- La troisième ligne correspond au niveau réseau. On y détaille les champs du protocole réseau reconnu : adresses logiques et indicateurs d'état.
- La quatrième ligne correspond au niveau transport. On y détaille les champs du protocole de transport reconnu : état de la connexion, numéros de ports utilisés et diverses options.
- La cinquième ligne correspond au niveau application. On y trouve les données utilisateur.

  Pour le développement de chacun des champs de la trame, il faut cliquer sur le triangle situé à gauche au niveau de chaque couche.

Fenêtre d'affichage brut de la trame sélectionnée

Cette fenêtre affiche tous les octets de la trame en hexadécimal.

Capture d'une série de trame

Pour capturer du trafic on doit suivre la séquence suivante :

1. Sélectionnez Capture puis Options.

2. La ligne Capture Filter, permet de préciser un filtrage ***à priori.*** La syntaxe de ce filtrage est identique à celle de la commande **tcpdump**. La documentation est disponible à partir des pages de manuels de cette commande : `man tcpdump`. Vous pouvez aussi vous référer au manuel de Wireshark, fourni en annexe.

Voici 4 exemples :

- **ip** : en spécifiant le protocole réseau à analyser, on évite la capture des trames des autres protocoles de niveau réseau (IPX) et des protocoles de niveau liaison (STP, CDP, etc.).
- **host 192.168.0.1** : en spécifiant l'adresse IP d'un hôte, on ne retient que le trafic émis et reçu par cette adresse.
- **host 192.168.0.1 and host 10.0.0.1** : en spécifiant les adresses IP de 2 hôtes, on ne retient que le trafic entre ces 2 adresses.
- **ip and dst host 192.168.0.2** : capture le trafic ip à destination de la machine d'adresse IP 192.168.0.2

  D'une façon plus générale, on peut combiner plusieurs critères avec les opérateurs logiques `and` et| ou `or`.
- le type : `host`, `net` et `port`.
- la direction : `src` et `dst`.
- le protocole : `ether`, `fddi`, `tr`, `ip`, `ip6`, `arp`, `rarp`, `decnet`, `tcp` et `udp`.

En règle générale, il faut limiter au maximum de filtrage *à priori* de façon à disposer du maximum d'information pour l'analyse. Si vous laissez la ligne sans filtre vous capturez tout le trafic.

3. La rubrique **Stop Capture** permet de fixer plusieurs critères d'arrêt en fonction du nombre de trames et/ou du volume de données capturées.

4. Cliquez sur le bouton **Valider** pour lancer la capture.